PSP0201
Week 3
Writeup

Group Name: Amway

Members:

ID	Name	Role
1211100903	TAN XIN YI	Leader
1211101998	WESLEY WONG MIN GUAN	Member
1211101843	YAP HAN WAI	Member
1211101186	TAM LI XUAN	Member

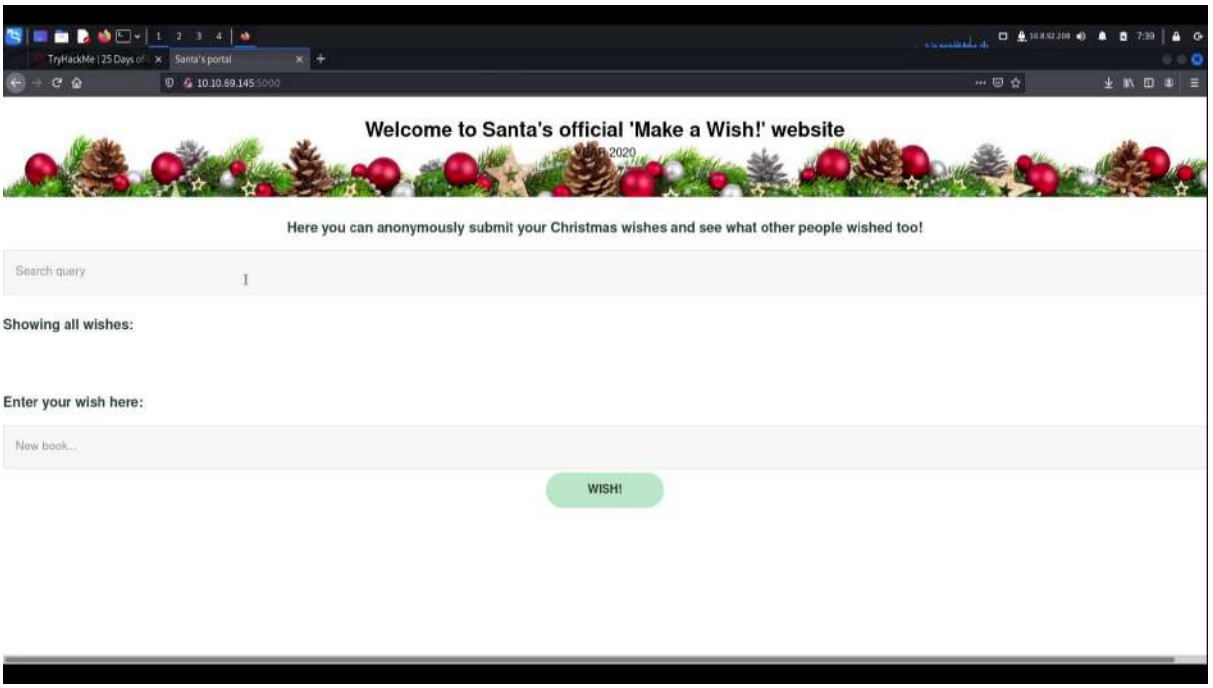
Day 6: Web Exploitation – Be careful with what you wish on a Christmas night

Tools used: Kali Linux, Firefox, Zaproxy

Solution/walkthrough:

Question 1

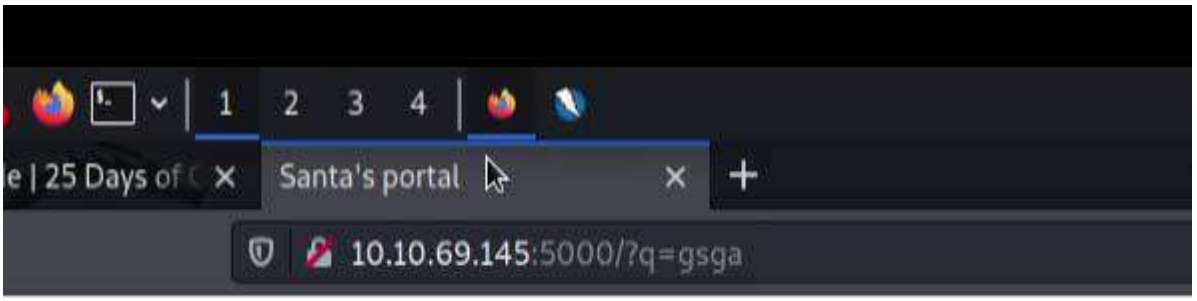
Enter the machine ip from *TryHackMe*



Question 2

Search for anything and press enter

Take a look at the link address

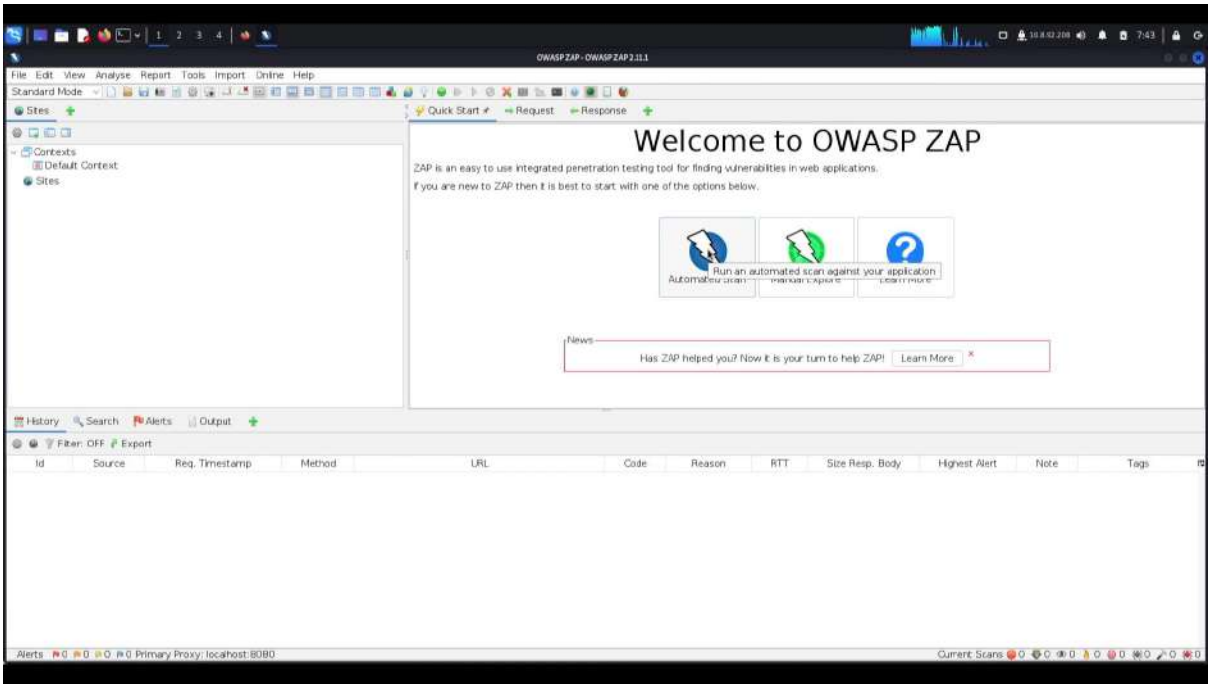


Question 3

Open *terminal* and install *Zaproxy* using the following command:
sudo apt install zaproxy

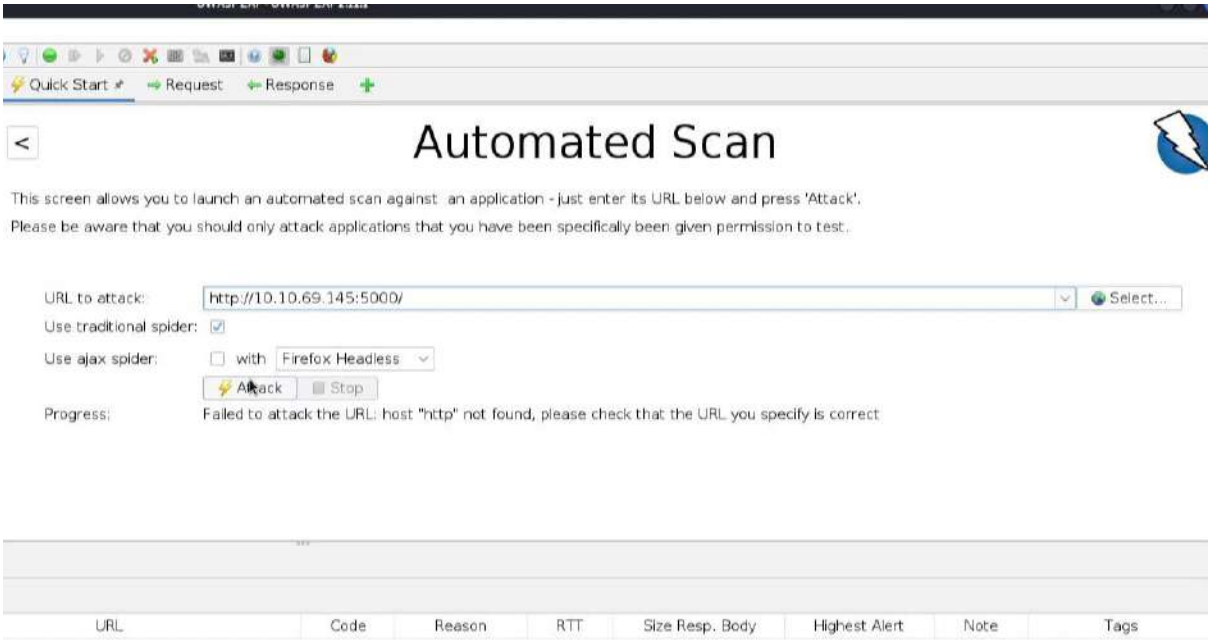
```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo apt install zaproxy
[sudo] password for kali:
kalSorry, try again.
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
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 377 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]
```

After installing, open *Zaproxy* and it will show the menu as below

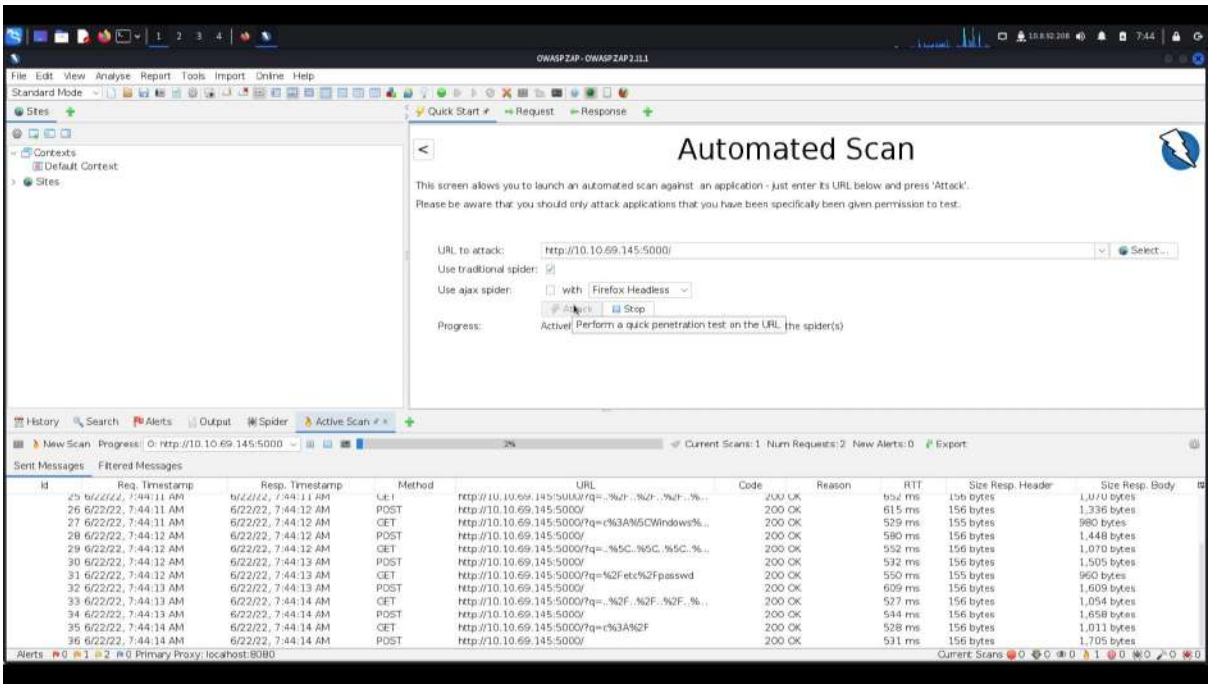


Question 4

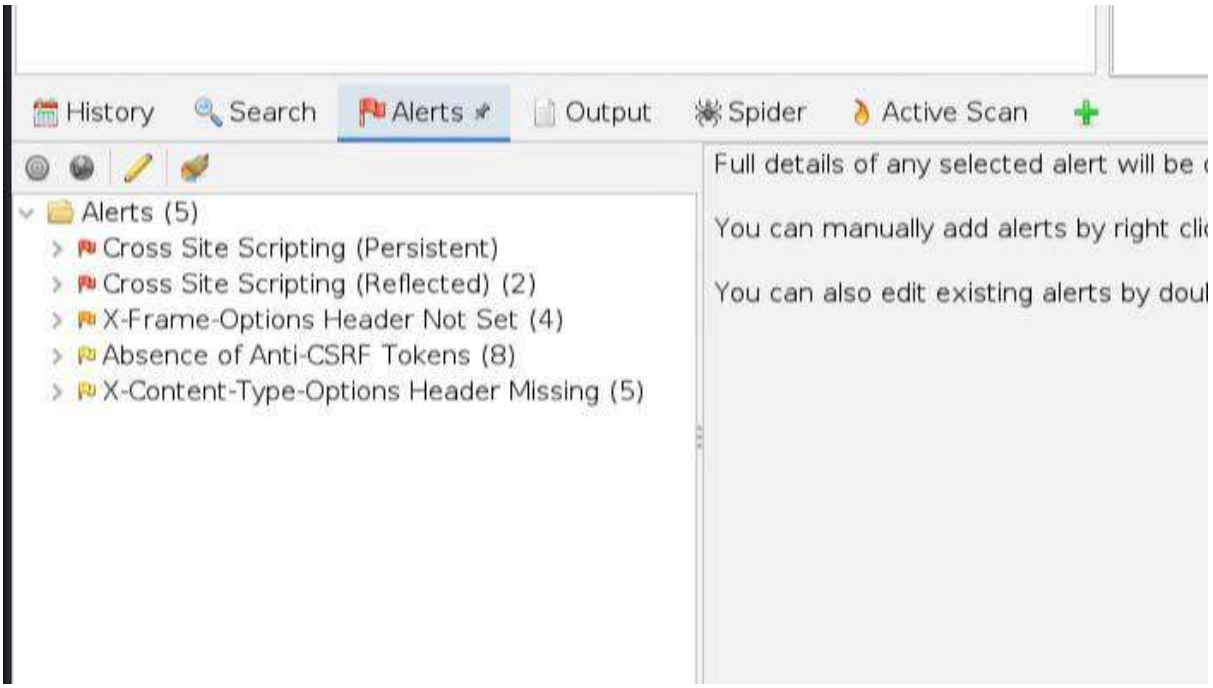
Now, go to *Automated Scan* and paste the machine ip



Press the *Attack* button

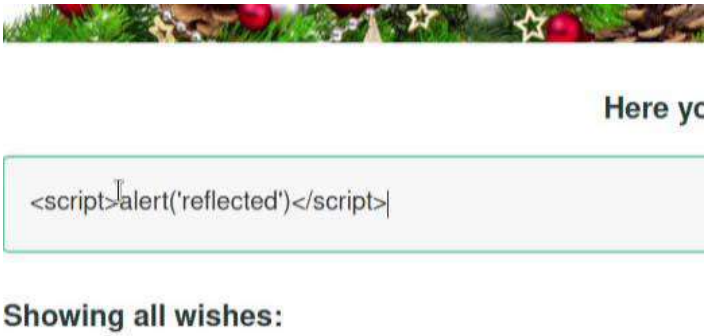


Go to the *Alerts* tab, count all the alerts

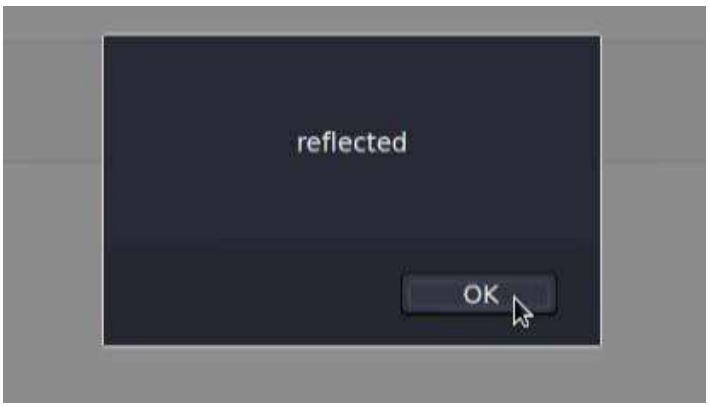


<u>Question 5</u>

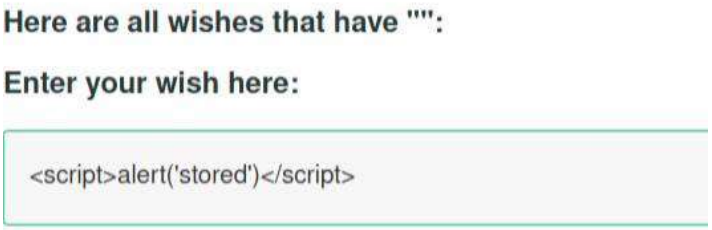
Go back to the Wish a Wish website, type *<script>alert('reflected')</script>* into the first search box



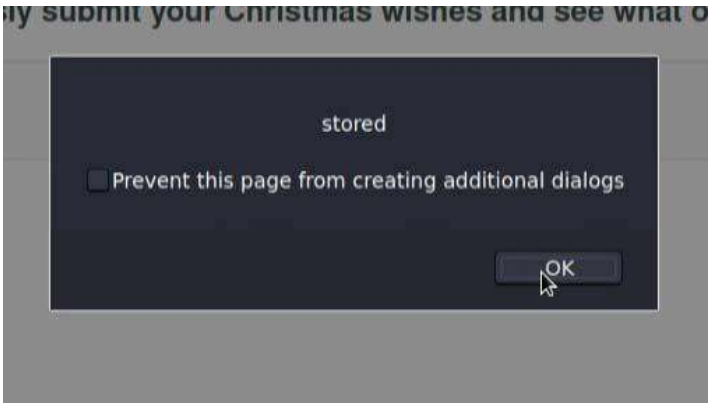
It will be *reflected*



Now for the second search box, type *<script>alert(‘stored’)</script>*



It will be *stored*



Thought Process/Methodology:
After entering the machine ip, the website shows something about making a wish and having 2 search boxes. I tried to search for anything and it will show *?q=<xxx> at the link address of the website.* After that, I need to install Zaproxy using the command *sudo apt install zaproxy* and attack the website. When attacking the website, the alerts will pop out inside the *alerts tabs* of *Zaproxy.* Here’s how I am able to make an alert appear on the website: type *<script>alert(‘reflected’)</script>* on the first search box and first alert which saying *reflected* will pop out; type *<script>alert(‘stored’)</script>* on the second search box and few alerts will pop out.

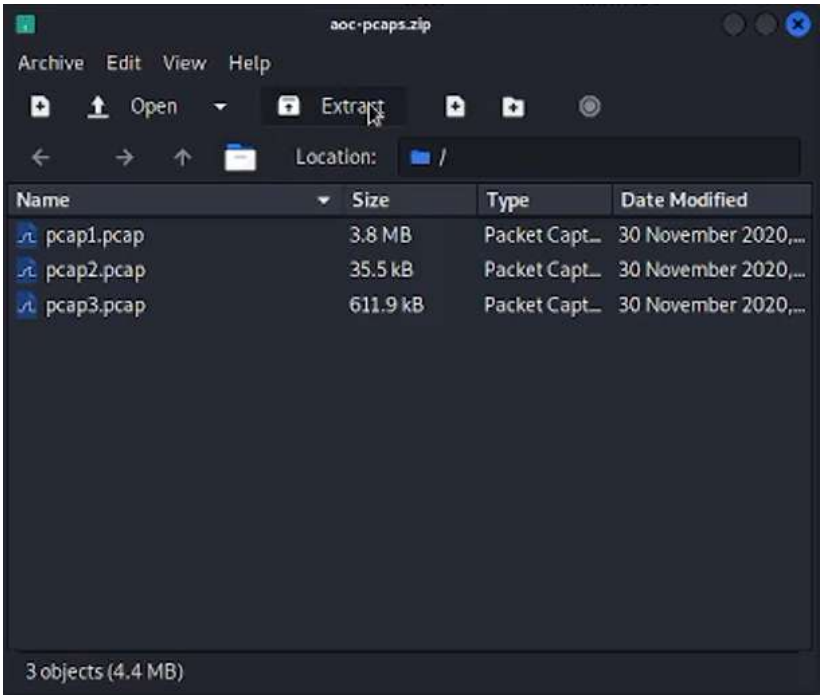
Day 7: Networking - The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Wireshark

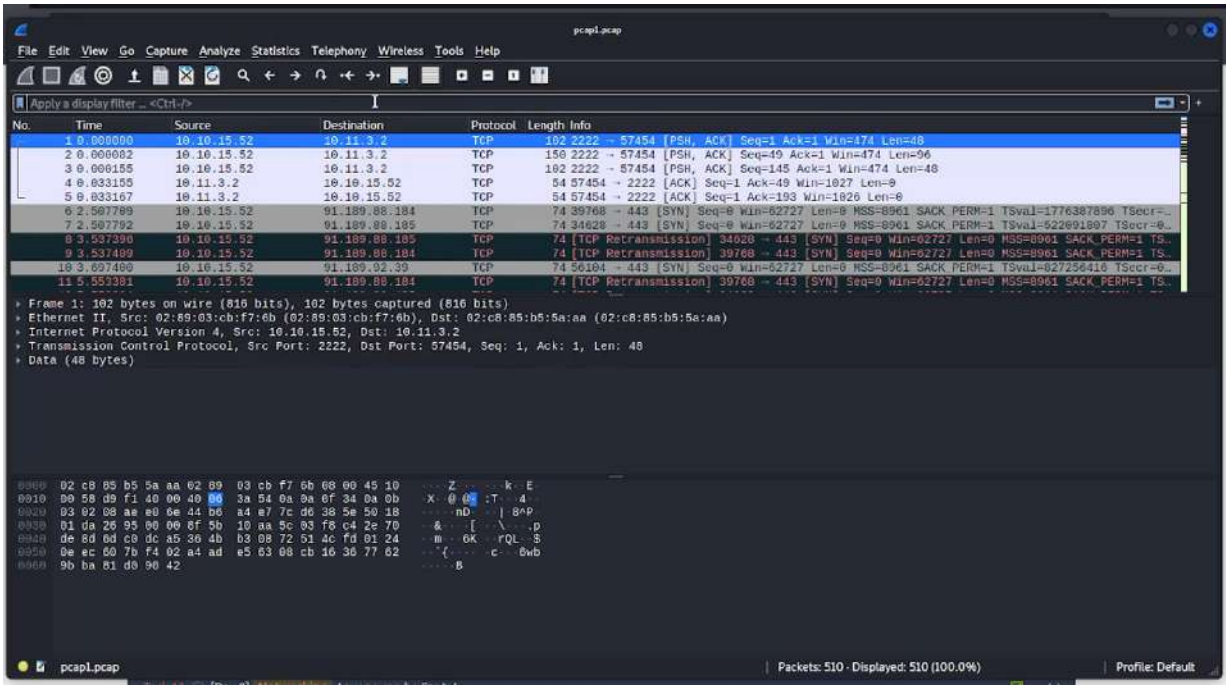
Solution/walkthrough:

Question 1

Download the files from THM and extract the zip file

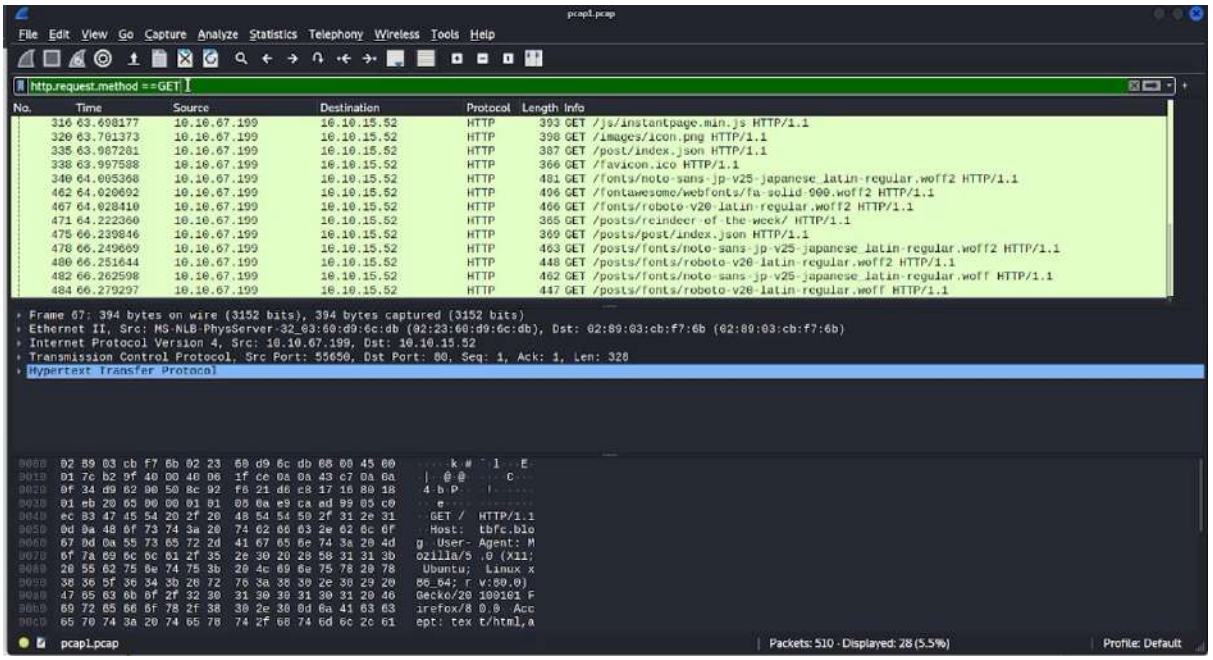


Find the IP address by searching *ICMP* from *pcap1.pcap* file



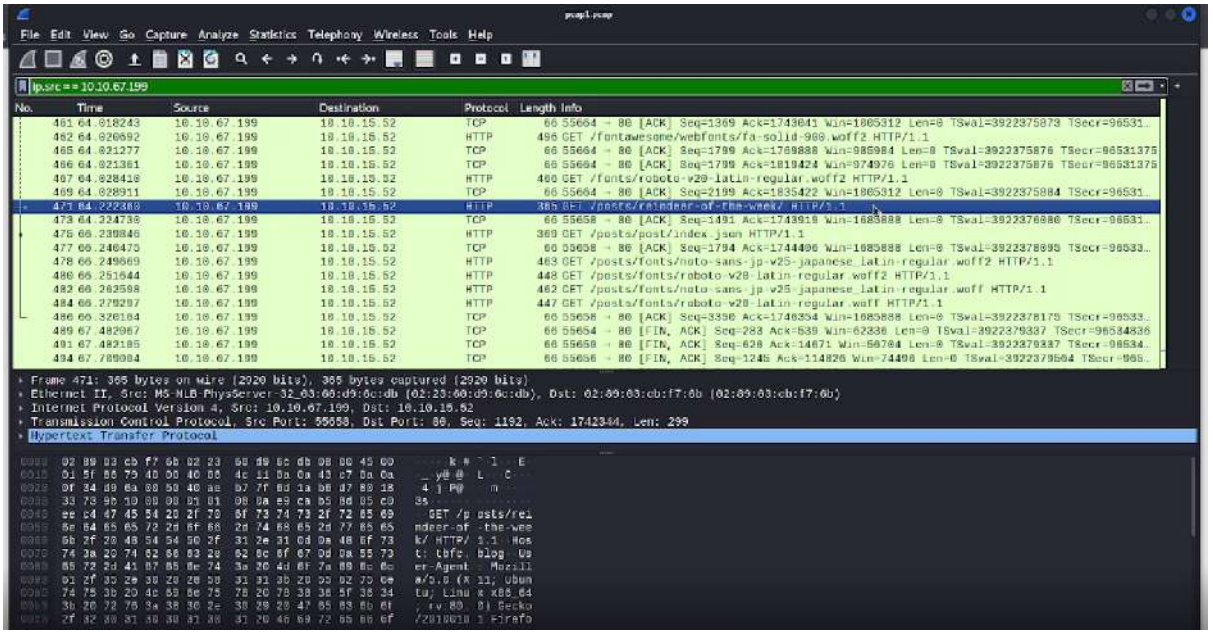
Question 2

We used the "*http.request.method == GET* " filter to *GET* request *HTTP* in the *pcap1.pcap* file



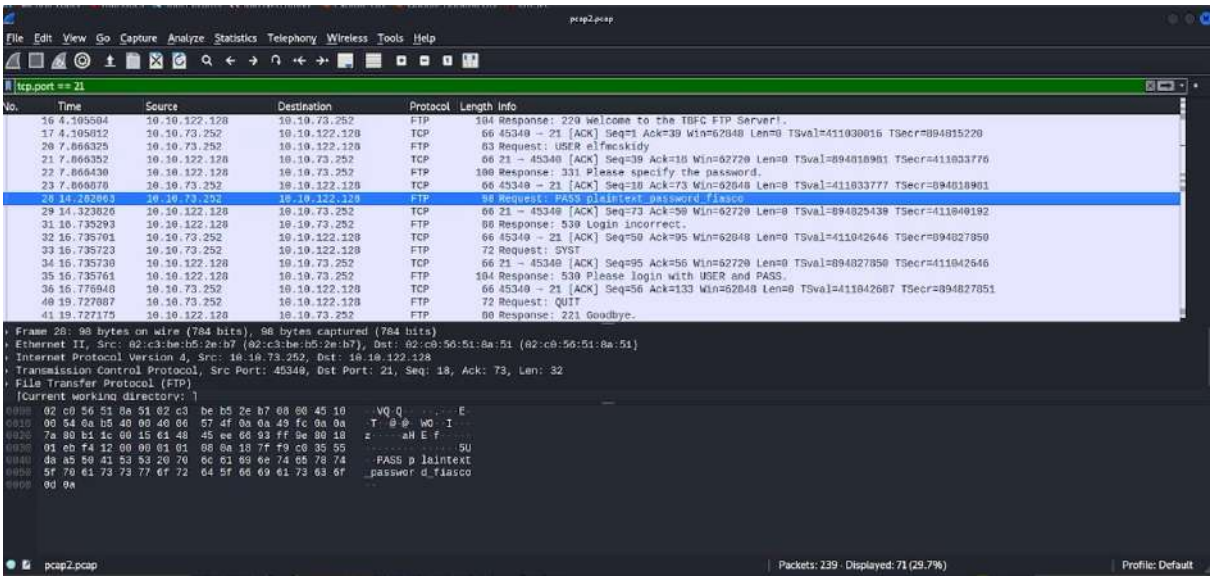
Question 3

To find the article of IP address *10.10.67.199*, we need to apply a filter in *pcap1.pcap*. Key in "*ip.src == 10.10.67.199*" to find the article name from the info column



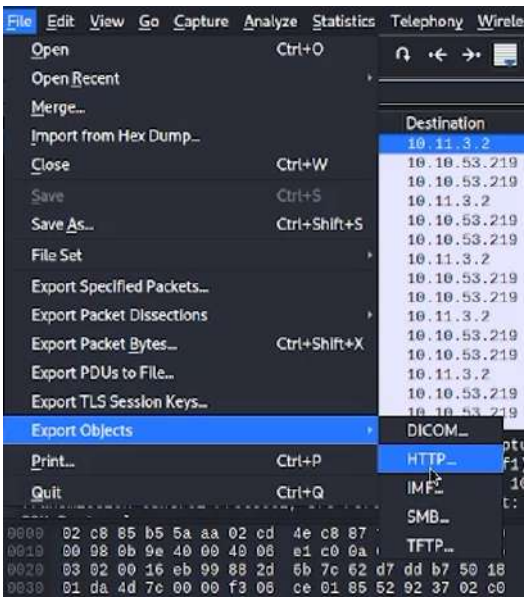
Question 4

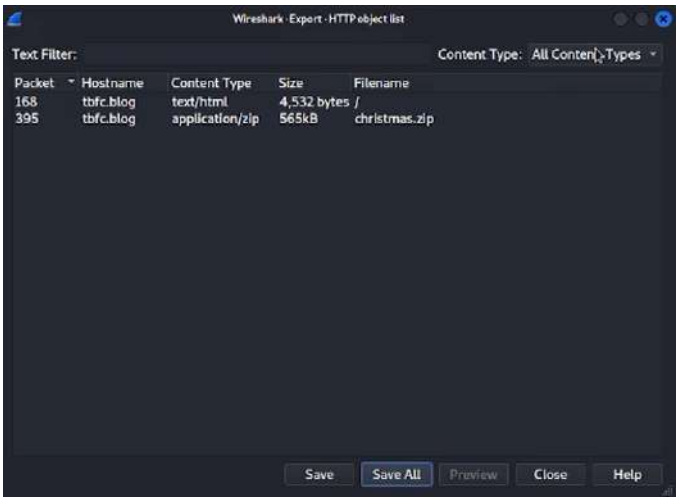
As *FTP* uses the *TCP* protocol, we apply the "*tcp.port == 21*" filter in *pcap2.pcap* file order to look for the leaked password



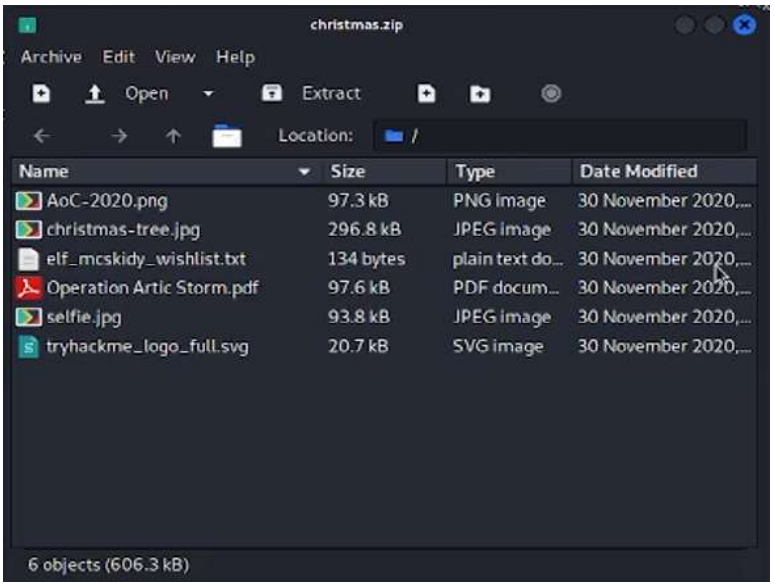
Question 5

We need to use *pcap3.pcap* file to recover the "*Christmas*" zip file. Then, *navigate File > Export Objects > HTTP* and save into a folder

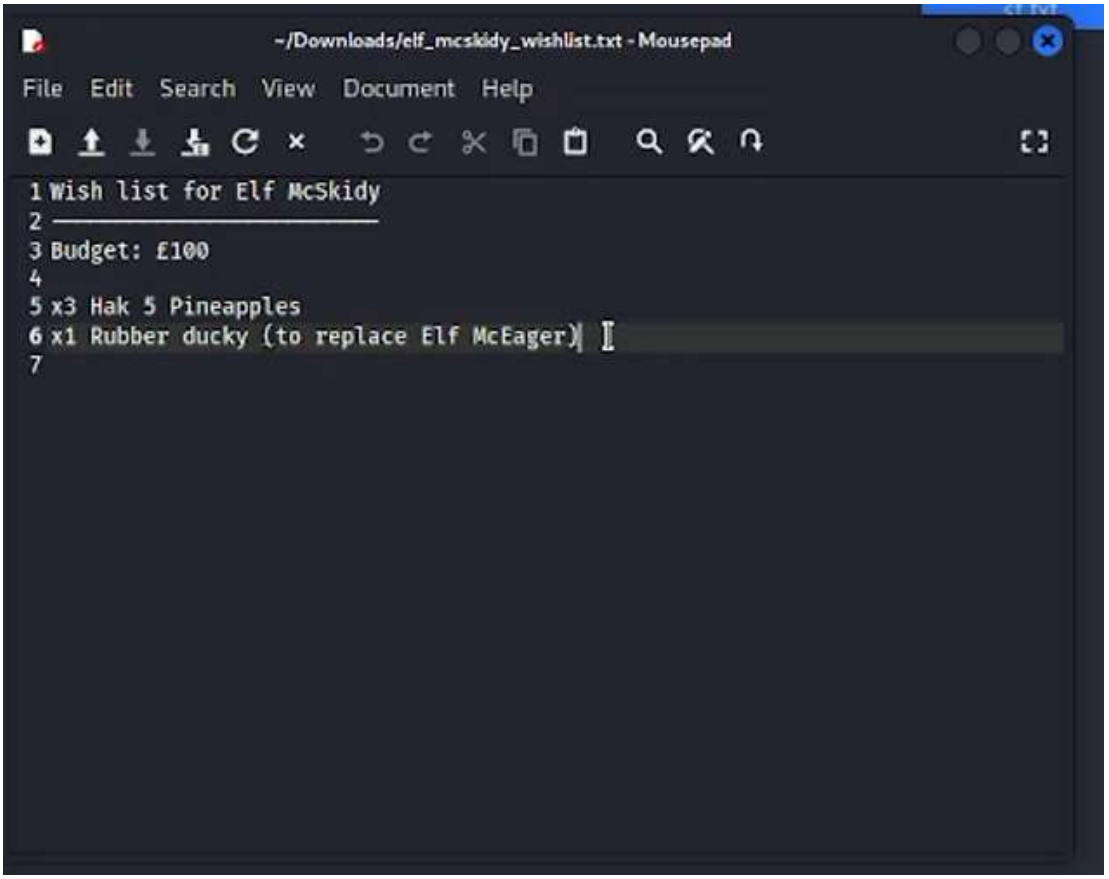




Extract the zip



Open the *elf_mcskidy_wishlist.txt file* to get the info we want



Thought Process/Methodology:

This task will guide us about Wireshark. First and foremost, we need to download and extract the zip files from TryHackMe first. Then, in order to find the IP address of the request and reply, we search *ICMP* from *pcap1.pcap* file. After that in the *pcap1.pcap* file, we use the "*http.request.method == GET* " filter to make an *HTTP GET* request. Next, we know that we need to use "*ip.src*" to filter out the packets. Hence, to find the article of IP address *10.10.67.199*, we apply the filter "*ip.src == 10.10.67.199*" in the *pcap1.pcap* file to find the article name from the *info* column. Then, in *pcap2.pcap* file order, we use the "*tcp.port == 21*" filter to look for all *FTP* traffic and follow the *TCP* stream we find the leaked password which is "*plaintext_password_fiasco*". Following that, we use *pcap3.pcap* file to recover the "Christmas" zip file. Then, navigate *File > Export Objects > HTTP* and save it, and extract the zip file and open the *elf_mcskidy_wishlist.txt file* to get the information we need, which is Rubber Ducky.

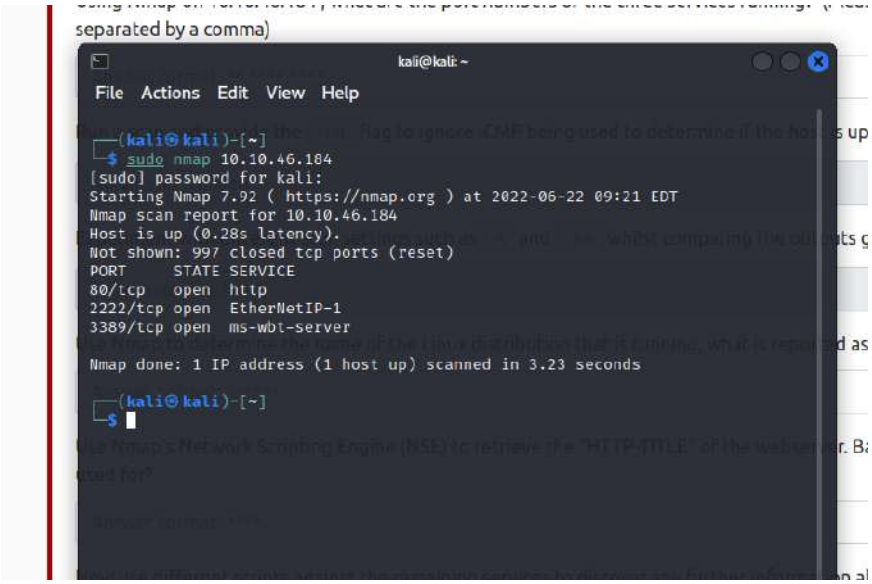
Day 8: Networking What's Under the Christmas Tree?

Tools used: Kali Linux, Firefox

Solution/walkthrough:

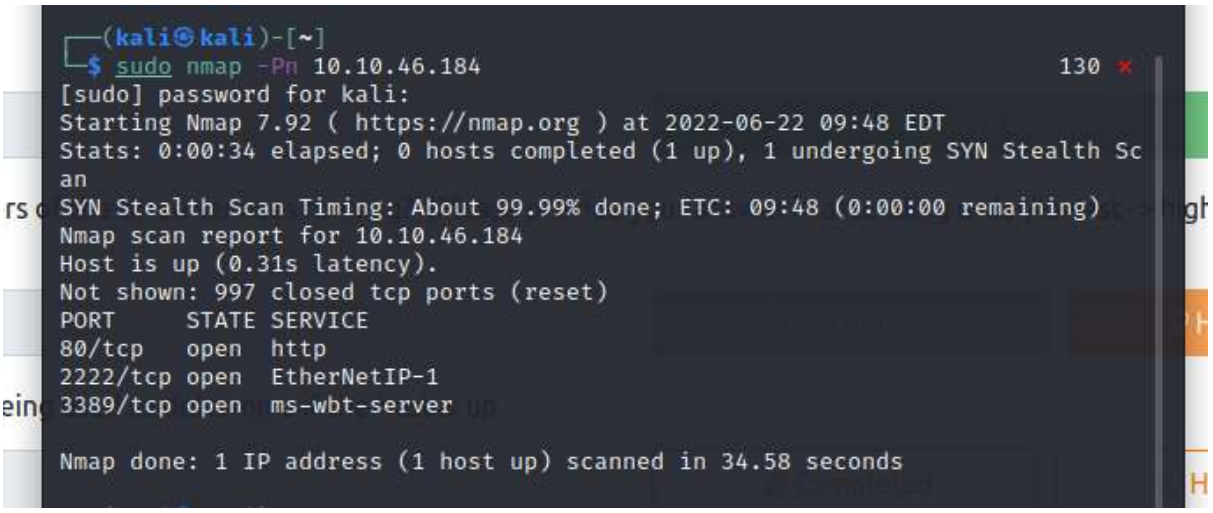
Question 1

Open the terminal and scan the IP given



Question 2

Run a scan and provide the *-Pn* flag to ignore *ICMP* being used to determine if the host is up



Question 3

Experiment with different scan settings such as *-A* and *-sV* while comparing the outputs.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 10.10.46.184
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 09:54 EDT
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Traceroute
Traceroute Timing: About 32.26% done; ETC: 09:55 (0:00:00 remaining)
Nmap scan report for 10.10.46.184
Host is up (0.30s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-title: TBFC&#39;s Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; p
rotocol 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
No exact OS matches for host (If you know what OS is running on it, see https
://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=6/22%OT=80%CT=1%CU=44404%PV=Y%DS=2%DC=T%G=Y%TM=62B31F5
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=105%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M506ST11NW6%O2=M506ST11NW6%O3=M506NNT11NW6%O4=M506ST11NW6%O5=M506ST1
OS:1NW6%O6=M506ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN
OS:(R=Y%DF=Y%T=40%W=F507%O=M506NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 23/tcp)
HOP RTT       ADDRESS
1   277.41 ms 10.18.0.1
2   278.42 ms 10.10.46.184

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.20 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 10.10.46.184
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 09:59 EDT
Nmap scan report for 10.10.46.184
Host is up (0.32s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; p
rotocol 2.0)
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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.49 seconds
```

Question 4

Use *Nmap* to determine the name of the Linux distribution that is running which is *Ubuntu* Linux

```
2222/tcp open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; p
rotocol 2.0)
```

Question 5

Use *Nmap's Network Scripting Engine (NSE)* to retrieve the "*HTTP-TITLE*" of the webserver which led us to the blog.

```
|_http-title: TBFC&#39;s Internal Blog
```

Thought Process/Methodology:

This task only requires a terminal. First of all, we scan the ip given by TryHackMe by using *nmap.* Then the terminal will display three port numbers which are *80, 2222, 3389*. After that to determine if the host is up, we can run the *-Pn* flag to ignore *ICMP* being used. As we all know, *-A* can be used in nmap to scan the host to identify services running by matching against the nmap database, and *-sV* can scan the host using *TCP* and perform version fingerprinting. Hence, we used *-A* and *-sV* to get the report. And both of the reports lead to the Linux distribution that is running in *Ubuntu* Linux. Lastly, we use nmap to get the "*HTTP-TITLE*" of the web server is a blog.

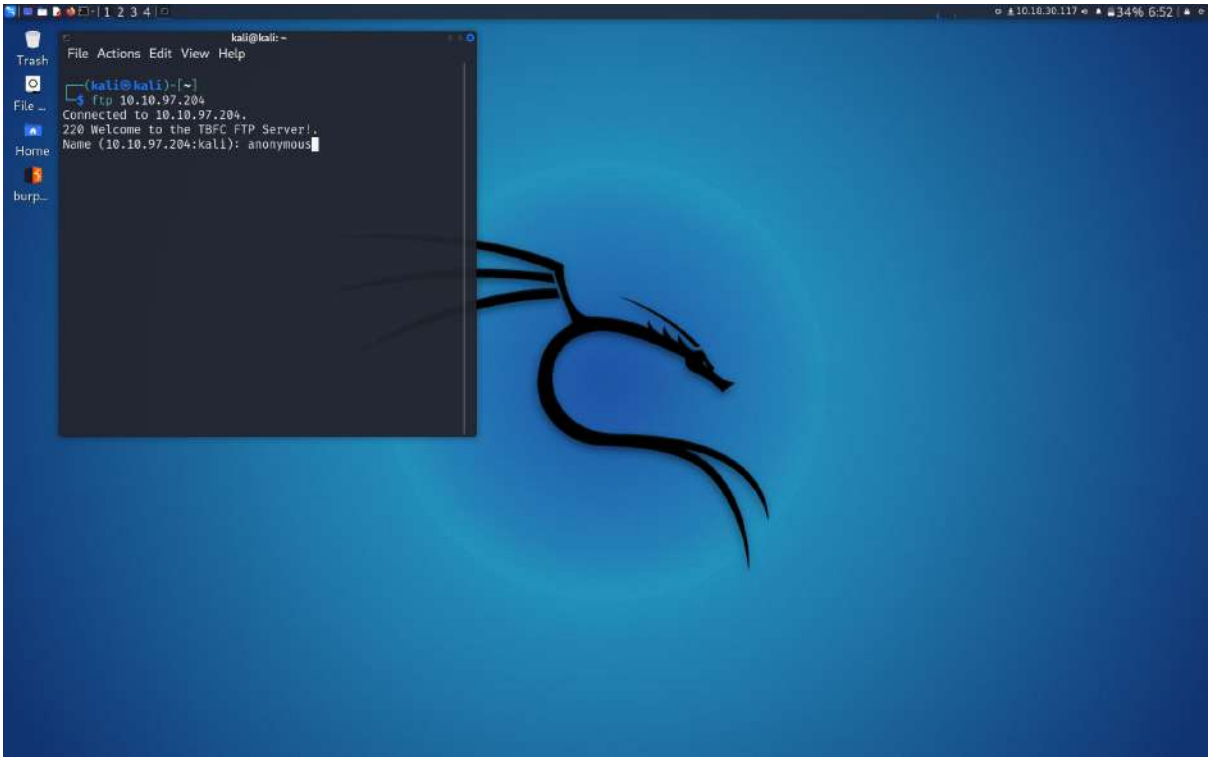
<u>Day 9: Anyone can be Santa!</u>

Tools used: Kali Linux, Mozilla Firefox

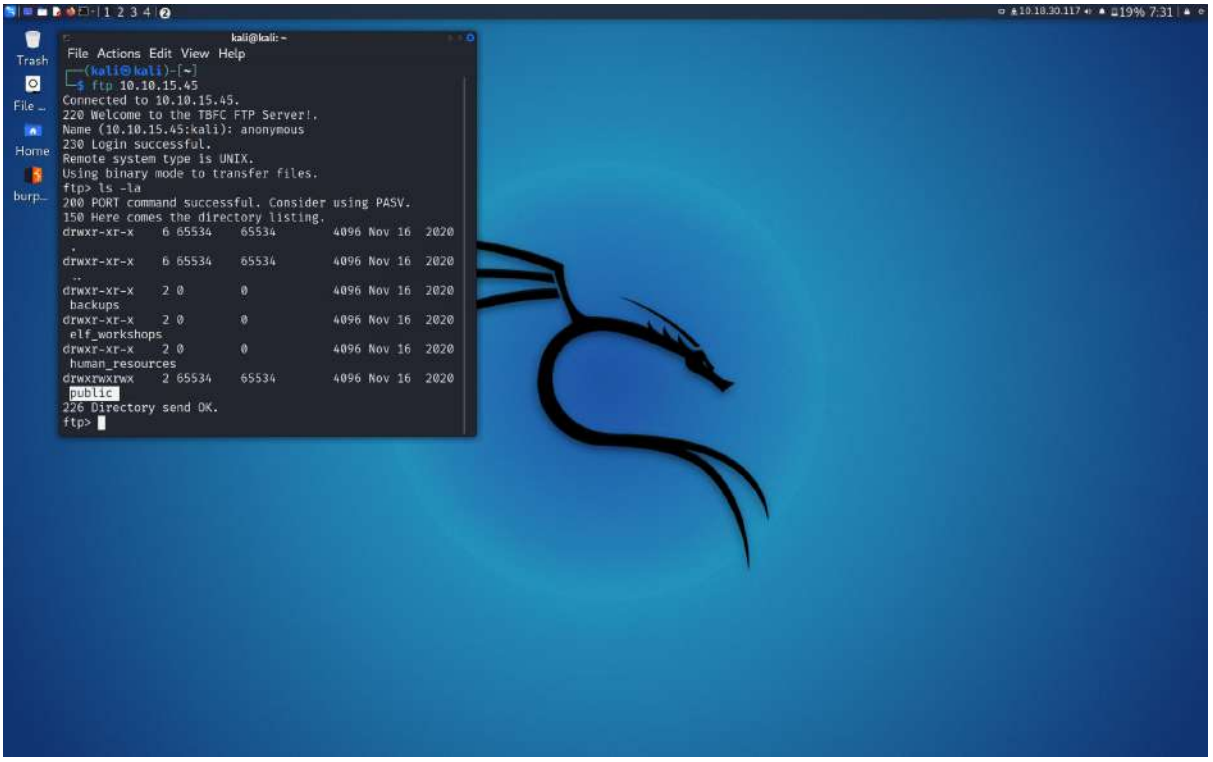
Solution/walkthrough:

<u>Question 1</u>

Ftp the IP address from TryHackMe and then name as anonymous

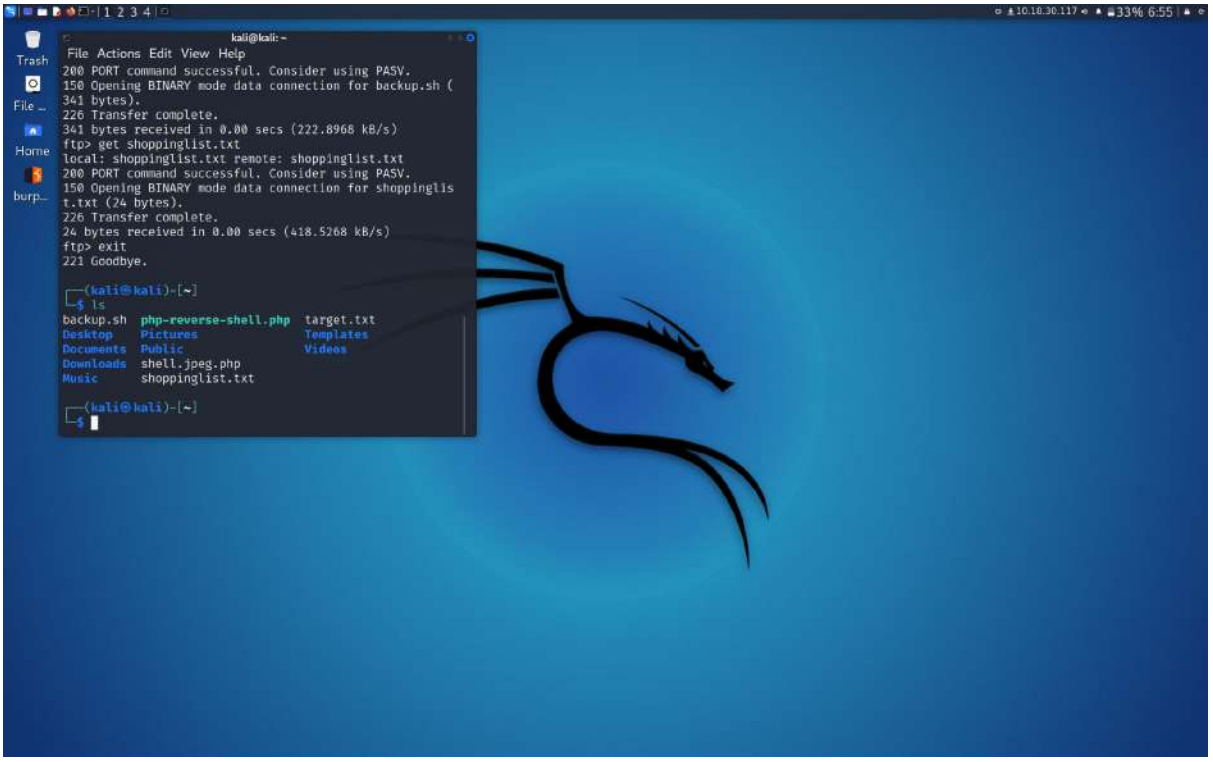


Type ls *-la* and it will show you the public

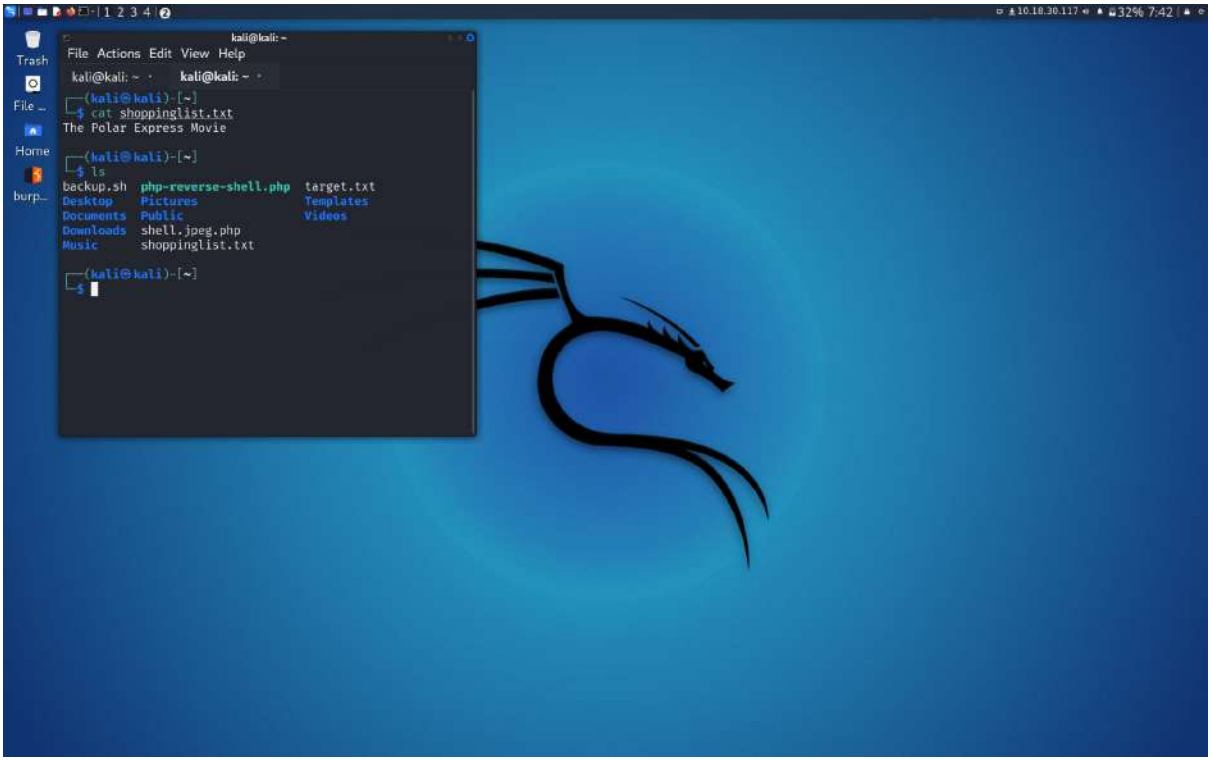


Question 2

List will be shown below after entering the *backup.sh* and *shoppinglist.txt*

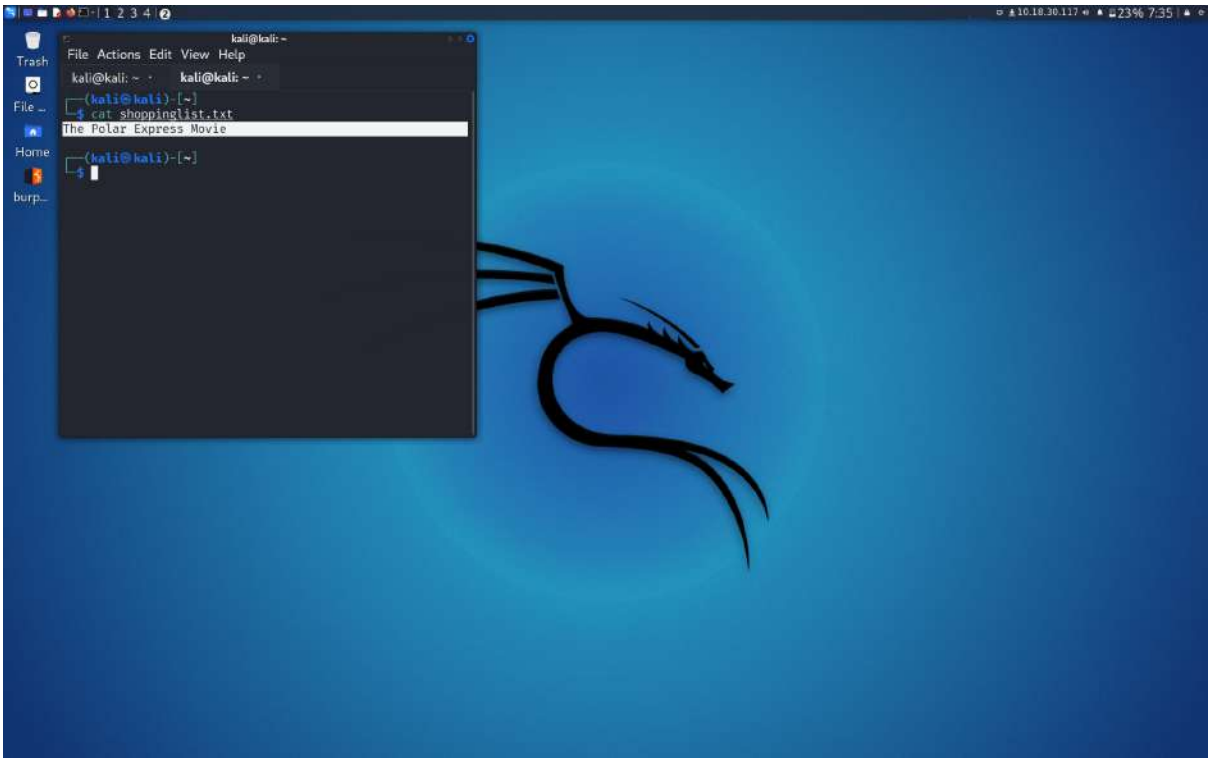


Type *ls* for the list, and it will show you *backup.sh*



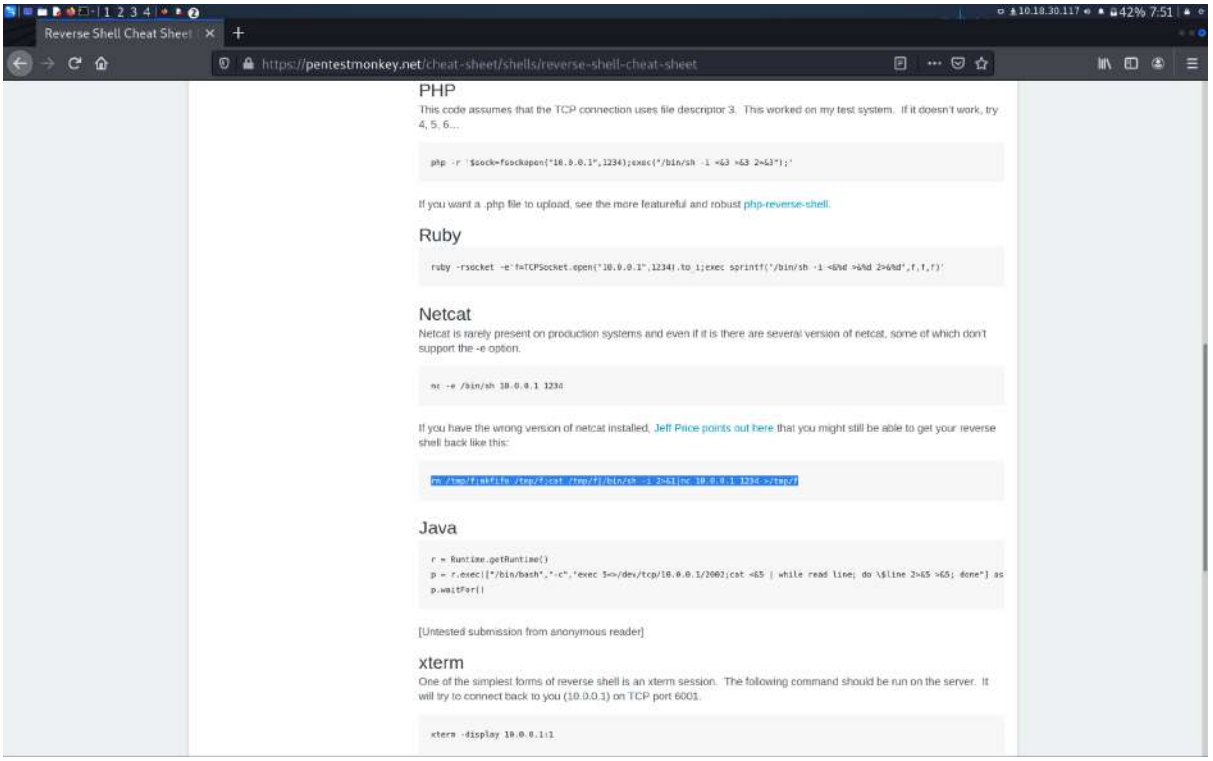
Question 3

On the other new tab, type *cat shoppinglist.txt* and you will be able to see what movie did Santa have on his Christmas shopping list

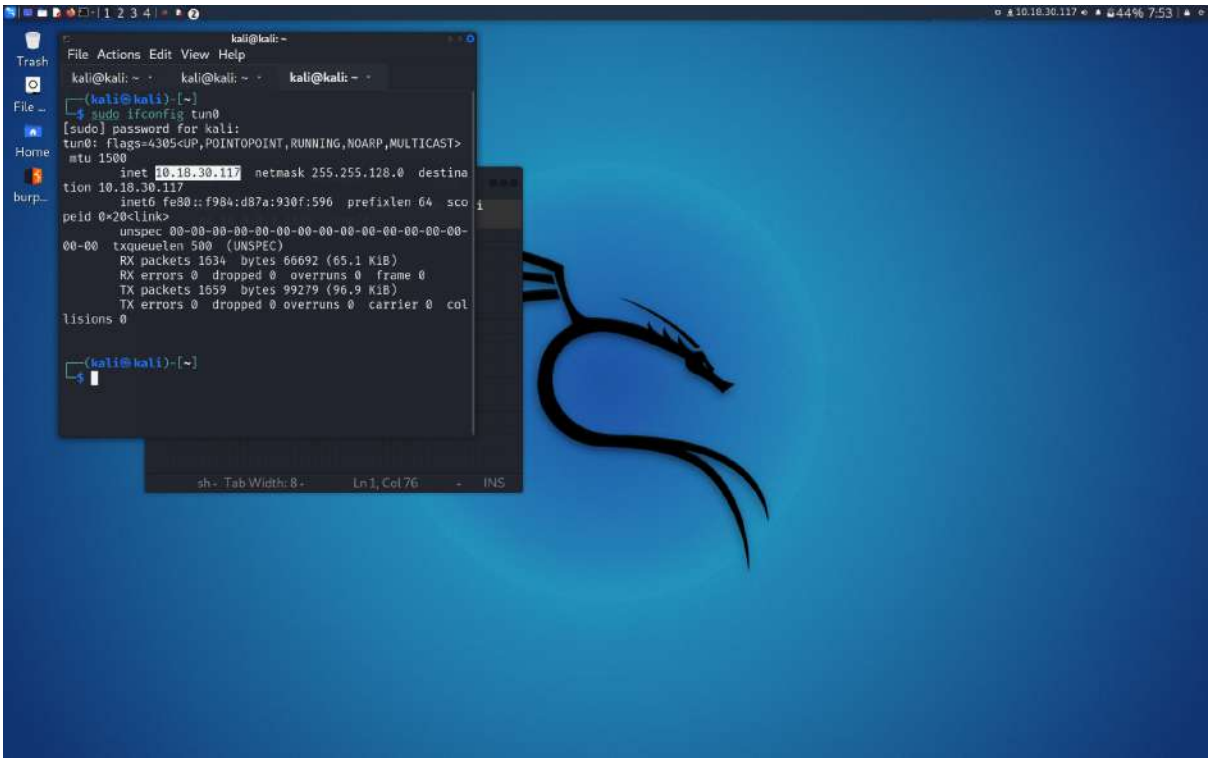


Question 4

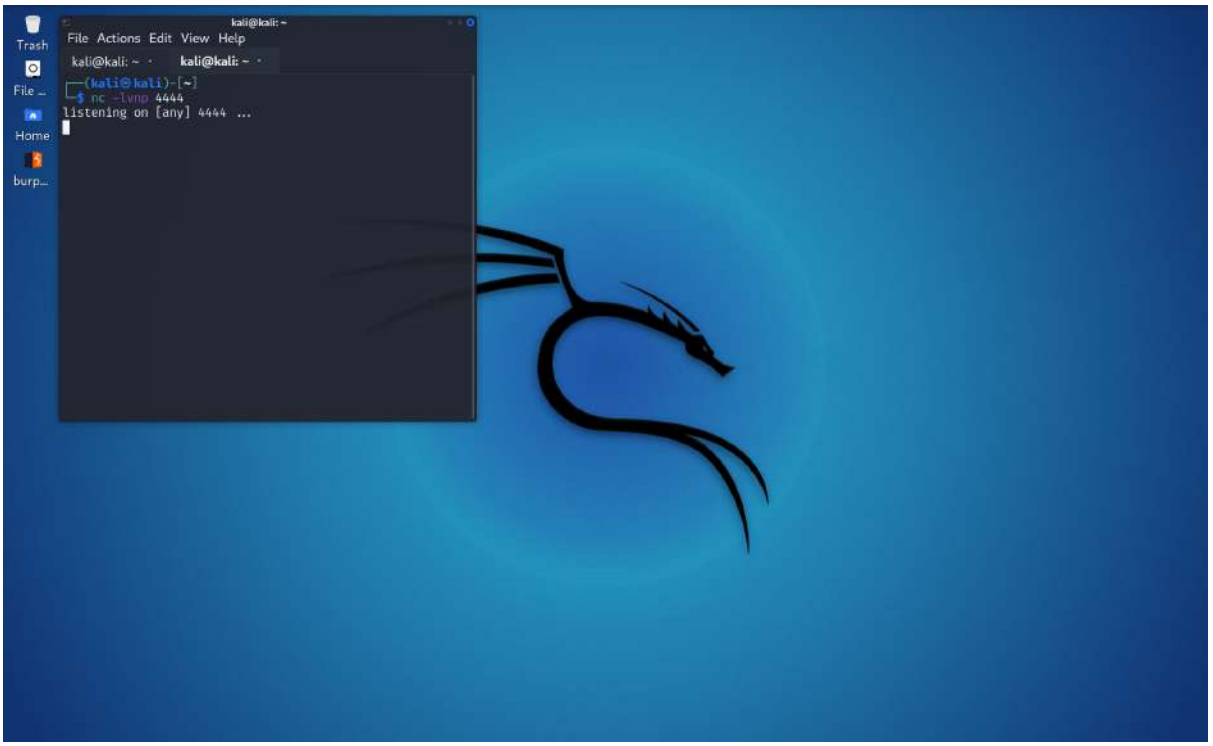
Browse *reverse shell pentestmonkey* and look for the *Netcat*



Type *sudo ifconfig tun0* . Thus enter the password to copy down the IP address



Open a new *terminal* tab. Hence, type nc *-lvnp 4444*



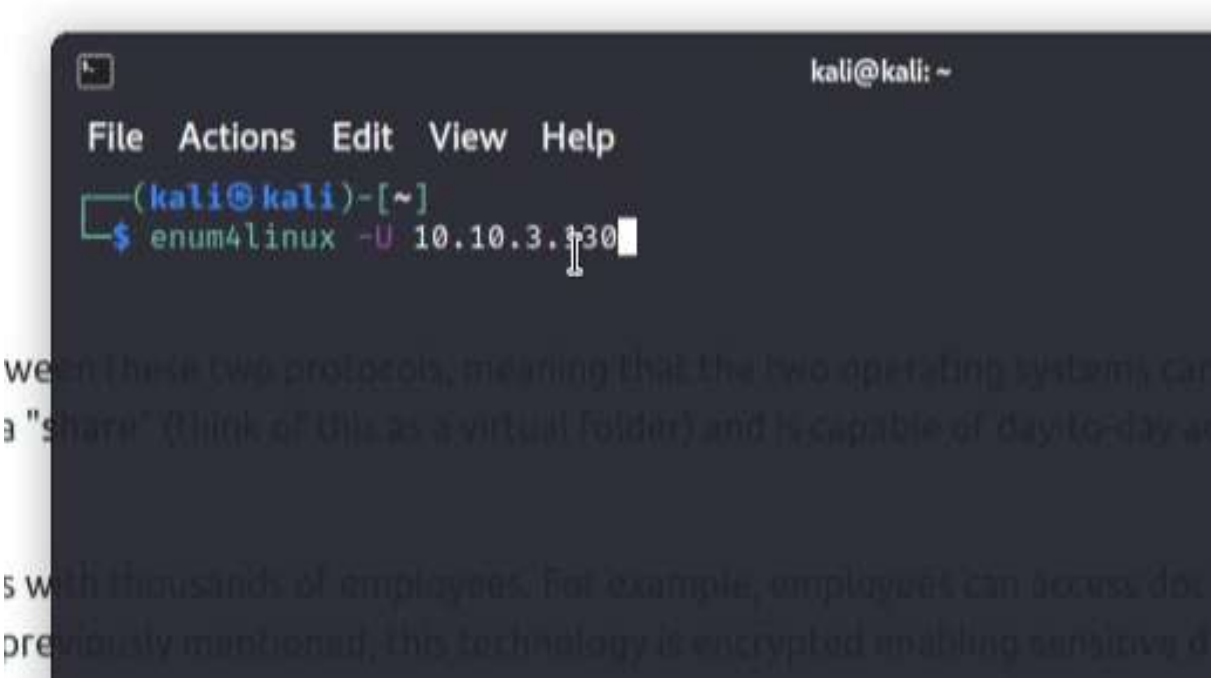
View the file using *cat flag.txt* command

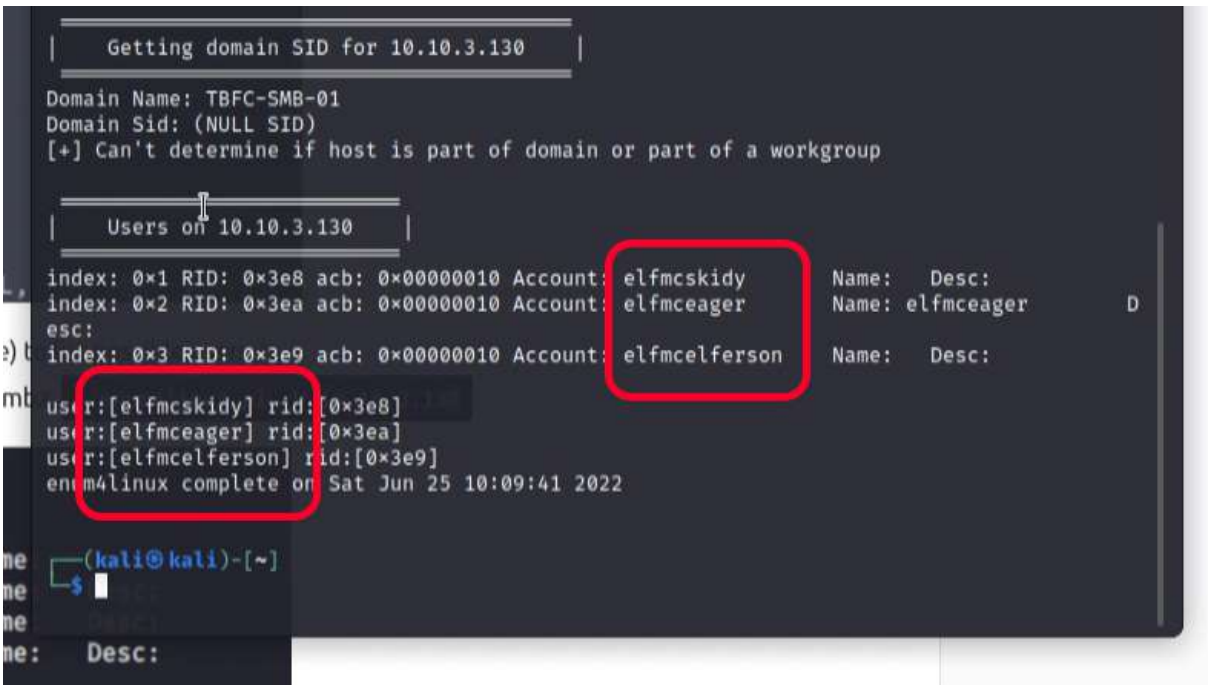
```
root
root@tbfc-ftp-01:~# ls
ls
flag.txt
root@tbfc-ftp-01:~# cat flag.txt
cat flag.txt
THM{even_you_can_be_santa}
root@tbfc-ftp-01:~#
```

Thought Process/Methodology:

This task doesn't really use the web browser, any browser can do it. First of all, copy and paste the IP address into the *terminal* and add *ftp* in front of it. *FTP* is also known as file transfer protocol. Later on, type *ls -la* to show you the directory listing and public. After type get *shoppinglist.txt* and *backup.sh*, enter exit and type *ls* to show the list. At the tool bar, click file and add a new tab to proceed. type *cat shoppinglist.txt* and you will be able to see what movie Santa has on his Christmas shopping list. On the other hand, browse *reverse shell pentestmonkey* on any browser and look for the Netcat. After setting up, type *sudo ifconfig tun0*, enter the password to copy down the IP address. Wait a while for the *Netcat listener* on the device. Last but not least, type *cat flag.txt* and it will show the answer.

<u>Day 10: Don't be sElfish!</u>
Tools used: Kali Linux
Solution/walkthrough:
<u>Question 1</u>
After connecting to the machine ip, open the *terminal* and type *enum4linux -U 10.10.3.130*





Question 2

Type the command *enum4linux -S 10.10.3.130*

```
index: 0×2 RID: 0×3ea acb: 0×00000010 Account: elfmceager
esc:
index: 0×3 RID: 0×3e9 acb: 0×00000010 Account: elfmcelferso

user:[elfmcskidy] rid:[0×3e8]
user:[elfmceager] rid:[0×3ea]
user:[elfmcelferson] rid:[0×3e9]
enum4linux complete on Sat Jun 25 10:09:41 2022

┌──(kali㉿kali)-[~]
└─$ enum4linux -S 10.10.3.130
```

```
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ==========================================
|    Share Enumeration on 10.10.3.130      |
 ==========================================

        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

[+] Attempting to map shares on 10.10.3.130
//10.10.3.130/tbfc-hr   Mapping: DENIED, Listing: N/A
//10.10.3.130/tbfc-it   Mapping: DENIED, Listing: N/A
```

Question 3

Type *smbclient //10.10.3.130/tbfc-santa*

```
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        TBFC-SMB-01          TBFC-SMB

[+] Attempting to map shares on 10.10.3.130
//10.10.3.130/tbfc-hr   Mapping: DENIED, Listing: N/A
//10.10.3.130/tbfc-it   Mapping: DENIED, Listing: N/A
//10.10.3.130/tbfc-santa        Mapping: OK, Listing: OK
//10.10.3.130/IPC$      [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
enum4linux complete on Sat Jun 25 10:14:07 2022


┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.3.130/tbfc-santa
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \>
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.3.130/tbfc-santa
Enter WORKGROUP\kali's password:
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

                10252564 blocks of size 1024. 5369392 blocks available
smb: \>
```

Question 4

After logging in using *tbfc-santa*, change the local working directory to *Music/* and type *get note_from_mcskidy.txt*

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.3.130/tbfc-santa
Enter WORKGROUP\kali's password:
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

                10252564 blocks of size 1024. 5369392 blocks available
smb: \> cat note_from_mcskidy.txt
cat: command not found
smb: \> lcd Music/
smb: \> get note_from_mcskidy.txt
getting file \note_from_mcskidy.txt of size 143 as note_from_mcskidy.txt (0.1 KiloBytes/s
ec) (average 0.1 KiloBytes/sec)
smb: \>
```

Open a new *terminal*, change the directory to *Music/* and view the *note_from_mcskidy.txt*

```
kali@kali: ~/Music
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ cd /home/kali/Music

┌──(kali㉿kali)-[~/Music]
└─$ ls
note_from_mcskidy.txt

┌──(kali㉿kali)-[~/Music]
└─$ cat note_from_mcskidy.txt
Hi Santa, I decided to put all of your favourite jingles onto this share - allowing you ac
cess it from anywhere you like! Regards ~ ElfMcSkidy

┌──(kali㉿kali)-[~/Music]
└─$
```

Thought Process/Methodology:
After starting the machine on *TryHackMe*, we can directly search for enum4linux or type *enum4linux* in the terminal. In *enum4linux*, *-U* is used to get a userlist which we can type the following command: *enum4linux -U 10.10.3.130* to get all the user list. Other than that, *-S* in *enum4linux* is used to get a sharelist which we can type this command: *enum4linux -S 10.10.3.130* to know the shares. After that, it shows 4 shares and one of them has "*Mapping: OK, Listing: OK*" which is *//10.10.3.130/tbfc-santa*. We can log in using the login command: *smbclient //10.10.3.130/tbfc-santa* and the password is no password. When we are logged in, we can type *ls* for listing all the files contained inside and files consist of *jingle-tunes* and *note_from_mcskidy.txt*. Then, we need to look inside the *.txt* file where we can type *lcd Music/* to change the local working directory and *get note_from_mcskidy.txt* to move the file to *Music/*. Lastly, we open a new *terminal* and change the directory using *cd Music/* to view the *.txt* file using command *cat note_from_mcskidy.txt*.