PSP0201

Week 3

Writeup

Group name: The Convocation

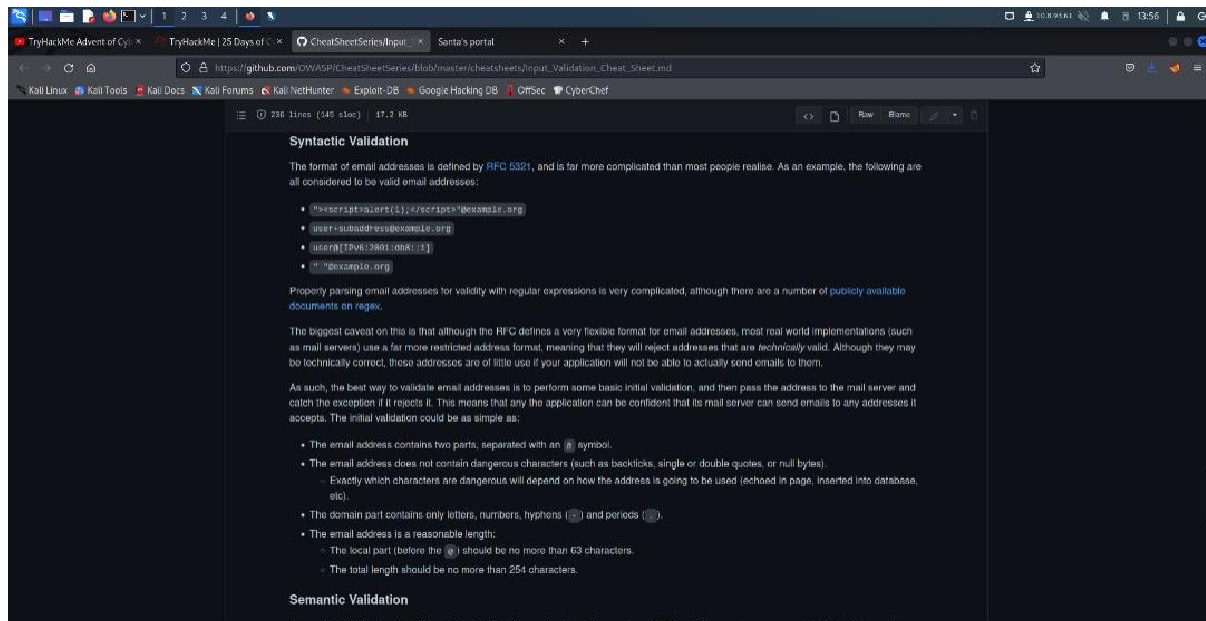Group members:

ID Number	Name	Role
1211101903	Daniysh bin Ahmad Azwang Aisram	Leader
1211102301	Muhammad Aqrel bin Shahrulanuar Mushaddat	Member
1211102601	Adil Azraie bin Razman	Member

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

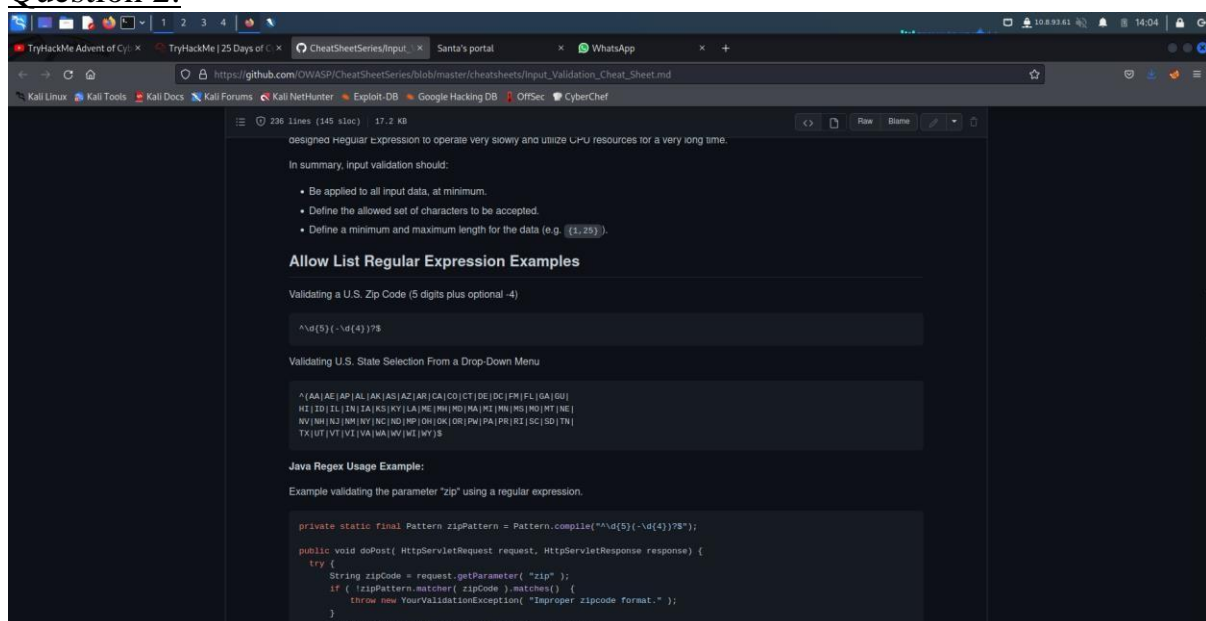**Tools used:** Kali Linux, Firefox, OWASP ZAP
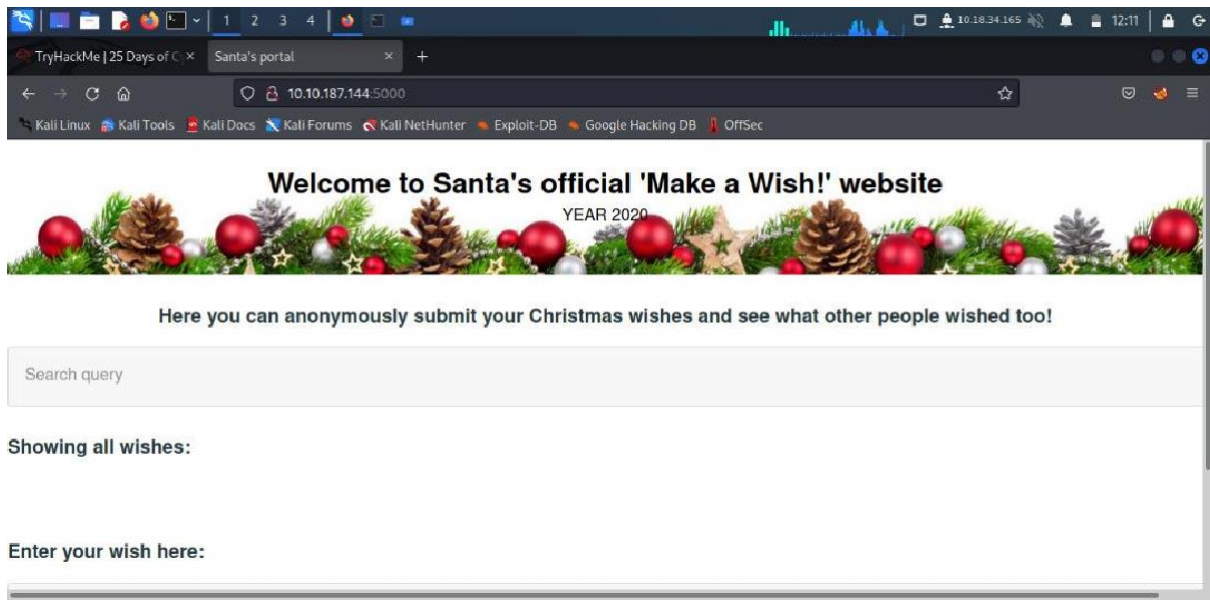
Solution/Walkthrough:

Question 1:

Finding the definition of Syntactic and Sematic in the OWASP ZAP Cheat Sheet in Github Forum.
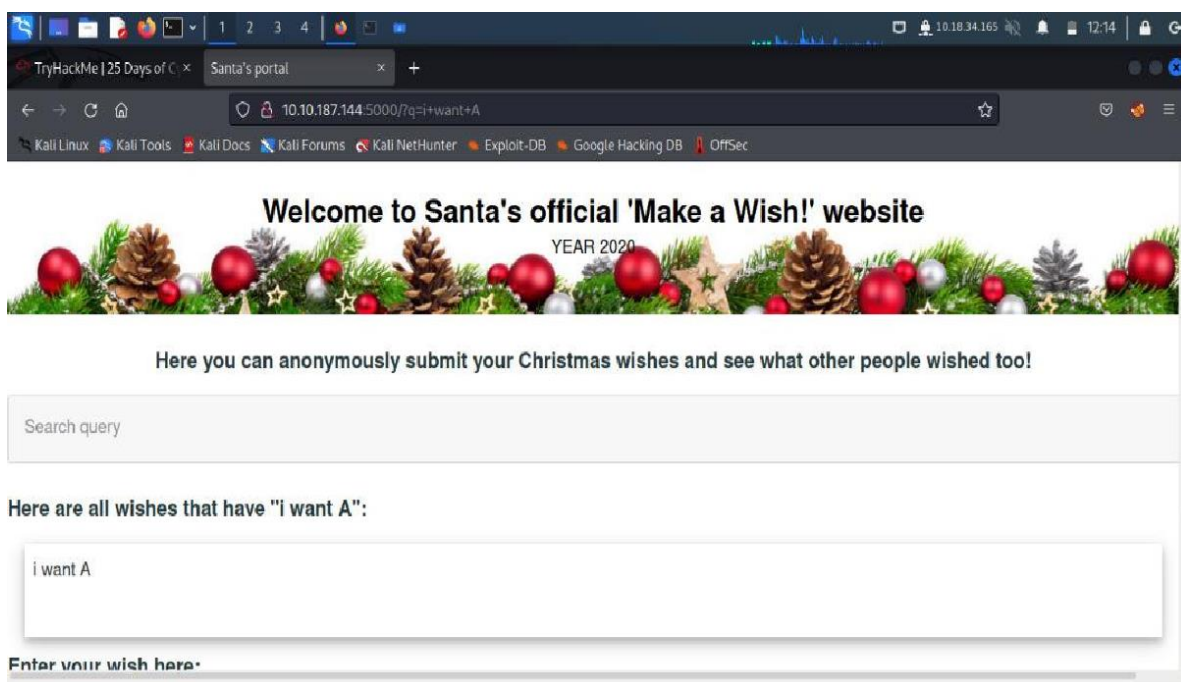
Question 2:

To find the regular expression used to validate a US ZIP CODE we have to use the Cheat Sheet in the Github Forum.
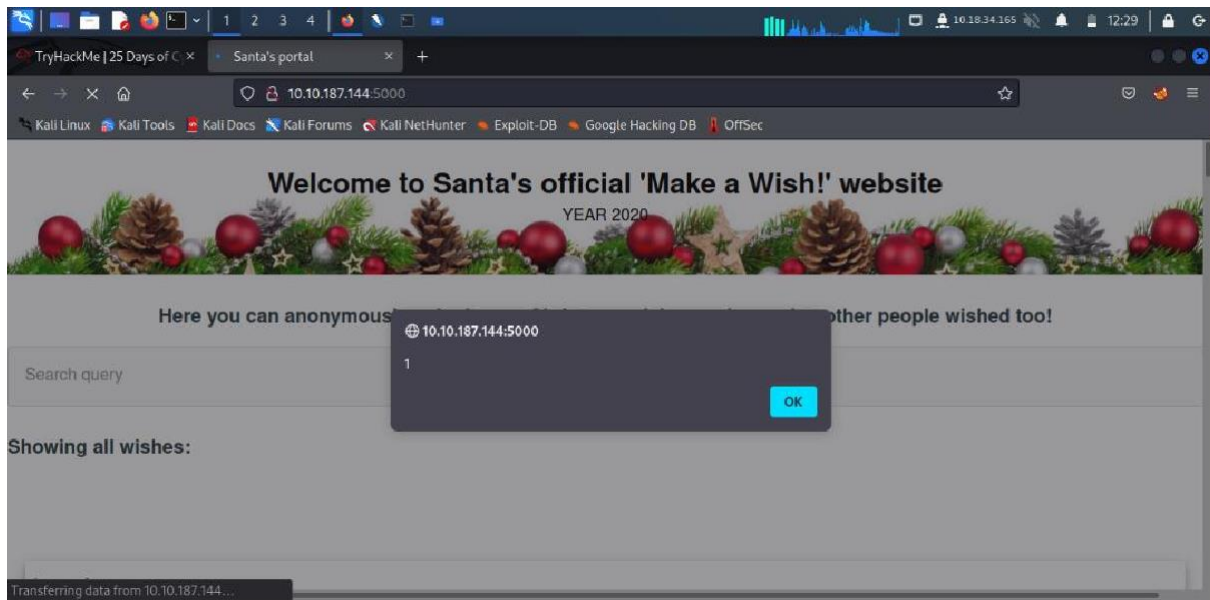
Question 3:

To find the vulnerability type of the website we have to see first how the website works.
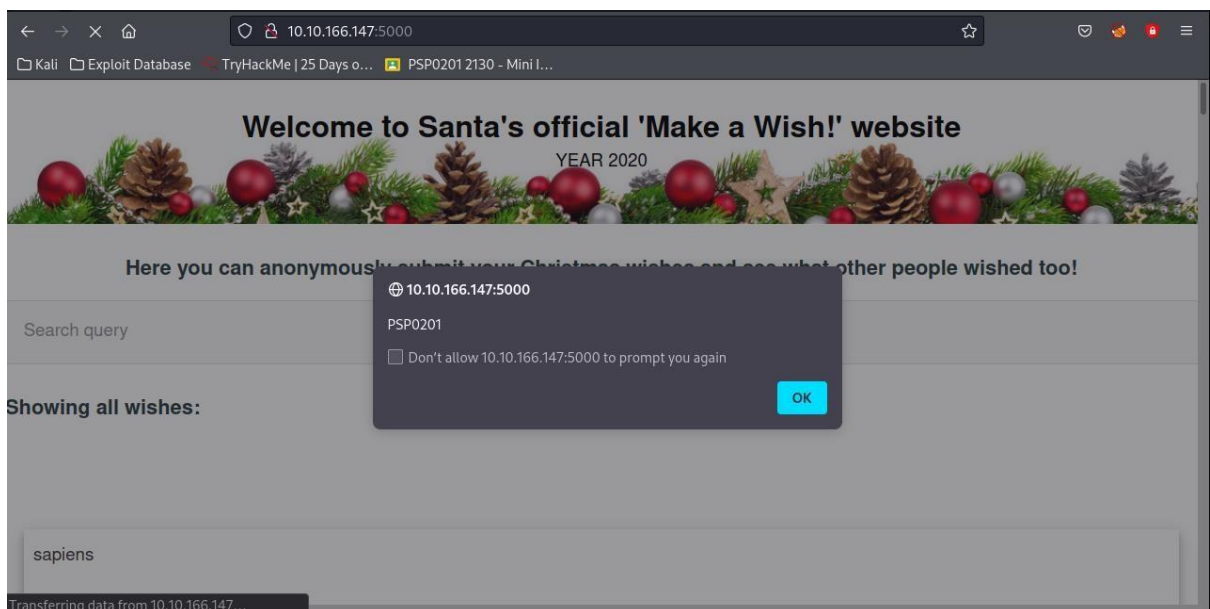
Question 4:

To test and find the query string type of the website is just to test the website by trying multiple strings to find the right one.

Question 5:

There is only 2 high priory alerts that we can get from the XSS scan

Question 6:

Go to the wish list page and put in **<script>alert("PSP0201") </script>** into the wish text box and ull get the notification.

If we revisit the page after getting the alert, we will still have the same alert asshown in question 5.

Thought Process / Methodology:

First before starting we have to download the app **'OWASP ZAP'** as we will use the URL to make the attacks on the server page. Then we will visit the page tosee what we have to do. After opening the page, we will be required to make a wish so to notify ZAP that we are trying to make an attack. Then we have to copy the page URL and put it in the ZAP app to make an attack. Lastly if the attack is successful, we will get an alert notification.
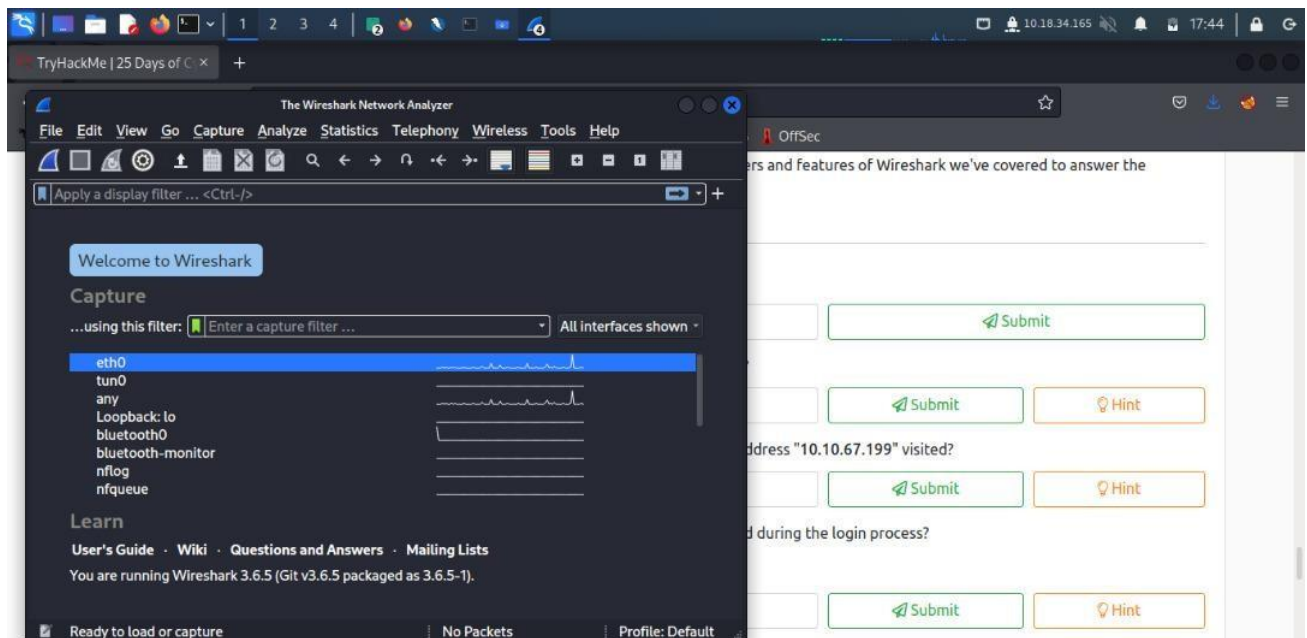
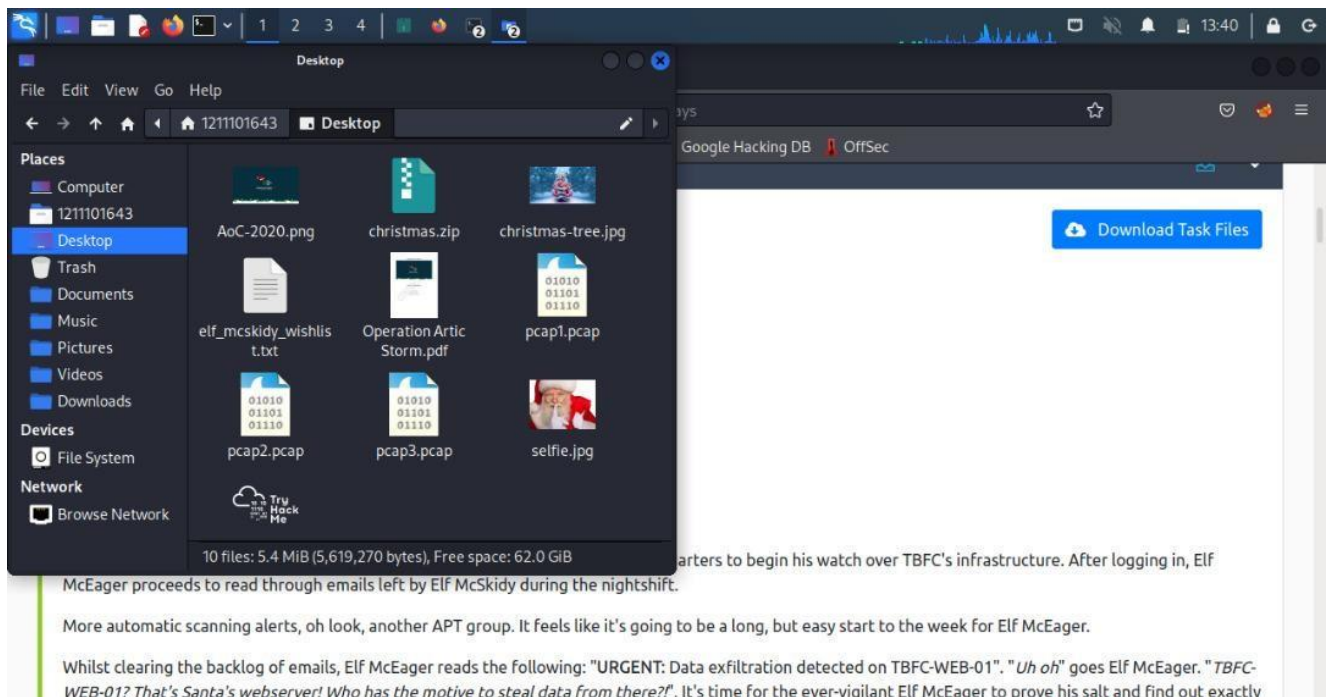**Day 7:** Networking The - Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox, Wire Shark

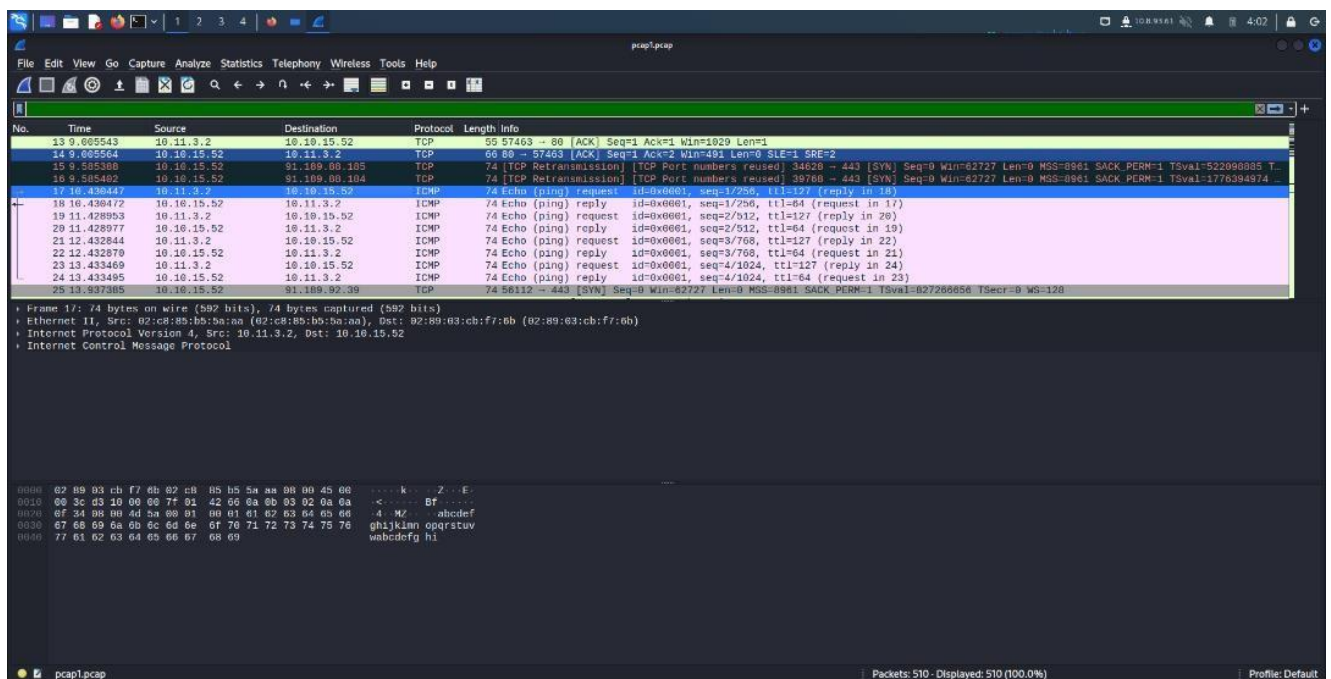**Solution/walkthrough:**

Question 1:

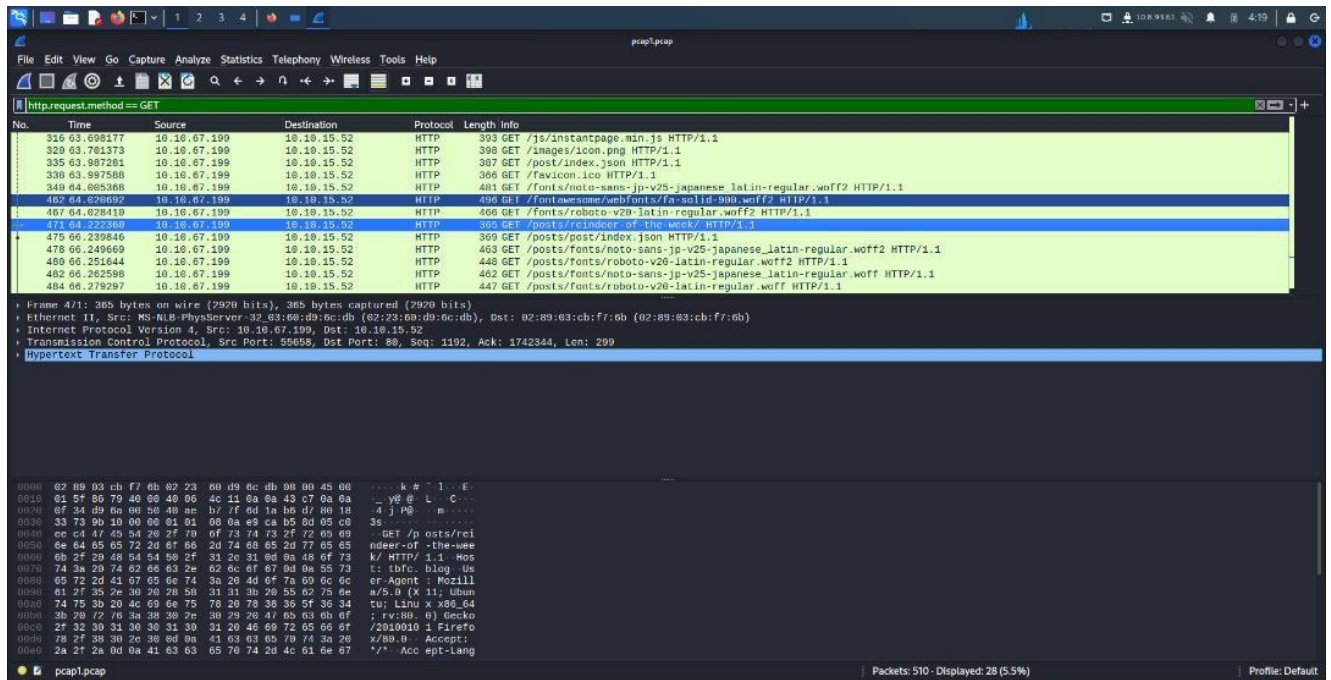Install Wireshark and download task files for the process.

Question 2:

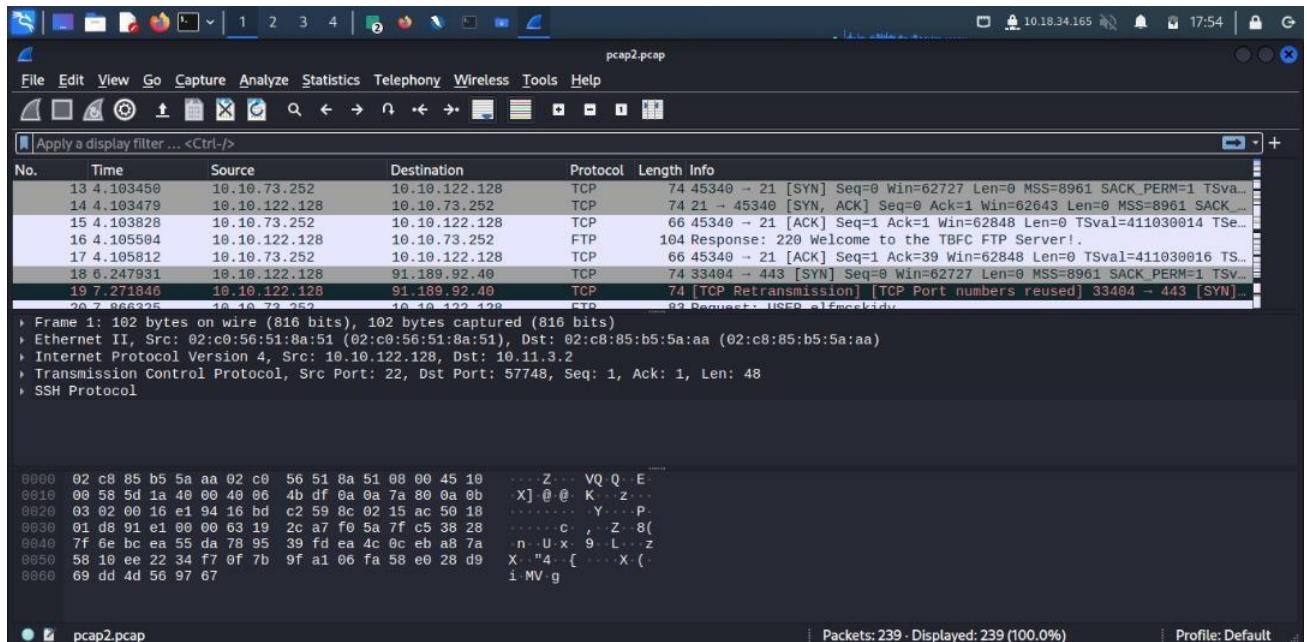Open first file which is pcap1.pcap and find for the first instance of ICMP initiated
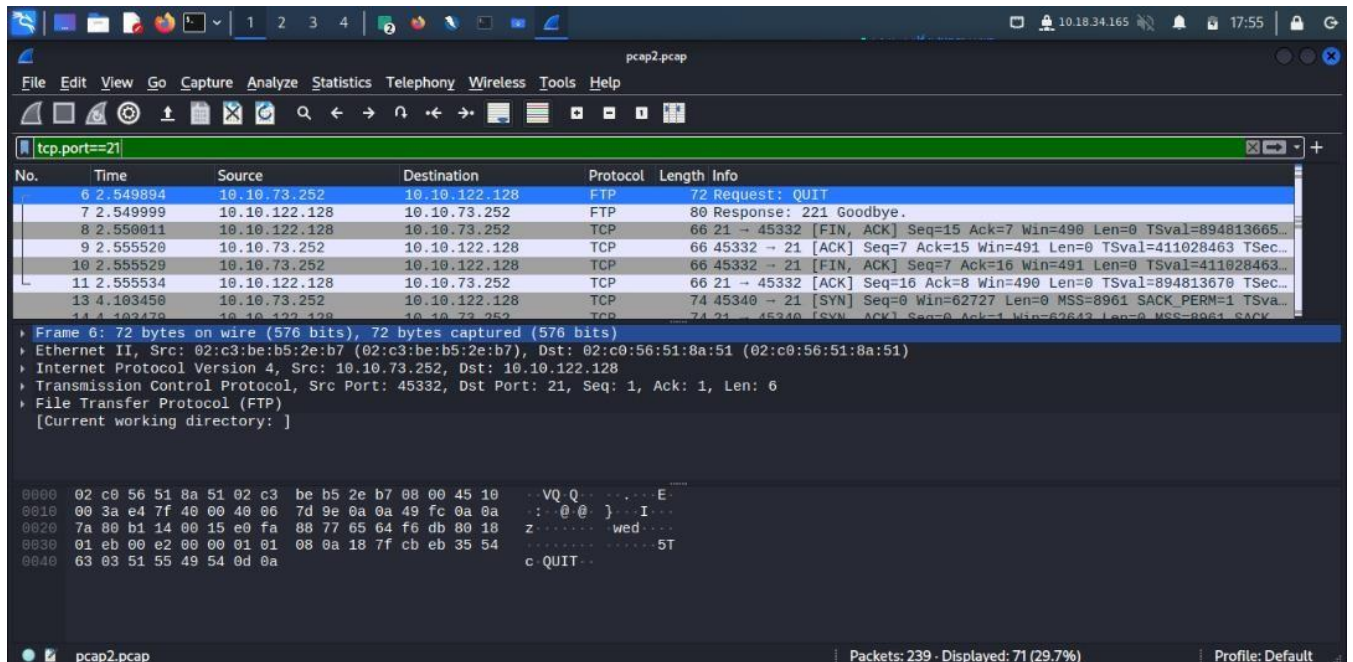

Question 3:

We get the HTTP request by using filter "http.request.method == GET" and find the /post/ with the name of the article.
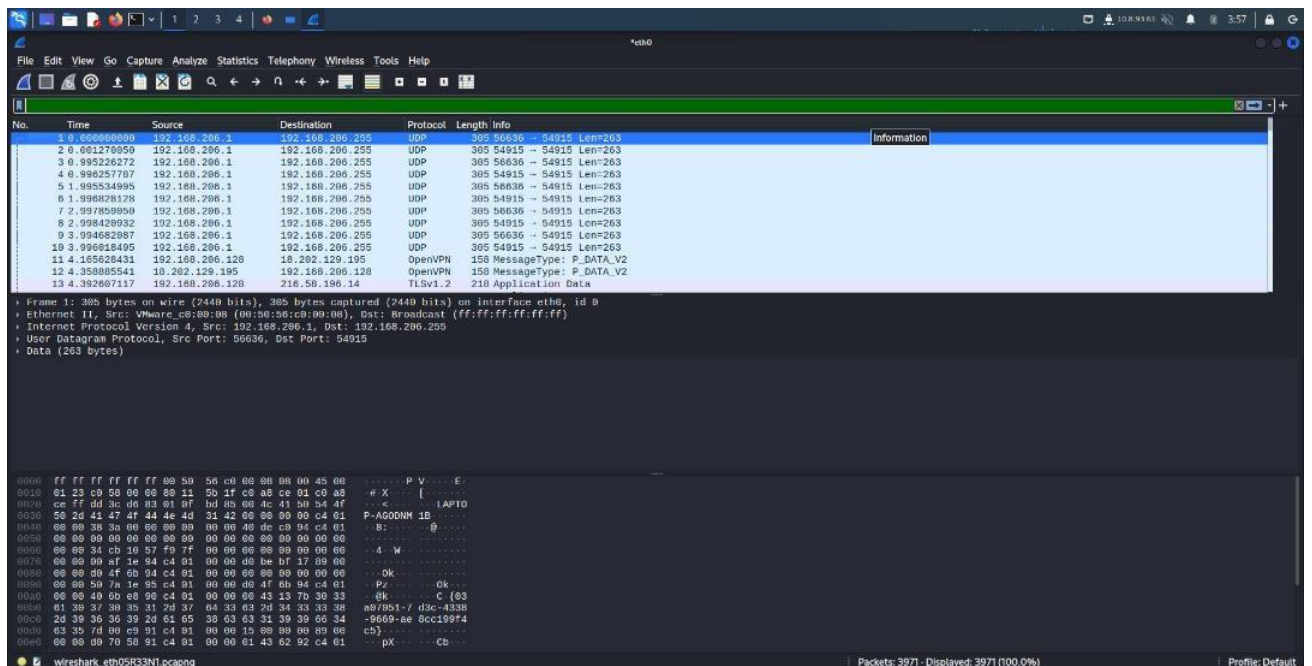
Question 4:

FTP uses the TCP protocol, and port 21 is the default port. Use the filter
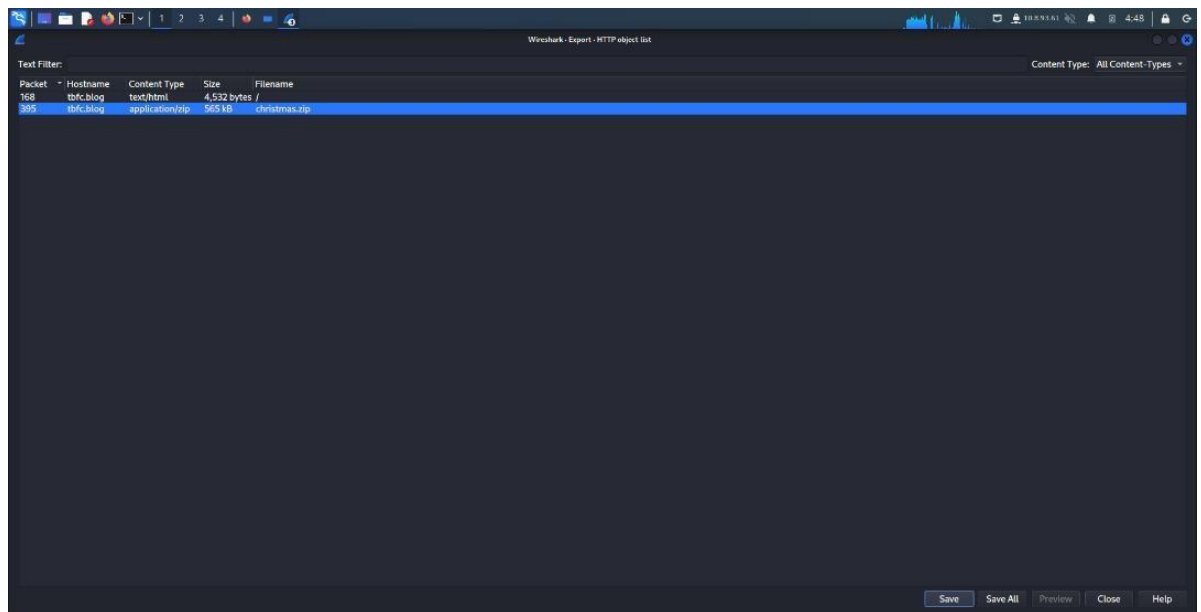"tcp.port == 21" to ensure that it does.

Question 5:

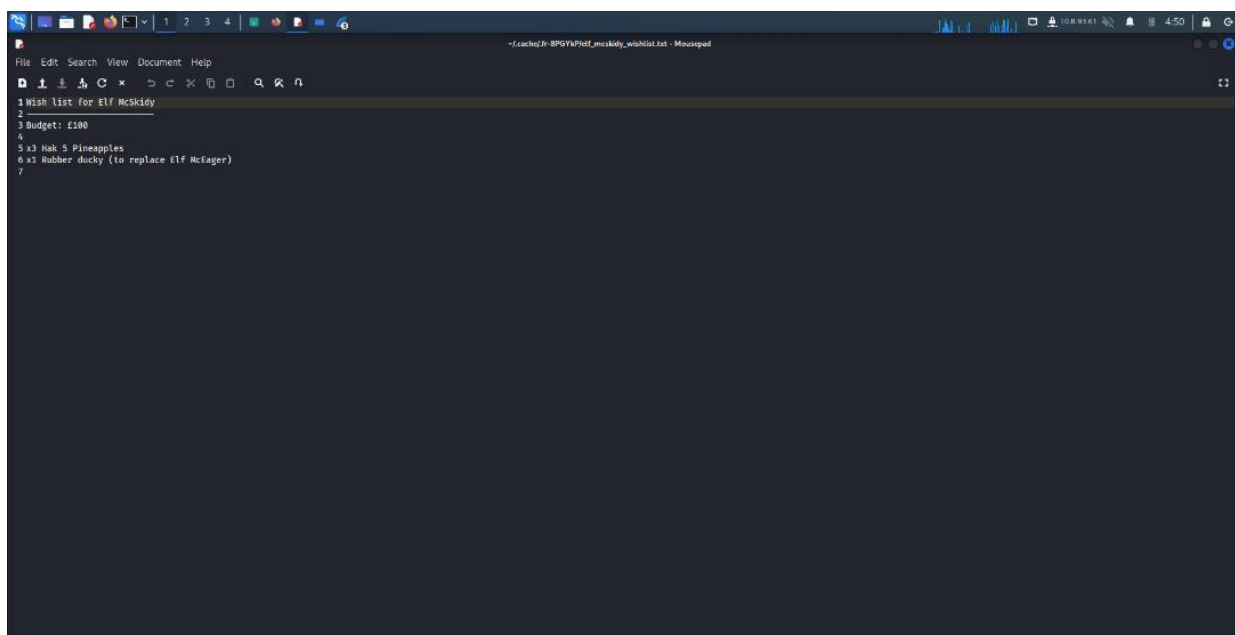Look for the encrypted package by analysing "pcap2.pcap".

Question 6:

Export the "christmas.zip" file.

Question 7:

Open the "elf_mcskiddy_wishlist.txt" in the ZIP file and open the "Operation Arctic Storm.pdf".

Thought Process/Methodology:

First of all, download zip file from the website and extract it. Using Wireshark we identify the IP address that initiates the ICMP/ping from the first file. After we get the IP address we type the filter which is "http.request.method == GET" to get the HTTP GET request. Then, we identify the name of the article. By using the second file, we get to know the password that leaked during the login process by using "TCP port==21" filter. We also find the SSH protocol. After that, we also find the Elf McSkidy's wishlist by using the third file and choose the HTTP. We export the file and open the file to see the wish list.
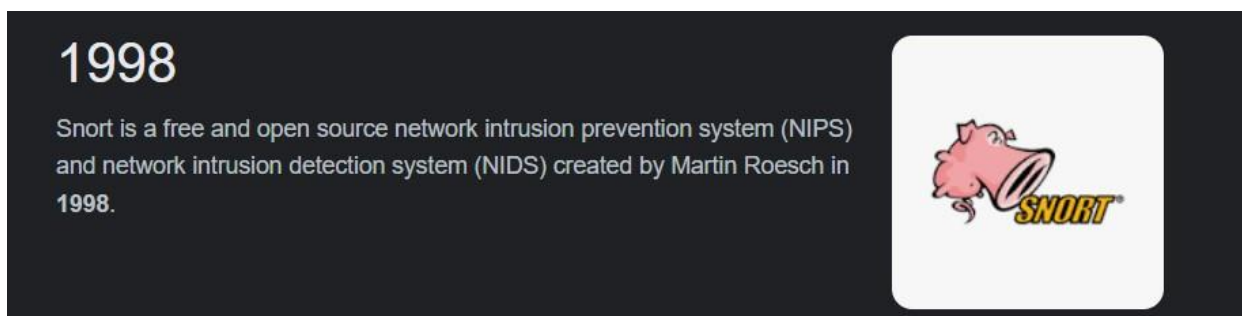
Day 8: What's Under the Christmas Tree?

Tools: Kali Linux, Nmap

Solution:

Question 1: When was snort created?

Open the browser and type in "when was snort created?" and then answer shown as 1998

Question 2: Using nmap on: ip address: what are the port numbers of the three services running?

Open terminal and type in nmap :ip address: ,it will scan the host using nmap.

```
┌──(1211101120㉿kali)-[~]
└─$ nmap 10.10.251.215
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-24 21:16 EDT
Nmap scan report for 10.10.251.215
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 35.23 seconds
```

Question 3,4 and 5: Experiment the host using different types of scans of nmap.

Typing different scan such as -Pn -A -sV insert it inside; nmap 'scan' :ip address:

```
┌──(1211101120㉿kali)-[~]
└─$ nmap -Pn 10.10.251.215
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-24 21:37 EDT
Nmap scan report for 10.10.251.215
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 35.86 seconds
```

Question 6: What do we think this website might be used for?

By using '-A' scan, we can see the http title which is TBFC's Internal Blog and so we can conclude the website is used for blogs.

```
┌──(1211101120㉿kali)-[~]
└─$ nmap -A 10.10.251.215
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-24 21:45 EDT
Nmap scan report for 10.10.251.215
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-title: TBFC&#39;s Internal Blog
|_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/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.71 seconds
```

Methodology:

Nmap, short for Network Mapper, is a free and open-source tool used for vulnerability checking, port scanning and, of course, network mapping. Despite being created back in 1997, Nmap remains the gold standard against which all other similar tools, either commercial or open source, are judged.

Nmap has maintained its pre-eminence because of the large community of developers and coders who help to maintain and update it. The Nmap community reports that the tool, which anyone can get for free, is downloaded several thousand times every week.

In conclusion, it can be modified to work within most customized or heavily specialized environments because of its flexibility of being an open-source code base. There are distributions of Nmap specific to Windows, Mac and Linux environments, but Nmap also supports less popular or older operating systems like Solaris, AIX or AmigaOS. The source code is available in C, C++, Perl and Python.

Day 9: Anyone can be Santa!

Tools used: Root account, terminal command

Solution/walkthrough

Setting up

Insert MACHINE_IP target.txt and cat target.txt on your own MACHINE_IP before running the ftp. ftp would not detect if the target.txt didn't run.

Question 1:

let's ftp in and login as anonymous. So, we can cd into the public directory
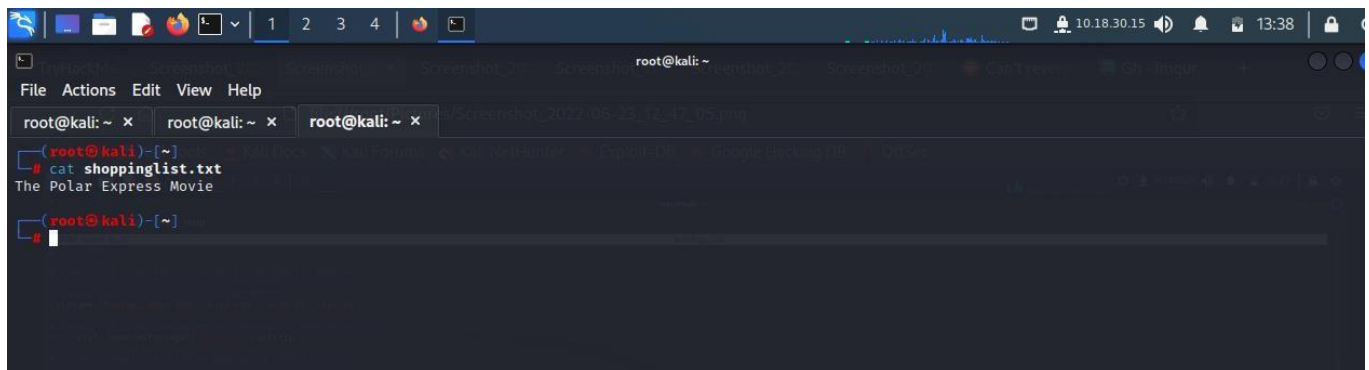

ANSWER: CD PUBLIC

Question 2:

To find the answer to this question, I changed directories into "public" and then looked at the contents. There is a script called backup.sh located within.

```
230 Directory successfully changed.
ftp> get backup.sh
local: backup.sh remote: backup.sh
229 Entering Extended Passive Mode (|||62796|)
150 Opening BINARY mode data connection for backup.sh (341 bytes).
100% |**********************************************************************************
226 Transfer complete.
341 bytes received in 00:00 (1.33 KiB/s)
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
229 Entering Extended Passive Mode (|||35989|)
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
100% |**********************************************************************************
226 Transfer complete.
24 bytes received in 00:00 (0.09 KiB/s)
```

ANSWER: BACKUP.SH

Question 3:

To retrieve the shopping list, I used the "get" command. It is now located on my own system for me to view.

ANSWER: THE POLAR EXPRESS MOVIE

Question 4:

Going to kind of go past just outputting the contents of the file and get a reverse shell instead. We can add just a simple one liner and setup our netcat listener. And re-upload the file to FTP server and let it run, may take a minute but should get us a shell…so after not getting a shell and playing around I noticed that the file that was uploaded didn't have execute permissions. Already root we founded the flag the already rooted

ANSWER: THM{EVEN_YOU_CAN_BE_SANTA}

Methodology

FTP or File Transfer Protocol offers file sharing in comparison to alternative protocols available. This protocol isn't encrypted which means it is easily accessible. FTP uses two connections when transferring data which is Port 20 and Port 21. Before any data can be shared a client must log in to the FTP server which determines the command. Log in as anonymous mode allows default username to be used with any password by a client. FTP being used over a terminal in a package which could be use with IP address and an anonymous account. Set up a netcat listener to catch the connection on KALI. With netcat we could upload our malicious script so we could see an output shown. Conclude we learned how simple misconfigurations can lead a full-blown hack on an FTP Server.

Day 10: Networking - Don't be sElfish!

Tools used: Kali Linux, Firefox, Terminal

Solution/Walkthrough:

Question 1:

The picture shows all the list of commands/flags that we can get from the command 'HELP' using enum4linux.

Question 2:

By using enum4linux we can get the number of users exist by using the command '-U' and it will show all the available user that exist.
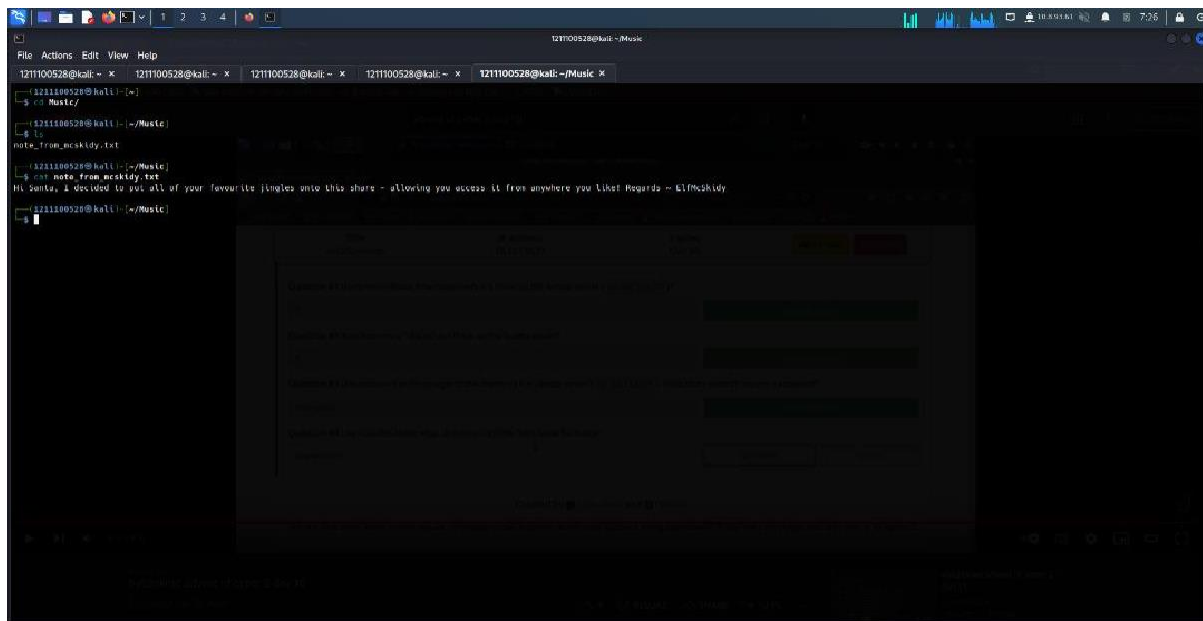
Question 3:
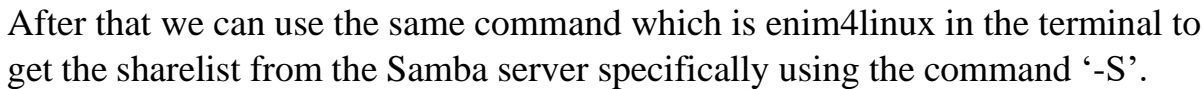
After that we can use the same command which is enim4linux in the terminal to get the sharelist from the Samba server specifically using the command '-S'.

Question 4:

To find the user that we can use the Samba server we try and use the smbclient to find the useí that doesn't íequiíe passwoíd to enteí which is **'tbfc-santa'.**

Question 5:

To get to the directory of ElfMcSkidy we have to use the command **'ls'** after we got in the Samba server and store the directory in lcd to get the notes.

Thought Process / Methodology:

The first thing that we need to do is to start the Samba Server by using the command enim4linux then we can use the command **'-h'** to see the commands that we can use such as the command **'-U'** to get the user list that is available in the server. Then we have to get the share list by using the command **'-S'** and to also see the user that we can use to login in the Samba server to find the directory that we need.