PSP0201

Week 3

Write-up

Group Name: **SuiBian**

Members:

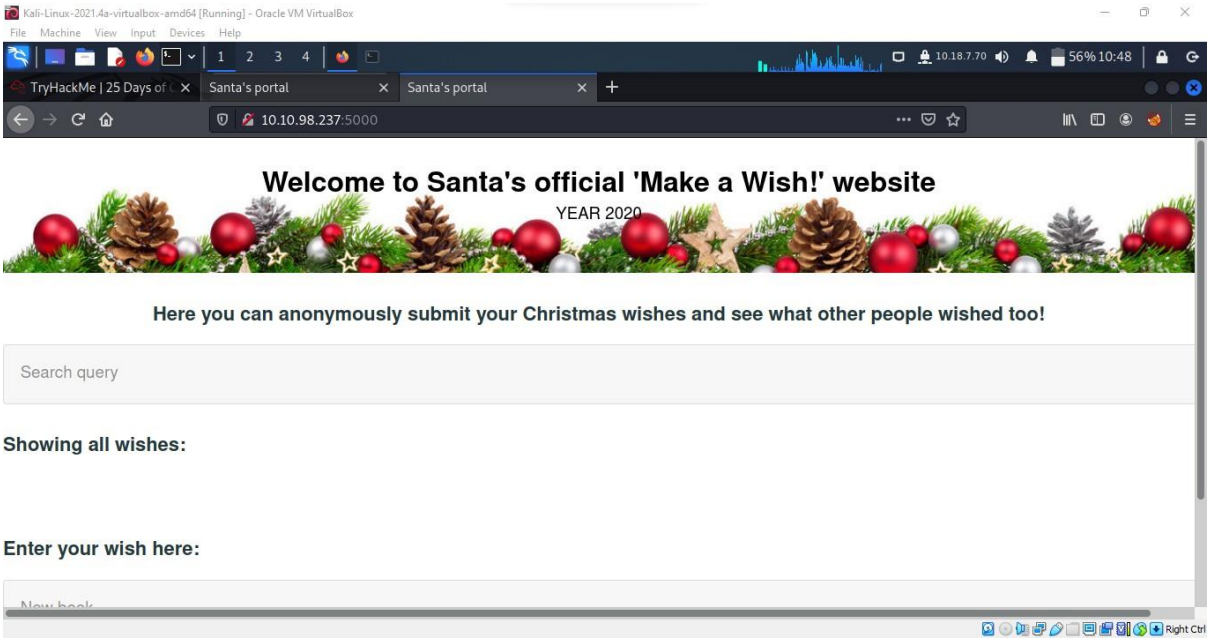
ID	**Name**	**Role**
1211101851	Ang Zhe Jie	Leader
1211103039	Ooi Yi Siang	Member
1211103790	Kok Yew Yan	Member
121110	Wong Chun Rong	Member

Day 6: [Exploitation] Be careful with what you wish on a Christmas Night

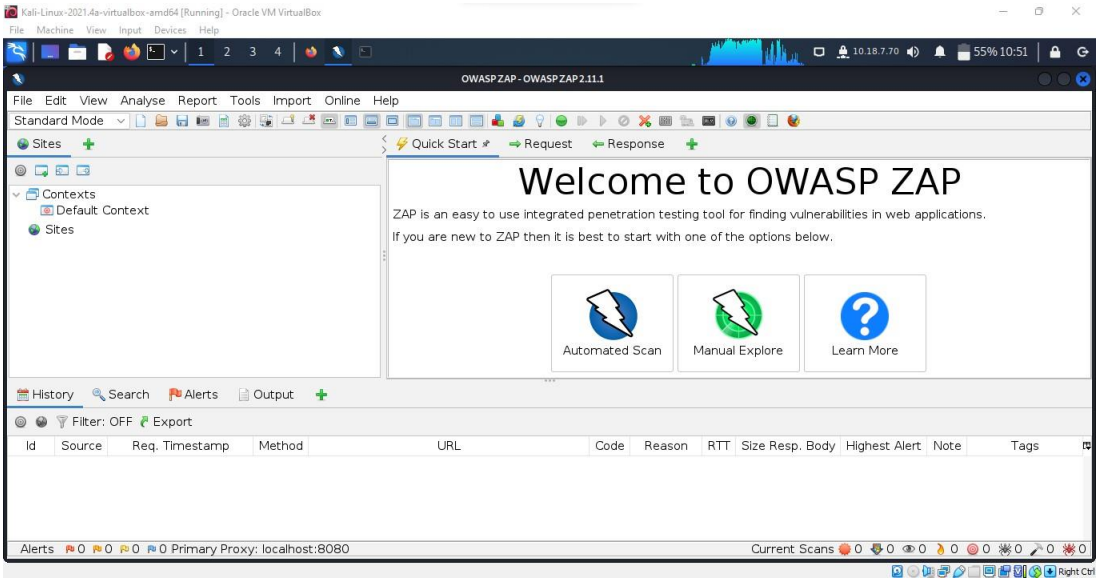
Tools used: Kali Linux, Firefox, OWASP ZAP

Walkthrough:

Question 1:
We paste the ip address and the page below is shown.

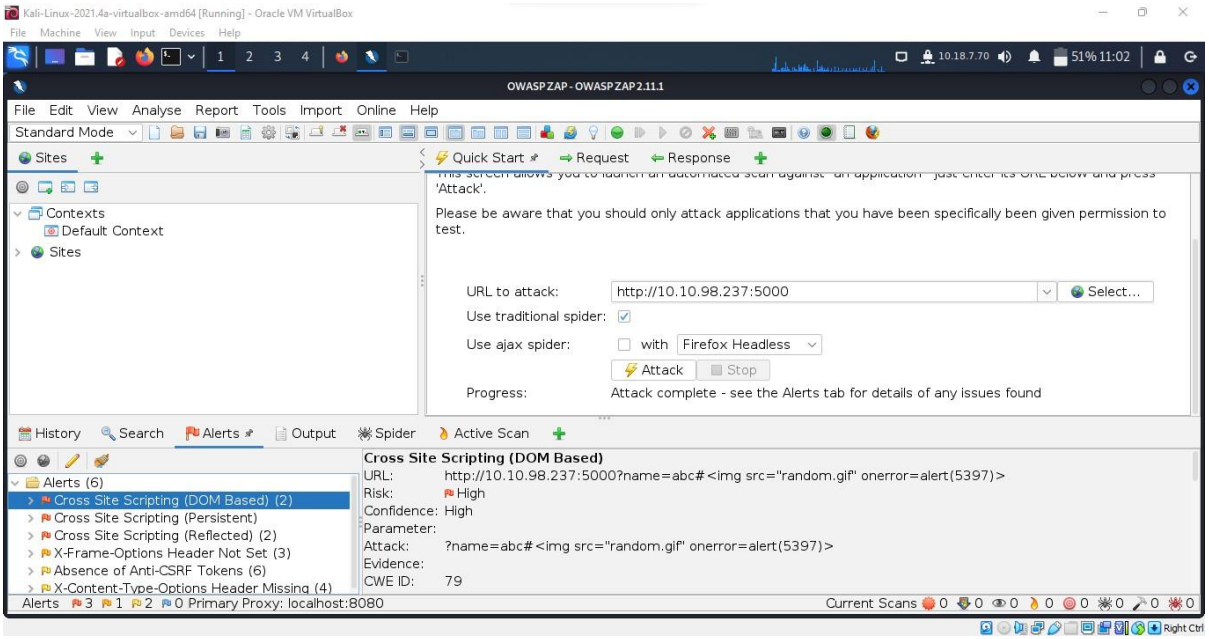


Question 2:
We open OWASP ZAP in Kali Linux machine to detect vulnerabilities, we use automated scan.



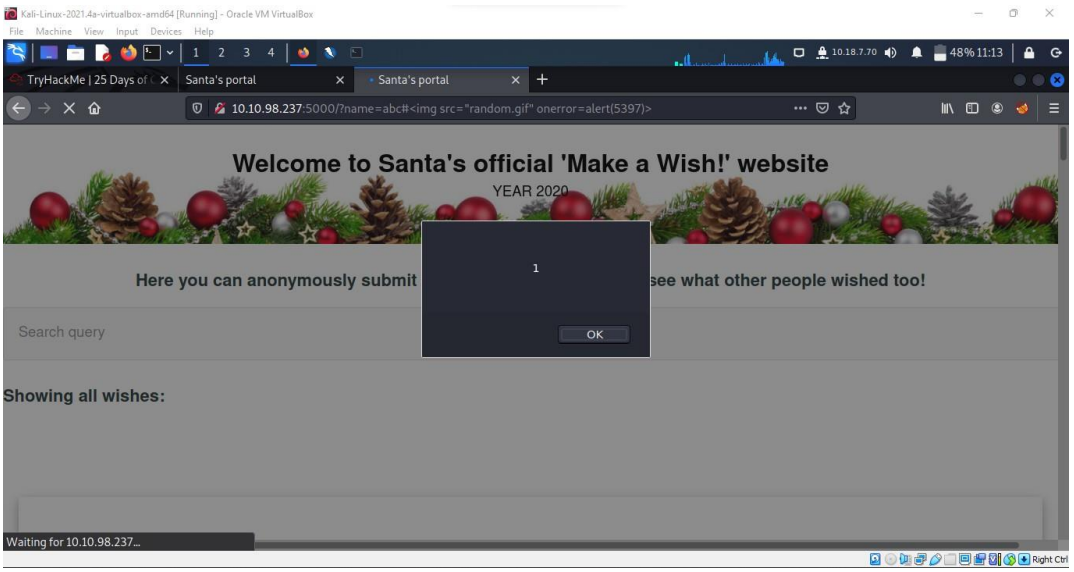
Question 3:

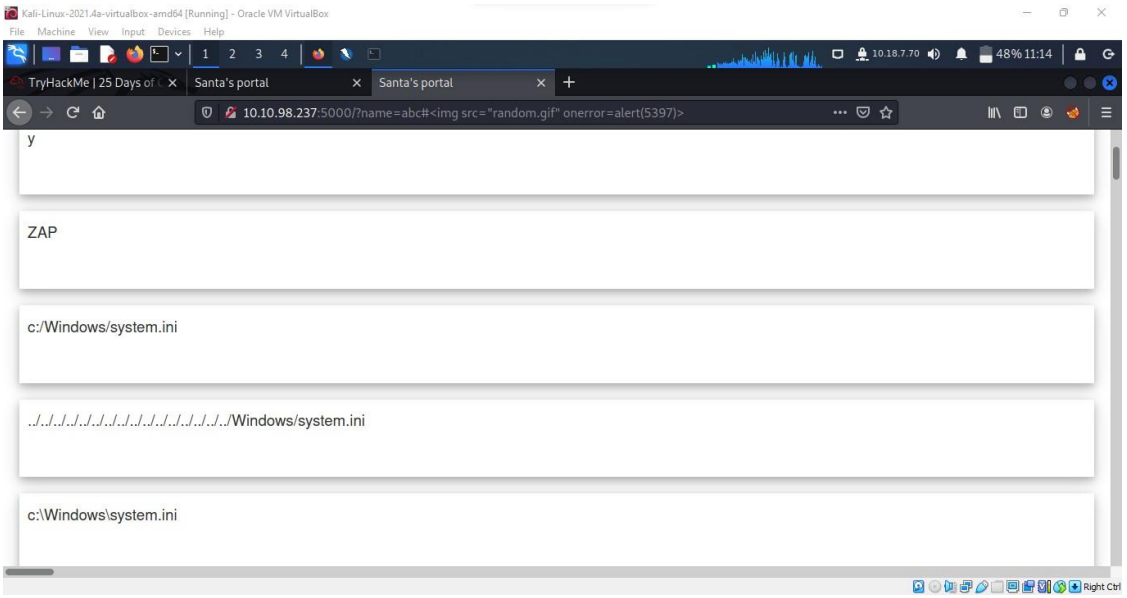
We start the attack after pasting the given URL of our webpage. After scanning, we notice a XSS (DOM Based) vulnerability with a malicious URL and copy the URL.



Question 4:

Then we paste the URL in the Firefox browser. Multiple pop-ups will appear. The list of the wishes will be shown some abnormal entries. It means we have successfully done the attack.





Thought Process/Methodology:

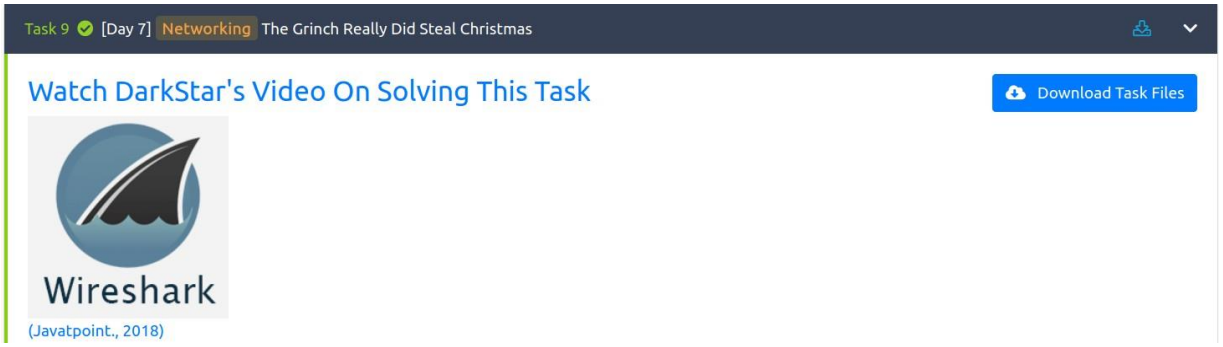
We go through the given IP address in the browser. We scan for vulnerabilities of the website using OWASP ZAP. We use automated scan. Later, we pasted the website's IP address in the column given and clicked on the attack button. Thus, a XSS (DOM Based) vulnerability can be seen after some times. A URL was there, and we copied the URL as we planned to perform a stored XSS attack. We pasted the URL in the browser to attack the website. During the running of URL, several pop-ups will appear. The list of the wishes will show some abnormal entries.

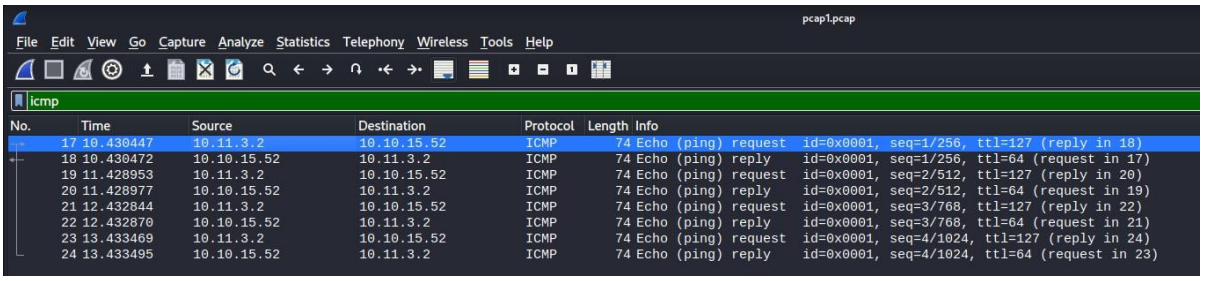
Day 7 - [Networking] The Grinch Really Did Steal Christmas

Tools used: Kali linux, Wireshark, Terminal, Mousepad

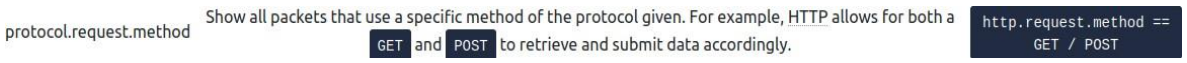
Walkthrough and Question:

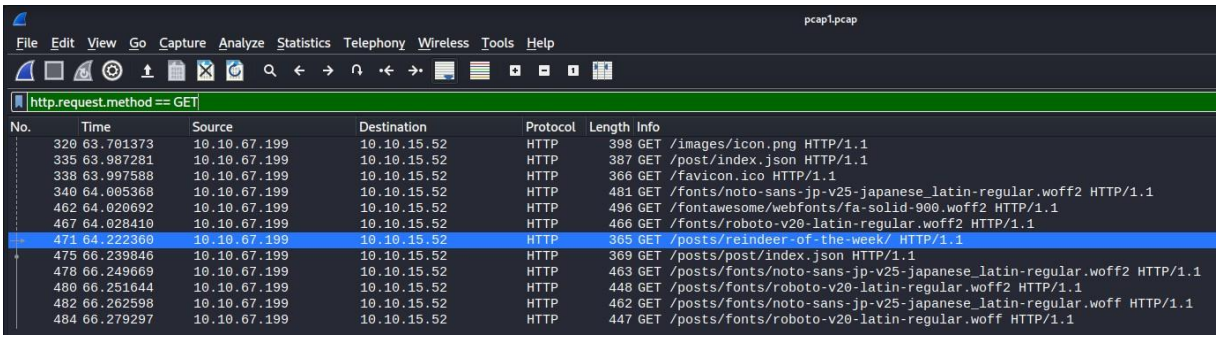
Question 1:
Download the pcap files



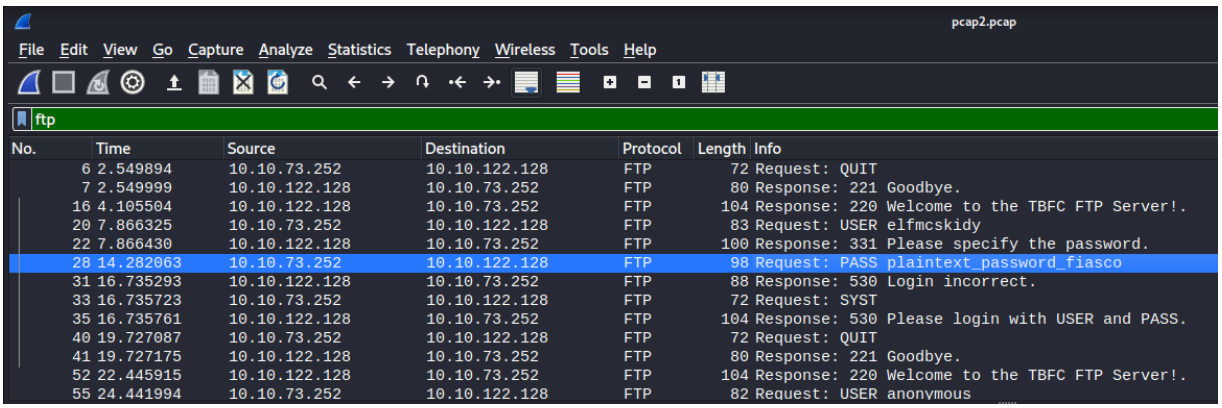


Question 2:
We are able to find the source of the request after opening it.

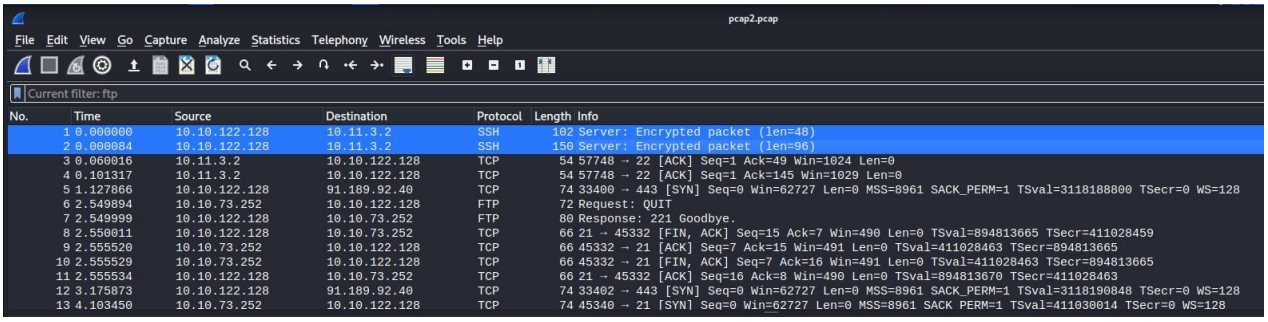




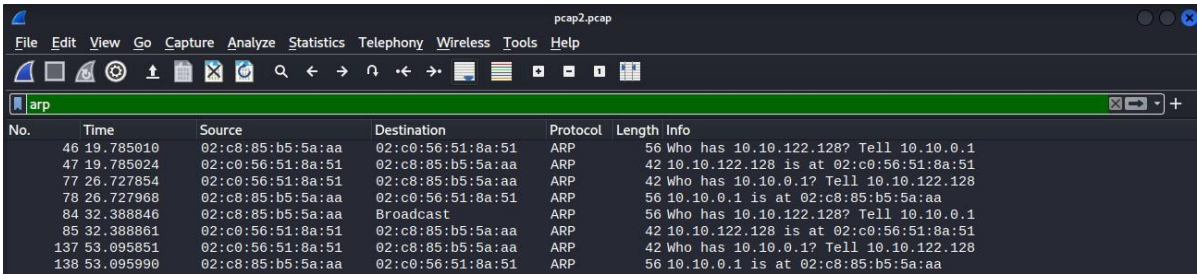
Question 3:
We find the source of ip address entering the password.



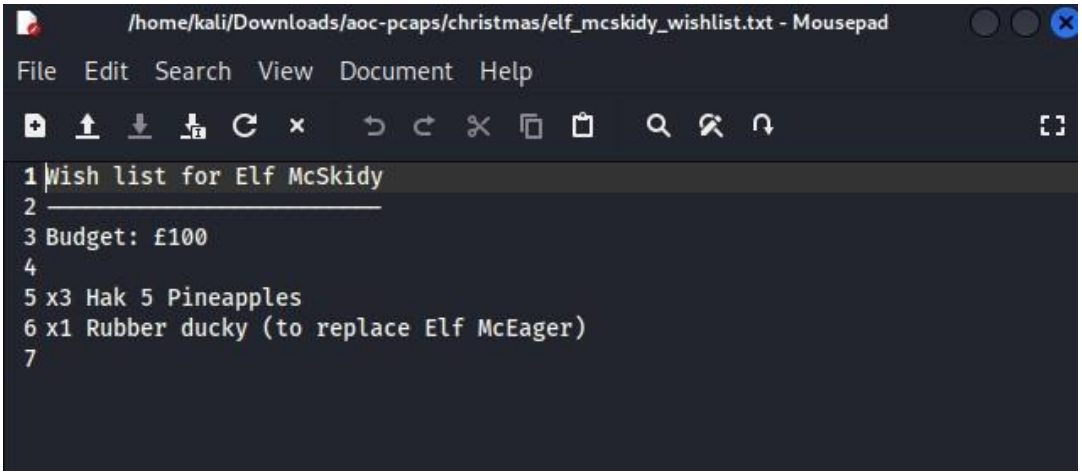
Question 4:
We find the protocol that has encrypted packets.



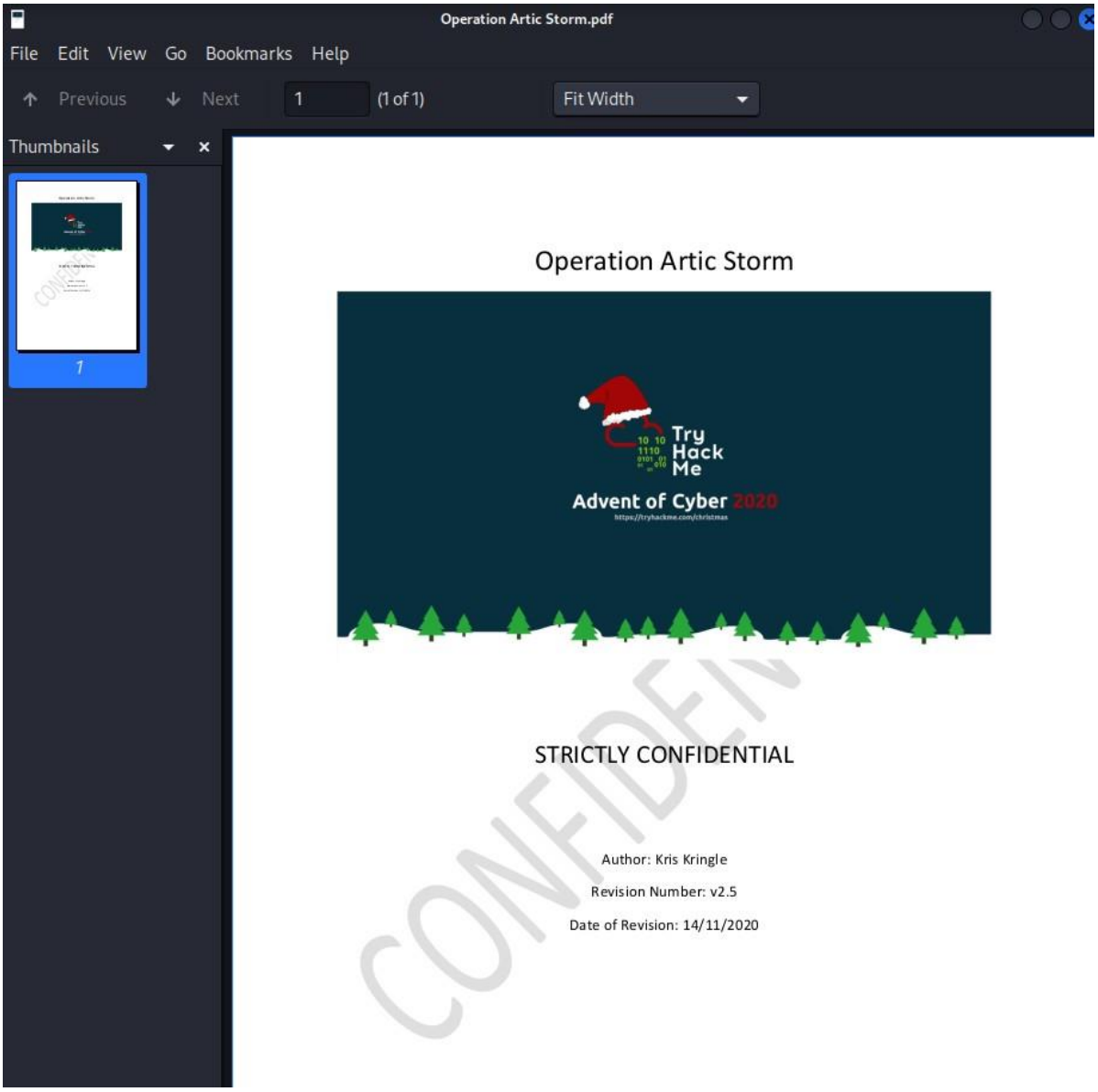
Question 5:
Examine the ARP communications.



Question 6:
Open “pcap3.pcap” file.



Question 7:
Find the text file from the zip downloaded and unzip the pdf file in the zip and look for the author.



Thought Process/Methodology:

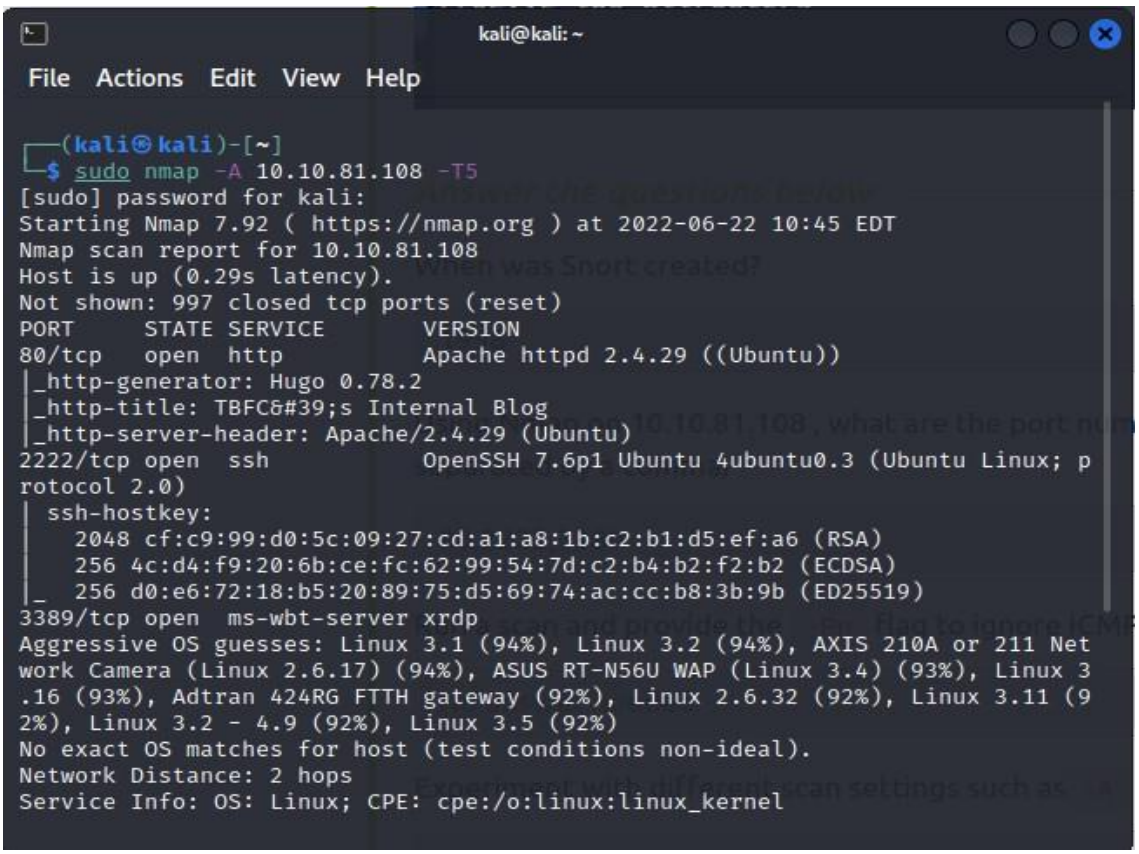
We open Wireshark. Firstly, open pcap1.pcap and filter ICMP to look for the IP address that initiates an ICMP/ping.Filter with http.request.method == GETto find the article visited by the given IP address. We also open pcap2.pcap and apply ftp filter to find the password used to login. We also looking for the protocol that has encrypted packets. We open pcap3.pcap and download the christmas.zip file to look for what is used to replace Elf Mc Eager and who is the author of Operation Artic Storm after we examine the ARP.

Day 8 - [Networking] What's Under the Christmas Tree?

Tools used: Kali Linux, Firefox, Nmap, Terminal

Walkthrough:

Question 1:
Open the terminal and type Nmap with IP address command. Then the information as below will be seen.



Question 2:
Type Nmap script command.

```
┌──(kali㉿kali)-[~]
└─$ nmap --script http-title 10.10.81.108 -T5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 11:02 EDT
Warning: 10.10.81.108 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.81.108
Host is up (0.29s latency).
Not shown: 687 closed tcp ports (conn-refused), 311 filtered tcp ports (no-re
sponse)
PORT     STATE SERVICE
80/tcp   open  http
|_http-title: TBFC&#39;s Internal Blog
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 38.13 seconds
```

Thought Process/Methodology:
Firstly, we typed the Nmap and open all command together with our IP address in terminal. We able to see some information and figure out the port numbers, name of the Linux distribution which is running and the certain version of Apache. We use Nmap script command to check what is the website for after that.

Day 9 - [Networking] Anyone can be Santa!

Tools used: Kali Linux, FTP, Terminal

Question 1:
Enter the File Transfer Protocol (FTP) server of the given IP Address as anonymous and list the directories.

```
ftp> ls
229 Entering Extended Passive Mode (|||50284|)
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>
```

Question 2:
Only the directory - ‘public’ has data in it.

Question 3:
backup.sh is found in the directory.

```
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||46783|)
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
```

Question 4:
Find the shoppinglist.txt in the public directory and The Polar Express is in it. Find theflag.

```
  GNU nano 6.2                    shoppinglist.txt *
The Polar Express Movie
```

```
root@tbfc-ftp-01:/root# cat flag.txt
cat flag.txt
THM{even you can be santa}
```

Thought Process/Methodology:
Fill in the File Transfer Protocol (FTP) server of the given IP address with the terminal and login as an anonymous, we list out all the directories, check for the directory that has data accessible by the “anonymous” user. We can see the scripting language commands file that will be run to back up the server then download the file and replace the command in the script to our own reverse shell script. We upload themodified scripting language commands file after setting up a listener to catch the connection. We now take overthe server with the help of reverse shell and now able to find the flag in the server’s directory.

Day 10 -[Networking] Don't be sElfish!

Tools used: Kali Linux, enum4linux, smbclient, Terminal

Walkthrough and Question:

Question 1:
Examine the help options for enum4linux.

```
Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
    -U        get userlist
    -M        get machine list*
    -S        get sharelist
    -P        get password policy information
    -G        get group and member list
    -d        be detailed, applies to -U and -S
    -u user   specify username to use (default "")
    -p pass   specify password to use (default "")

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,kr
btgt,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)
    -n        Do an nmblookup (similar to nbtstat)
    -v        Verbose.  Shows full commands being run (net, rpcclient, etc.)
    -A        Aggressive. Do write checks on shares etc
```

Question 2:
Use command ./enum4linux.pl -U MACHINE_IP to check for the number of users on the server.

```
 ========================================( Users on 10.10.58.231 )==========================
 ==================

index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: elfmcskidy       Name:   Desc:
index: 0×2 RID: 0×3ea acb: 0×00000010 Account: elfmceager       Name: elfmceager  D
esc:
index: 0×3 RID: 0×3e9 acb: 0×00000010 Account: elfmcelferson    Name:   Desc:

user:[elfmcskidy] rid:[0×3e8]
user:[elfmceager] rid:[0×3ea]
user:[elfmcelferson] rid:[0×3e9]
enum4linux complete on Mon Jun 20 20:32:35 2022
```

Question 3:
Use command ./enum4linux.pl -S MACHINE_IP to check for the number of shares on the server.

```
 ========================================( Share Enumeration on 10.10.58.231 )=============
 ==================

        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:
Login each share found on the server and looking for the share can be login successfully without the password.

Question 5:
Two directories in the tbfc-santa share were found.

```
┌──(1211102575㉿kali)-[/usr/share/enum4linux]
└─$ smbclient //10.10.58.231/tbfc-santa
Password for [WORKGROUP\1211102575]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Nov 11 21:12:07 2020
  ..                                  D        0  Wed Nov 11 20:32:21 2020
  jingle-tunes                        D        0  Wed Nov 11 21:10:41 2020
  note_from_mcskidy.txt               N      143  Wed Nov 11 21:12:07 2020
```

Thought Process/Methodology:
After navigating to enum4linux, we use enum4linux to check for the users and shares on the server. We find the share that we can access without a password. Therefore, we list out the directory in the share, download and read through the note_from_mcskidy.txt. Then, we are able to find the directory Elf McSkidy leaves for Santa.