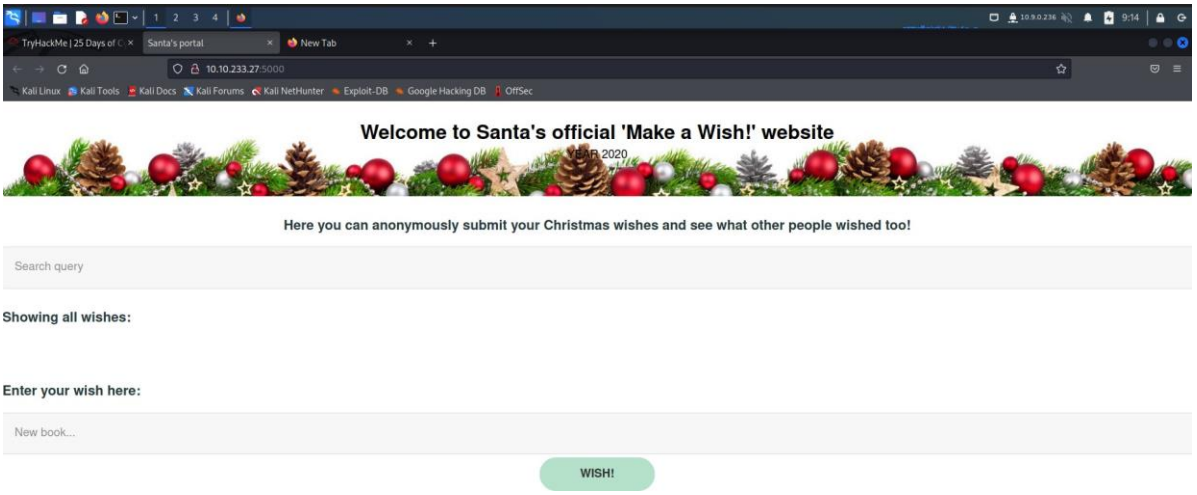
Day 6: Web Exploitation - Be careful with what you wish on a Christmas night

Tools Used: Kali Linux, OWASP

Solution/ Walkthrough

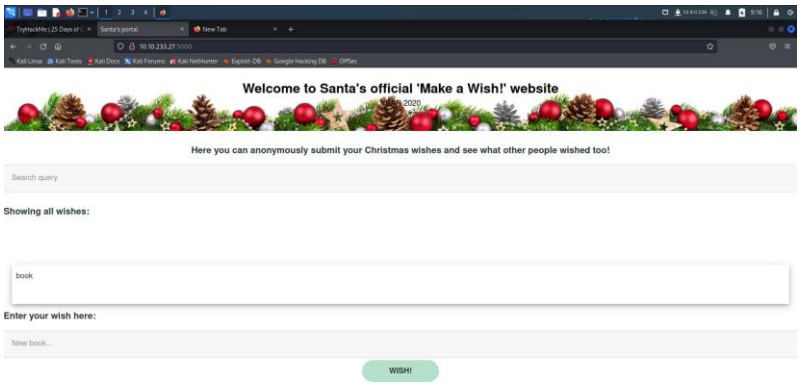
Question 1-3

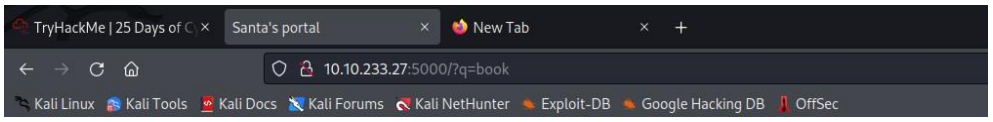
We got to the machine IP on port 5000



Stored Cross-site Scripting is used in order to exploit this application

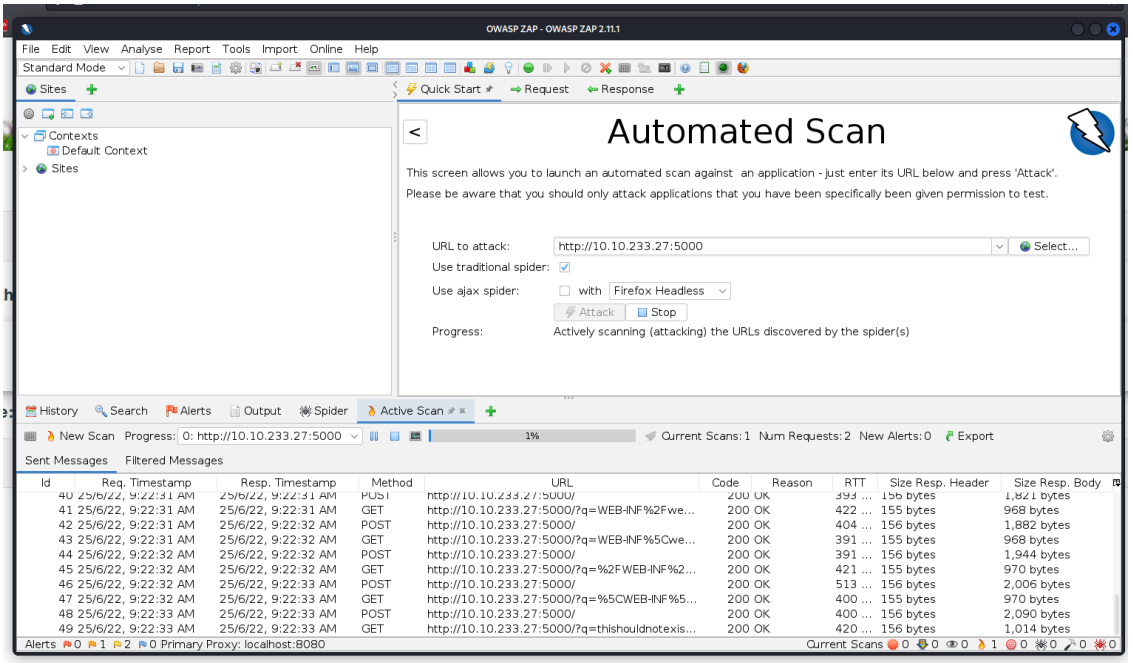
"q" as the query string





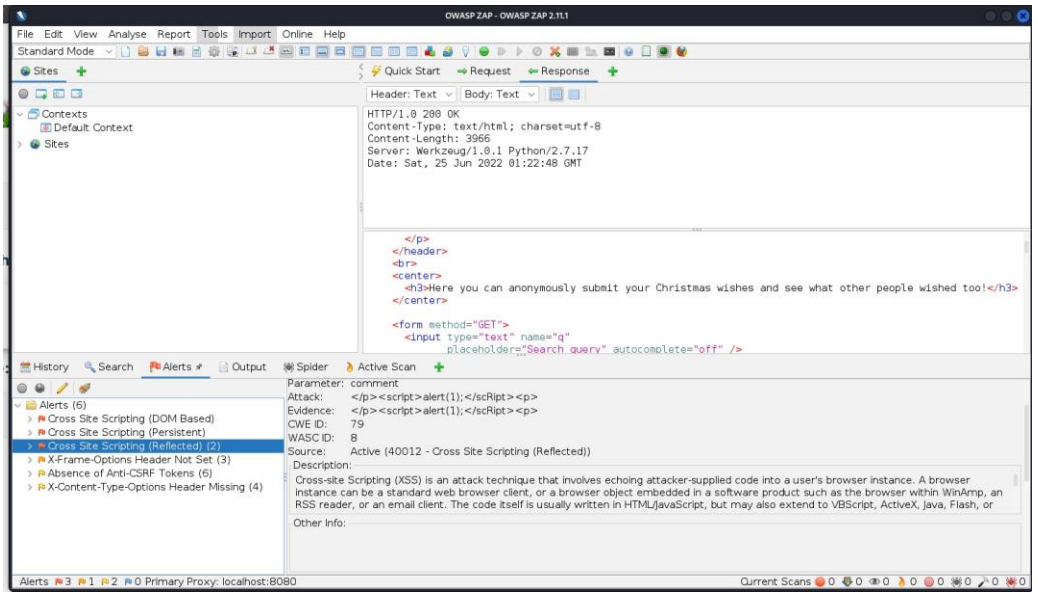
Question 4

We used OWASP ZAP and ran a scan.



Question 5

We obtain 3 types of XSS Alerts from the results but reflected XSS is the one we're interested in.



Question 6

An interesting line from source is discovered.

Header: Text | Body: Text

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 3966
Server: Werkzeug/1.0.1 Python/2.7.17
Date: Sat, 25 Jun 2022 01:22:48 GMT
```

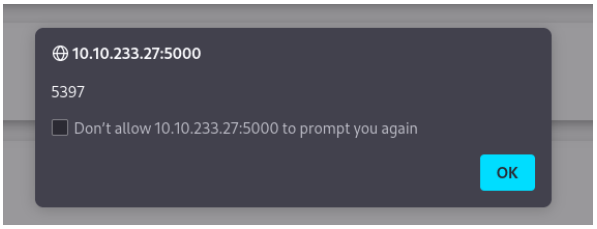
```
        <p">><!--#EXEC cmd="dir \"--><</p>
      </div>

      <div>
        <p>0W45pz4p</p>
      </div>

      <div>
        <p></p><scrIpt>alert(1);</scRipt><p></p>
      </div>


    <h3>Enter your wish here:</h3>
    <form action="/" method="POST">
      <input type="text" name="comment"
             placeholder="New book..." autocomplete="off" />
      <input type="submit" value="Wish!" />
    </form>

  </body>
</html>
```

Spider | Active Scan

Parameter: comment
Attack: <scrlpt>alert(1);</scRipt>

Question 7:

Alert(1) is shown with the numbers 5397.



Thought Process/ Methodology:

We go to the machine ip provided with port 5000, it seems like this app stores data on the website, meaning Stored Cross-site Scripting could be used to exploit this application. This app seems like this app stores data on the website, meaning Stored Cross-site Scripting could be used to exploit this application. We found out "q" is used as the query string, which can be abused to craft a reflected XSS. Using OWASP ZAP to run a scan on it, There seems to be 3 types of XSS Alerts from the results, but reflected XSS should be the one we're looking for. There is a javascript that looks suspicious, we ran iit in the "Enter your wish" slot and It seems like it broke the website, random strings and code and exposed and omitted, with a random alert with numbers 5397 popping up.

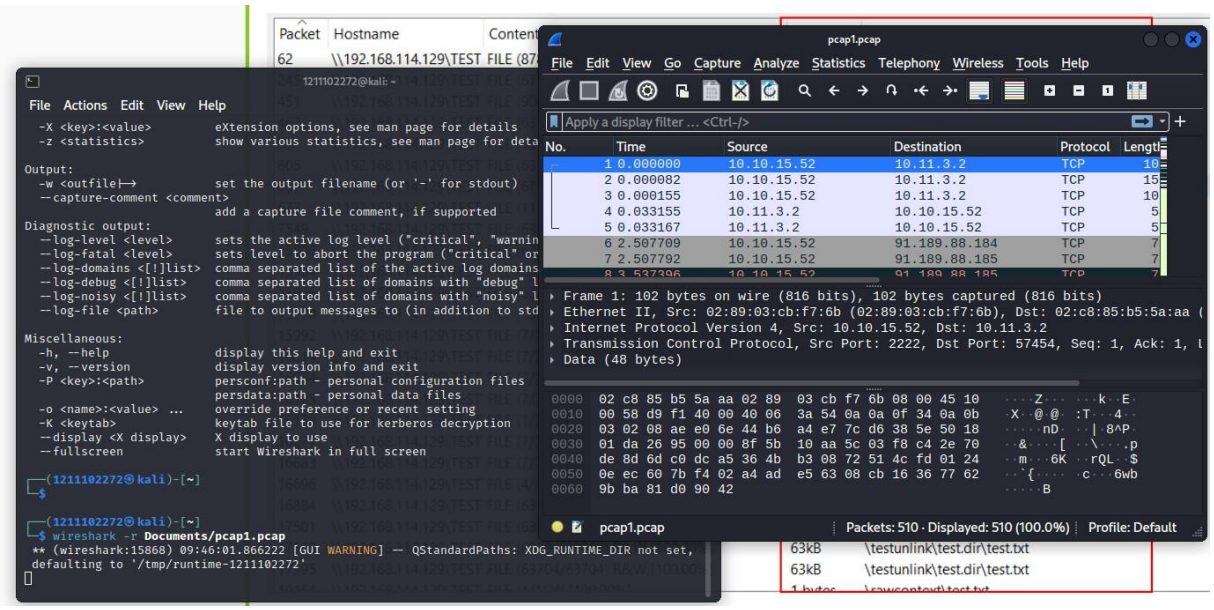
Day 7: Networking - The Grinch really did Steal Christmas

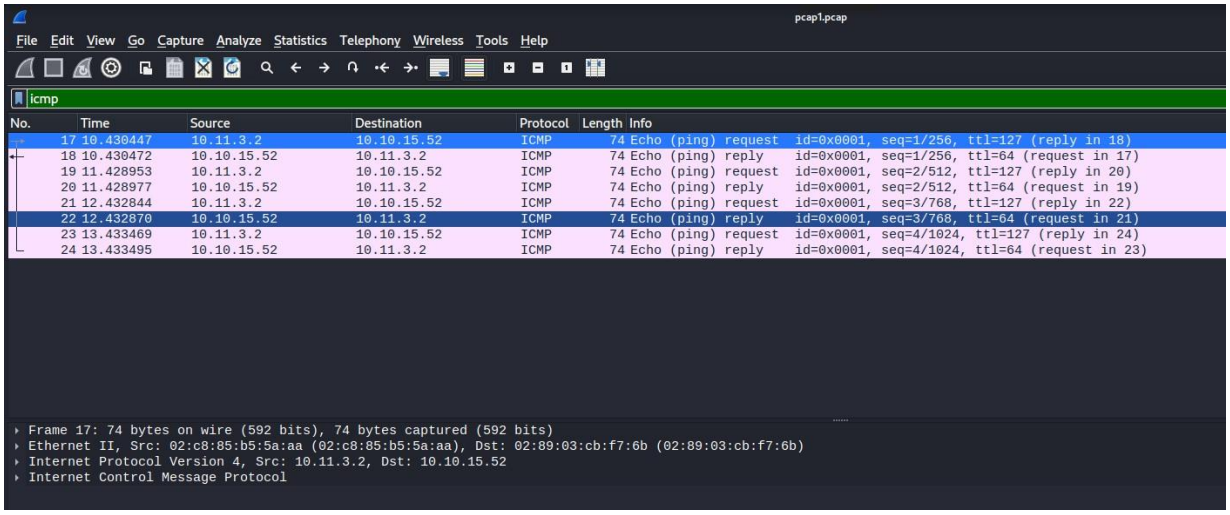
Tools Used: Kali Linux, WireShark

<u>Question 1</u>

We launch wireshark with -r to read the .pcap file

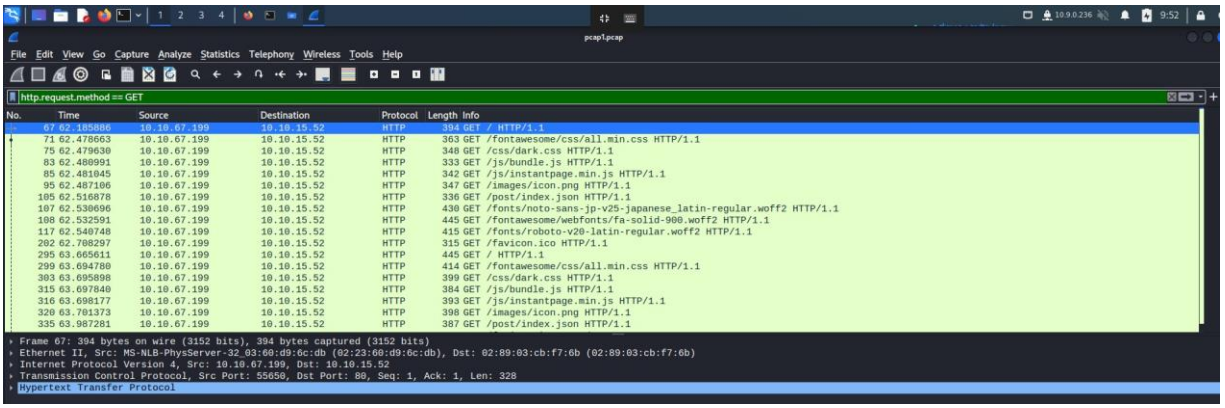
After applying an ICMP display filter, we can see the address responsible for initiation is 10.11.3.2





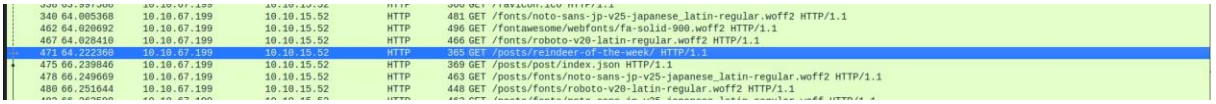
Question 2

The filter used is "`HTTP.REQUEST.METHOD == GET`".



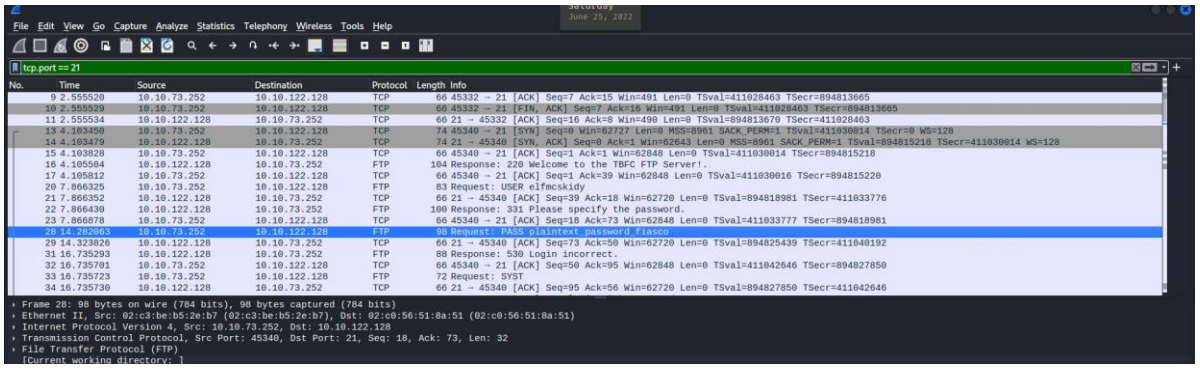
Question 3

IP Address "`10.10.67.199`" visited the article called "reindeer-of-the-week"



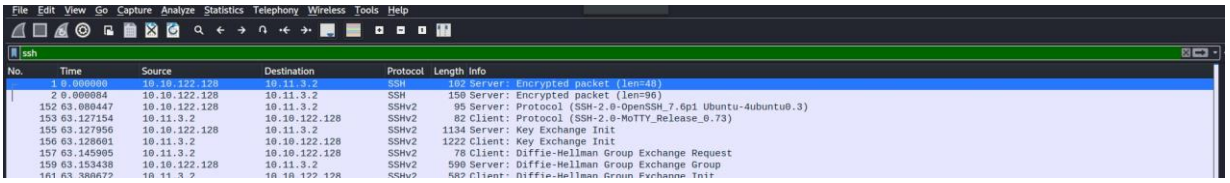
Question 4

After launching pcap2.pcap using the exact steps, we applied "`tcp.port == 21`" to filter out the logs, and see that the correct password for logging in is "`plaintext_password_fiasco`"



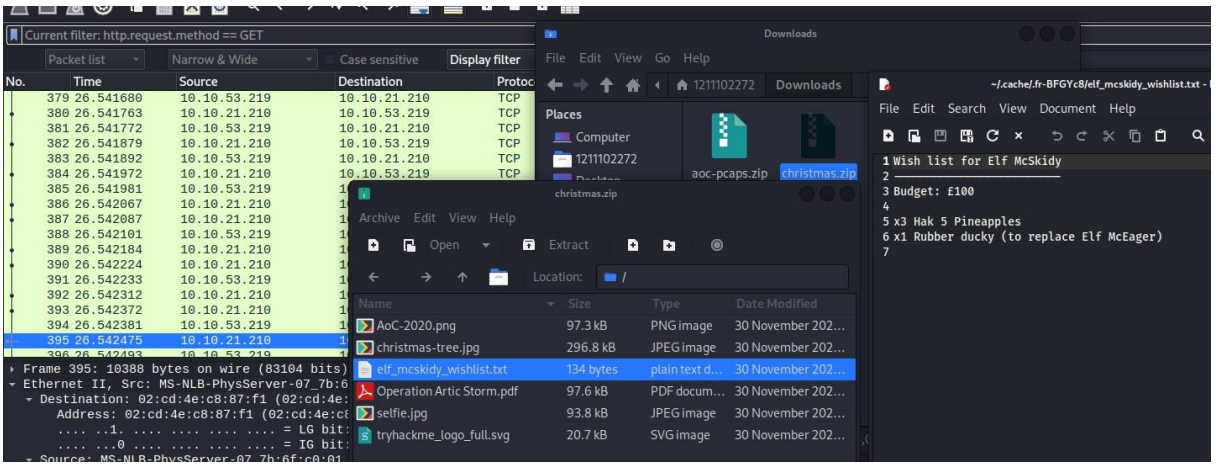
Question 5

The SSH protocol is encrypted.



Question 6

After analysing pcap3.pcap, a zip filled called "`christmas.zip`" was found, it was exported as HTTP, then extracted it to find a .txt file that said a rubber ducky would be used to replace Elf McEager.



Thought process/ Methodology:

We launched wireshark with the -r flag to read the .pcap file provided. After applying the ICMP display filter, the address which initiated it was found to be `10.11.3.2` as seen from the "source" tab. To filter out all the HTTP GET requests, the filter "`HTTP.REQUEST.METHOD == GET`" was used. After analysing, IP Address "`10.10.67.199`" was found to have visited an article called "reindeer-of-the-week". After that, we launched pcap2.pcap with the same steps, and applied "`tcp.port == 21`" to filter out the logs since FTP ran on port 21. We see the correct password for login is "`plaintext_password_fiasco`". The SSH protocol is encrypted.
We started analysing pcap3.pcap, and found a christmas.zip file, which we exported as HTTP, then extracted to find a .txt file saying that a rubber ducky would be used to replace ElfMcEager.

Day 8: Networking - What's under the Christmas Tree?

Tools used: Kali Linux, nmap

Question 1:

Run the nmap scan on the machine IP

```
┌──(1211102272㉿kali)-[~]
└─$ nmap -A 10.10.146.238
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 11:30 +08
Nmap scan report for 10.10.146.238
Host is up (0.22s 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/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.33 seconds
```

Question 2

Scanning using -Pn flag

```
┌──(1211102272㉿kali)-[~]
└─$ nmap -Pn 10.10.146.238
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 11:37 +08
Nmap scan report for 10.10.146.238
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 24.45 seconds
```

Question 3

Comparebetween -A and -sV flags

```
┌──(1211102272㉿kali)-[~]
└─$ nmap -sV 10.10.146.238
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 11:43 +08
Nmap scan report for 10.10.146.238
Host is up (0.22s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
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 42.56 seconds
```

Question 4

Determining the Linux Distro: Ubuntu

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

Question 5

Using NSE to determine the possible use for the website

```
┌──(1211102272㉿kali)-[~]
└─$ nmap --script http-title 10.10.146.238
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 11:48 +08
Nmap scan report for 10.10.146.238
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
80/tcp   open  http
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  EtherNetIP-1
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 26.25 seconds
```

Thought Process/ Methodology:

We ran the nmap scan on the machine IP. We then scanned using the -Pn flag. We compare between -A and -sV flags, one displayed the running process and one didn't. We went ahead to determine the Linux Distro, which is Ubuntu. We searched for a script using NSE to determine the possible use for the website on nmap.org, which found out the website is used for a blog.

Day 9: Networking - Anyone can be Santa!

Tools Used: Kali Linux, FTP

Question 1

The "Public" directory is available for access

```
┌──(1211102272㉿kali)-[~]
└─$ ftp 10.10.148.22
Connected to 10.10.148.22.
220 Welcome to the TBFC FTP Server!.
Name (10.10.148.22:1211102272): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||20872|)
150 Here comes the directory listing.
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
226 Directory send OK.
```

Question 2

Backup.sh is an executable script

```
ftp> cd public
250 Directory successfully changed.
ftp> ls -a
229 Entering Extended Passive Mode (|||7267|)
150 Here comes the directory listing.
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 .
drwxr-xr-x    6 65534    65534        4096 Nov 16  2020 ..
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp>
```

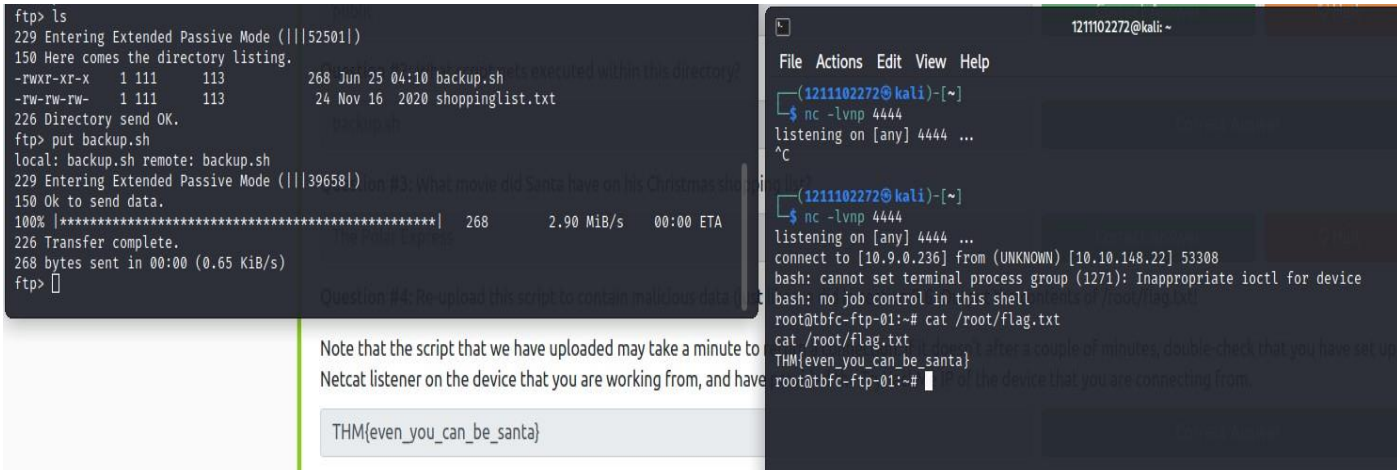
Question 3

The Polar Express Movie is on santa's shopping list

```
File  Actions  Edit  View  Help
┌──(1211102272㉿kali)-[~]
└─$ cat shoppinglist.txt
The Polar Express Movie

┌──(1211102272㉿kali)-[~]
└─$
```

Question 4

Change the contents of the .sh file, set up net cat and reupload the script to gain root access, then concatenate the THM flag



Thought Process/ Methodology:
When we use the ftp to connect to the server, the "Public" directory is available for access, we found out there was a backup.sh which we can use it to exploit for access. Santa had a shopping list saying he wanted to watch The Polar Express Movie. After that, we downloaded the script, changed the contents, mean while we set up netcat for a listener port, after that we uploaded the file back to gain root access, we outputted the contents with cat to find the THM flag.

<u>Day 10: Networking - Don't be</u>

<u>sElfish!</u>Tools Used: Kali Linux,

samba <u>Question 1</u>

Displaying all the users on samba server

```
user:[elfmcelferson] rid:[0×3e9]

 ==========================( Share Enumeration on 10.10.64.58 )=========================
=========

        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))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        TBFC-SMB-01          TBFC-SMB

[+] Attempting to map shares on 10.10.64.58

//10.10.64.58/tbfc-hr   Mapping: DENIED Listing: N/A Writing: N/A
//10.10.64.58/tbfc-it   Mapping: DENIED Listing: N/A Writing: N/A
//10.10.64.58/tbfc-santa        Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.10.64.58/IPC$      Mapping: N/A Listing: N/A Writing: N/A
enum4linux complete on Sat Jun 25 12:40:43 2022
```

Question 2

Shares on the server

```
 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))
ecting with SMB1 for workgroup listing.
```

Question 3

Logging into share

```
┌──(1211102272㉿kali)-[~]
└─$ smbclient //10.10.64.58/tbfc-santa
Password for [WORKGROUP\1211102272]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Nov 12 10:12:07 2020
  ..                                  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

                10252564 blocks of size 1024. 5369404 blocks available
```

Question 4

Directory left for santa

```
jingle-tunes                        D        0  Thu Nov 12 10:10:41 2020
```

Thought Process/ Methodology:

We used enum4linux to display all the users on the samba server. As well as shares on the server. We found out there was a share which didn't require a password for login. There is a directory left for santa called Jingle Tunes.