PSP0201 Week 3 Writeup

Group Name: Gold
Members:

ID	Name	Role
1211101707	Nur’aina Binti Ikhwan Moeid	Leader
1211103984	Nur Afreen Junaidah Binti Noorul Mohamed Eliyas	Member
1211101519	Aisyah Binti Ahmad Komarolaili	Member
1211102590	Nur Hanisah Binti Mohd Pauzi	Member

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

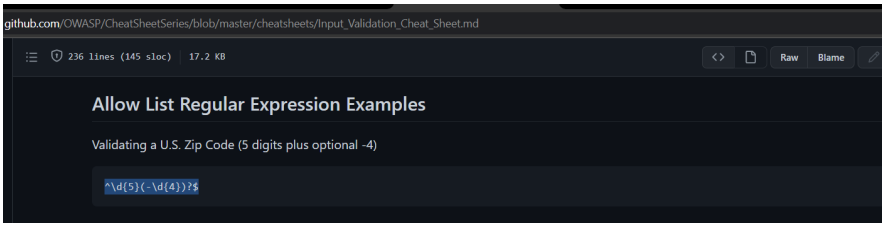
Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1:

Examine the OWASP Cheat Sheet. What is the regular expression used to validate a US Zip code?

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



Question 2:

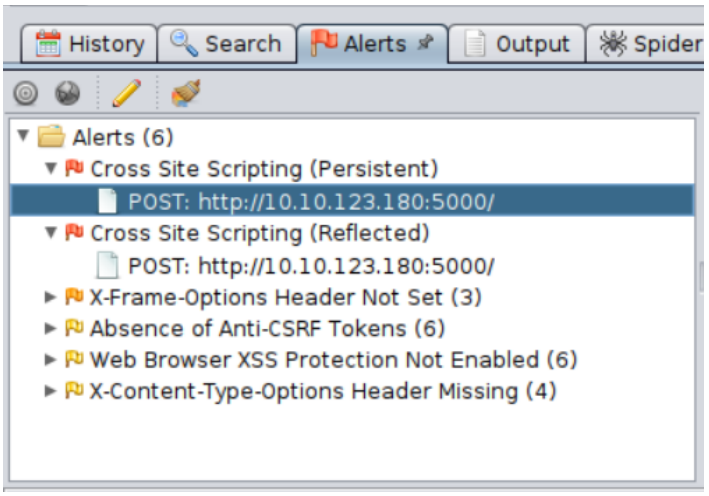
What vulnerability type was used to exploit the application? -Stored

Question 3:

What query string can be abused to craft a reflected XSS? -q

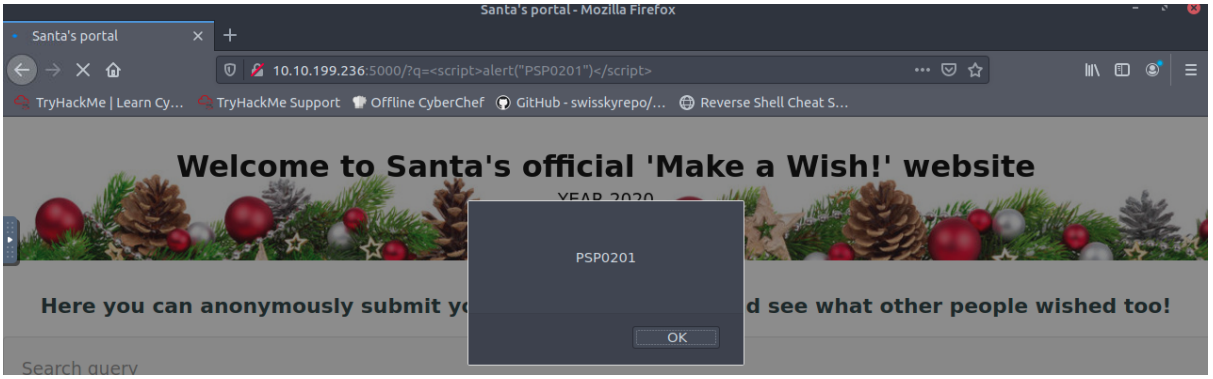
Question 4:

Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts of high priority are in the scan? -2



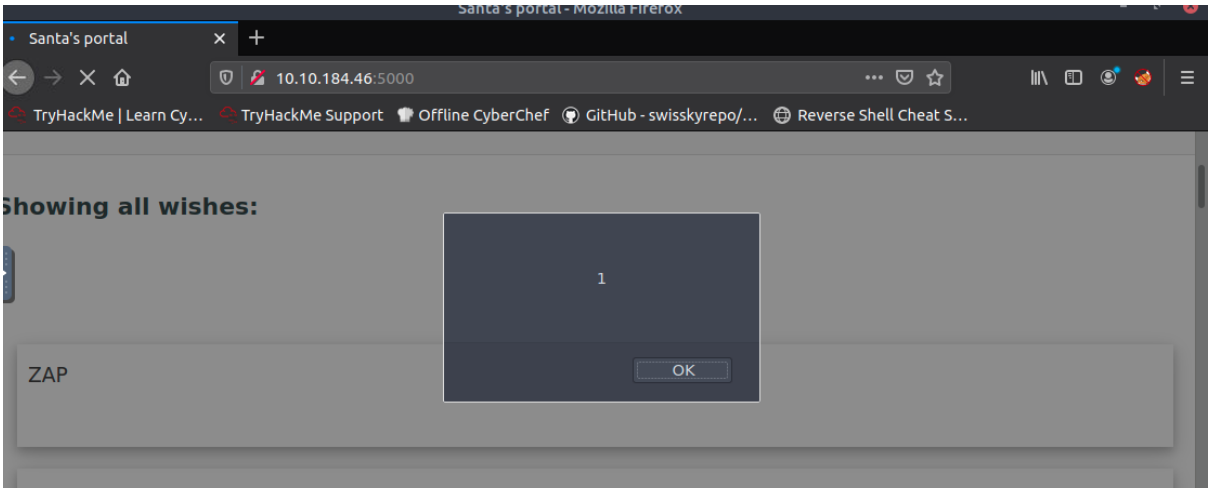
Question 5:

What Javascript code should you put in the wish text box if you want to show an alert saying "PSP0201"? -<script>alert("PSP0201")</script>



Question 6:

Close your browser and revisit the site MACHINE-IP:5000 again. Does your XSS attack persist? -yes



Thought Process/ Methodology:

After typing in in IP address given along with ":5000", we will access Santa's official "Make a Wish!" website. When we type out a wish in the box provided, we can see from the URL that the query string abused to craft a reflected XSS is the letter "q". To attack the XSS, we launch the OWASP ZAP Application. On the application, we type in the URL of the site we wish to attack and the machine will do the work for you. From there, we can find details on the website such as the amount of XSS alerts are in the scan, which was 2. When the application is closed, the attack persists.

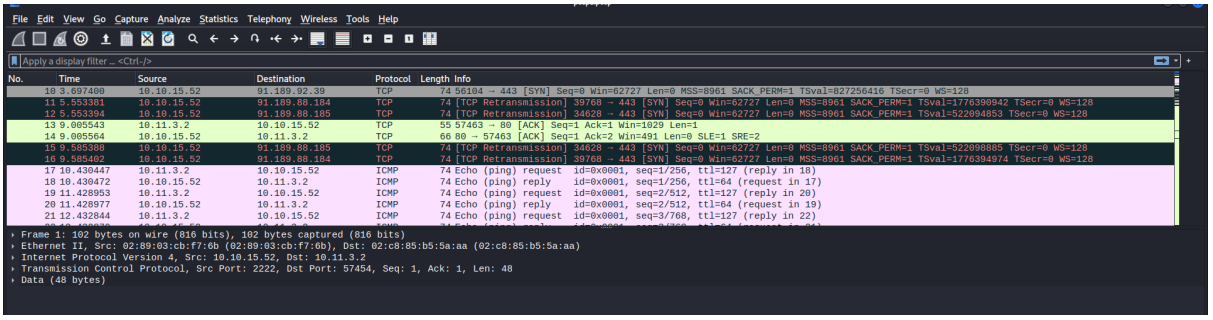
Day 7: Networking - The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox, Wireshark

Solution/walkthrough:

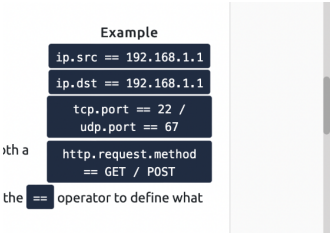
Question 1:

Open "pcap1.pcap" in Wireshark. What is the IP address that initiates an ICMP/ping? - 10.11.3.2



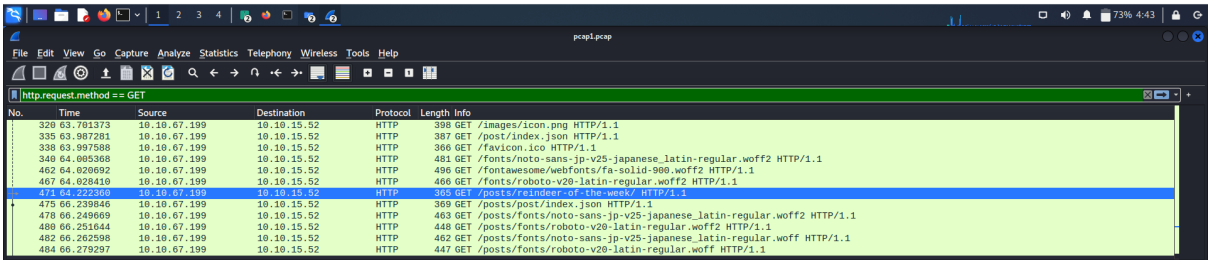
Question 2:

If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use? - http.request.method == GET



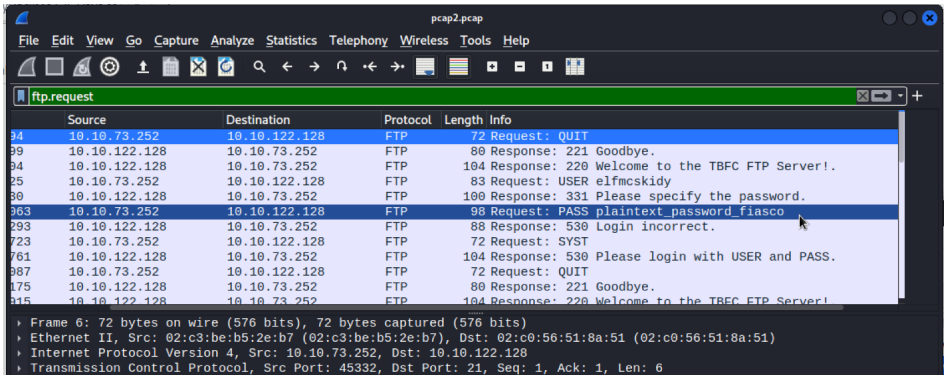
Question 3:

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? - reindeer-of-the-week



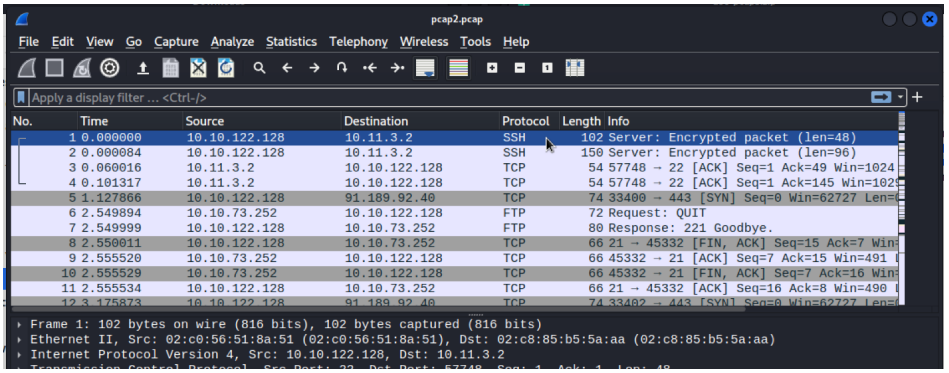
Question 4:

Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process? - plaintext_password_fiasco



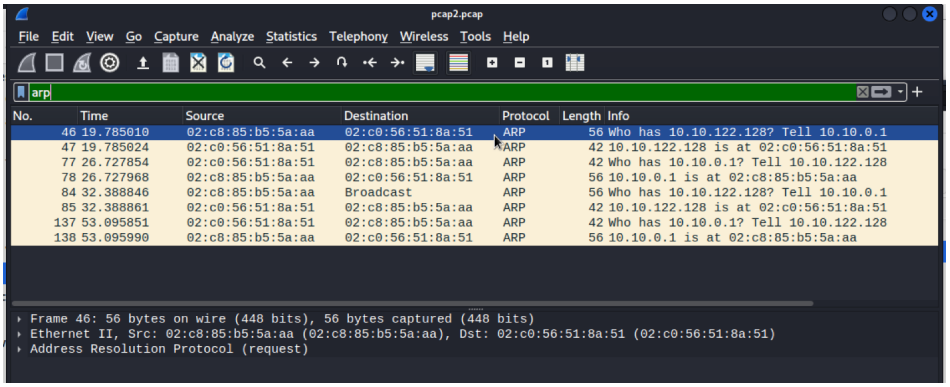
Question 5:

Continuing with our analysis of "pcap2.pcap", what is the name of the protocol that is encrypted? - SSH



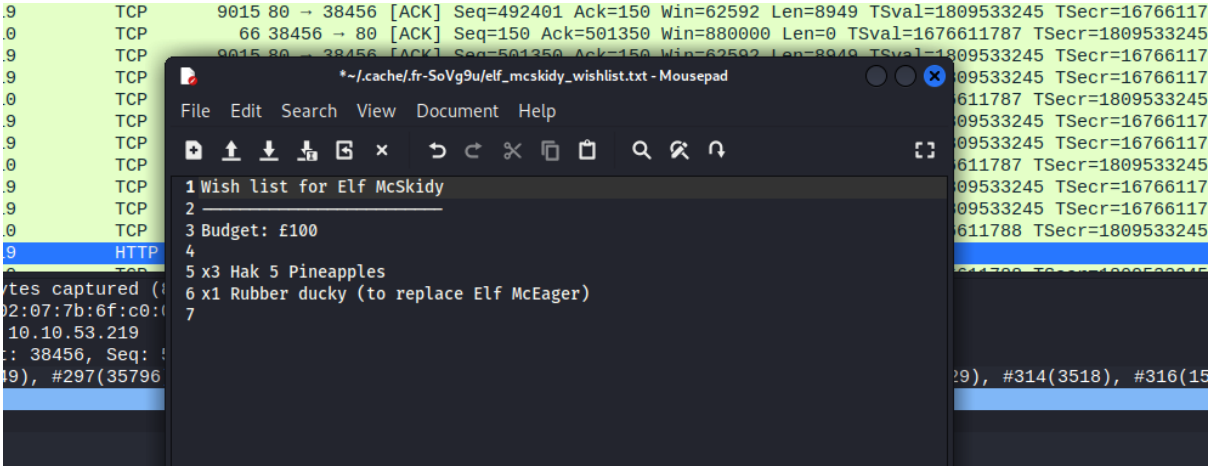
Question 6:

Examine the ARP communications. Who has 10.10.122.128? Tell 10.10.10.1. Answer: 10.10.122.128 is at - 02:c0:56:51:8a:51



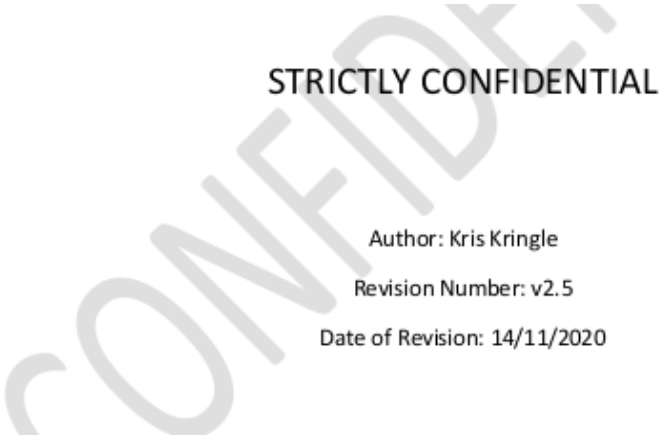
Question 7:

Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager? - rubber ducky



Question 8:

Who is the author of Operation Artic Storm? - Kris Kringle



Thought Process/ Methodology:

After having downloaded the file from THM, we can open **pcap1.pcap** file in Wireshark and find the IP address that initiates an ICMP/ping. We use **http.request.method == GET** filter to find the article that the IP address visited. We use the same process for **pcap2.pcap** file to find the password that was leaked. This filter is useful to find specific protocol types that we need to find such as SSH and ARP rather than spending a lot of time going through the list.

Day 8 : Networking - What's Under The Christmas Tree?

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1:

When was Snort created? - 1998

> 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:

Using Nmap on MACHINE_IP , what are the port numbers of the three services running? -

80,2222,3389

```
Nmap scan report for 10.10.149.237
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-title: TBFC&#39;s Internal Blog
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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 (ED25519)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 847.88 seconds
```

Question 3:

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

```
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-title: TBFC&#39;s Internal Blog
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
```

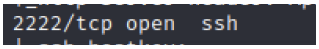
Question 4:

What is the version of Apache? - 2.4.29

```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
```

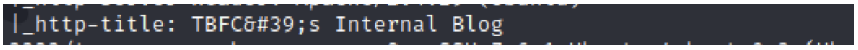
Question 5:

What is running on port 2222? - SSH



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? - blog



Thought Process/ Methodology:

Using **nmap** on our machine's IP, we can see all the information we need such as ports and the distribution that is running.

Day 9 : Anyone can be Santa - Prelude:

Tools used : Kali Linux, FireFox, Attackbox

Solution/Walkthrough:

Question 1 :

What are the directories you found on the FTP site? - backups , elf_workshops, human_resources, public

```
4096 Nov 16  2020 backups
4096 Nov 16  2020 elf_workshops
4096 Nov 16  2020 human_resources
4096 Nov 16  2020 public
```

Question 2 :

Name the directory on the FTP server that has data accessible by the "anonymous" user - public

```
4096 Nov 16  2020 public
```

Question 3 :

What script gets executed within this directory - backup.sh

```
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
```

Question 4:

What movie did Santa have on his Christmas shopping list? -The Polar Express Movie

```
root@ip-10-10-18-129:~# cat shoppinglist.txt
The Polar Express Movie
```

Question 5:

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

```
cat /root/flag.txt
THM{even_you_can_be_santa}
```

Thought Process/ Methodology:

We only use the attackbox to start this machine and then click on the terminal then put the 'ftp [IP Addresses given]' in the terminal. After that click enter until it says connected. Put 'anonymous' at the name until it says login successful. You can use the help command to list some of the commands you can run whilst connected to the FTP Server. ook at the directories available to use ls. We'll navigate to this using cd to change our working directory and then ls to list the contents. Then use get to get the file from the server onto our device. With the file downloaded, open it on our device using a terminal text editor such as nano. Next,, replacing the IP_ADDRESS with your TryHackMe IP, this address is displayed on the navigation bar on the access page. set up a netcat listener to catch the connection on our AttackBox: nc -lvnp 4444. now attempt to upload our malicious script to the folder that we have write permissions on the FTP server by returning to our FTP prompt and using put to put the file into that directory. Return to our netcat listener, after waiting one minute, you should see an output like below and we're done.

Day 10 : Networking -Don't be sElfish!

Tools used : THM Attackbox

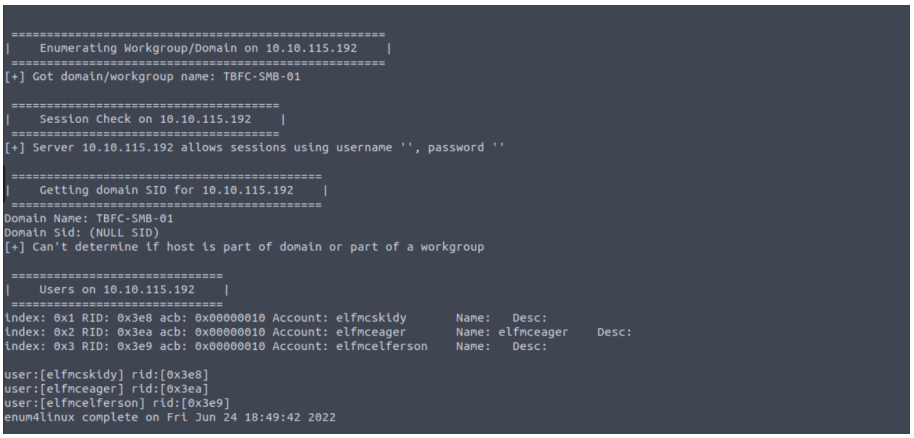
Solution/Walkthrough:

Question 1

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

Question 2

Using enum4linux, how many users are there on the Samba server? -3



Question 3

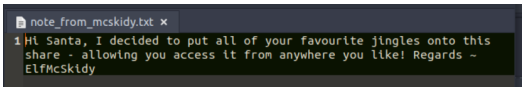
Now how many "shares" are there on the Samba server? -4

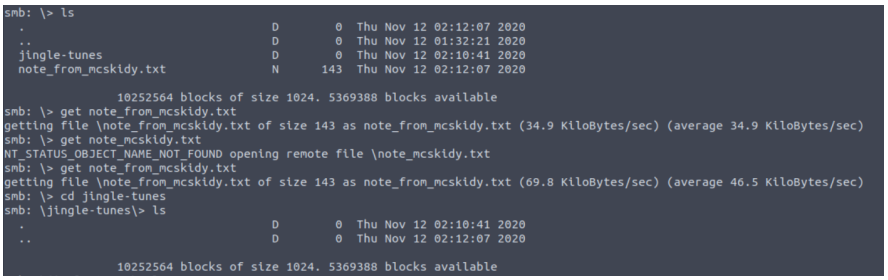
Question 4

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? - jingle-tunes





Thought Process/ Methodology:

We're using the THM AattackBox to solve this task. Using the terminal prompt in the attackbox, we navigate to enum4linux. We run the enum4linux and it list all the possible options for us to use. By referring to all the options listed, we use -U to figure out total of users and -S to list out all the "shares" on Samba server. Then, we use smbclient tool to access the Samba server and its shares by replacing "sharename" in `smbclient //10.10.119.152/**sharename**` with all the possible sharename listed before using try and error method until we found one that doesn't require a password. After logging in the share, we use the ls command to list files and directories in the share.Using the get command to get the directory ElfMcSkidy leave for Santa.