PSP0201 Week 3 Writeup

Group Name: Siuuu

Members

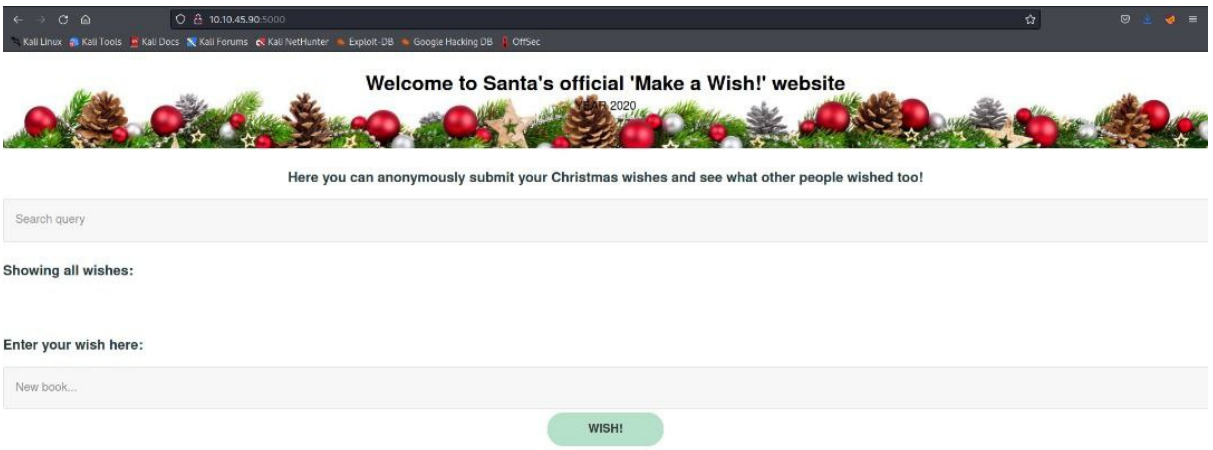
ID	Name	Role
1211103423	Rino Frawidya bin Suheri	Leader
1211104232	Muhammad Amirul Haiqal Bin Zameri	Member
1211101924	Nur Ayu Farisha Binti Hamdan @ Hood	Member

Day6: Web Exploitation – Be careful what you wish on Christmas night

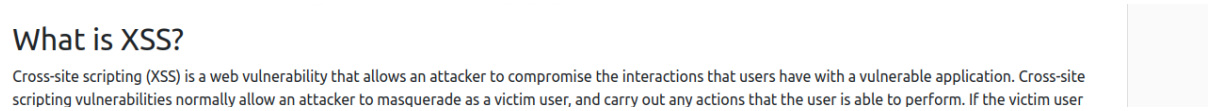
Tools used: Kali Linux, Firefox, OWASP ZAP

Solution/Walkthrough:

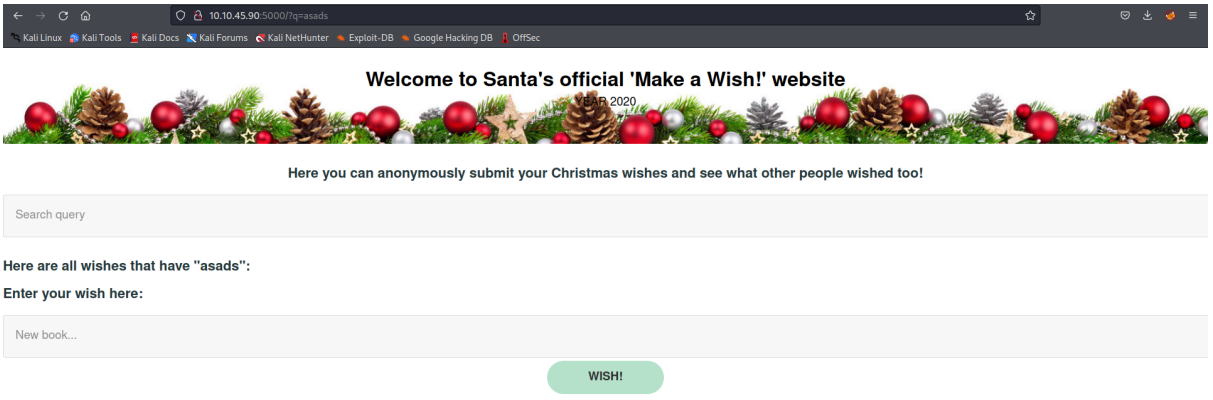
Question 1



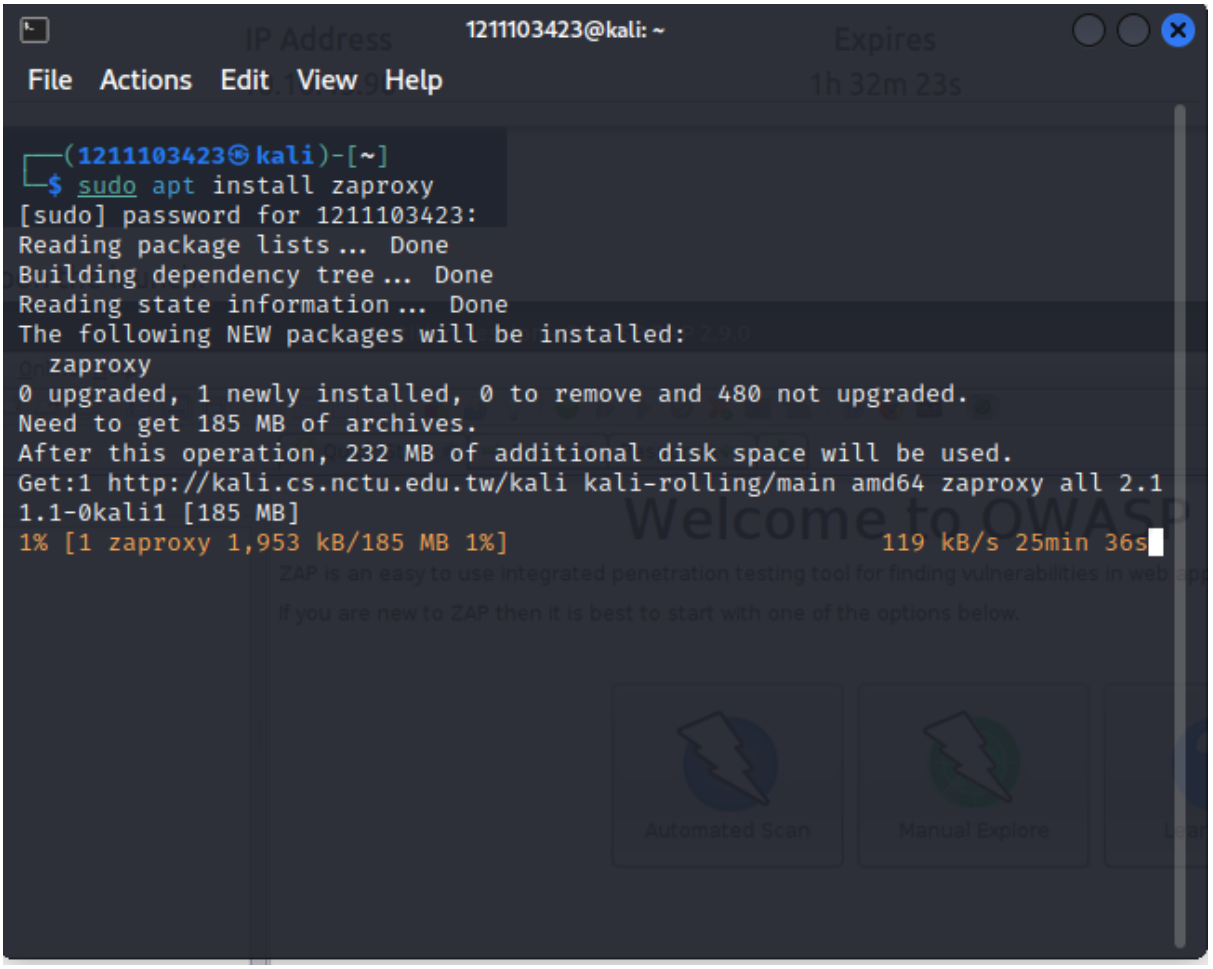
Question 2

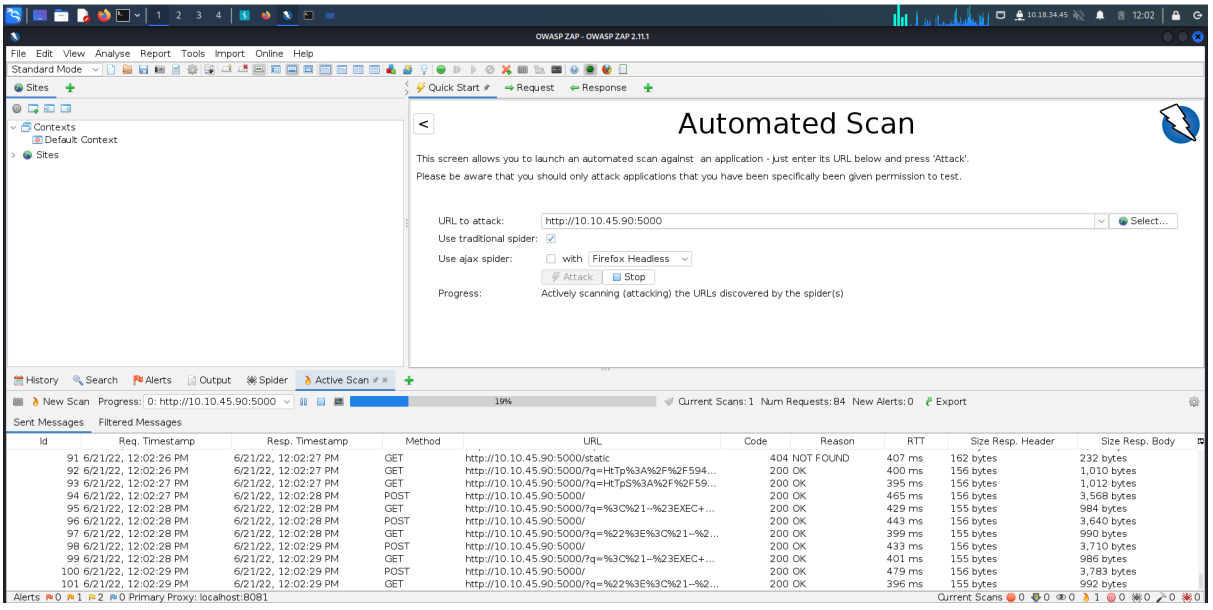


Question 3

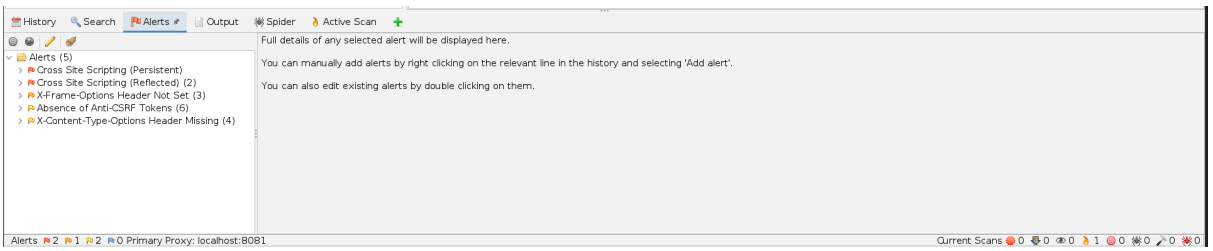


Question 4

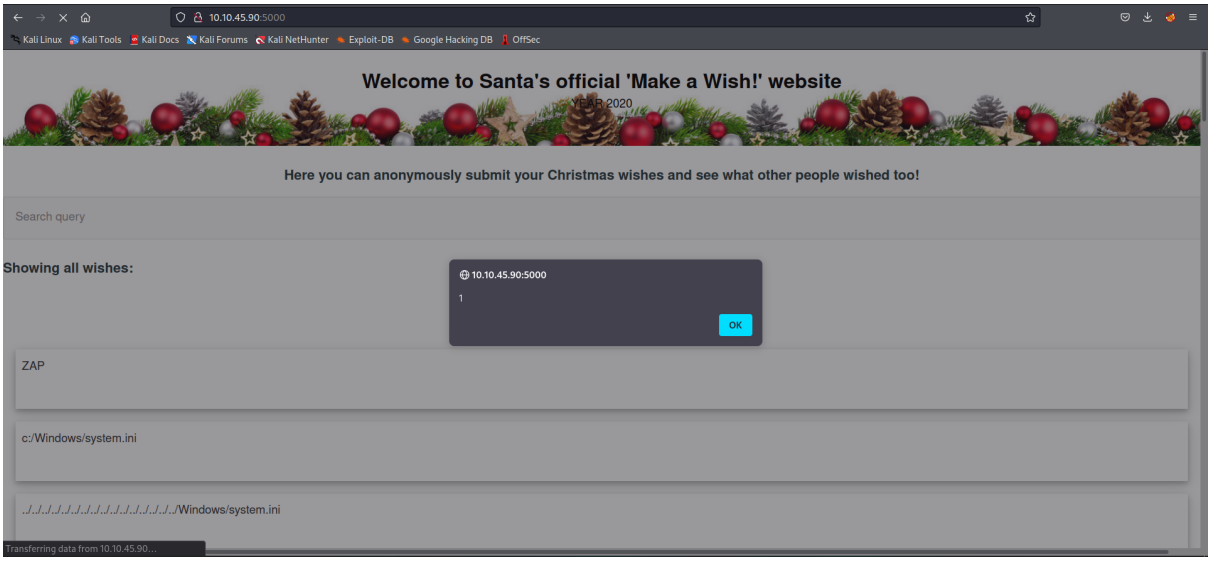

1211103423@kali: ~
File Actions Edit View Help
(1211103423㉿kali)-[~]
$ sudo apt install zaproxy
[sudo] password for 1211103423:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
zaproxy
0 upgraded, 1 newly installed, 0 to remove and 480 not upgraded.
Need to get 185 MB of archives.
After this operation, 232 MB of additional disk space will be used.
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 zaproxy all 2.1
1.1-0kali1 [185 MB]
1% [1 zaproxy 1,953 kB/185 MB 1%] 119 kB/s 25min 36s


OWASP ZAP - OWASP ZAP 2.11.1
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://10.10.45.90:5000
Select...
Use traditional spider:
Use ajax spider: with Firefox Headless
Attack
Stop
Progress: Actively scanning (attacking) the URLs discovered by the spider(s)
History Search Alerts Output Spider Active Scan
New Scan Progress: 0: http://10.10.45.90:5000 19% Current Scans: 1 Num Requests: 84 New Alerts: 0 Export
Sent Messages Filtered Messages
Id Req. Timestamp Resp. Timestamp Method URL Code Reason RTT Size Resp. Header Size Resp. Body
91 6/21/22, 12:02:26 PM 6/21/22, 12:02:27 PM GET http://10.10.45.90:5000/static 404 NOT FOUND 407 ms 162 bytes 232 bytes
92 6/21/22, 12:02:26 PM 6/21/22, 12:02:27 PM GET http://10.10.45.90:5000/?q=HtTp%3A%2F%2F594... 200 OK 400 ms 156 bytes 1,010 bytes
93 6/21/22, 12:02:27 PM 6/21/22, 12:02:27 PM GET http://10.10.45.90:5000/?q=HtTpS%3A%2F%2F59... 200 OK 395 ms 156 bytes 1,012 bytes
94 6/21/22, 12:02:27 PM 6/21/22, 12:02:28 PM POST http://10.10.45.90:5000/ 200 OK 465 ms 156 bytes 3,568 bytes
95 6/21/22, 12:02:28 PM 6/21/22, 12:02:28 PM GET http://10.10.45.90:5000/?q=%3C%21-%23EXEC+... 200 OK 429 ms 155 bytes 984 bytes
96 6/21/22, 12:02:28 PM 6/21/22, 12:02:28 PM POST http://10.10.45.90:5000/ 200 OK 443 ms 156 bytes 3,640 bytes
97 6/21/22, 12:02:28 PM 6/21/22, 12:02:28 PM GET http://10.10.45.90:5000/?q=%22%3E%3C%21-%2... 200 OK 399 ms 155 bytes 990 bytes
98 6/21/22, 12:02:28 PM 6/21/22, 12:02:29 PM POST http://10.10.45.90:5000/ 200 OK 433 ms 156 bytes 3,710 bytes
99 6/21/22, 12:02:28 PM 6/21/22, 12:02:29 PM GET http://10.10.45.90:5000/?q=%3C%21-%23EXEC+... 200 OK 401 ms 155 bytes 986 bytes
100 6/21/22, 12:02:29 PM 6/21/22, 12:02:29 PM POST http://10.10.45.90:5000/ 200 OK 479 ms 156 bytes 3,783 bytes
101 6/21/22, 12:02:29 PM 6/21/22, 12:02:29 PM GET http://10.10.45.90:5000/?q=%22%3E%3C%21-%2... 200 OK 396 ms 155 bytes 992 bytes
Alerts 0 1 2 0 Primary Proxy: localhost:8081
Current Scans 0 0 0 1 0 0 0 0

Question 5



Question 6



Thought Process/Methodology:

We copy the machine IP address into the browser search bar and it appears a Santa's official 'Make a Wish' website. After that, we searched for 'asads' in the search query and it showed the query string 'q' in the browser search bar. Then, we open the OWASP ZAP application and run the automated scan. After that, we copy our IP address and paste it into the 'URL to attack' box. Then we press the attack button. After that, we can see how many alerts we got.Later, we are able to make an alert appear on the 'Make a Wish' website.

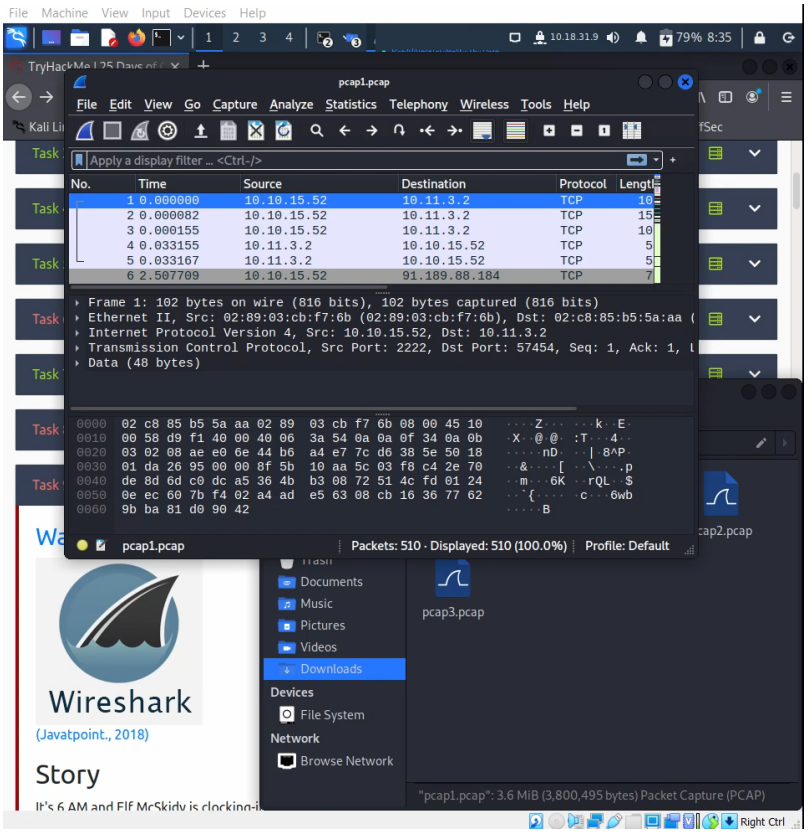
Day7: Networking – The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

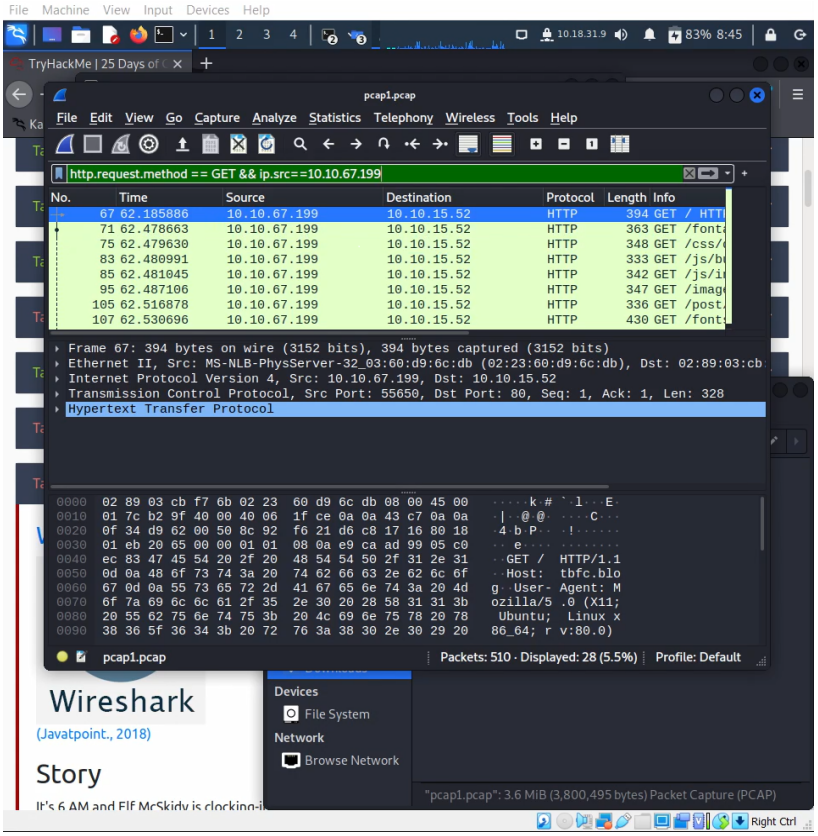
Question 1

Open pcap1.pcap using wireshark.



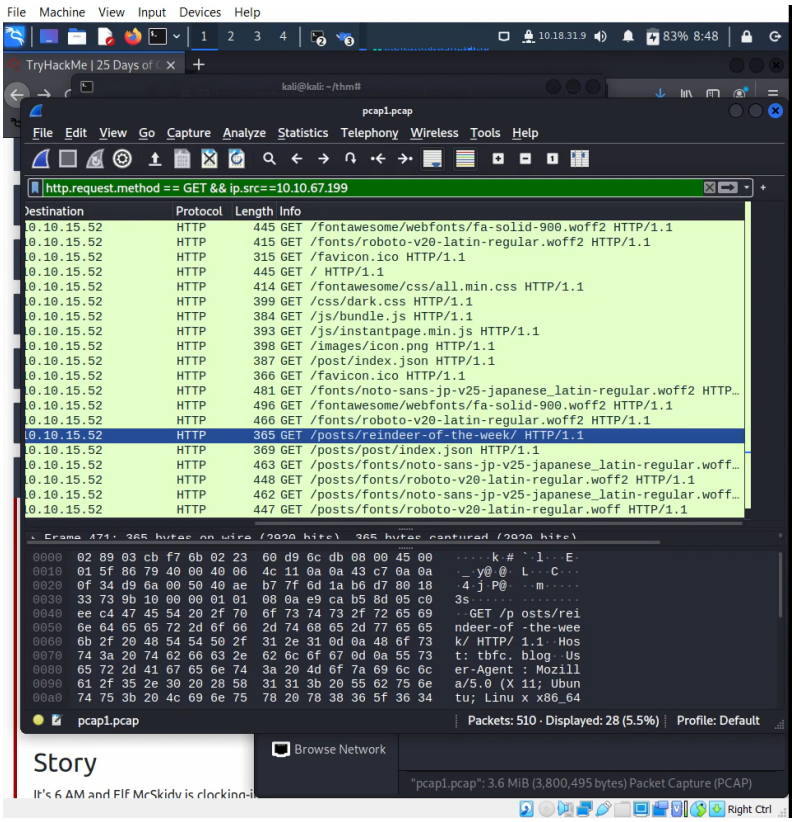
Question 2

Search the ip address using the request method.



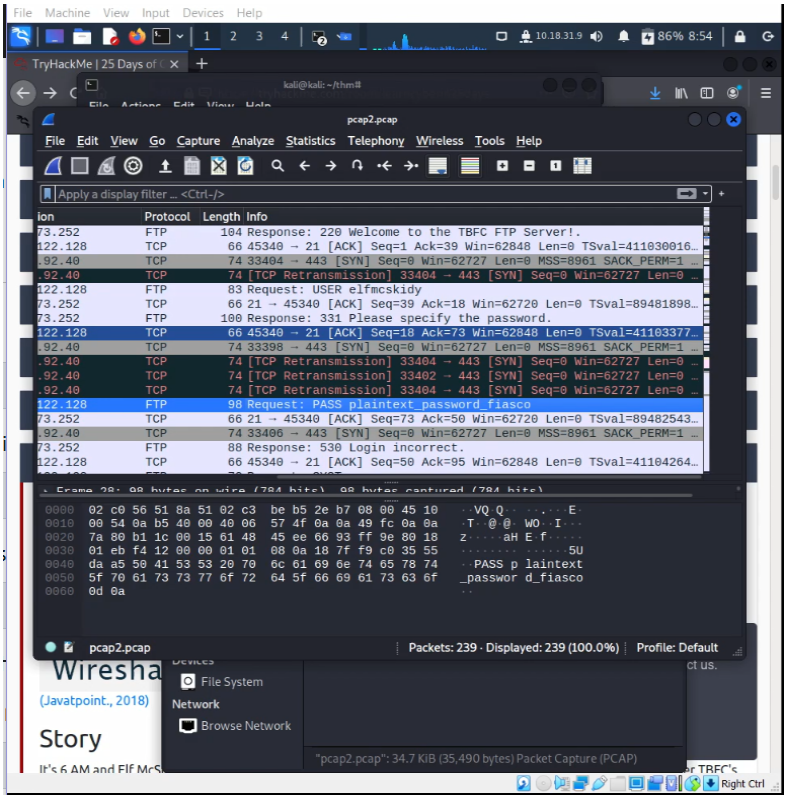
Question 3

From the hint we go through one by one that have “/post/”.



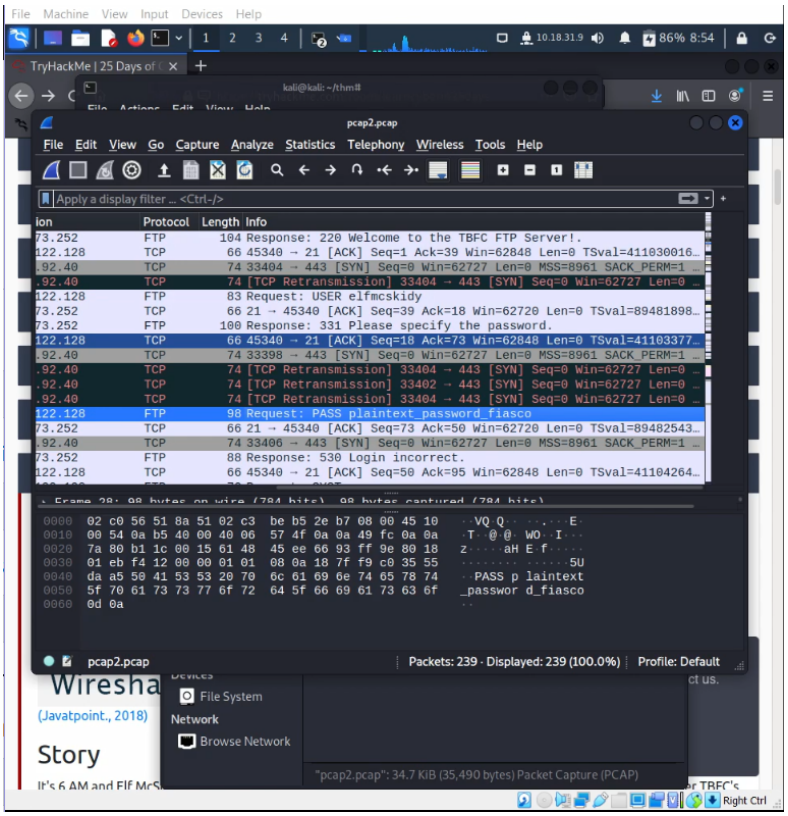
Question 4

Open the pcap2.pcap file and find the password.



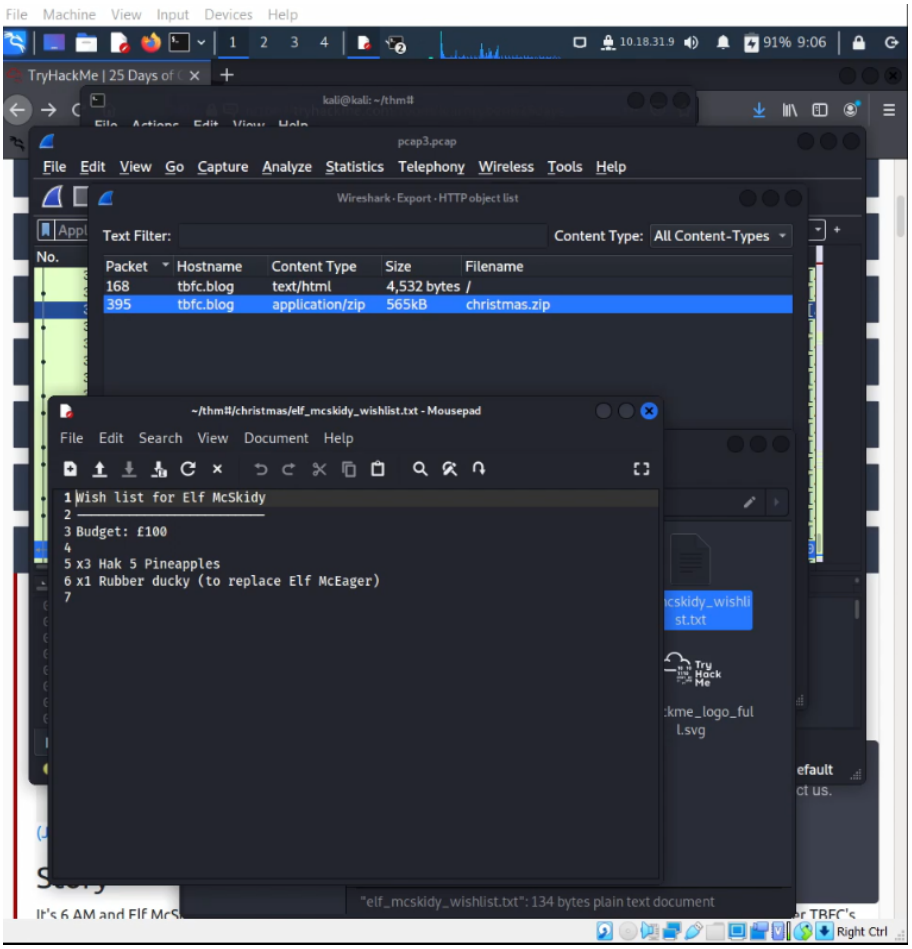
Question 5

Open the pcap2.pcap file and find the password.



Question 6

Open pcap3.pcap file and download the .zip file.



Thought Process/Methodology:

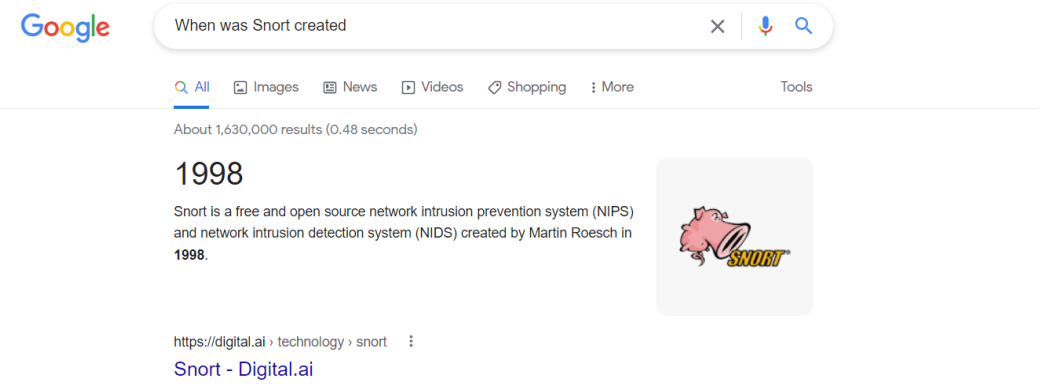
First, we download and run wireshark. We download the task files that tryhackme provides. Wireshark is used to open "pcap1.pcap". The IP address is displayed after that. To obtain the HTTP GET, we used "http.request.method == GET" and the IP address provided to find the name of the article. It shows a lot of data, and we tried to find it by searching "/posts/" and obtained the article name. After that, when we open "pcap2.pcap," the traffic is displayed. We searched for the user who successfully logged in with a password and located the password that had been leaked. We later found the encrypted protocol's name. After that, we open "pcap3.pcap" and export objects, then download "christmas.zip" and proceed to wishlist.txt.

Day8: Networking – What's Under the Christmas Tree?

Tools used: Kali Linux, Firefox

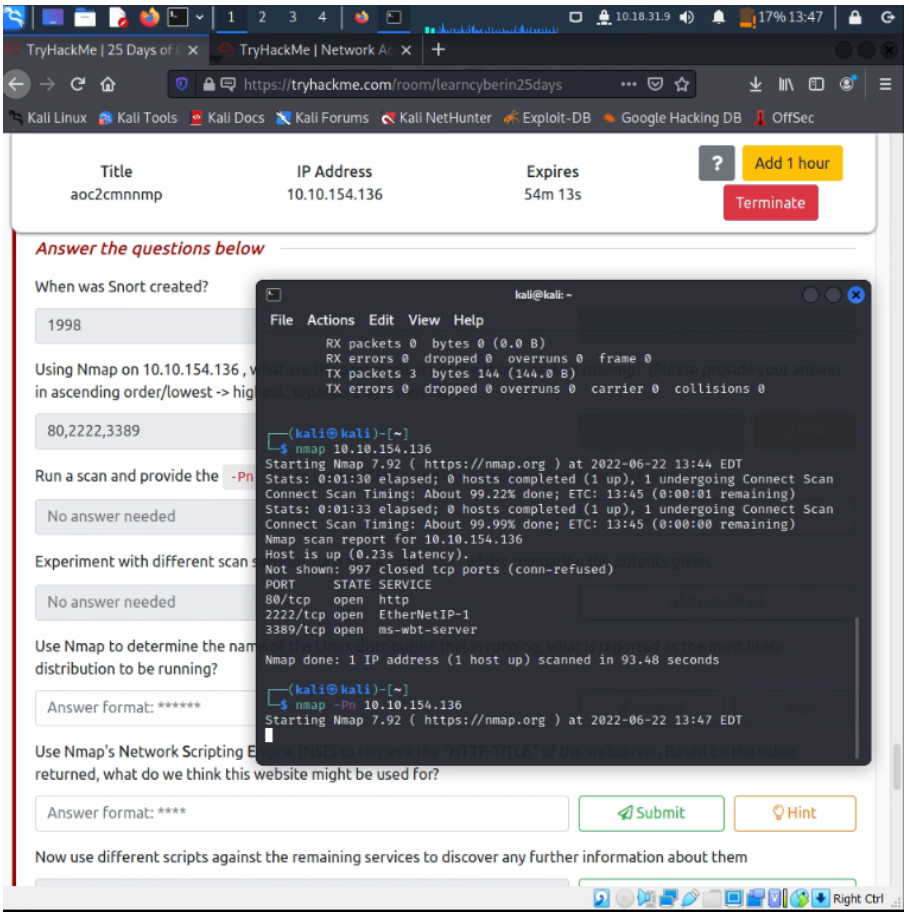
Solution/Walkthrough:

Question 1



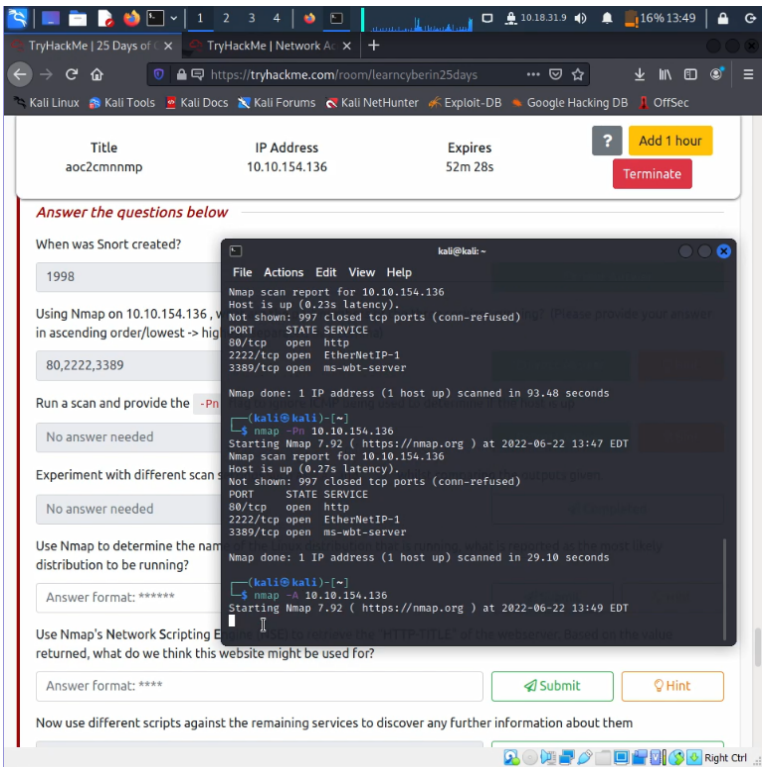
Question 2

Open terminal and use the nmap command for our ip address.



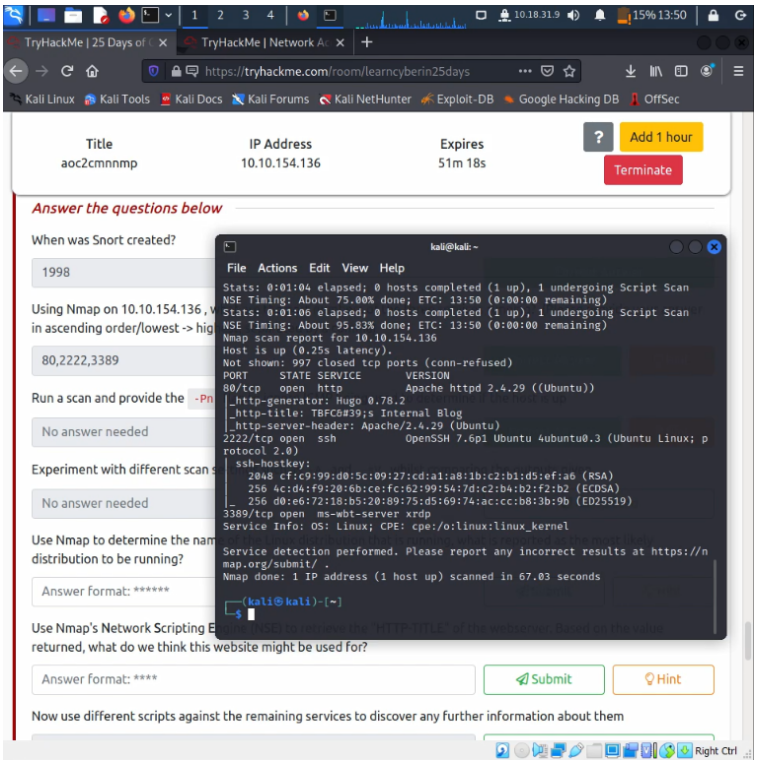
Question 3

Using the same command but with the “-Pn” command.

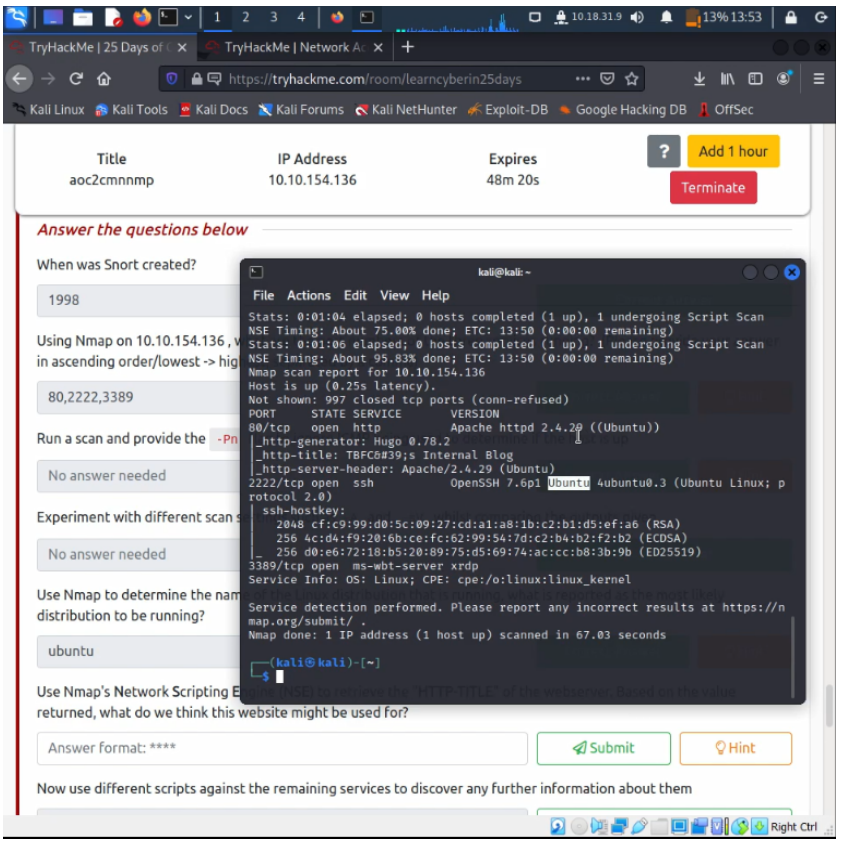


Question 4

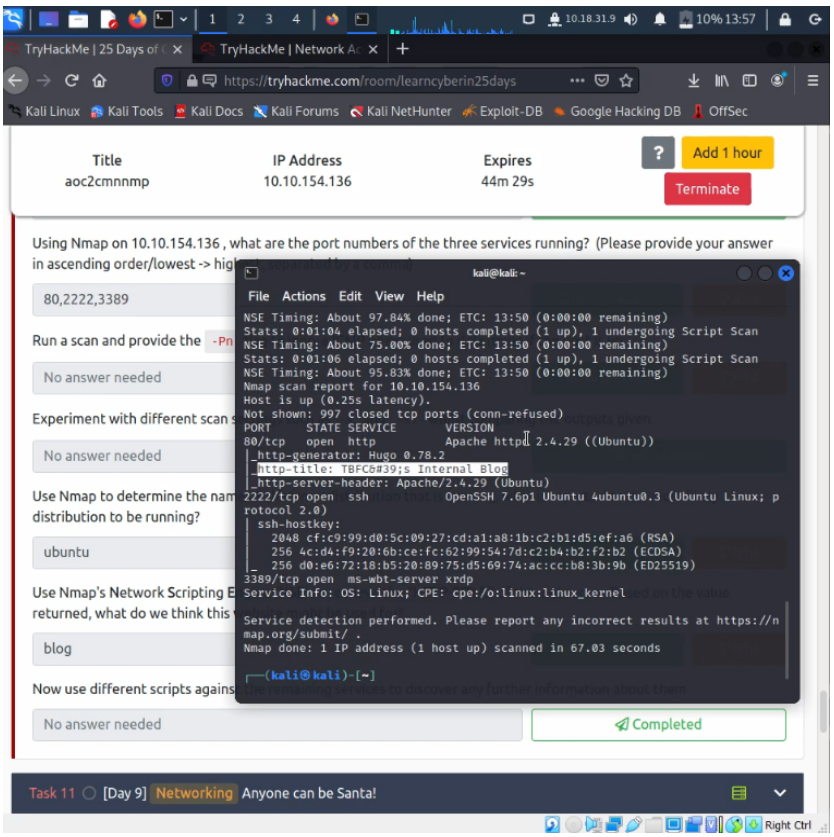
Using the nmap command but using “-A” and “-sV”.



Question 5


TryHackMe | 25 Days of
TryHackMe | Network Ac
https://tryhackme.com/room/learncyberin25days
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Title
aoc2cmnnmp
IP Address
10.10.154.136
Expires
48m 20s
Add 1 hour
Terminate
Answer the questions below
When was Snort created?
1998
Using Nmap on 10.10.154.136 , w
in ascending order/lowest -> hig
80,2222,3389
Run a scan and provide the -Pn
No answer needed
Experiment with different scan s
No answer needed
Use Nmap to determine the nam
distribution to be running?
ubuntu
Use Nmap's Network Scripting E
returned, what do we think this website might be used for?
Answer format: ****
Submit
Hint
Now use different scripts against the remaining services to discover any further information about them
kali@kali: ~
File Actions Edit View Help
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 75.00% done; ETC: 13:50 (0:00:00 remaining)
Stats: 0:01:06 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 95.83% done; ETC: 13:50 (0:00:00 remaining)
Nmap scan report for 10.10.154.136
Host is up (0.25s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-title: TBFC's Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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 (ED25519)
3389/tcp open ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.03 seconds
(kali㉿kali)-[~]
$
Right Ctrl

Question 6


TryHackMe | 25 Days of
TryHackMe | Network Ac
https://tryhackme.com/room/learncyberin25days
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Title
aoc2cmnnmp
IP Address
10.10.154.136
Expires
44m 29s
Add 1 hour
Terminate
Using Nmap on 10.10.154.136 , what are the port numbers of the three services running? (Please provide your answer in ascending order/lowest -> hig
80,2222,3389
Run a scan and provide the -Pn
No answer needed
Experiment with different scan s
No answer needed
Use Nmap to determine the nam
distribution to be running?
ubuntu
Use Nmap's Network Scripting E
returned, what do we think this
blog
Now use different scripts agains
No answer needed
Completed
Task 11 [Day 9] Networking Anyone can be Santa!
kali@kali: ~
File Actions Edit View Help
NSE Timing: About 97.84% done; ETC: 13:50 (0:00:00 remaining)
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 75.00% done; ETC: 13:50 (0:00:00 remaining)
Stats: 0:01:06 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 95.83% done; ETC: 13:50 (0:00:00 remaining)
Nmap scan report for 10.10.154.136
Host is up (0.25s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-title: TBFC's Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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 (ED25519)
3389/tcp open ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.03 seconds
(kali㉿kali)-[~]
Right Ctrl

Thought Process/Methodology:

Using Google, we looked up the answer to the first question. Next, we open a terminal and run the nmap command for our IP address. It displayed the results of a nmap scan for our IP address. After that, we ran the same scan as before, but this time we included "-Pn" between nmap and the IP address, and it displayed the results. We also performed some scans with various scan parameters, such as "-A" and "-sV," and obtained different result. Next, we read through the scan findings; there are multiple mentions of Ubuntu, therefore we thought it is the name of the linux that is running. Once more, the "http-title" is mentioned in the scan results for port 80. It is clear from this that it serves as a blog.

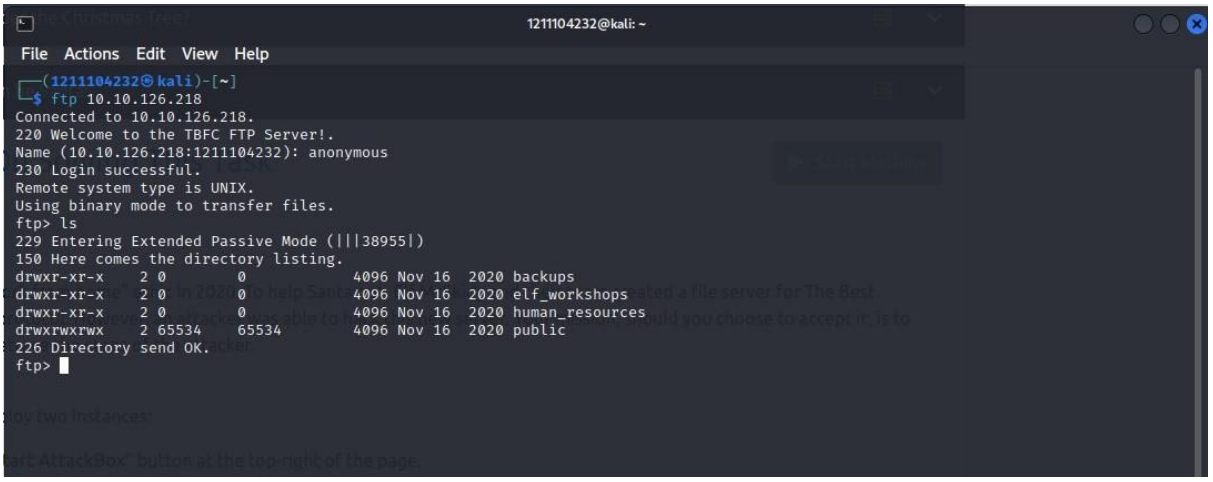
Day9: Networking – Anyone can be Santa!

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

Logging into the FTP server as ‘anonymous’



Question 2

Change directories into ‘public’ and look at the contents

```
ftp> ls
229 Entering Extended Passive Mode (|||41940|)
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> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
229 Entering Extended Passive Mode (|||61370|)
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
100% |*****************************************************************************|    24      509.51 KiB/s    00:00 ETA
226 Transfer complete.
24 bytes received in 00:00 (0.09 KiB/s)
ftp> get backup.sh
local: backup.sh remote: backup.sh
229 Entering Extended Passive Mode (|||16521|)
150 Opening BINARY mode data connection for backup.sh (341 bytes).
100% |*****************************************************************************|   341        7.74 MiB/s    00:00 ETA
226 Transfer complete.
341 bytes received in 00:00 (1.21 KiB/s)
ftp>
```

Question 3

Use ‘get’ command

```
┌──(1211104232㉿kali)-[~]
└─$ cat shoppinglist.txt
The Polar Express Movie
```

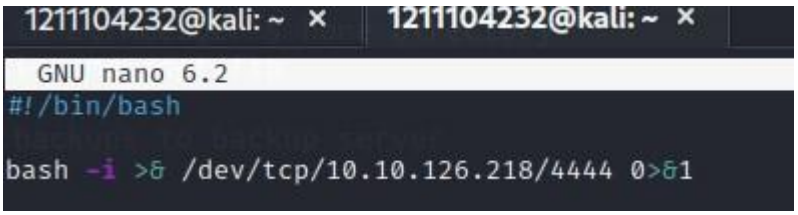
Question 4

Grab file from FTP server

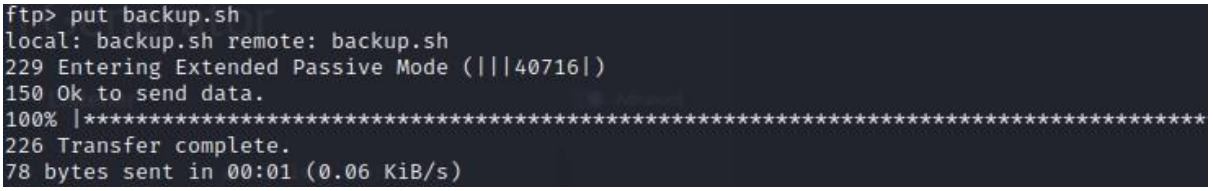
```
ftp> get backup.sh
local: backup.sh remote: backup.sh
229 Entering Extended Passive Mode (|||47139|)
150 Opening BINARY mode data connection for backup.sh (341 bytes).
100% |*****************************************************************************
226 Transfer complete.
341 bytes received in 00:00 (1.15 KiB/s)
```

```
┌──(1211104232㉿kali)-[~]
└─$ ls
backup.sh  Documents  Music                Pictures  shell.jpeg      shell.jpg.php     Templates
Desktop    Downloads  php-reverse-shell.php  Public    shell.jpeg.php  shoppinglist.txt  Videos

┌──(1211104232㉿kali)-[~]
└─$ cat backup.sh
#!/bin/bash

# Created by ElfMcEager to backup all of Santa's goodies!

# Create backups to include date DD/MM/YYYY
filename="backup_`date +%d`_`date +%m`_`date +%Y`.tar.gz";

# Backup FTP folder and store in elfmceager's home directory
tar -zcvf /home/elfmceager/$filename /opt/ftp

# TO-DO: Automate transfer of backups to backup server
```

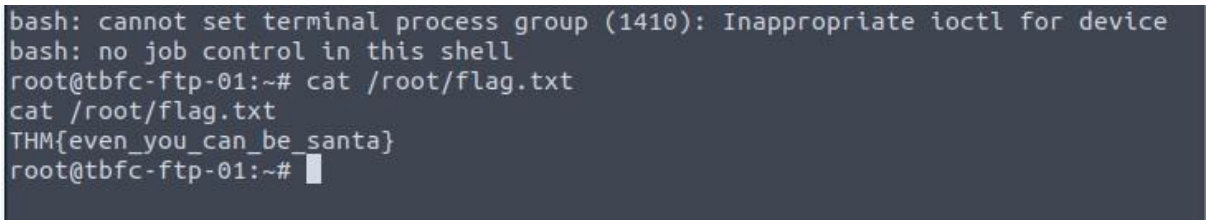
Open in nano to edit



Use Ctrl + X to close and save, then upload with ‘put’ command



Type ‘nc -lvnp 4444’ into terminal



Thought Process/Methodology:

Started off by logging into the FTP server as ‘anonymous’. After seeing through the directories, we can see that there is one available for the user to access which is ‘public’. We changed the directories into ‘public’ and then looked for the contents. There is a script named ‘backup.sh’ located there. To see the shopping list, we used the ‘get’ command and it was ready to be viewed on the system. Then, we grabbed the ‘backup.sh’ file by using the ‘get’ command again and were able to view the content. We opened it up on nano so we could edit it. Before we send it over, we set up a listener using netcat with the same port we specified in the script which is 4444. We usedCtrl + X to close and save, then upload with ‘put’ command into the same public file we have access to. Then we navigated it to the flag.txt file.

Day10: Networking – Don’t be sElfish!

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

We used following command to show all the users

```
┌──(1211104232㉿kali)-[~]
└─$ enum4linux -U 10.10.214.27
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Jun 23 11:57:51 2022

 ========================( Target Information )=========================

Target ........... 10.10.214.27
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
 ========================( Users on 10.10.214.27 )=========================

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:
```

Question 2

We used this command to see ‘shares’ on the server

```
┌──(1211104232㉿kali)-[~]
└─$ enum4linux -S 10.10.214.27
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Jun 23 12:01:01 2022
```

```
 ========================( Share Enumeration on 10.10.214.27 )=========================


        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
```

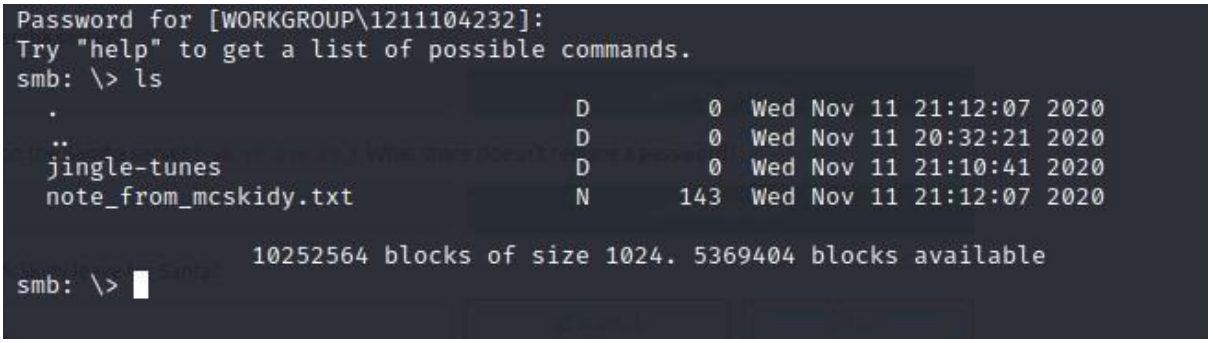
Question 3

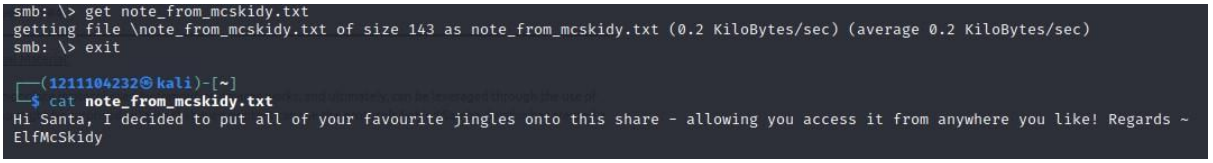
‘tbfc-hr’ share requires password and we proceeded to use ‘tbfc-santa’ which is unprotected

```
┌──(1211104232㉿kali)-[~]
└─$ smbclient //10.10.214.27/tbfc-hr
Password for [WORKGROUP\1211104232]:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(1211104232㉿kali)-[~]
└─$ smbclient //10.10.214.27/tbfc-santa
Password for [WORKGROUP\1211104232]:
Try "help" to get a list of possible commands.
smb: \>
```

Question 4

Using following command we saw two directories





Thought Process/Methodology:

We began by using ‘enum4linux -U’ to reveal all the users. To search for how many shares are there on the Samba server, we used ‘enum4linux -S’ command to produce info about all the shares. After that, by using ‘smbclient’ command to try to login to the shares. We could not get onto the ‘tbfc-hr’ share without a password, so we used the ‘tbfc-santa’ share which is unprotected. After we successfully logged into that share, we used ‘ls’ command and found two directories are available. “jingle-tunes” is the correct answer. However, the directory was empty, but we found something to read on the note_from_mcskidy.txt.