Report PSP0201 T2130 - Tutorial Week 3

Group: **Marceline**

ID	Name	Role
1211100899	Muhammad Shahril Aiman	Leader
1211101533	Muhammad Aniq Fahmi	member
1211101303	Aiman Faris	member
1211102759	Muhammad Zaquan	member

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

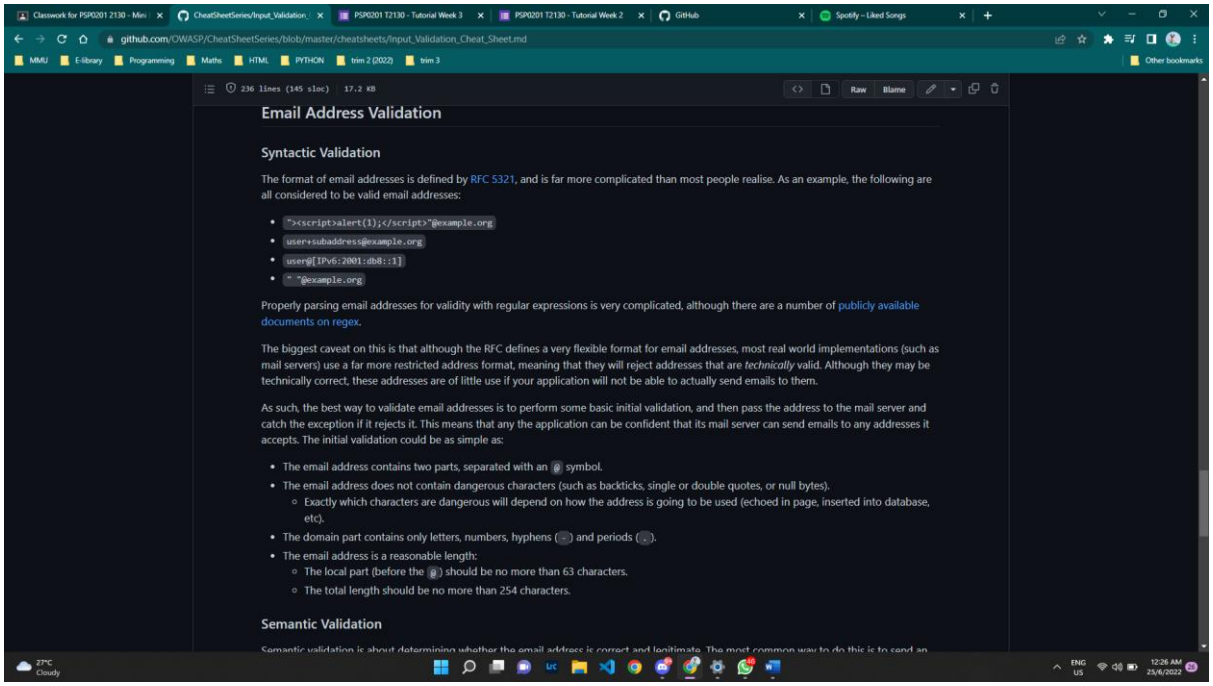
Tools used: Kali Linux, Firefox, OWASP

Solution/walkthrough:

Question 1: Examine the OWASP Cheat Sheet. Match the input validation level with the correct description.

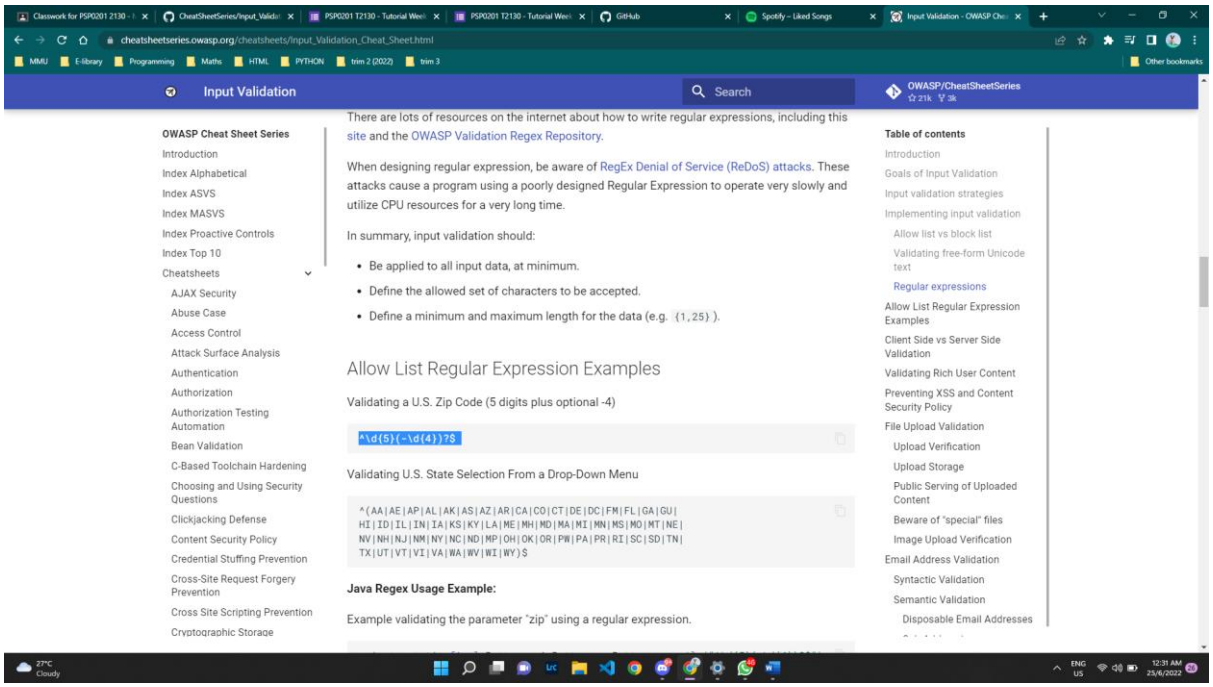
-enforce correct syntax of structured fields (SYNTHETIC)

-enforce correctness of their values in the specific business context (SEMANTIC)



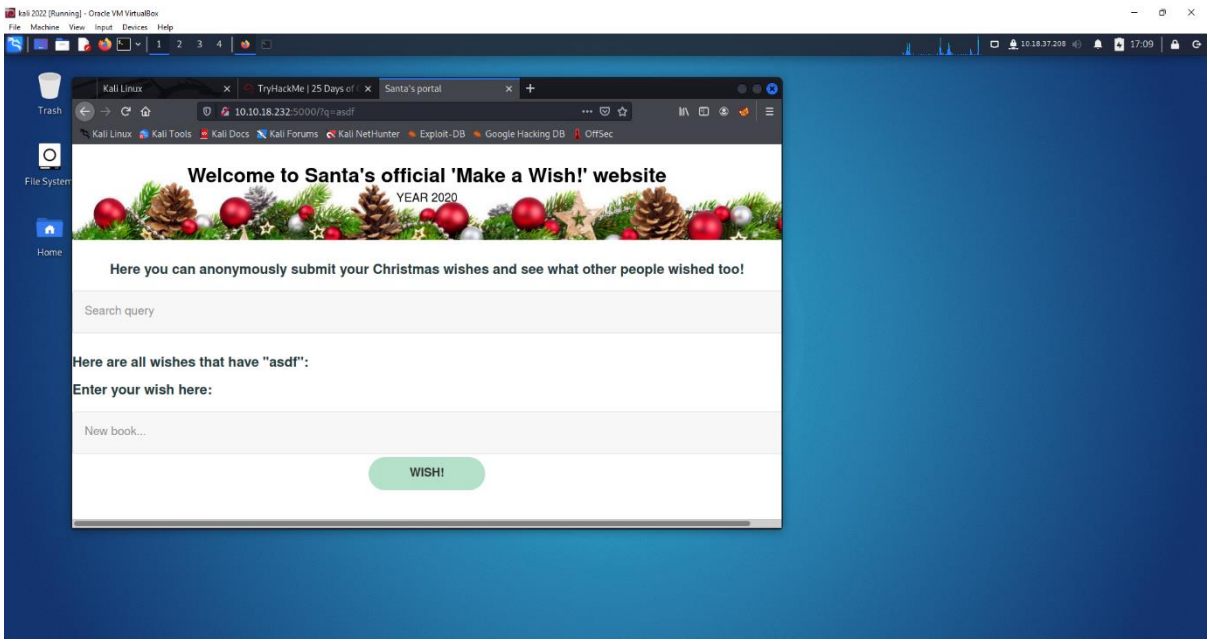
QUESTION 2: Examine the OWASP Cheat Sheet. What is the regular expression used to validate a US Zip code?

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



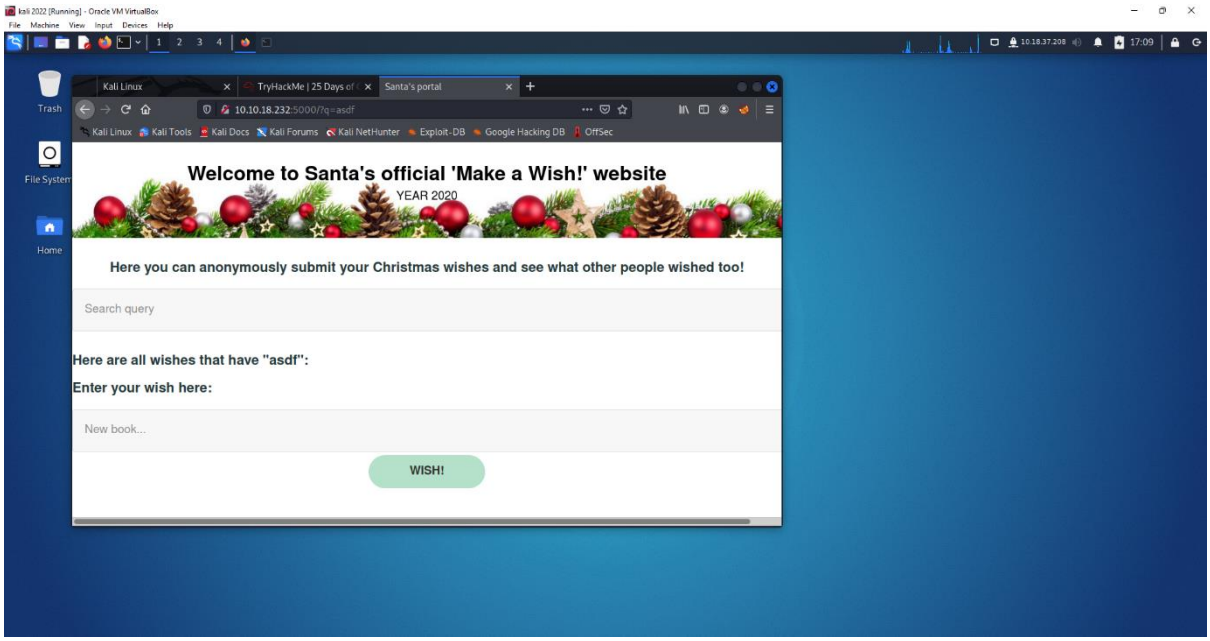
Question 3: What vulnerability type was used to exploit the application?

ANSWER: Stored



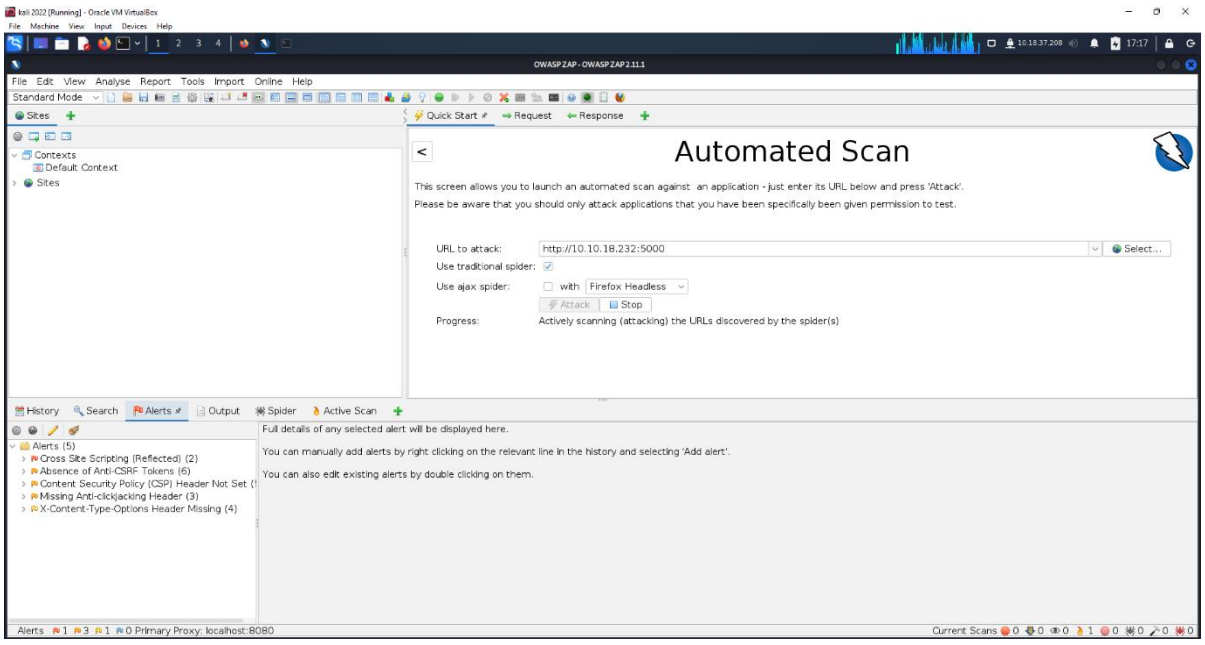
QUESTION 4: What query string can be abused to craft a reflected XSS?

ANSWER: q



QUESTION 5: Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts of high priority are in the scan?

ANSWER: 2

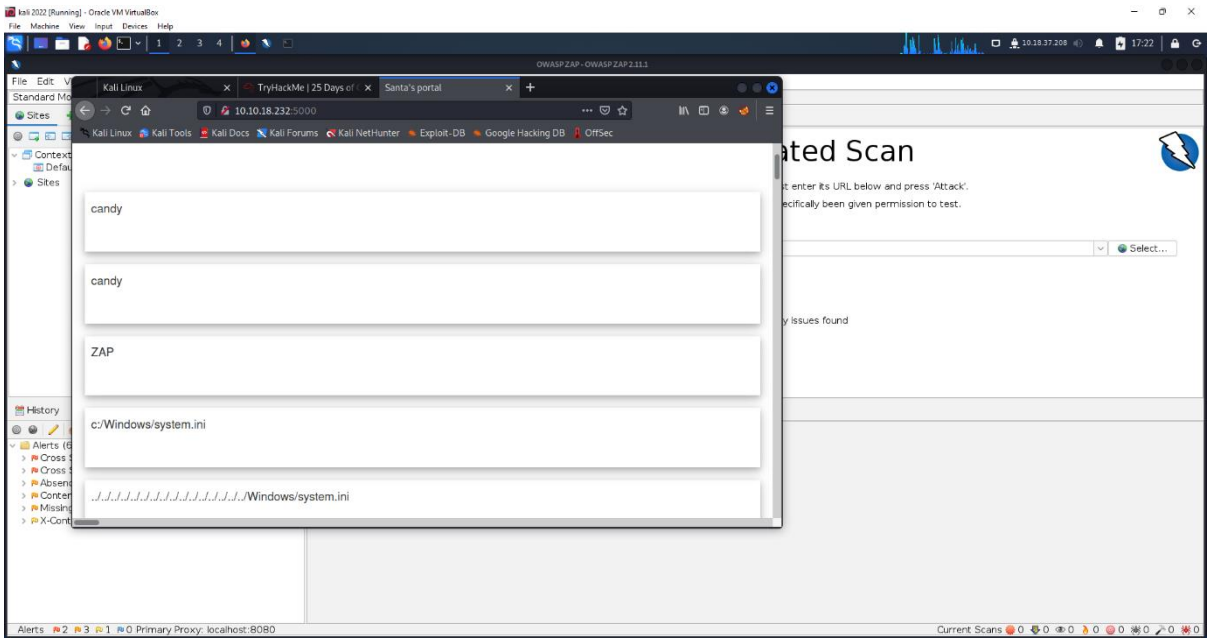


QUESTION 6: What JavaScript code should you put in the wish text box if you want to show an alert saying "PSP0201"?

ANSWER: <script>alert('PSP2021')</script>

QUESTION 7: Close your browser and revisit the site MACHINE-IP:5000 again. Does your XSS attack persist?

ANSWER: YES



METHODOLOGY:

Firstly, I open the try hack and read the question. So, the first question, I read at the OWASP Cheat Sheet to answer the Q1. For Q2 I use the OWASP Cheat Sheet to check the regular expression used to validate a US Zip code. We check and get the answer for Q2. Then for Q3, I start the machine, got the Ip address and paste it to the Firefox. It will lead us to “welcome to Santa official make a wish website”. I put the wish that I wanted and enter it. Then, the data store and it means Stored vulnerability. So, for the Q4, I already entered my wish and its show the URL show “q” at first of the URL. So, the query string is “q” can be abused to craft a reflected XSS. For the Q5, I open the OWASP and put the ip address to scan the website at there and the OWASP will check there have error or not. They show 2 error at Alert Section. For the Q6, I open the Santa’s wish website to put the command at the wish, so the code that I put is “<script>alert('PSP2021')</script>”. After that, the website shows error. Lastly for the Q7, I re check the website and put a new wish at the Santa’s wish website, our XSS attack persist still can attack the website.

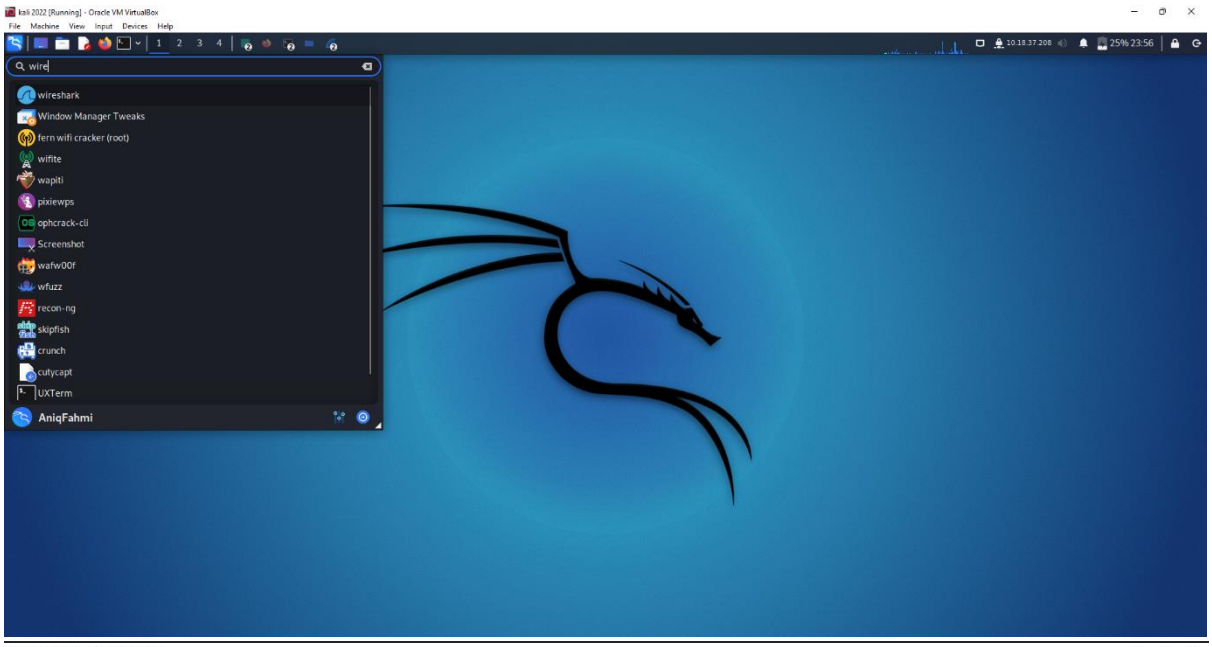
Day 7: Web Exploitation -- The Grinch Really Did Steal Christmas

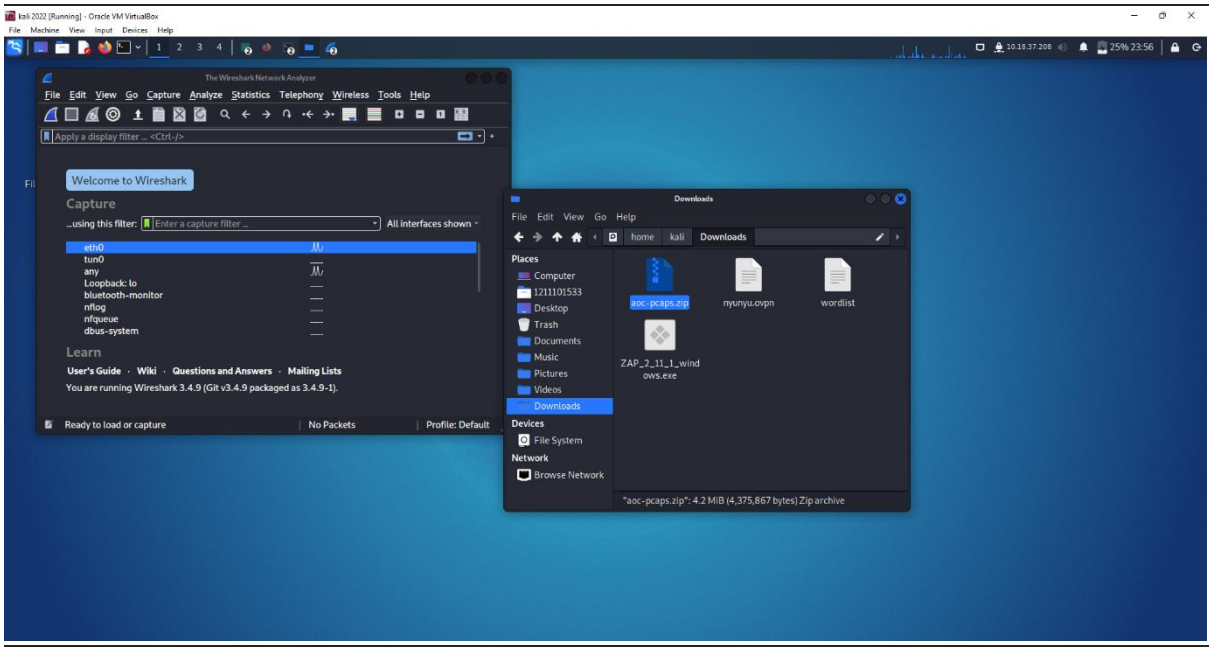
Tools used: Kali Linux, Firefox, Wireshark

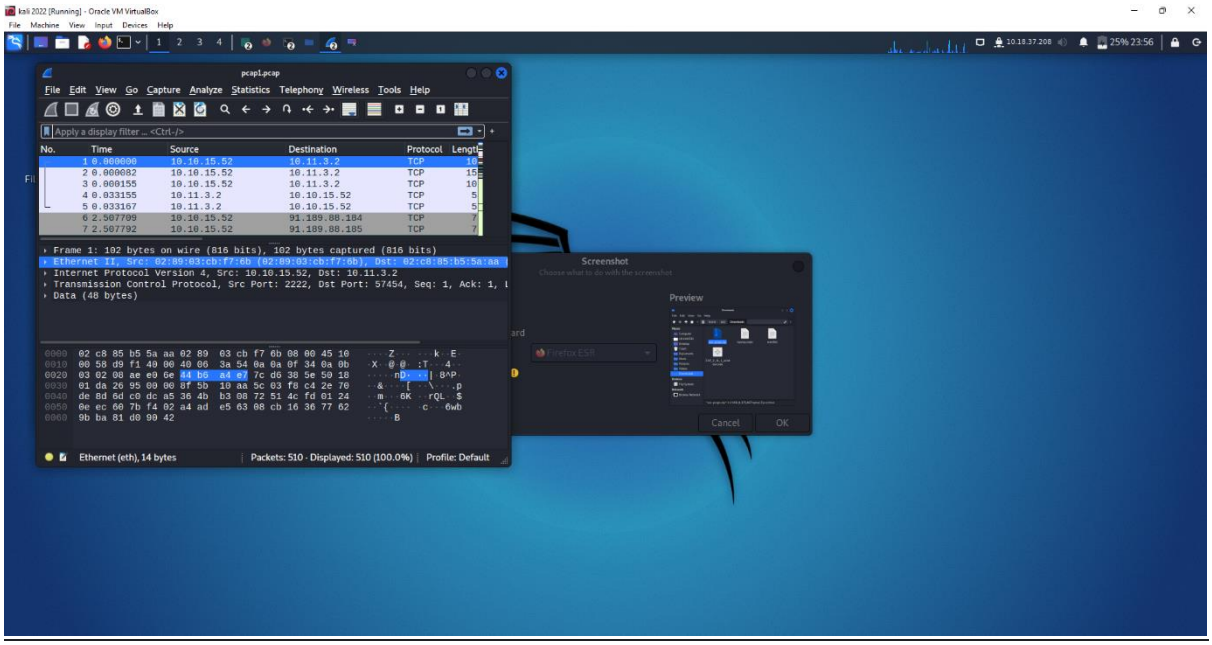
Solution/walkthrough:

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

ANSWER: 10.11.3.2

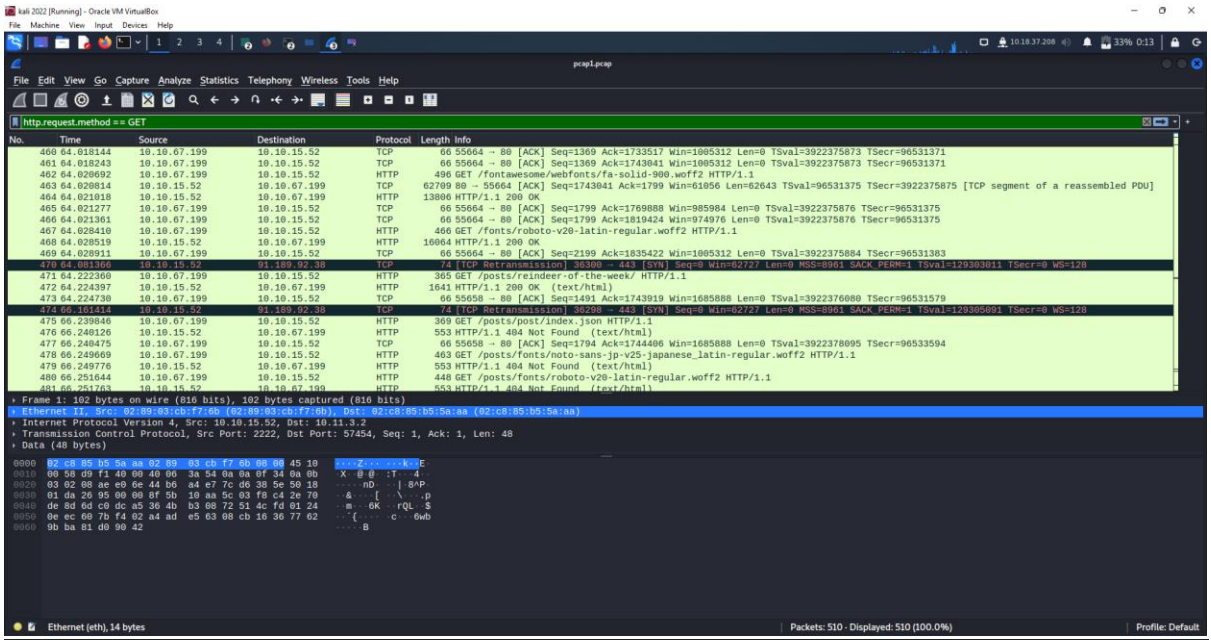






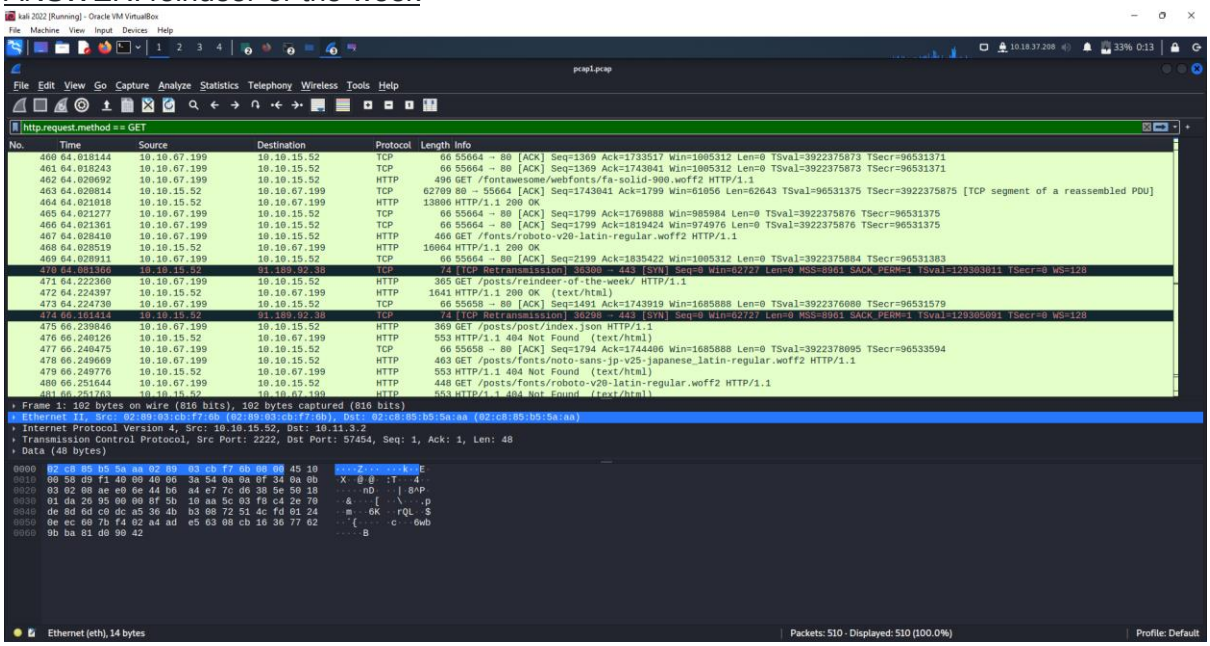
QUESTION 2: If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

ANSWER: http.request.method == GET



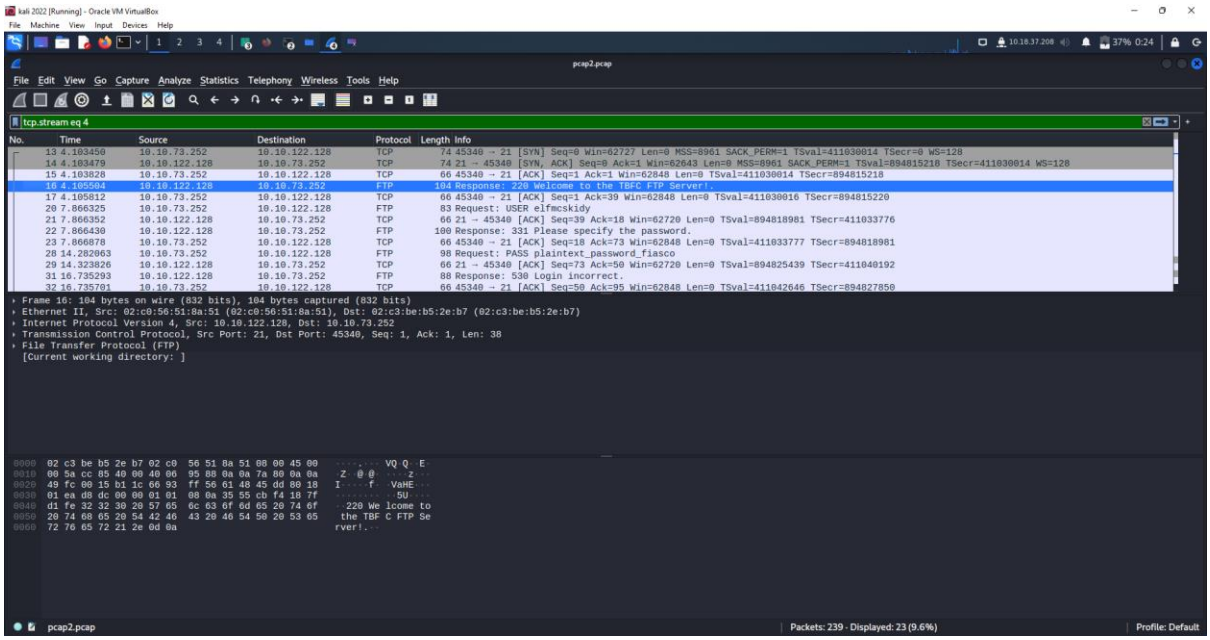
QUESTION 3: Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "**10.10.67.199**" visited

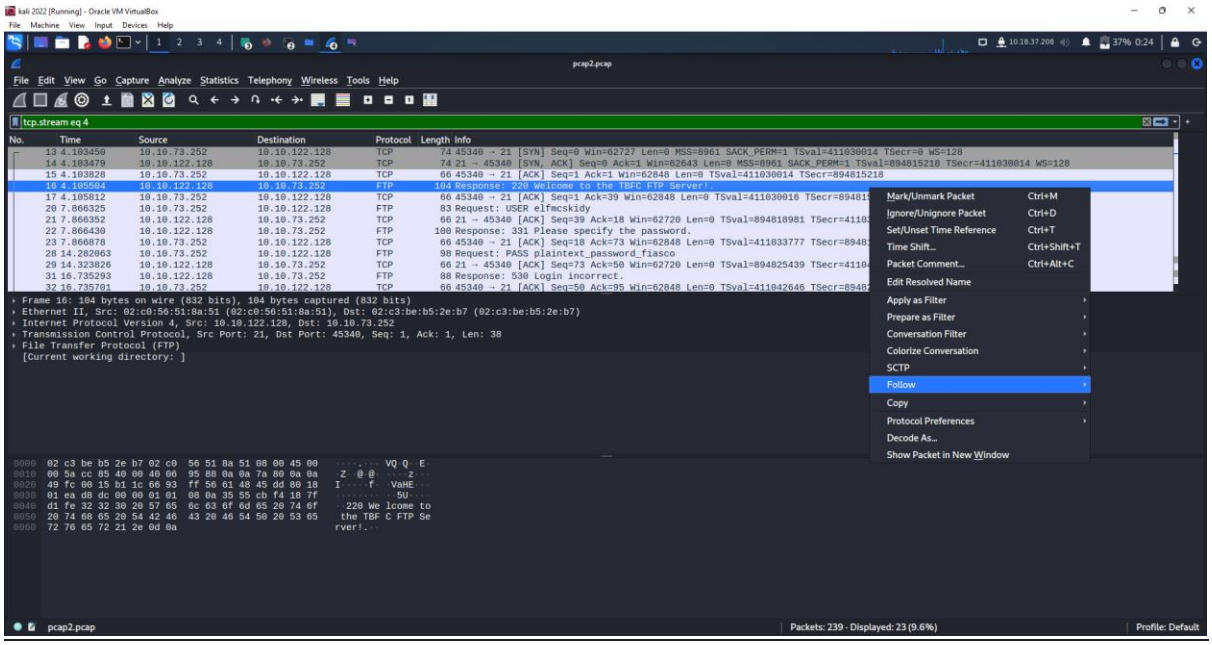
ANSWER: reindeer-of-the-week

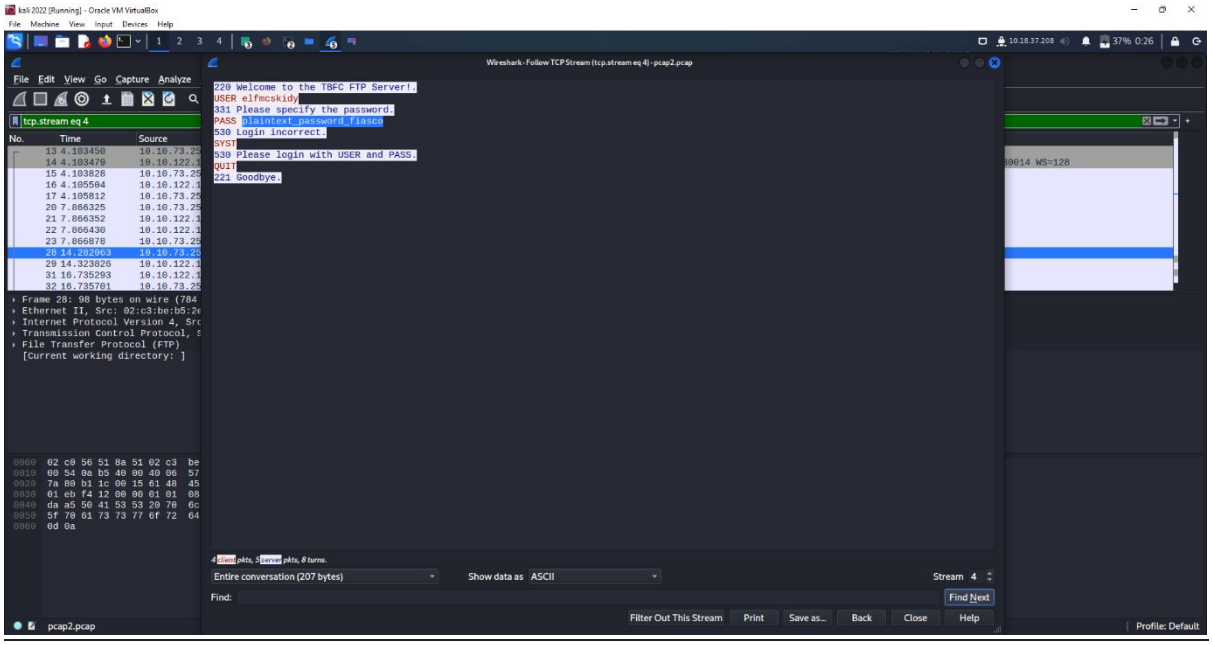


QUESTION 4: Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process?

ANSWER: plaintext_password_fiasco

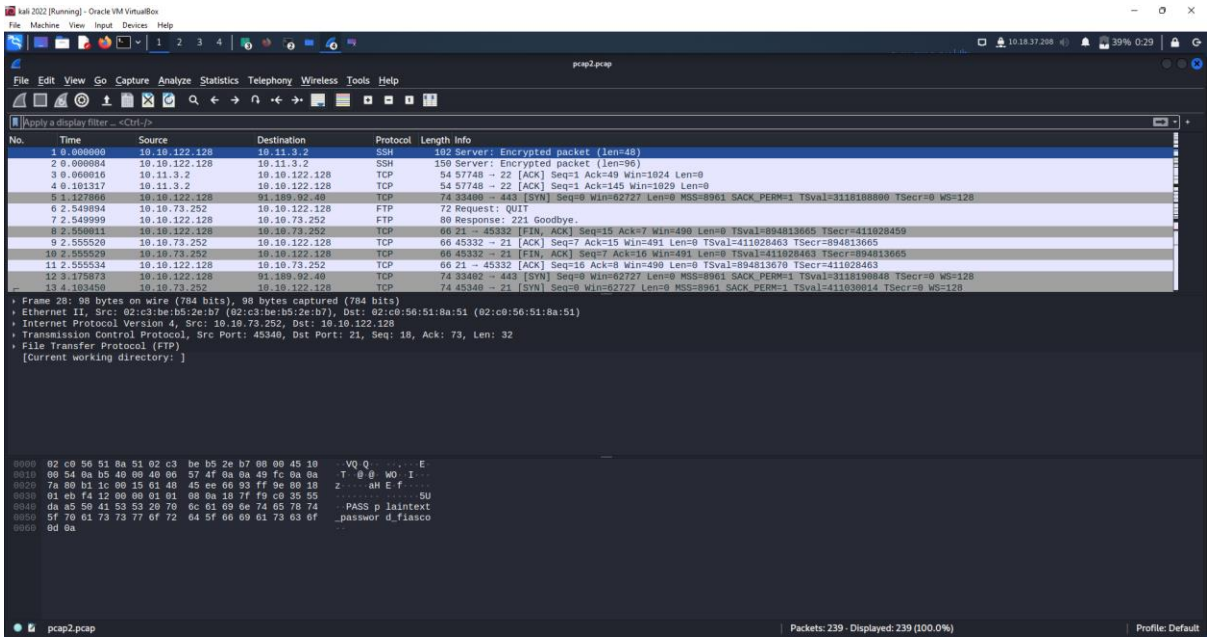



kali 2022 [Running] - Oracle VM VirtualBox
pcap2.pcap
tcp.stream eq 4
No. Time Source Destination Protocol Length Info
13 4.103450 10.10.73.252 10.10.122.128 TCP 74 45340 → 21 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=411030014 TSecr=0 WS=128
14 4.103479 10.10.122.128 10.10.73.252 TCP 74 21 → 45340 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM=1 TSval=894815216 TSecr=411030014 WS=128
15 4.103828 10.10.73.252 10.10.122.128 TCP 66 45340 → 21 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=411030014 TSecr=894815218
16 4.105504 10.10.122.128 10.10.73.252 FTP 104 Response: 220 Welcome to the TBFC FTP Server!.
17 4.105812 10.10.73.252 10.10.122.128 TCP 66 45340 → 21 [ACK] Seq=1 Ack=39 Win=62848 Len=0 TSval=411030016 TSecr=894815
20 7.866325 10.10.73.252 10.10.122.128 FTP 83 Request: USER elfmcskidy
21 7.866352 10.10.122.128 10.10.73.252 TCP 66 21 → 45340 [ACK] Seq=39 Ack=18 Win=62720 Len=0 TSval=894818981 TSecr=4110
22 7.866430 10.10.122.128 10.10.73.252 FTP 100 Response: 331 Please specify the password.
23 7.866878 10.10.73.252 10.10.122.128 TCP 66 45340 → 21 [ACK] Seq=18 Ack=73 Win=62848 Len=0 TSval=411033777 TSecr=8948
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=62720 Len=0 TSval=894825439 TSecr=4110
31 16.735293 10.10.122.128 10.10.73.252 FTP 88 Response: 530 Login incorrect.
32 16.735701 10.10.73.252 10.10.122.128 TCP 66 45340 → 21 [ACK] Seq=50 Ack=95 Win=62848 Len=0 TSval=411042646 TSecr=8948
Frame 16: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c3:be:b5:2e:b7 (02:c3:be:b5:2e:b7)
Internet Protocol Version 4, Src: 10.10.122.128, Dst: 10.10.73.252
Transmission Control Protocol, Src Port: 21, Dst Port: 45340, Seq: 1, Ack: 1, Len: 38
File Transfer Protocol (FTP)
[Current working directory:]
0000 02 c3 be b5 2e b7 02 c0 56 51 8a 51 08 00 45 00
0010 00 5a cc 85 40 00 40 06 95 88 0a 0a 7a 80 0a 0a
0020 49 fc 00 15 b1 1c 66 93 ff 56 61 48 45 dd 80 18
0030 01 ea d8 dc 00 00 01 01 08 0a 35 55 cb f4 18 7f
0040 d1 fe 32 32 30 20 57 65 6c 63 6f 6d 65 20 74 6f
0050 20 74 68 65 20 54 42 46 43 20 46 54 50 20 53 65
0060 72 76 65 72 21 2e 0d 0a
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
pcap2.pcap
Packets: 239 · Displayed: 23 (9.6%)
Profile: Default


kali 2022 [Running] - Oracle VM VirtualBox
Wireshark · Follow TCP Stream (tcp.stream eq 4) · pcap2.pcap
220 Welcome to the TBFC FTP Server!.
USER elfmcskidy
331 Please specify the password.
PASS plaintext_password_fiasco
530 Login incorrect.
SYST
530 Please login with USER and PASS.
QUIT
221 Goodbye.
4 client pkts, 5 server pkts, 8 turns.
Entire conversation (207 bytes)
Show data as ASCII
Stream 4
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
pcap2.pcap
Profile: Default

QUESTION 5 : Continuing with our analysis of "pcap2.pcap", what is the name of the protocol that is encrypted?

ANSWER: SSH

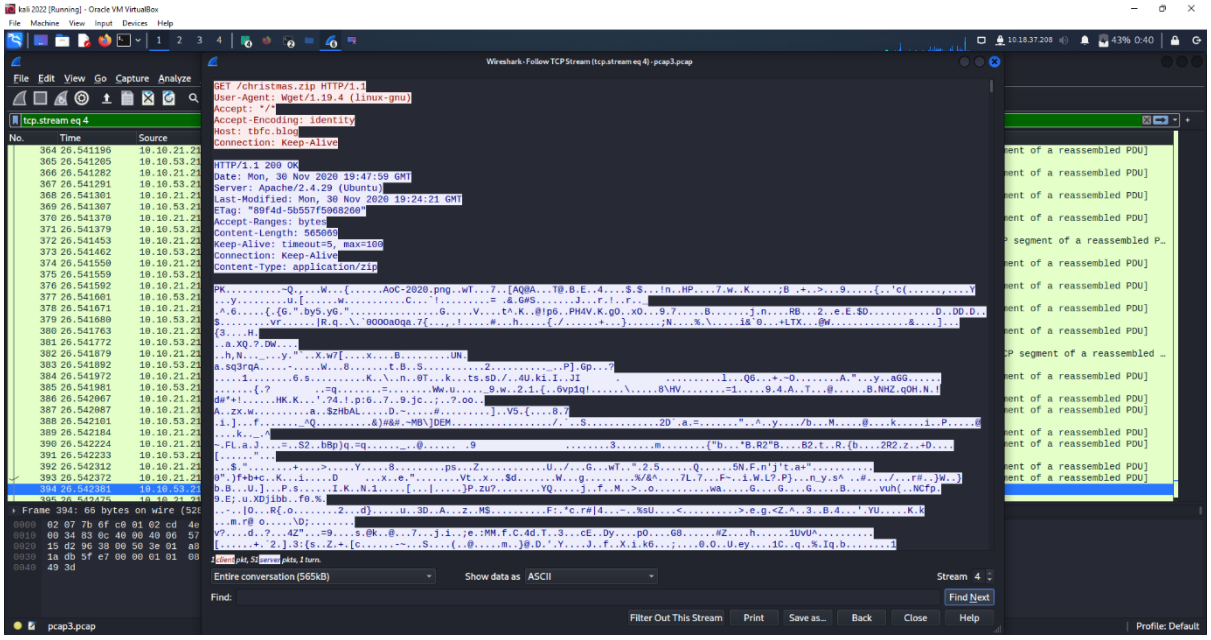


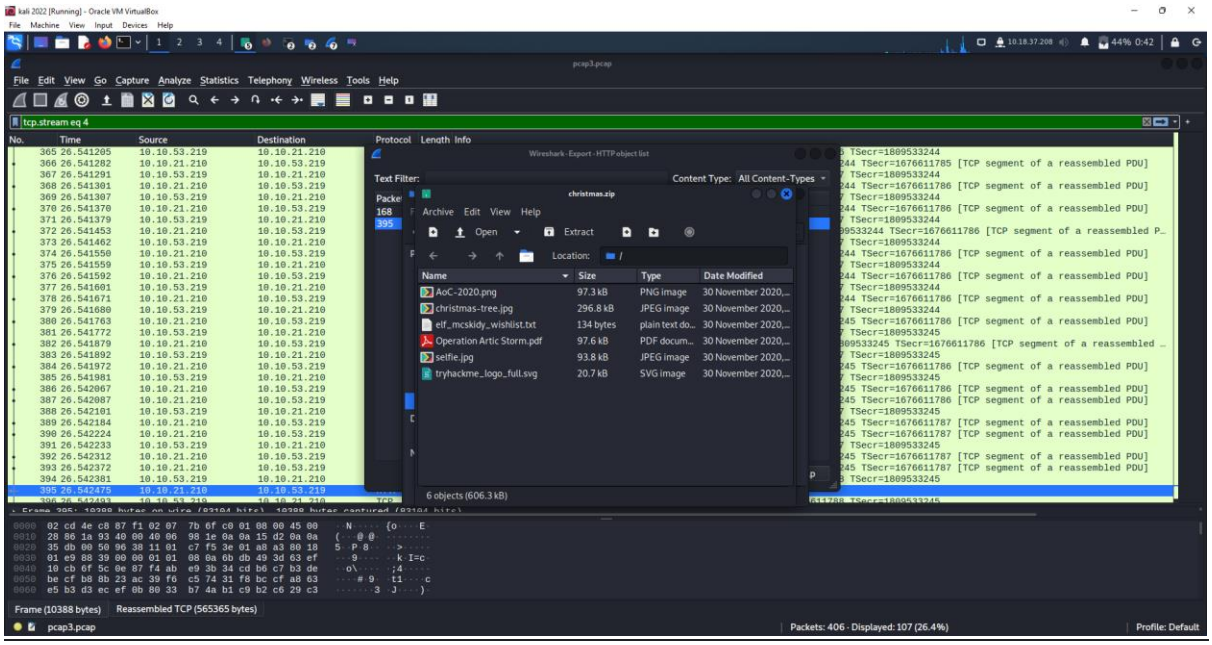
QUESTION 6: Examine the ARP communications. Who has 10.10.122.128? Tell 10.10.10.1. Answer: 10.10.122.128 is at

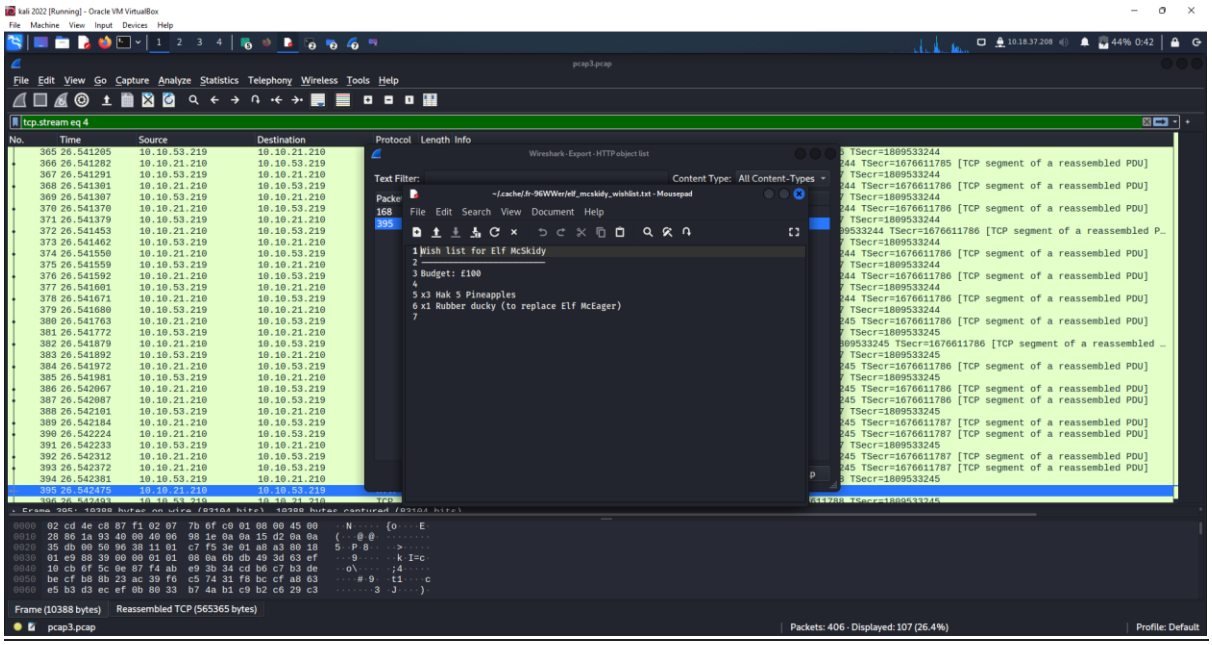
ANSWER: 02:c0:56:51:8a:51

QUESTION 7: Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

ANSWER: RUBBER DUCKY

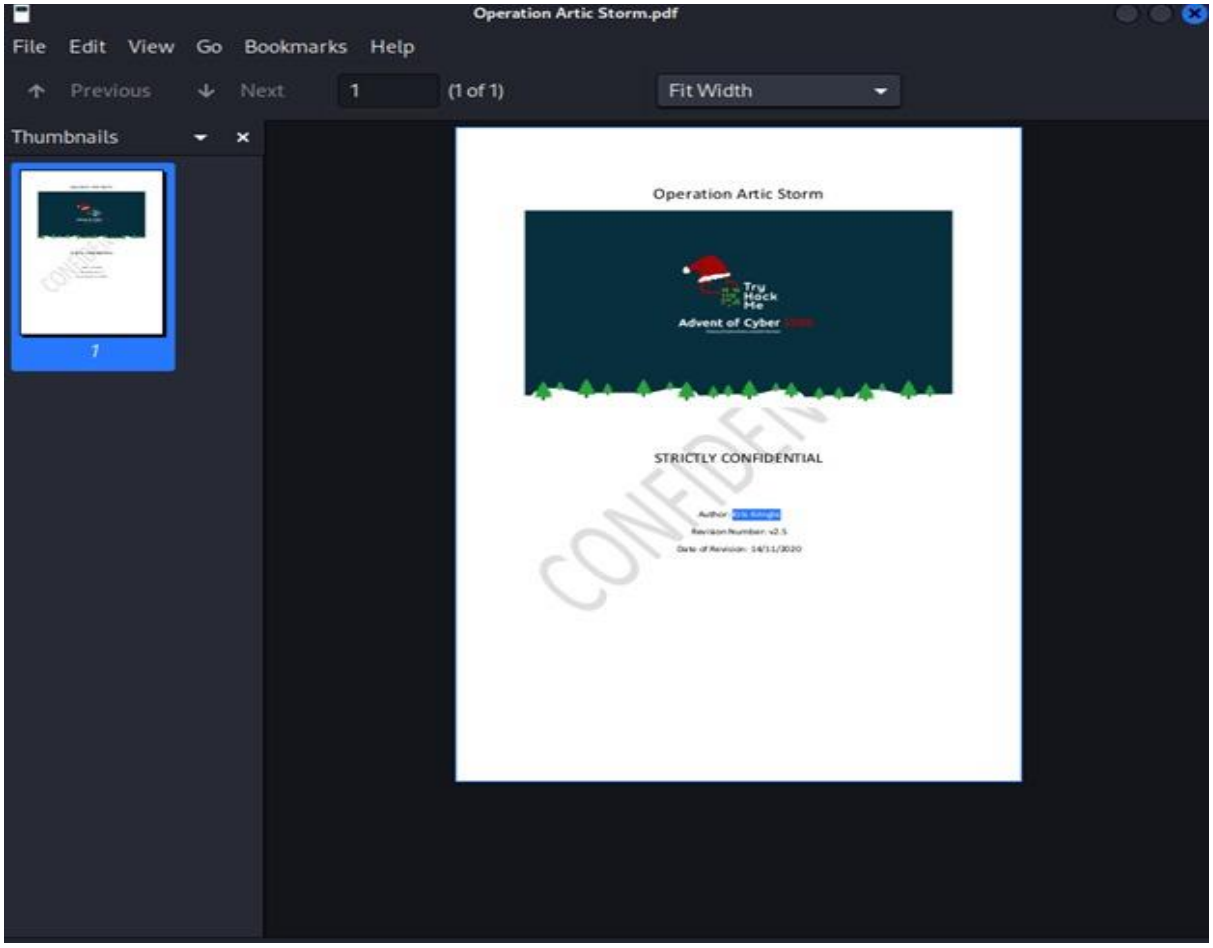






QUESTION 8 : Who is the author of Operation Artic Storm?

ANSWER: Kris Kringle



METHODOLOGY:

Firstly, I open the try hack and read the question. I download the file that shows at the tryhackme. After that, I open Wireshark at my application on my kali Linux. Then I open the pcap1.pcap at Wireshark and that's for the Q1. For the Q2, I use filter "http.request.method == GET" at the url section. This thing will show HTTP GET requests in our "pcap1.pcap" file. After that, the Q3 asked me to find the the name of the article that the IP address "10.10.67.199" visited. The name of the article is "reindeer-of-the-week". So, for the Q4, I open the pcap2.pcap. I find where the login was successful. Then, I follow the Ip address and lead us to the leaked password. For Q5, I checked the name of the protocol that is encrypted is SSH. After that Q6, I examine the ARP communication, and it says 02:c0:56:51:8a:51 at the Answer: 10.10.122.128. Then, for Q7, I open the code that leads us to Elf McEager, and we download it and shows the Wishlist of Elf McEager, at that text. For the last question, I open the file that I downloaded it at pcap3.pcap and open it. The author of Operation Artic Storm is Kris Kringle.

Day 8 - What's Under the Christmas Tree?

Tools used: AttackBox

Solution/Walkthrough:

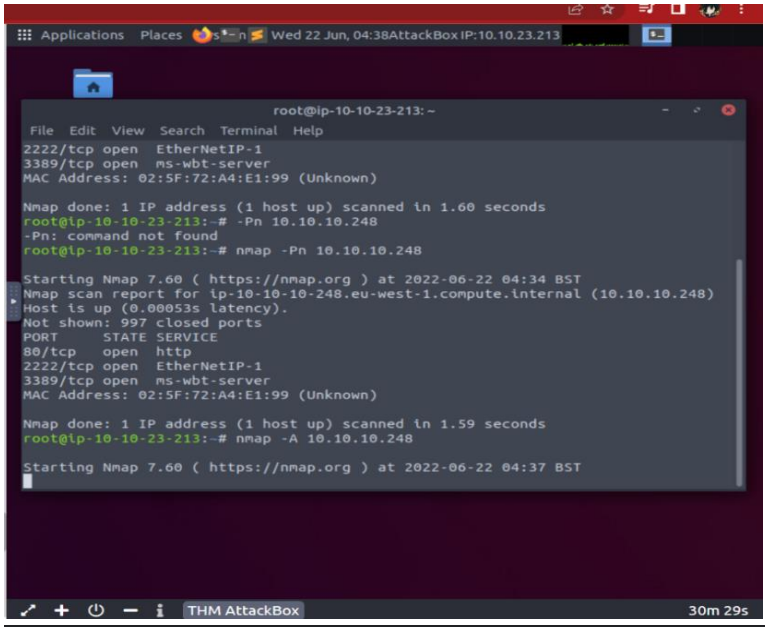
Question 1:

When was Snort created?

=1998

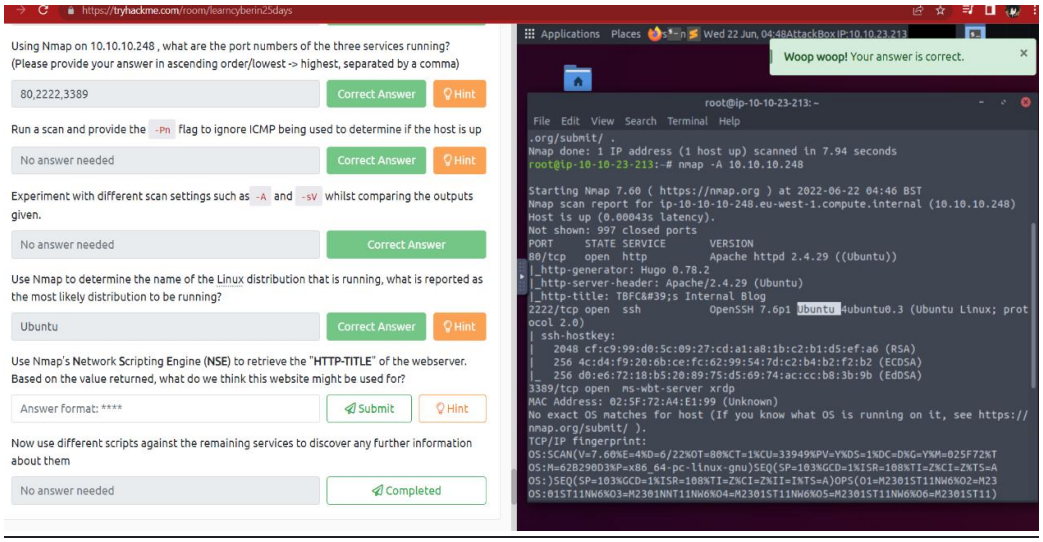
Question 2:

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



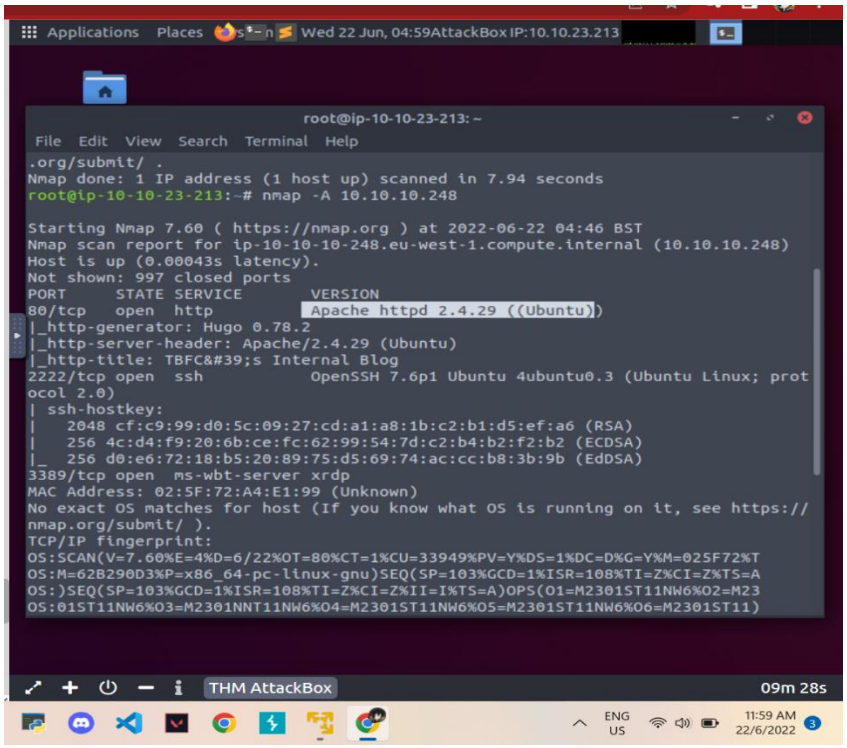
Question 3:

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



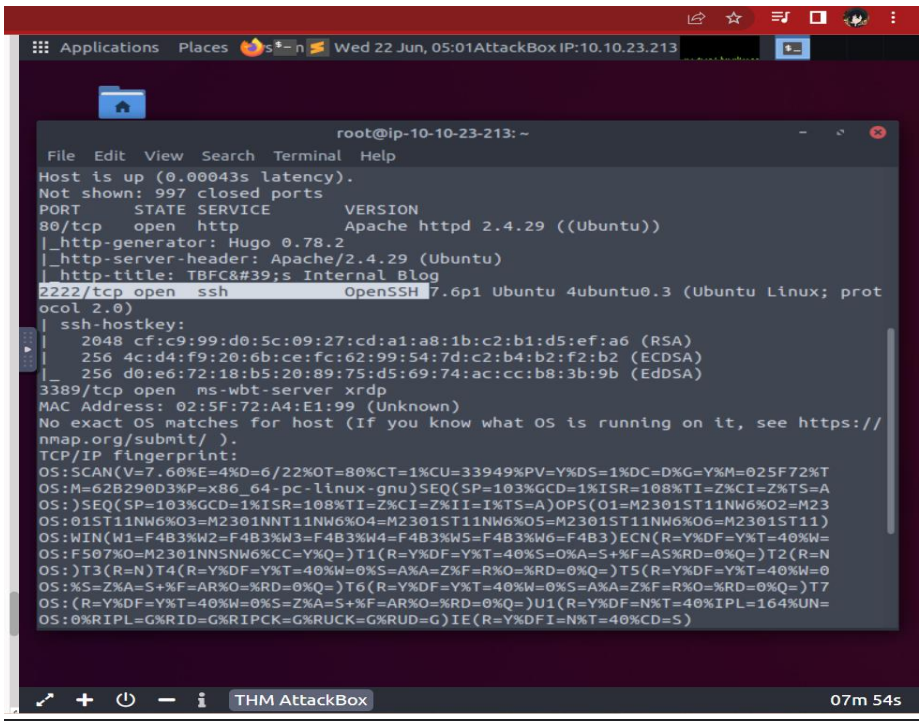
Question 4:

What is the version of Apache?



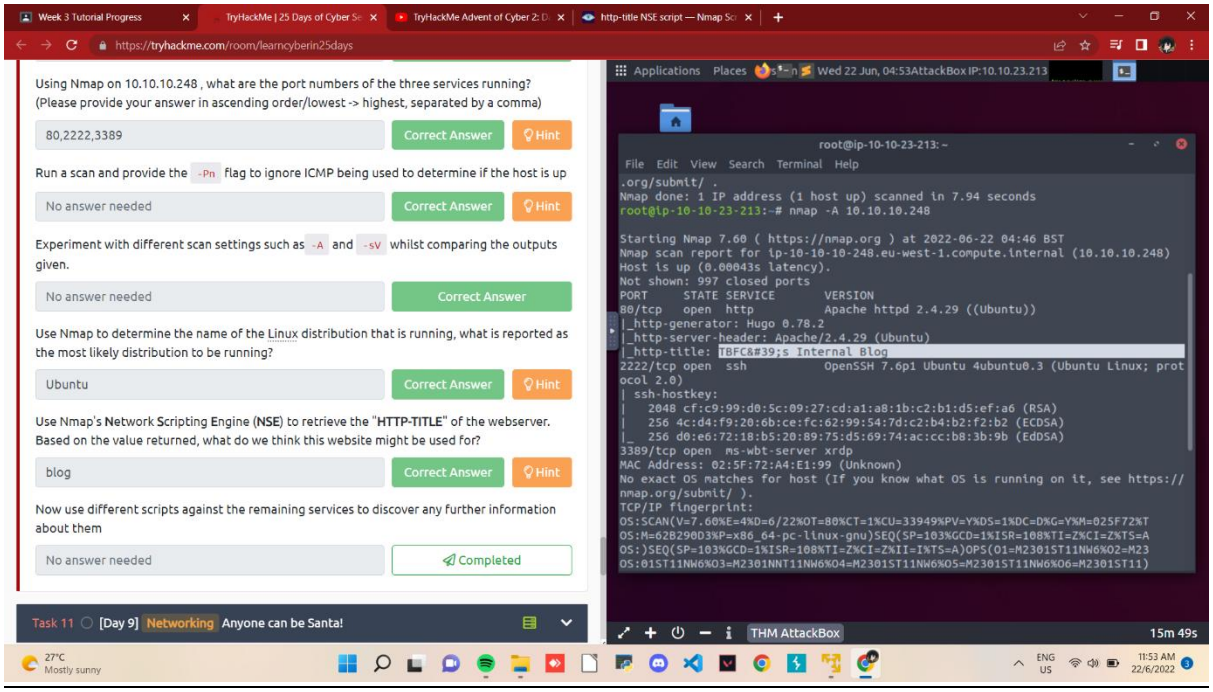
Question 5:

What is running on port 2222?



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

METHODOLOGY

First of all, we started the Machine and the AttackBox waiting to obtain Ip address. Then, we open the terminal and run the scan using Nmap with the Ip provided to get the port numbers of the three services running it. Lastly, we scan again the Nmap with different scan settings using -A to retrieve the outputs to solve the name of the Linux distribution that is running, the version of Apache, type running of the port numbers and the value of the webserver.

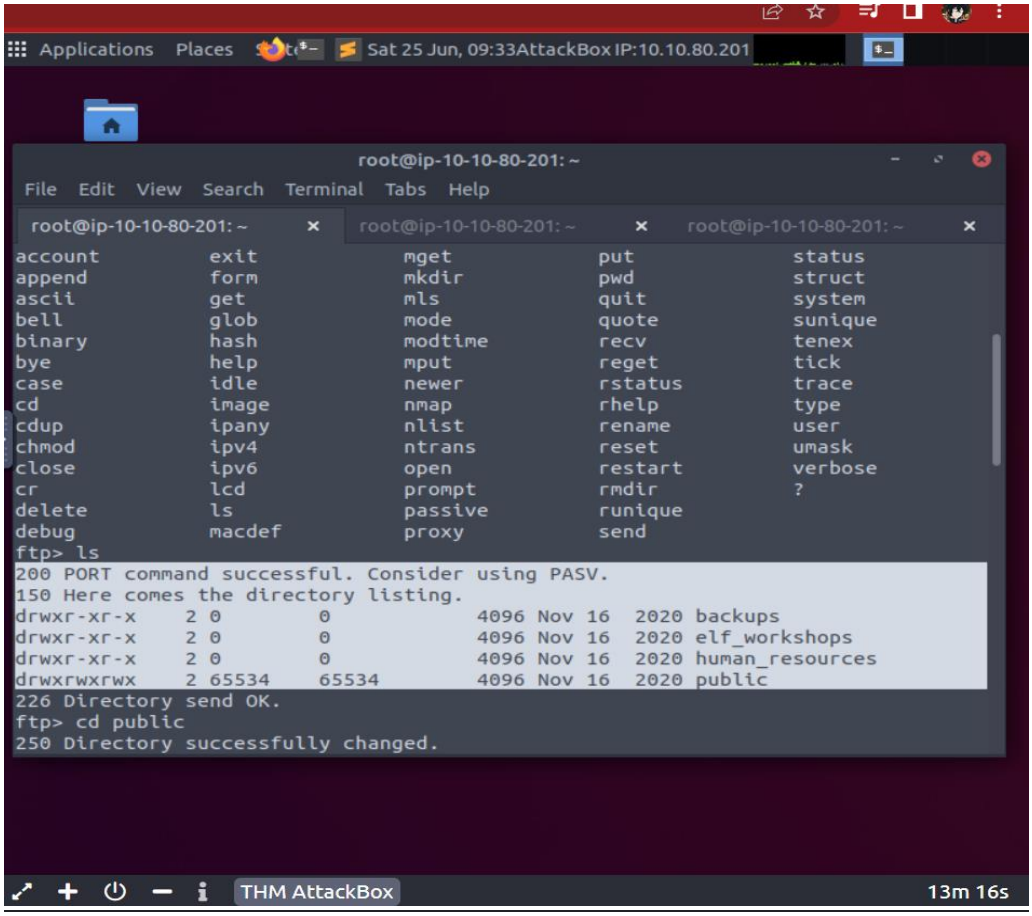
Day 9 – Anyone can be Santa!

Tools used: AttackBox

Solution/ Walkthrough:

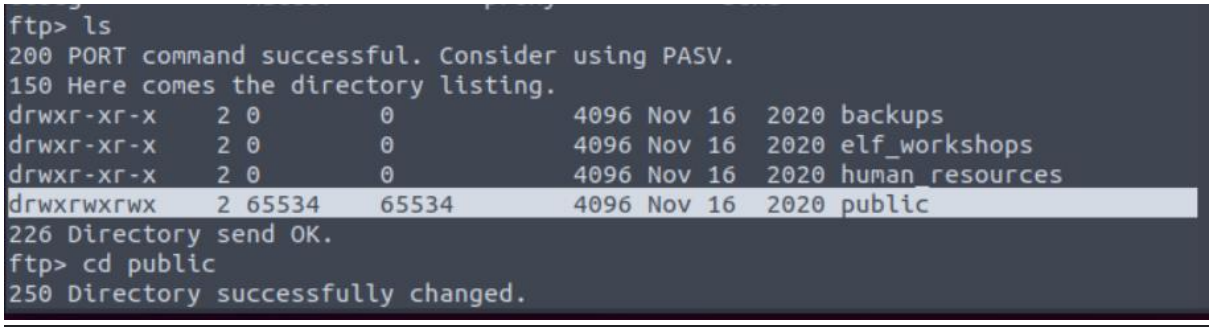
Question 1:

What are the directories you found on the FTP site?



Question 2:

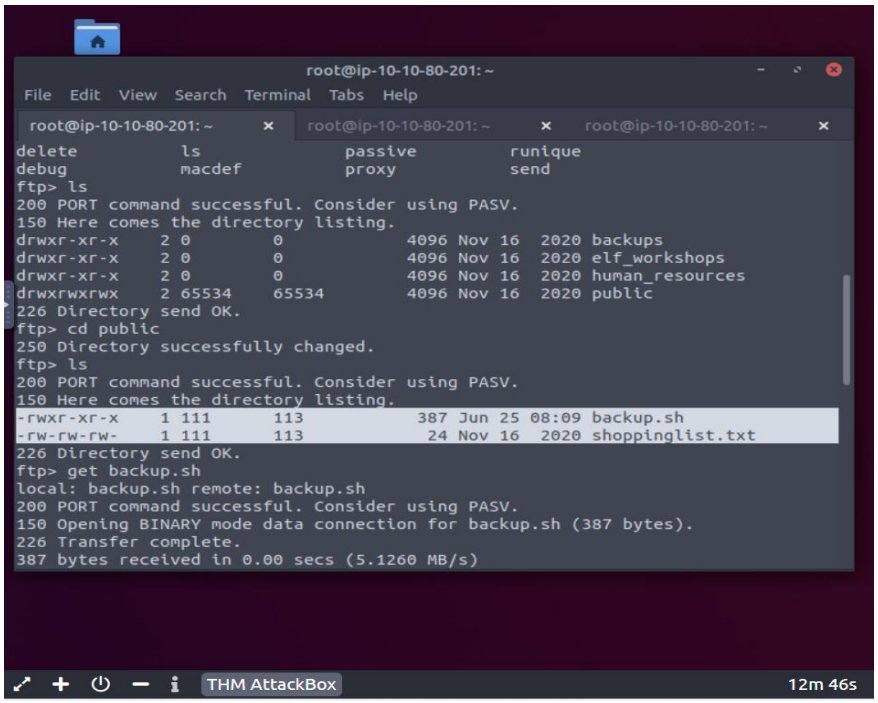
Name the directory on the FTP server that has data accessible by the "anonymous" user



Question 3:

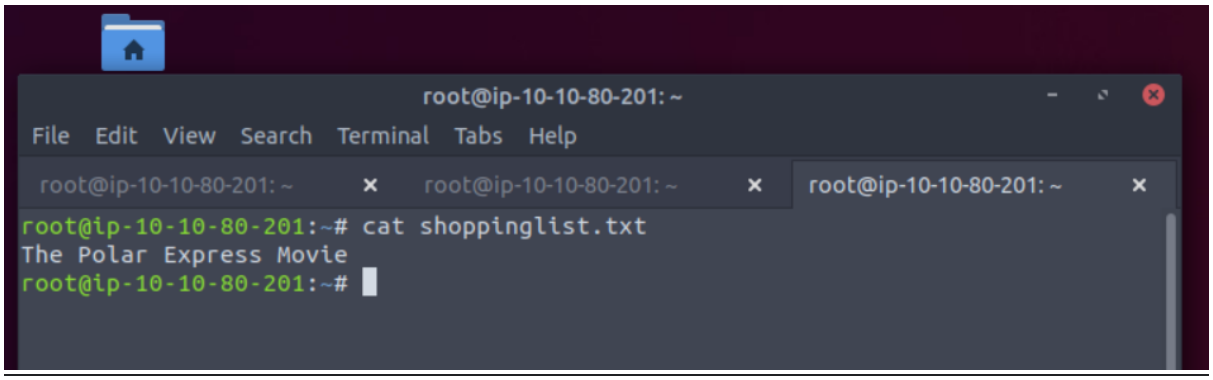
What script gets executed within this directory?

=backup.sh



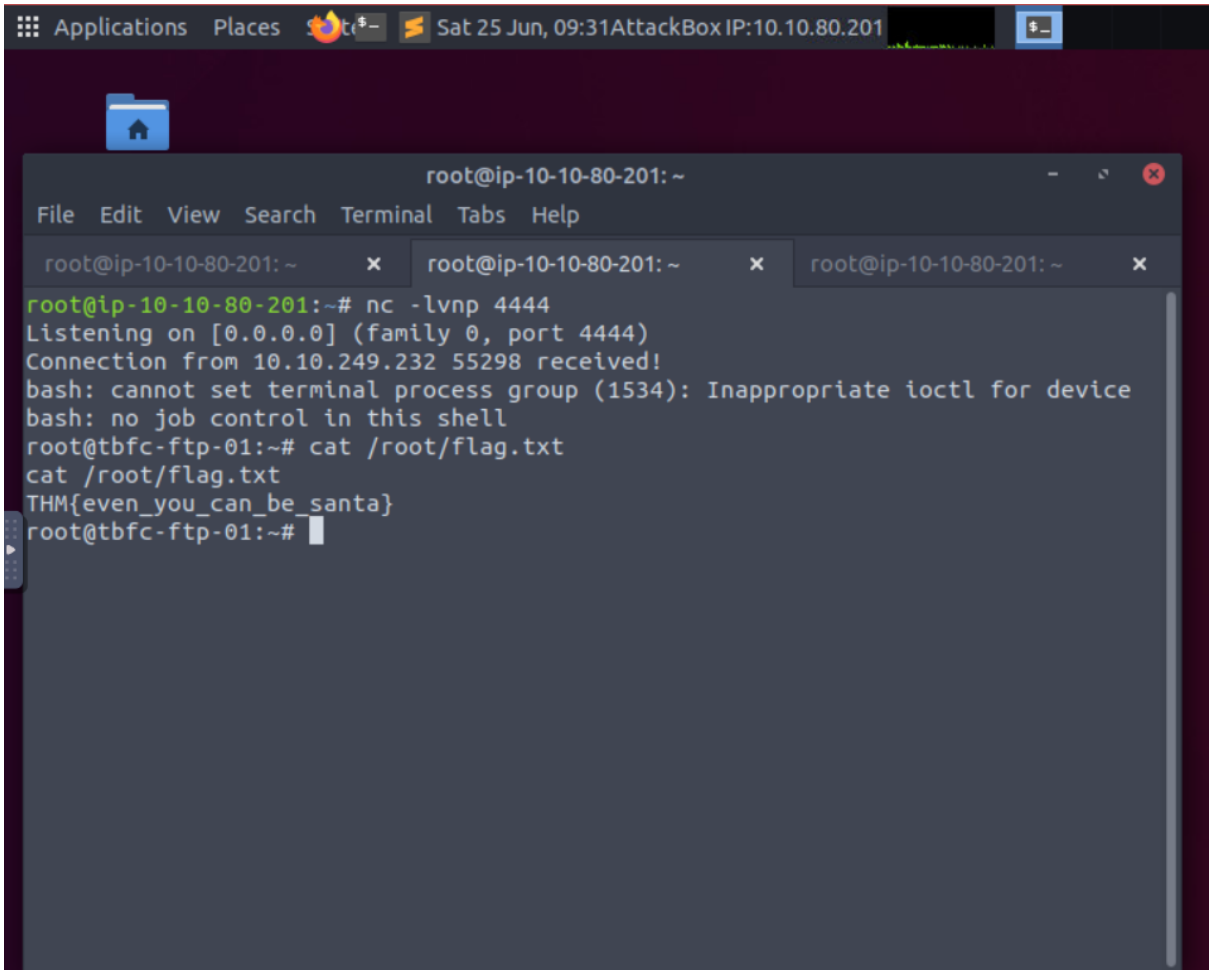
Question 4:

What movie did Santa have on his Christmas shopping list?



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!



METHODOLOGY:

We run the Machine and the AttackBox. To connect, we simply use ftp and provide the IP address of the Instance. When prompted for our "Name", we enter "anonymous". If successful, we have confirmed that the FTP Server has "anonymous" mode enabled - successful login. We apply command “ls” to look at the directories available in the FTP server and find out which directory that has data accessible by the anonymous user. Then we use nano to see the scripts. By that we work pentesters cheatsheet to get a good command that will be executed by the server to generate a shell to our AttackBox, replacing the IP_ADDRESS with the TryHackMe IP. We set up a netcat listener to catch the connection on our AttackBox and return to our FTP prompt and employ put to put the file into that directory. Lastly, we go back to our netcat listener, wait for about one minute to succeed. Now we have a reverse system shell on the FTP Server as the most powerful user that we can re-upload the script by putting the output contents of /root/flag.txt!

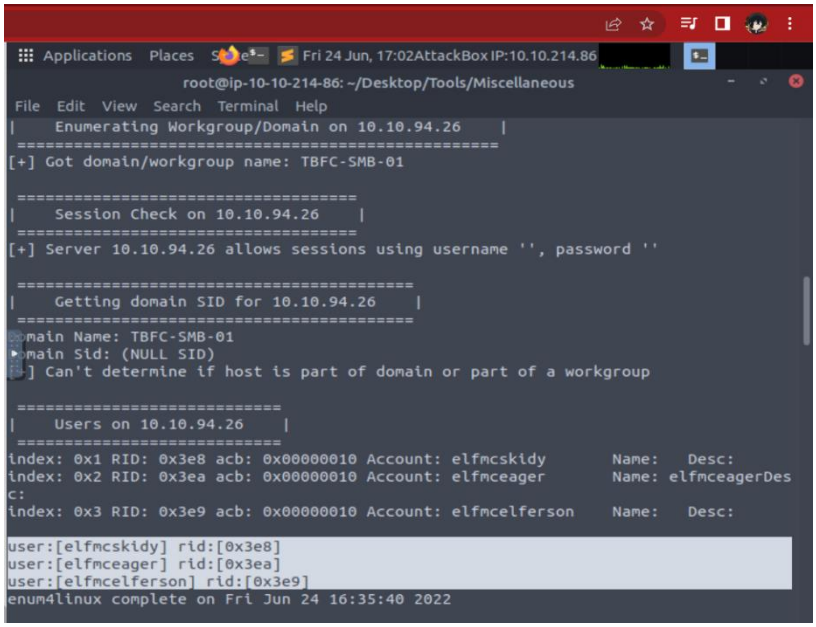
Day 10 - Don't be sElfish!

Tools used: AttackBox

Solution/ Walkthrough:

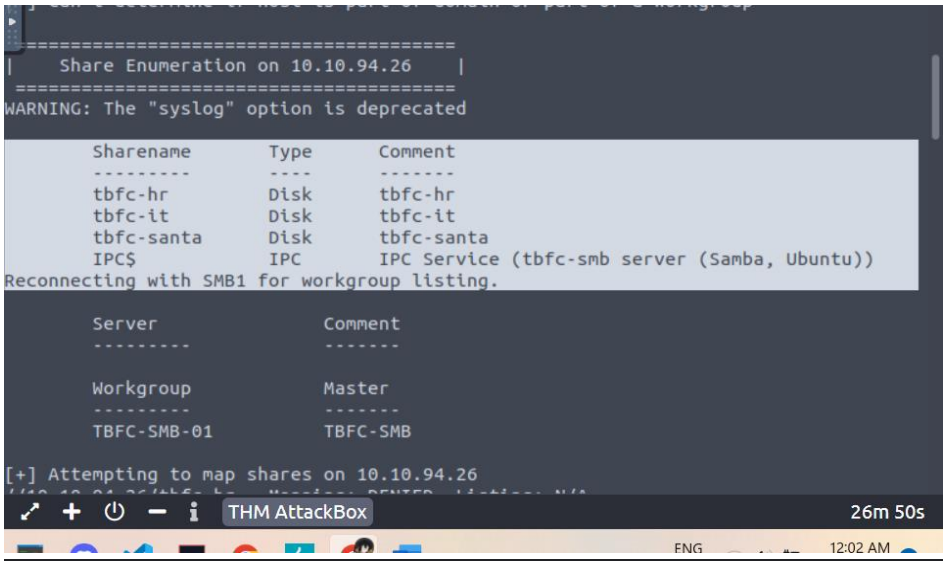
Question 2:

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



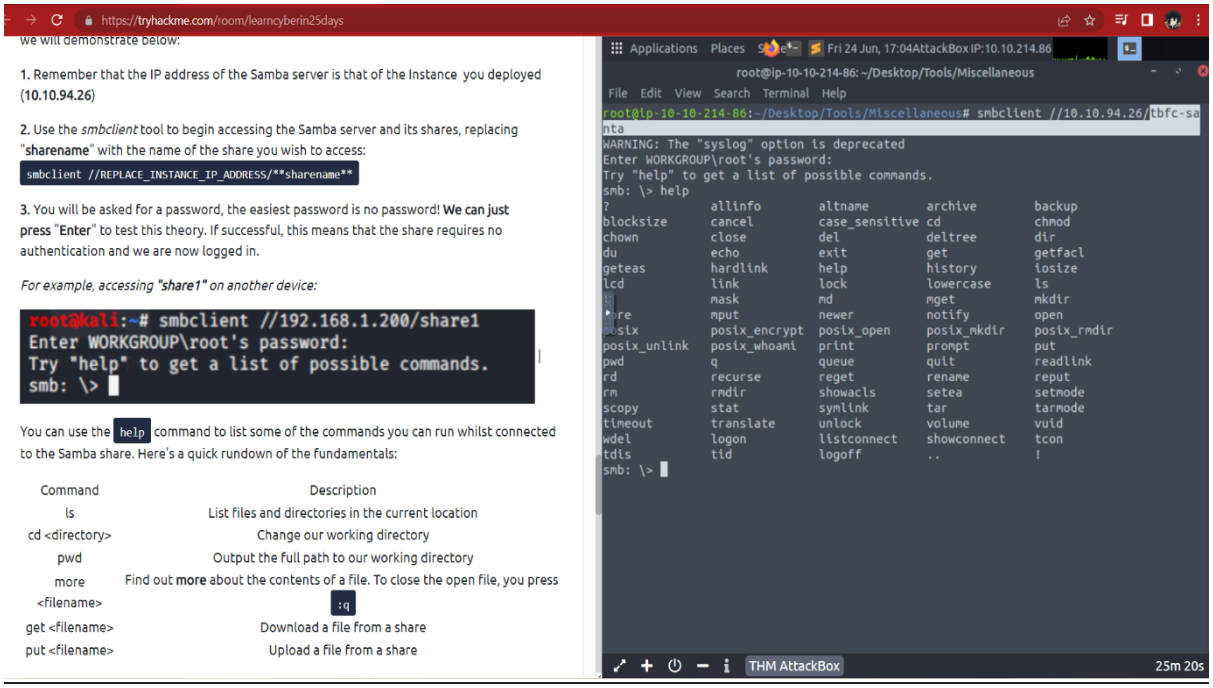
Question 3:

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



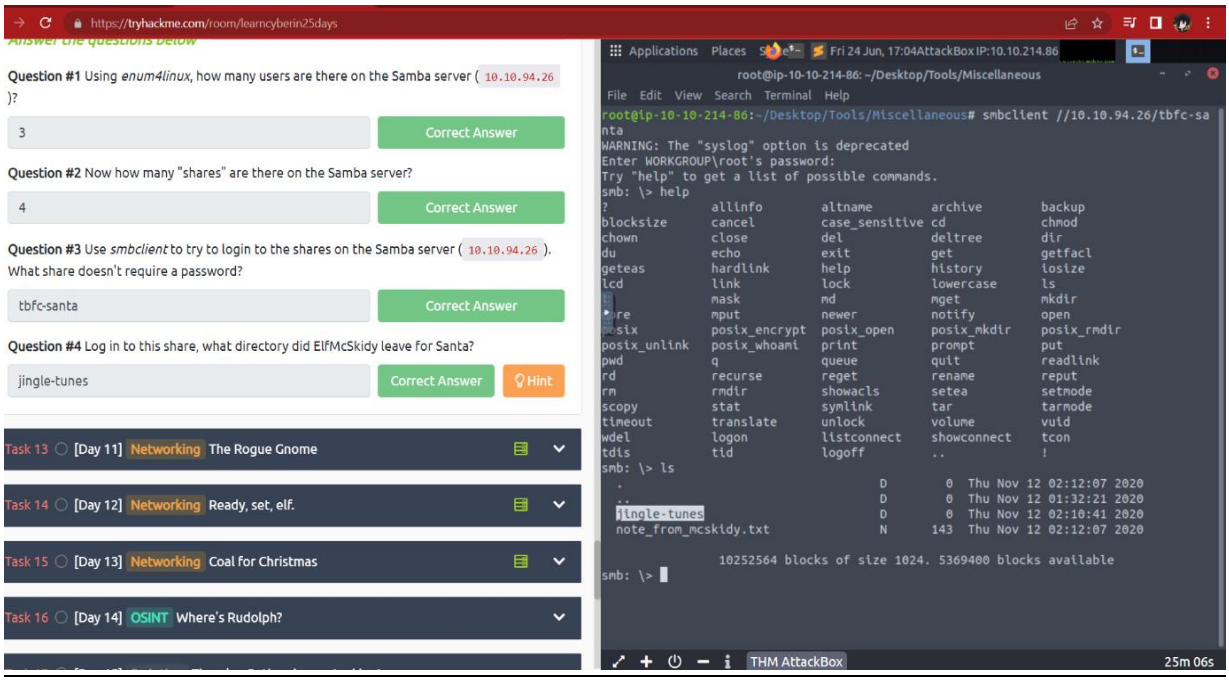
Question 4:

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



Question 5:

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



METHODOLOGY:

As usual we started the Machine and the AttackBox, then we open a terminal prompt and navigate to enum4linux: cd /root/Desktop/Tools/Miscellaneous. We continue running enum4linux using (./enum4linux.pl -h) to study all the list possible options we can use. Next, we want to find out who can be used to access the server through Samba: (./enum4linux.pl -U [the Ip address]) then enum4linux showed four users in the Samba server. Now we want to know how many “shares” in the Samba server so we use (./enum4linux.pl -S [Ip address]) to obtain the share list. Moving on we use the smbclient tool to accessing the share that doesn’t require a password. Lastly, we use command “ls” in the smbclient tools to receive the directory.