PSP0201

Week 3 Writeup

Group Name : Ilomilo

Members:

ID NUMBER	STUDENT NAME	Role
1211103196	Adriana Iman binti Noor Azrai	Leader
1211103282	Aida Maisarah binti Hisam	Member
1211103216	Sofea Hazreena binti Hasdi	Member
1211103227	Wan Alia Adlina binti Wan Azman	Member

Day 6 - Web Exploitation Be Careful with what you wish on Christmas Night

Tools Used : Firefox, Zap OWASP

Solution/Walkthrough:

Question 1 : Examine the OWASP Cheat Sheet. Match the input validation level with the correct description.

> **Input validation strategies**
>
> Input validation should be applied on both **syntactical** and **Semantic** level.
>
> **Syntactic** validation should enforce correct syntax of structured fields (e.g. SSN, date, currency symbol).
>
> **Semantic** validation should enforce correctness of their *values* in the specific business context (e.g. start date is before end date, price is within expected range).
>
> It is always recommended to prevent attacks as early as possible in the processing of the user's (attacker's) request. Input validation can be used to detect unauthorized input before it is processed by the application.

*from the OWASP cheat sheet, we got the description of syntactic and semantic

Question 2 : Examine the OWASP Cheat Sheet. What is the regular expression used to validate a US Zip code?

> **Allow List Regular Expression Examples**
>
> Validating a U.S. Zip Code (5 digits plus optional -4)
>
> `^\d{5}(-\d{4})?$`
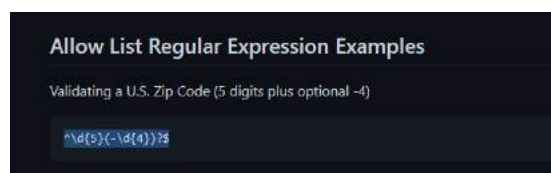
 *from the OWASP cheat sheet, we got the regular expression used to validate a US Zip code.

Question 3 : What vulnerability type was used to exploit the application?

On firefox, we click the application button and choose 'other' dropdown menu, from there we then click the OWASP Zap and turn it on. At OWASP Zap, we then click the 'automated scan' button and then enter the MACHINE-IP:50000 given. Then we click the 'attack' button. After that we received all the alerts and from there, we can see the vulnerability type is persistent (stored).
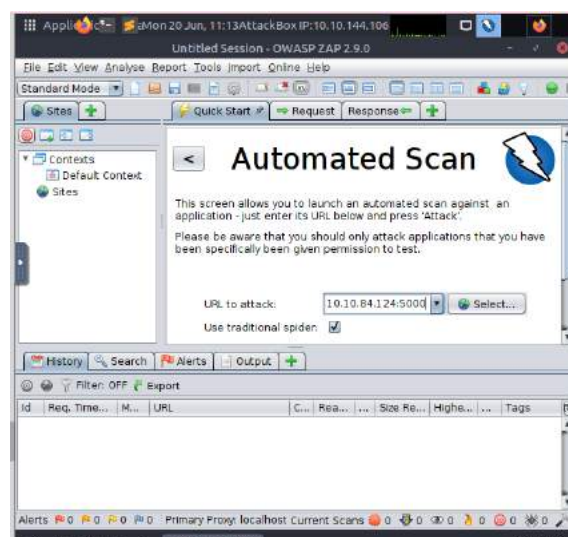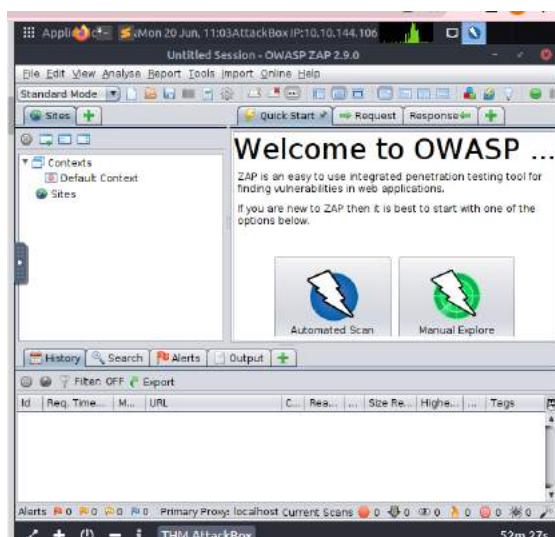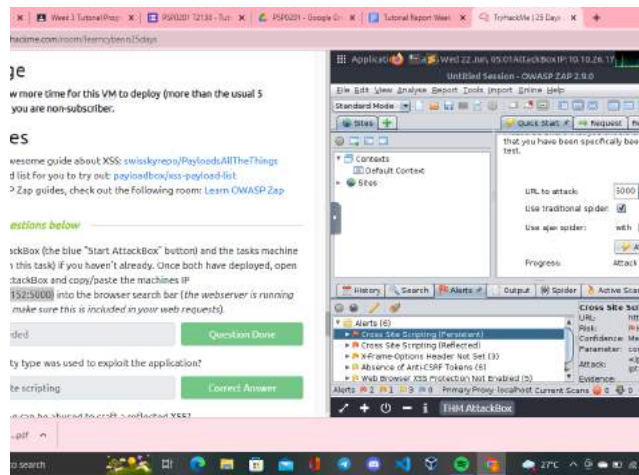
Question 4 : What query string can be abused to craft a reflected XSS?

At Firefox, we type in the MACHINE-IP:5000 given at the search bar. We then were directed to the Santa's Make a Wish page. At the 'query' search bar, we just type in any key and then press enter. From there, the search bar will show the query string which is located after the MACHINE-IP:5000.
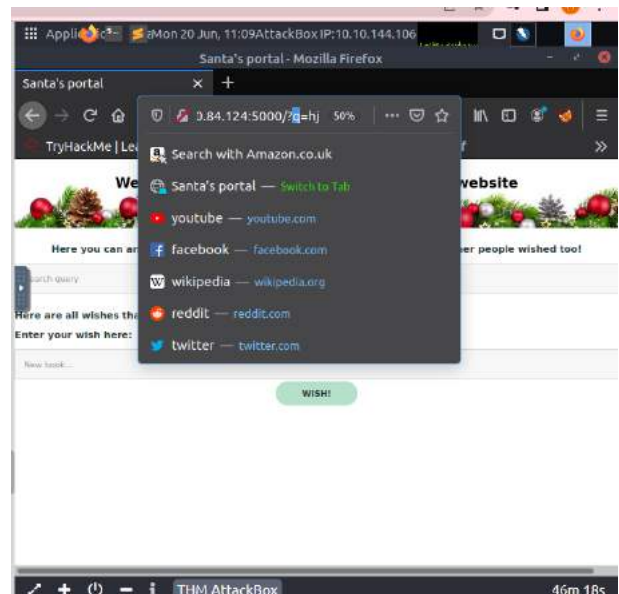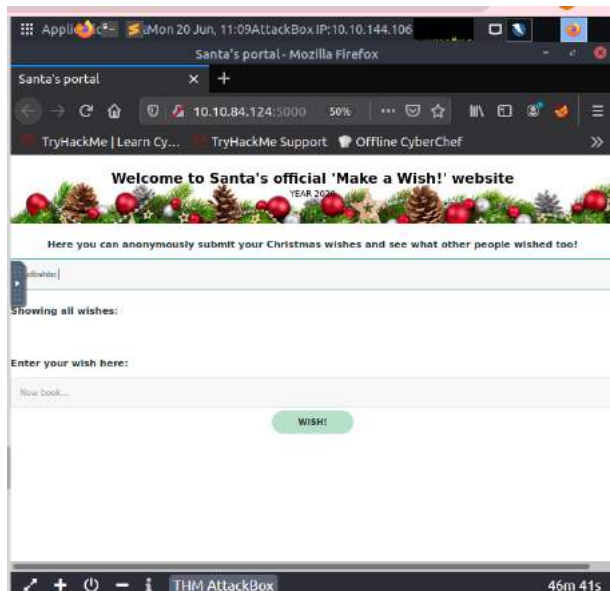
Question 5 : Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts of high priority are in the scan?

At the OWASP Zap, after we attack the MACHINE_IP:5000 given, we receive the alerts, arranged from high to low priority. We can see that there are 2 high priority XSS alerts.
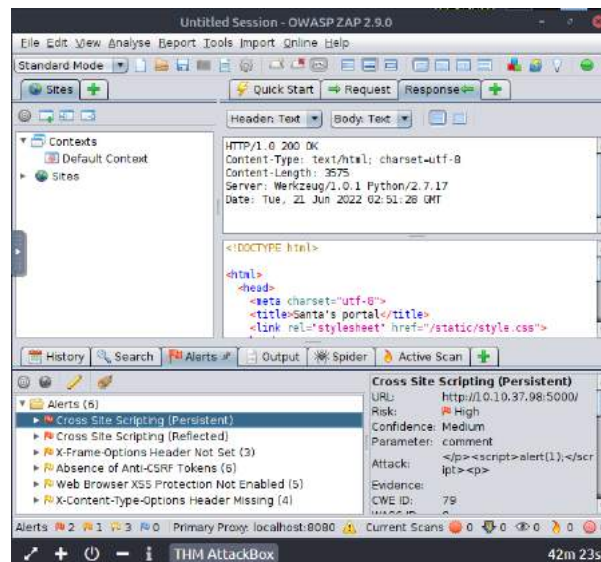
Question 6 : What Javascript code should you put in the wish text box if you want to show an alert saying "PSP0201"?

Back to Santa's portal, at the 'Enter your wish here:' box, we typed in;
'<script>alert("PSP0201")</script>' and then we pressed enter. Later we received the alert saying "PSP0201".
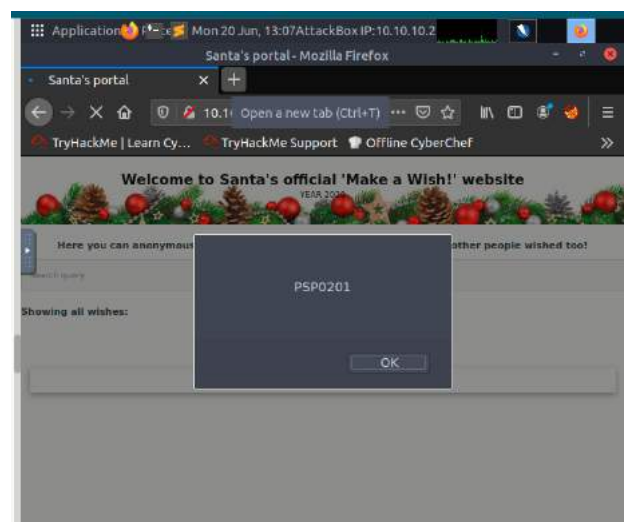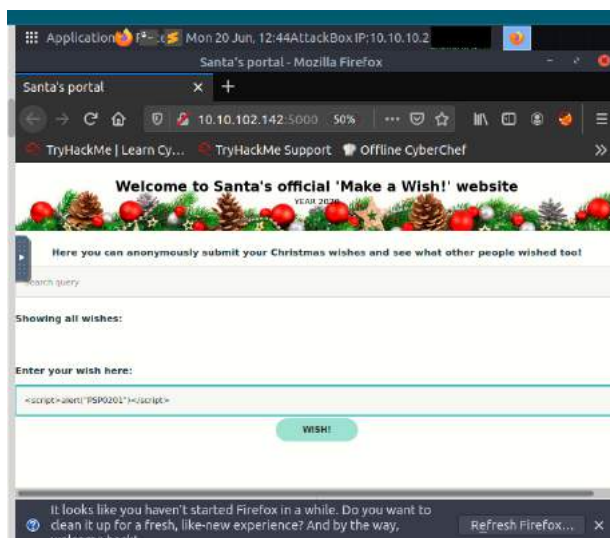
Question 7 : Close your browser and revisit the site MACHINE-IP:5000 again. Does your XSS attack persist?

We then close the OWASP Zap and the Firefox, after that we reopen the Firefox and revisit the MACHINE-IP:5000 again. We then received lots of alerts again and again, one after another. This shows that the XSS attack still persists.
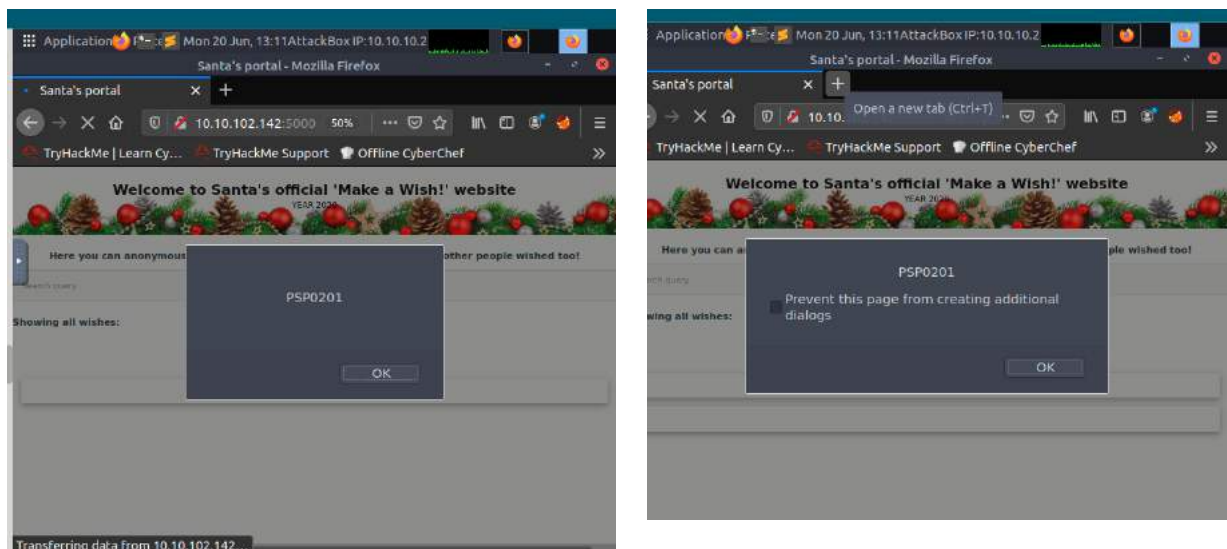

Throughout process:

For the very first two questions, we visit the OWASP/CheatSheetSeries to find the input validation level and the regular expression used to validate a US Zip code. Next, we activate the attackbox and start the Firefox. We then entered the MACHINE-IP:5000 in the search bar and were directed to Santa's portal page. We then typed in anything in the 'query' search bar and got the query string at the search bar, located next after the MACHINE-IP. Next, we clicked the application button, we chose the 'other' dropdown menu and clicked OWASP Zap. we activate the OWASP Zap, and then we click the 'automated scan' button. There, we type in the MACHINE-IP:5000 in the URL section. After that we clicked the 'attack' button. We then received all the alerts, arranged from high to low priority. We can see there are 2 high priority XSS alerts and also the vulnerability type which is reflected. We then go back to Firefox to the Santa's portal page. There, we typed in '<script>alert("PSP0201")</script>' at the 'make a wish' box. Pressed enter, and then we received the alert saying "PSP0201". After we received the alert, we closed the OWASP Zap and the Firefox. We then open the Firefox again and revisit the MACHINE-IP:5000. And then we received lots of alerts again again, one after another which shows that the XSS attack still persists.

Day 7 - Networking The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox, Wireshark

Solution/Walkthrough:

Question 1: Open "pcap1.pcap" in Wireshark. What is the IP address that initiates an ICMP/ping?

Open the downloaded file from tryhackme and open the file using 'Wireshark' and search for the first ICMP/ping.
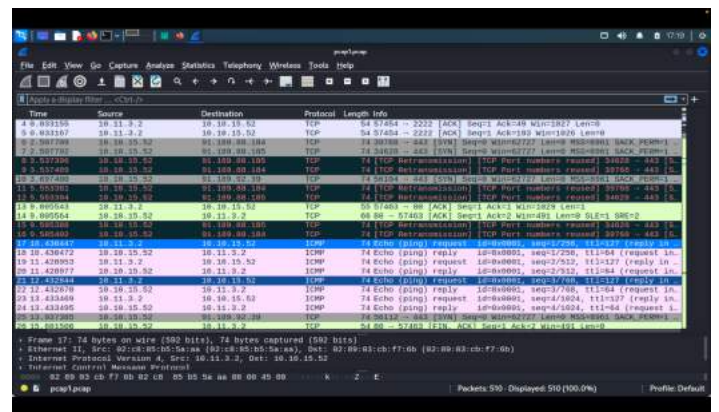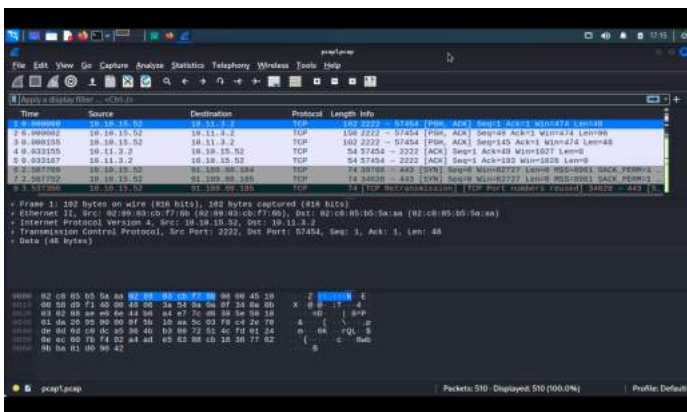
Question 2 : If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

We managed to get the answer from tryhackme website and information under the introducing WIreshark.

Networks are, however, rather noisy...Wireshark captured 2,648 packets after a single minute on my machine. This makes analysing very hard. Thankfully, we can use filters to narrow down the results. We can filter by many things, but we'll only cover a couple of important ones in the table below. Note that all the examples below use the `==` operator to see if the filter exactly matches the value we give it.

Filter	Description	Example
ip.src	Show all packets that originate from the specified IP address	`ip.src == 192.168.1.1`
ip.dst	Show all packets that are destined to the specified IP address	`ip.dst == 192.168.1.1`
tcp/udp.port	Show all packets that are sent via the protocol and port specified	`tcp.port == 22 /` `udp.port == 67`
protocol.request.method	Show all packets that use a specific method of the protocol given. For example, HTTP allows for both a `GET` and `POST` to retrieve and submit data accordingly.	`http.request.method == GET / POST`

In the screenshot below, I used the filter `ip.src` to list all the packets that were explicitly sent from a specific address, using the `==` operator to define what host I wish to search for (`145.254.160.237`). We'll quickly explore the use of these operators in the next section.

Question 3 : Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "10.10.67.199" visited?

Once we entered the filter we received a lot of information, however for the length info only reindeer-of-the-week seems like a title of article.
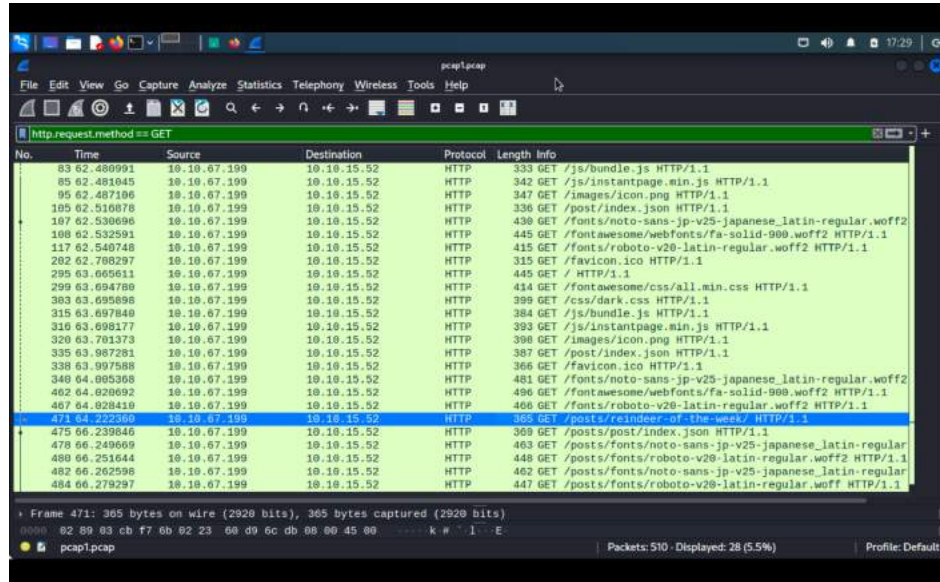
Question 4: Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process?

Entered pcap2.pcap and click on the follow TCP Stream to get the answer
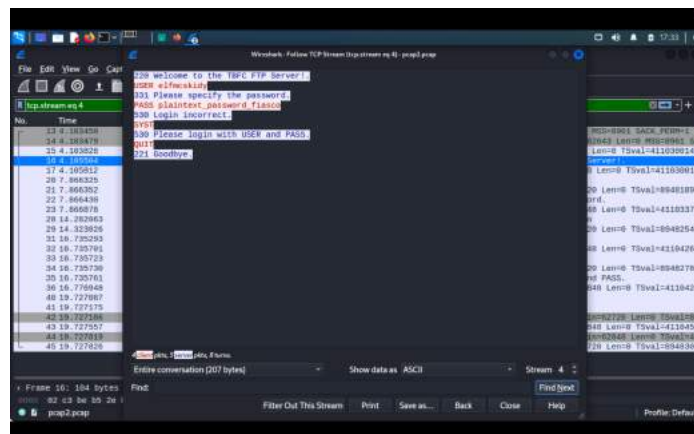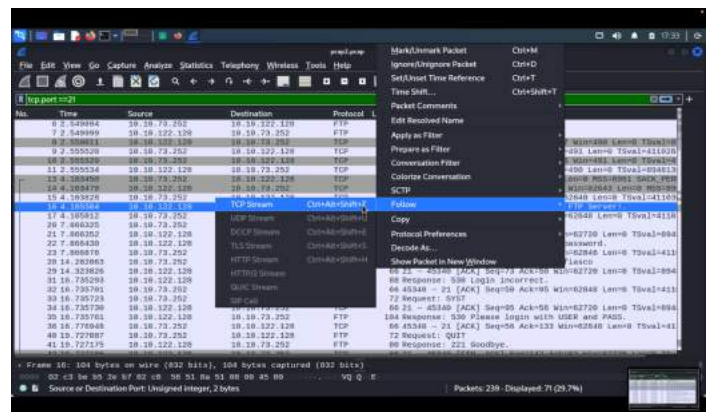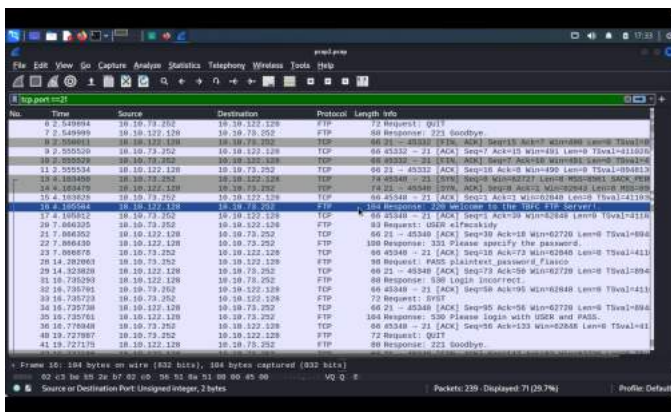
Question 5 : Continuing with our analysis of "pcap2.pcap", what is the name of the protocol that is encrypted?

We managed to get the answer by using the filter tcp.port == 21 and get the SSH protocol that is encrypted.
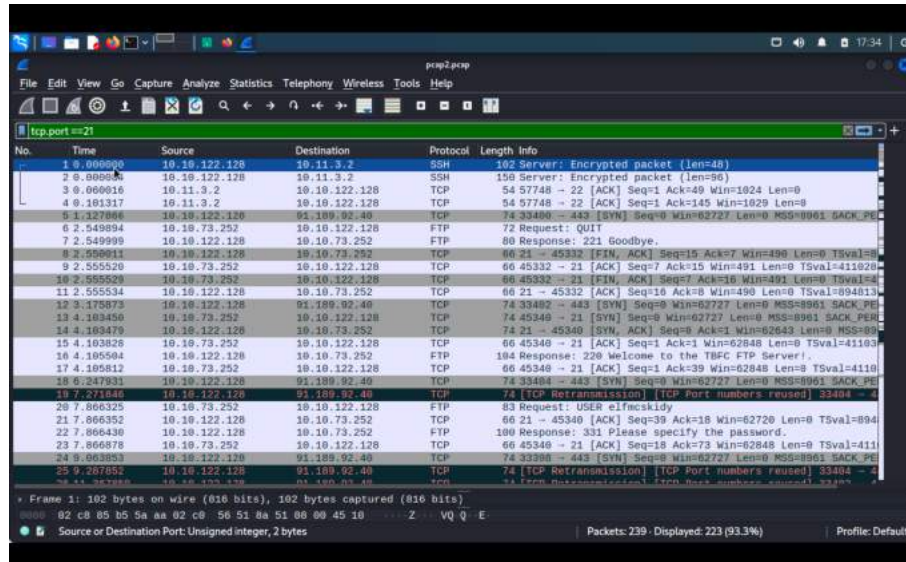
Question 6 : Examine the ARP communications. Who has 10.10.122.128? Tell 10.10.10.1. Answer: 10.10.122.128 is at

Continuing examining the pcap2.ppap, we searched for the ARP and managed to find the answer, 02:c0:56:51:8a:51
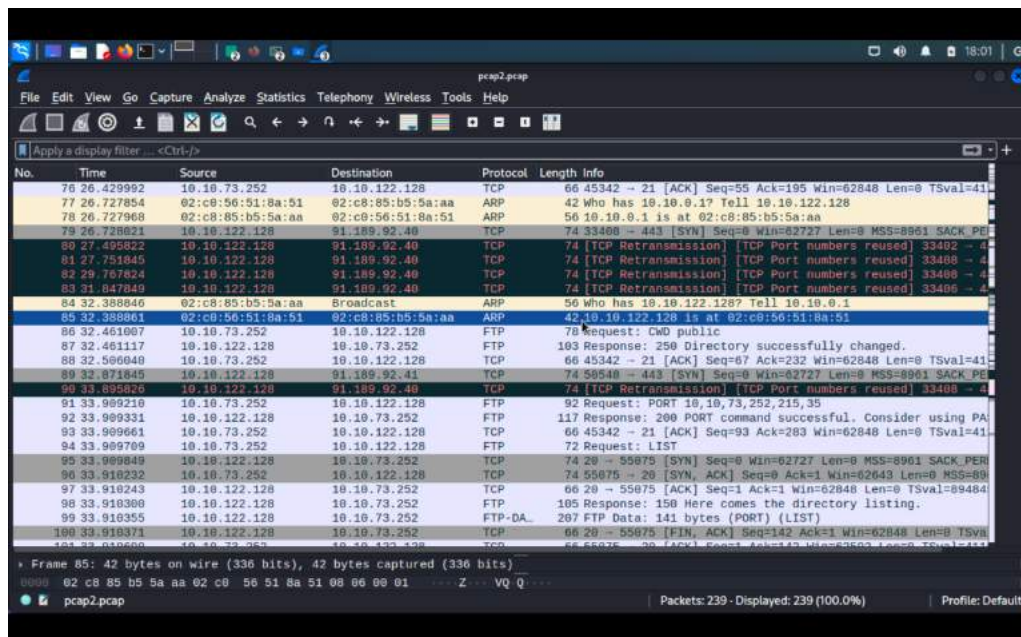
Question 7 : Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

We have to download a christmas.zip file by export object 'HTTP' and open the txt file to get the answer for question 7.
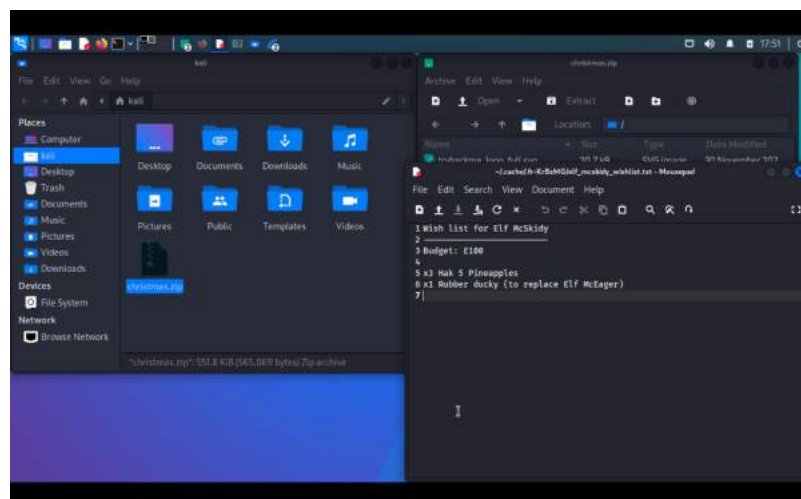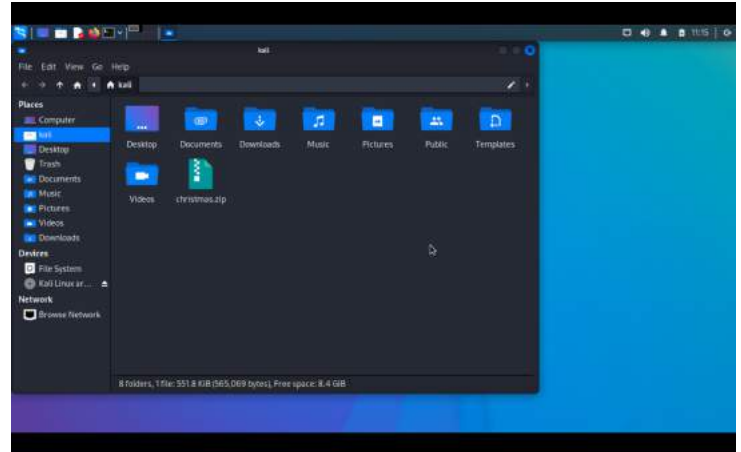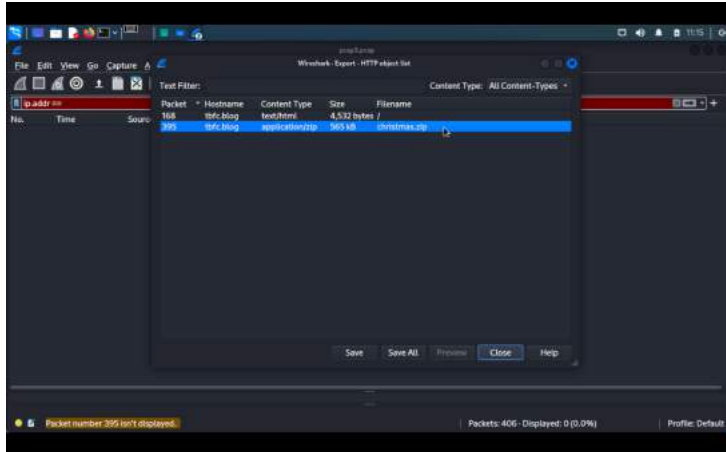
Question 8 : Who is the author of Operation Artic Storm?

From the christmas.zip file we managed to get the author name from the pdf provided.
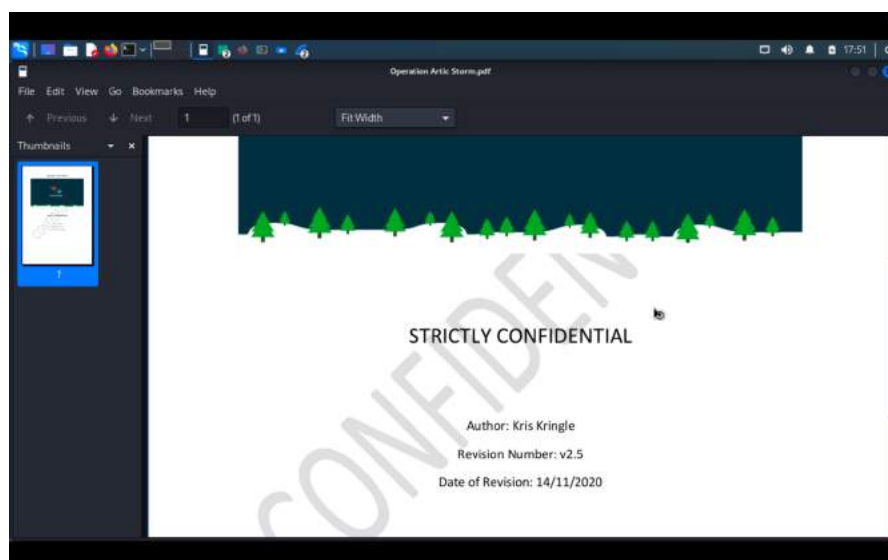
Throughout process:

Opening Kali, we accessed tryhackme and downloaded a required file for the pcap.ppap. We opened all 3 of the files using Wireshark. For pcap1.ppap, we managed to inspect the ip address that initiates an ICMP/ping. Next, using the same file, we used the filter 'http.request.method == GET' to get the name of the article that the IP address "10.10.67.199" visited. Once we entered the filter we received a lot of information, however for the length info only reindeer-of-the-week seems like a title of an article. Closing the pcap1.ppap, we opened the second file, pcap2.ppap using the same platform. Looking at the FTP server that looks like someone entered a website, we managed to get the password used by clicking the 'follow TCP Stream'. In the same file, using the filter 'tcp.port == 21' , we managed to get the protocol that is encrypted and by examining the ARP communications, we managed to receive the answer for where 10.10.122.128 is at. Lastly, by opening the pcap3.ppap, we managed to get a 'christmas.zip' file. To access the answer, we downloaded the file under 'File', 'Export Objects' and 'HTTP'. In the zip file we got 6 different files containing different information where we can get the wish list for Elf McSkidy from the txt file and the author's name under the pdf provided.

Day 8 - Networking What's Under The Christmas Tree?

Tools used: Kali Linux, Terminal

Solution/Walkthrough:

Question 1: When was Snort created?

This can be found on google.com
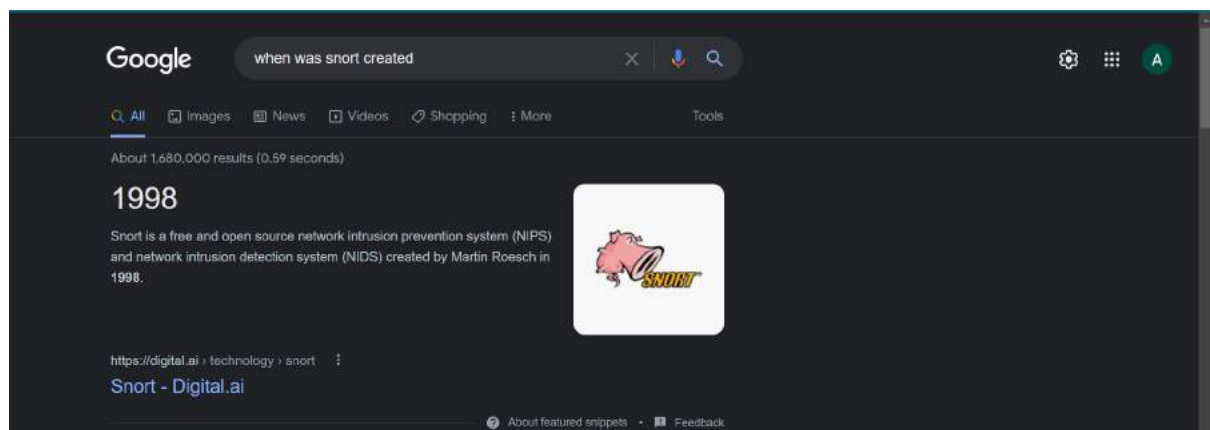
Question 2: Using Nmap on MACHINE_IP , what are the port numbers of the three services running?

Open terminal, type in nmap [ip address] and find the ports which are running in the results.

Question 3: Use Nmap to determine the name of the Linux distribution that is running, what is reported as the most likely distribution to be running?

In the terminal, type in nmap -A [ip address] and the name of Linux distribution will appear in the results

Question 4: What is the version of Apache?

From the same result, the version of Apache is stated

Question 5: What is running on port 2222?

From the same result, port 2222 is stated as well as what is running on this port

Question 6: Use Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. Based on the value returned, what do we think this website might be used for?

From the same result again, the "HTTP-TITLE" is "TBC'S Internal Blog" so from there, we can guess what this website might be used for.

Throughout process:

Firstly, open the terminal and type in nmap [ip address] to find running services and their port numbers. Then, type in nmap -A [ip address] to determine the name of the Linux distribution that is running. The results will contain all information needed such as the name of Linux distribution, version of Apache and "HTTP-TITLE" of the webserver.

Day 9 - Networking Anyone Can Be Santa!

Tools used: Kali Linux, Firefox, Terminal

Solution/Walkthrough:

Question 1: What are the directories you found on the FTP site?
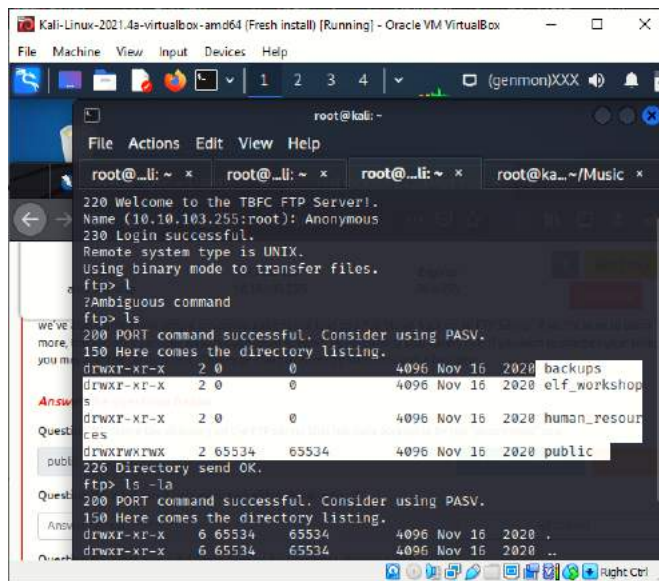
Go to the terminal, run the command ftp and ip address.
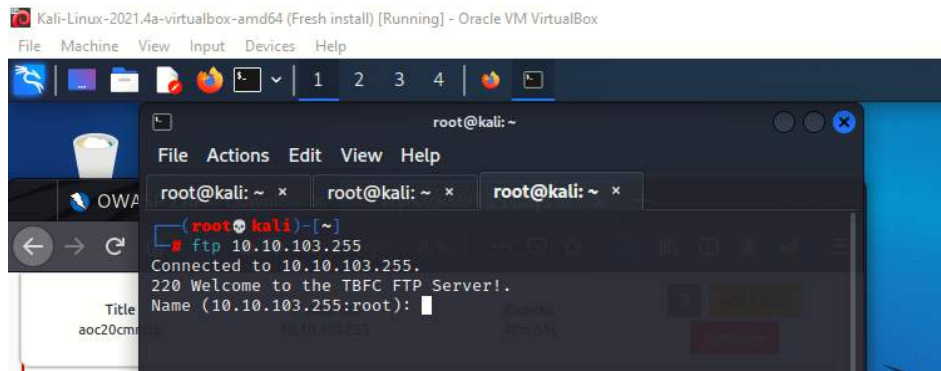
Enter anonymous and it says the FTP server has 'anonymous' mode enabled.
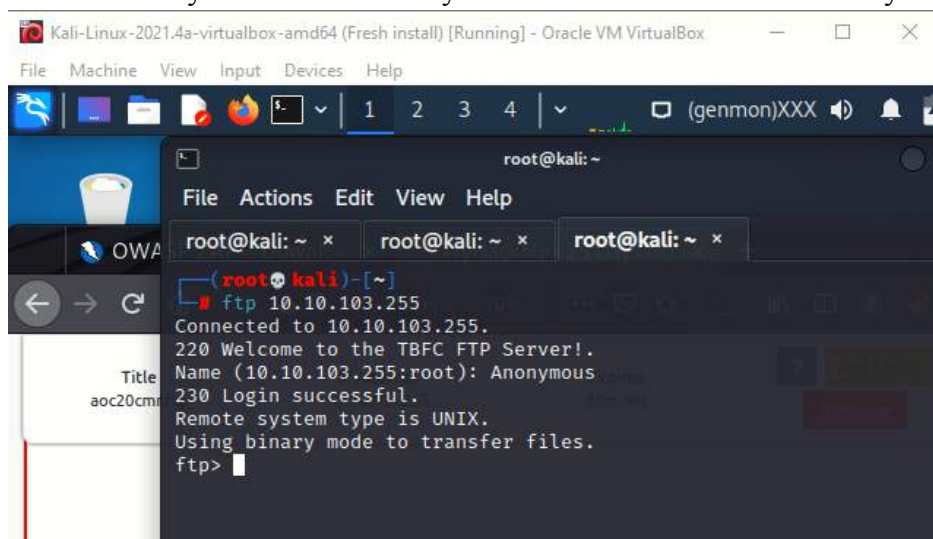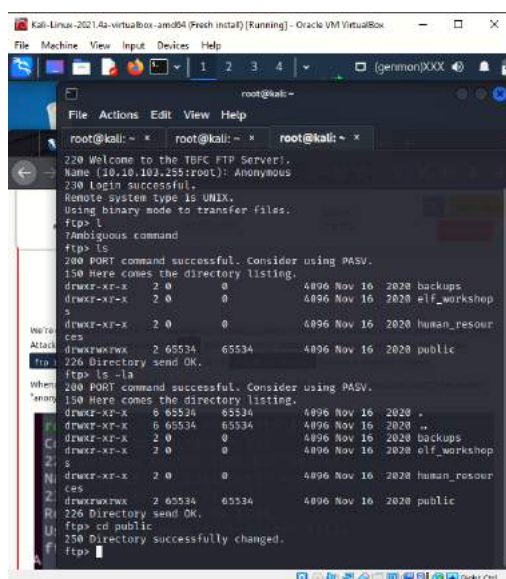
Use the help command to find the commands that we are looking for. We use ls command to list out the directories in the working directory.

Question 2: Name the directory on the FTP server that has data accessible by the "anonymous" user.
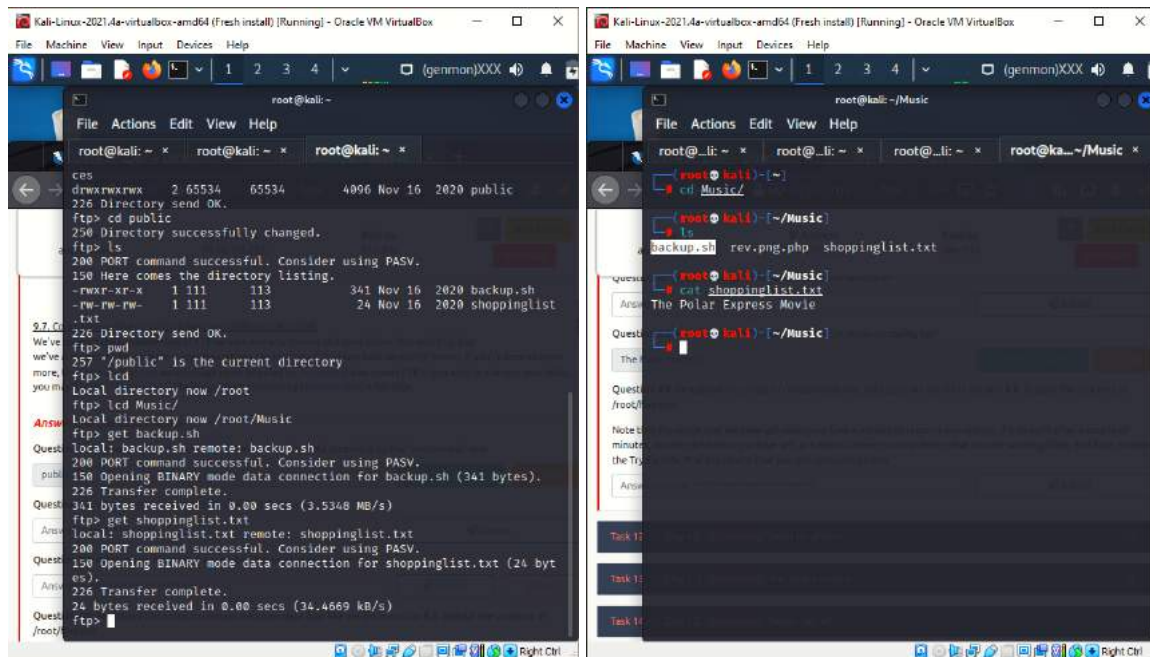
We change our current directory to public by using cd command.

Question 3: What script gets executed within this directory?

Enter ls command in the public directory. We can see backup.sh and shoppinglist.txt. We change the local current directory to music by using lcd command. Use get command to receive the files. Now the files are in the music directory. Enter cat backup.sh. It shows that backup.sh is an automatic transfer of backups.

Question 4: What movie did Santa have on his Christmas shopping list?

We enter the cat command to open the shoppinglist.txt and the title of the movie is displayed.

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!

Open the pentesters cheatsheet link and copy the Netcat OpenBsd. Use sudo ifconfig tun0 to get the IP.
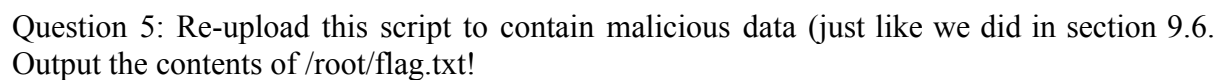
Use nano command in the directory. Paste the Netcat OpenBsd and rename the ip by using the ip that we get from the sudo command then save. We use cat commands to check.

To put the things in the port, we use the put command and it's successful so we can start the Netcat listener. Once we have the connection, we enter cat /root/flag.txt and the flag is displayed.

Throughout process:

Go to the terminal and type ftp and ip address. After it has started, type anonymous to see if the FTP server has 'anonymous' mode enabled. To locate the commands we're looking for, use the help command. To list the directories in the working directory, we use the ls command. Next, Using the cd command, we change our current directory to public. In the public directory, type ls. Backup.sh and shoppinglist.txt are visible. Using the lcd command, we change the local current directory to music. To obtain the files, use the get command. The files are now located in the music directory. Backup.sh should be entered. It demonstrates that backup.sh is a backup transfer script. We use the cat command to access the shoppinglist.txt file, and the title of the movie appears. Then, go to the pentesters cheatsheet link and copy the Netcat OpenBsd. To obtain an IP address, run sudo ifconfig tun0. In the directory, use the nano command. Paste the Netcat OpenBsd and rename the IP using the IP obtained from the sudo command before saving. To double check, we use cat commands. We use the put command to place the items in the port, and it is successful, so we can start the Netcat listener. Once we've established a connection, we type cat /root/flag.txt, and the flag appears.

Day 10 - Networking Don't be sElfish!

Tools used: Terminal

Solution/Walkthrough:

Question 1: Examine the help options for enum4linux. Match the following flags with the descriptions.

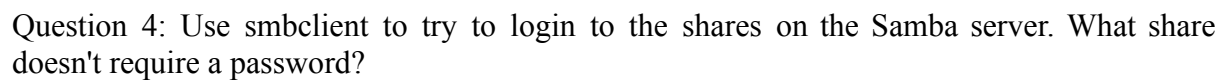We enter -h commands and the descriptions for each flag is displayed.

Question 2: Using enum4linux, how many users are there on the Samba server?

We use nmap commands for the enum4linux to get started. Next, enter -U commands and

the users in the directory are displayed.

Question 3: Now how many "shares" are there on the Samba server?

We refer to the flags descriptions and use -S to see the share list on the Samba server.

Question 4: Use smbclient to try to login to the shares on the Samba server. What share doesn't require a password?

We enter smbclient commands and the Ip Address and the name of the share which is tbfc-santa because it's stated that the mapping is OK instead of DENIED. Press enter and it's working without any password.
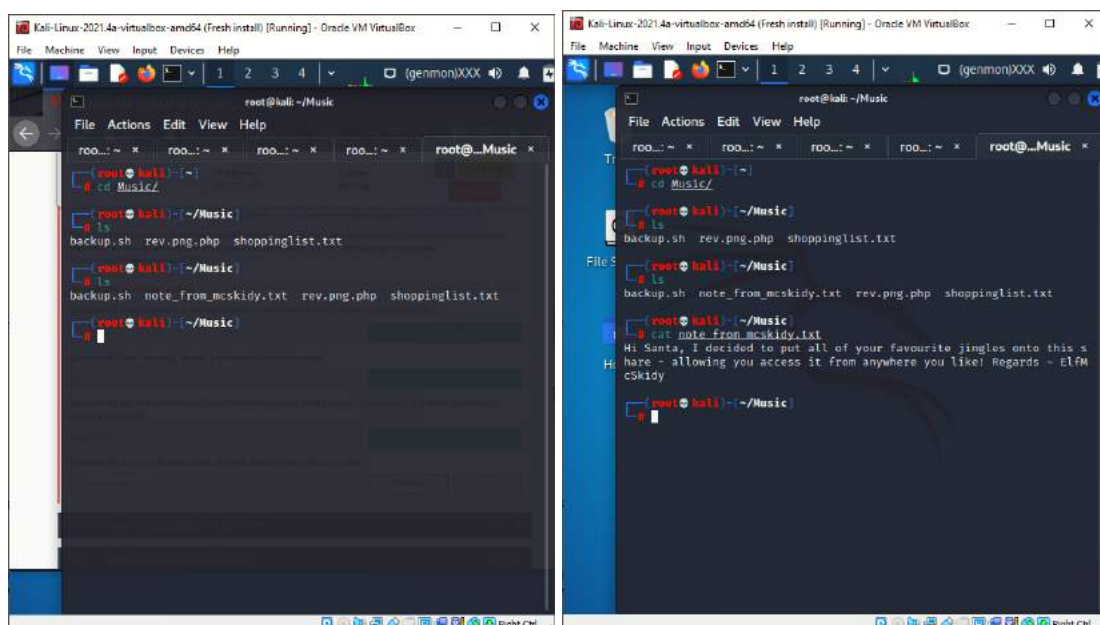
Question 5: Log in to this share, what directory did ElfMcSkidy leave for Santa?

We enter ls command to see what file is running in the directory. Next, we change the current local directory to music and receive the file by using the get command.

In the tab of the terminal, we open the music file and see the file that appears in the music file. We enter cat note_frommcskidy.txt to see what's inside the file and it's stated that ElfMcSkidy leaves jingle-tunes for santa.

Throughout process:

After having access to the target machine, we enter -h commands and the descriptions for each flag is displayed. Then, before the enum4linux gets started we use nmap commands. Then, we enter -U commands and the users in the directory are displayed. We refer to the flags descriptions and use -S to see the share list on the Samba server. Next, We enter smbclient commands and the Ip Address and the name of the share which is tbfc-santa because it's stated that the mapping is OK instead of DENIED. Press enter and it is do not need any password. Next, we enter ls command to see what file is running in the directory. Then, we change the current local directory to music and receive the file by using the get command. In the next tab of the terminal, we open the music file and see the file that appears in the music file. We enter cat note_frommcskidy.txt to see what's inside the file and it's stated that ElfMcSkidy leaves jingle-tunes for santa.