PSP0201

Week 3

Writeup

Group Name: SupremeChickens

Members

ID	Name	Role
1211103024	Yap Jack	Leader
1211102425	Ang Hui Yee	Member
1211101198	Fam YI Qi	Member
1211103978	DIckshen	Member

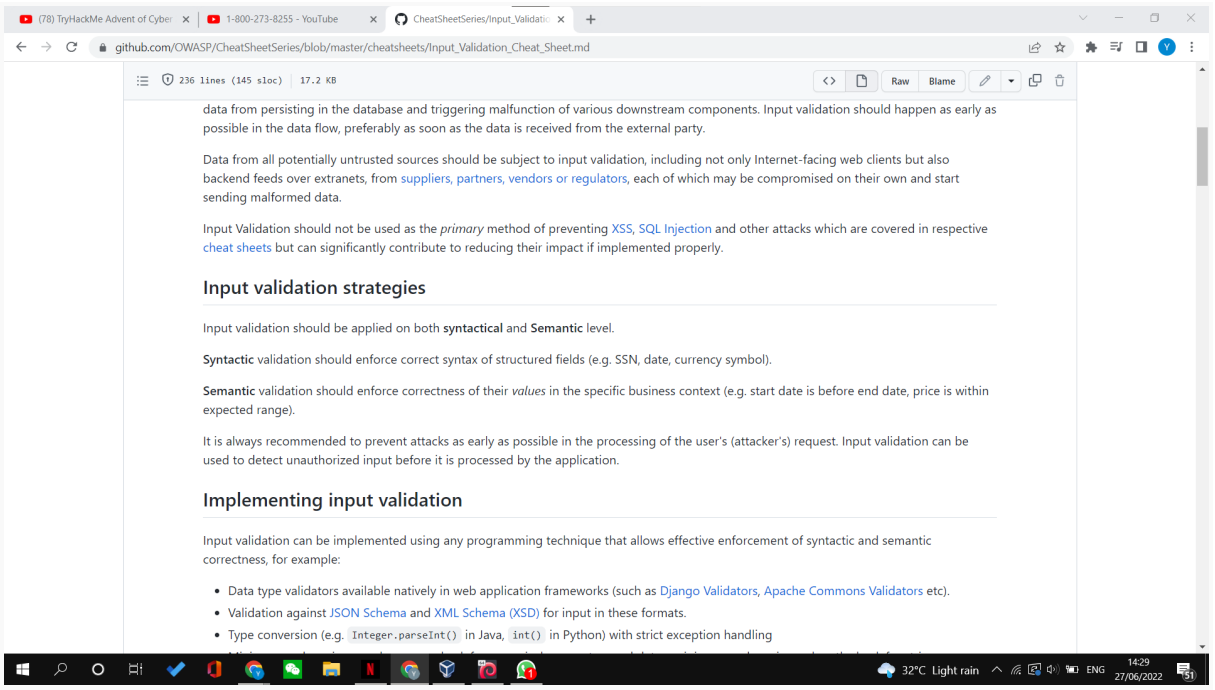
Day 6: Networking – Be careful with what you wish on a Christmas night

Tools used: Kali Linux, Chrome

Solution/walkthrough: DarkSec

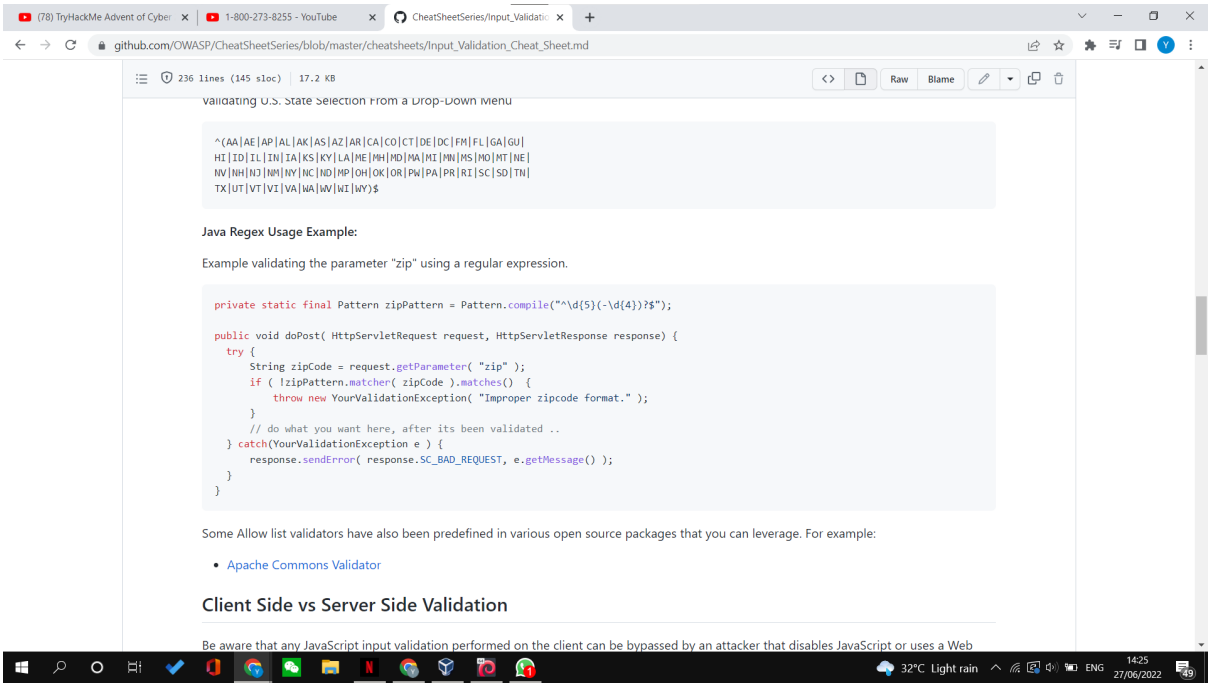
Question 1

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



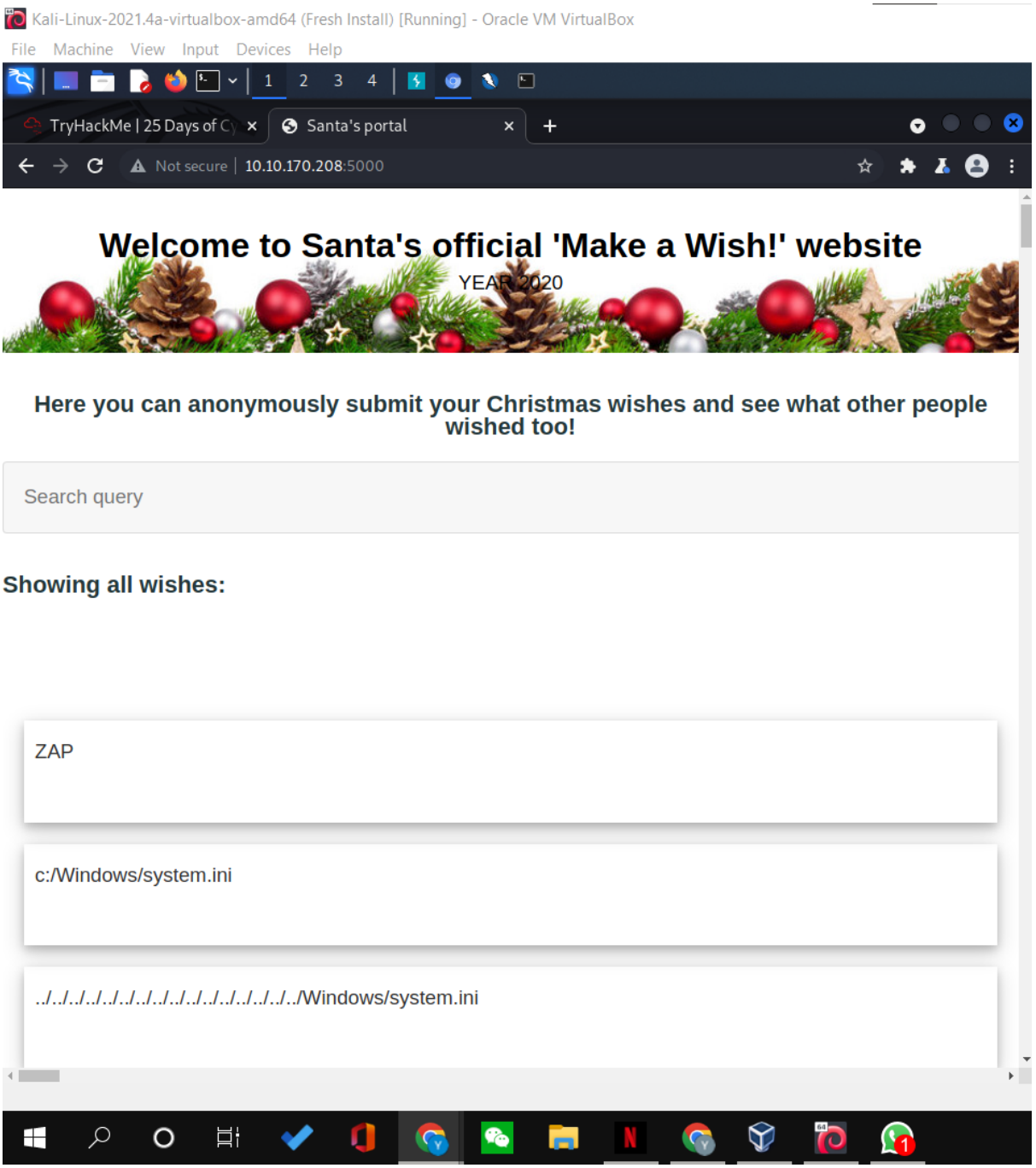
Question 2

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



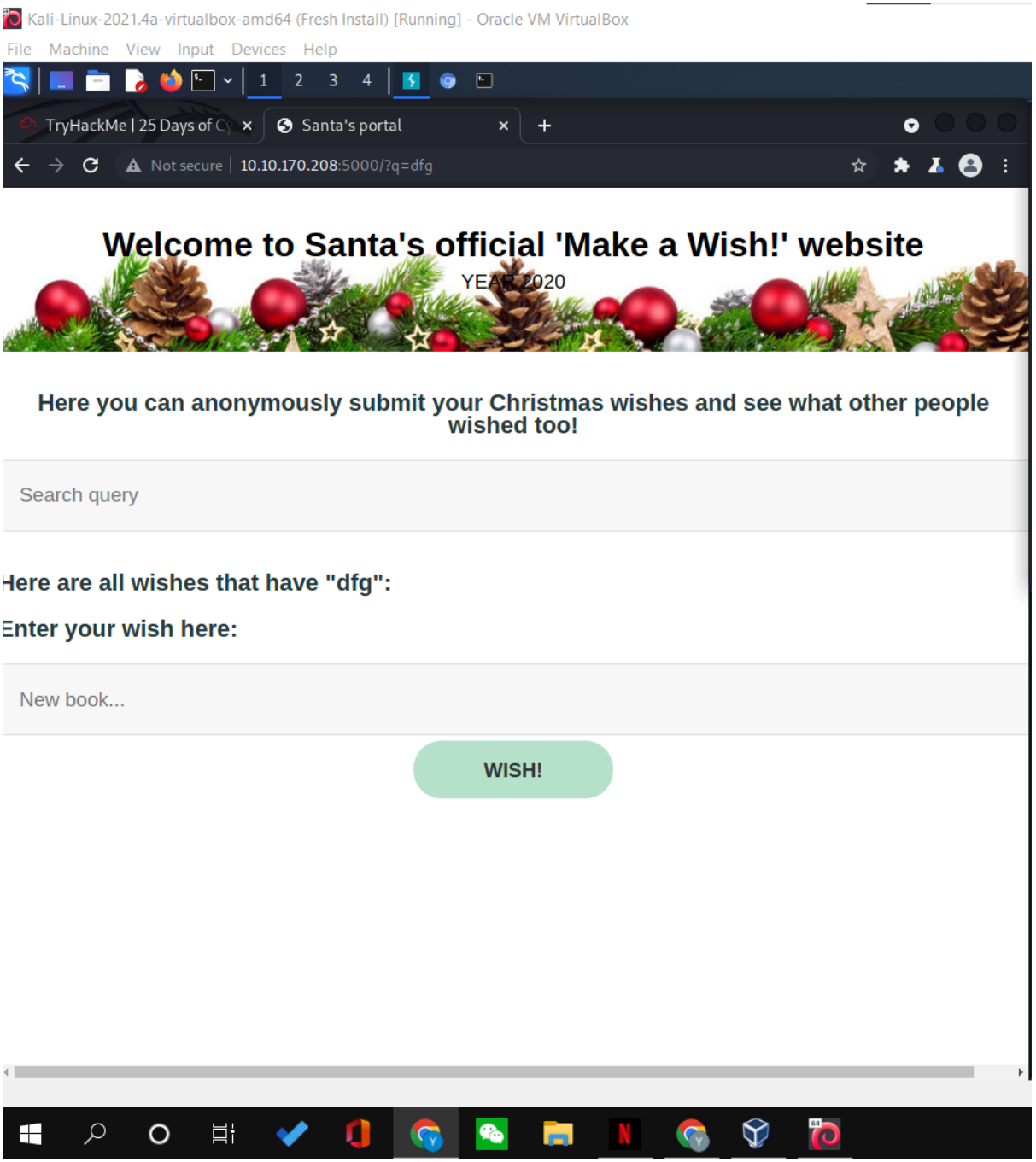
Question 3

What vulnerability type was used to exploit the application?



Question 4

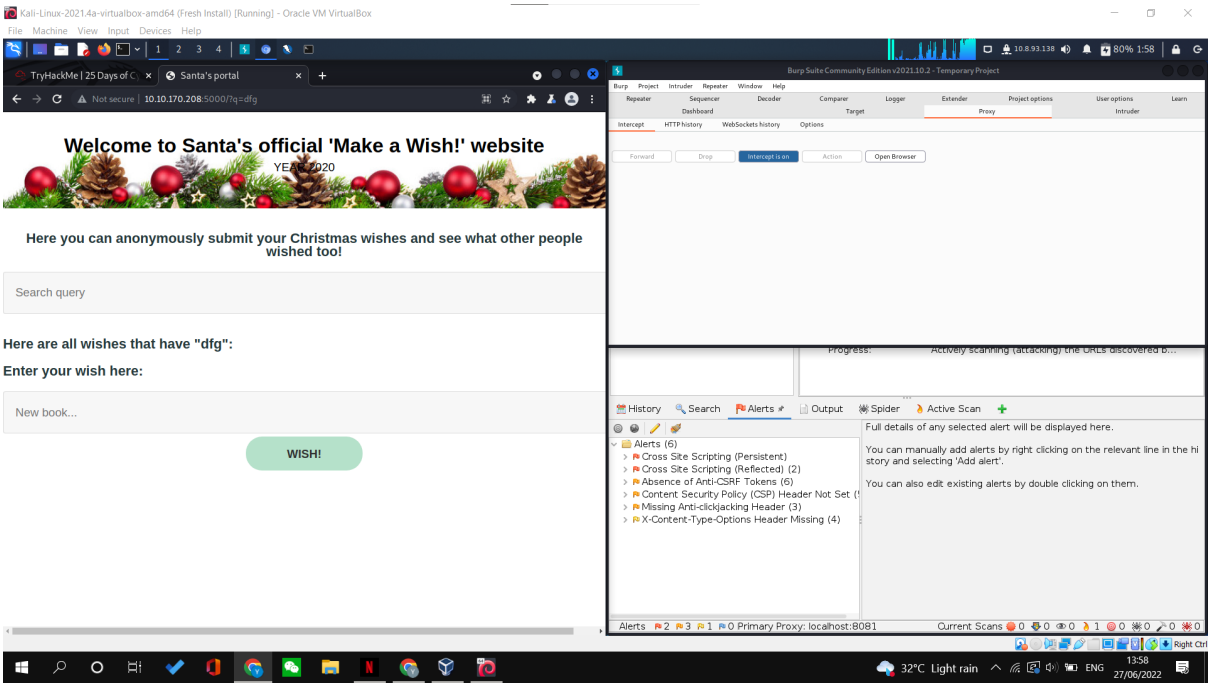
What query string can be abused to craft a reflected XSS?



Question 5

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

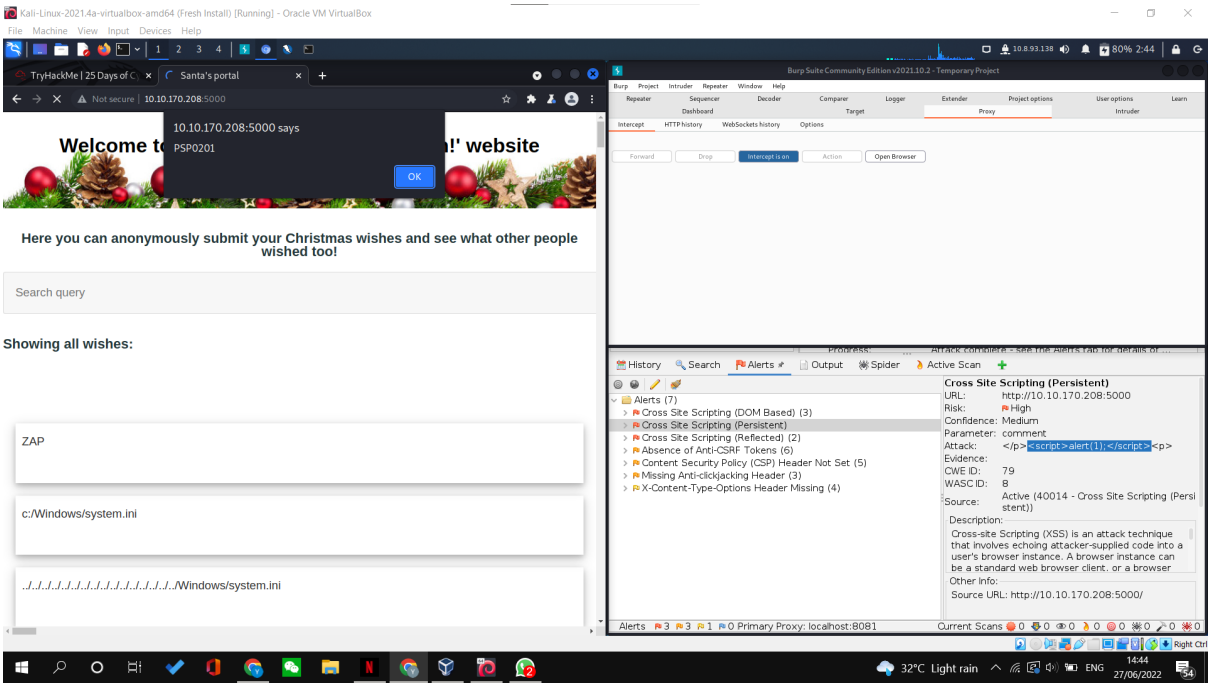
Use the AttackBox's Zap 2.9.0 or Kali's 2.11.1, otherwise you may get different answers



Question 6

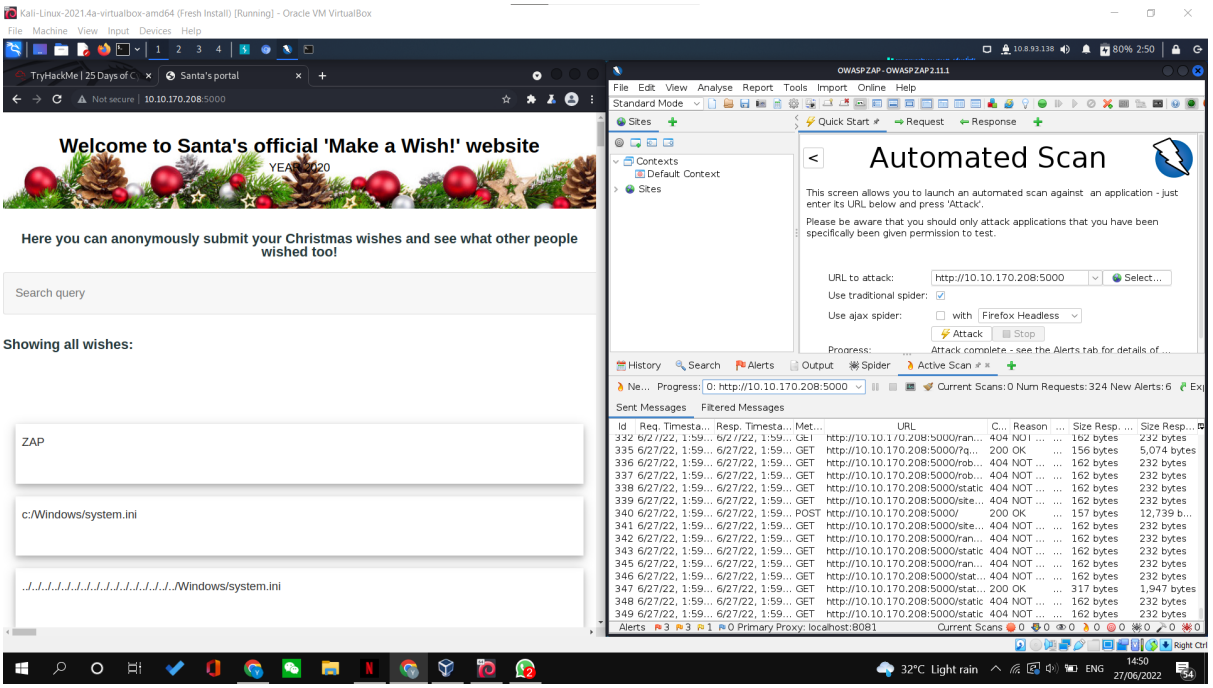
What Javascript code should you put in the wish text box if you want to show an alert saying "PSP0201"?

Answer hint: <script>xxxxxx</script> <--insert your answer TOGETHER with the script tags.



Question 7

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



Thought Process/Methodology:

I went into the OWASP cheatsheet series and viewed the needed information. Next, I went into the back-up server and keyed in random words in the query box to see what query string can be abused to craft a reflected XSS. Then, I opened up ZAP. After that, I keyed in the url and clicked attack to view the alerts.

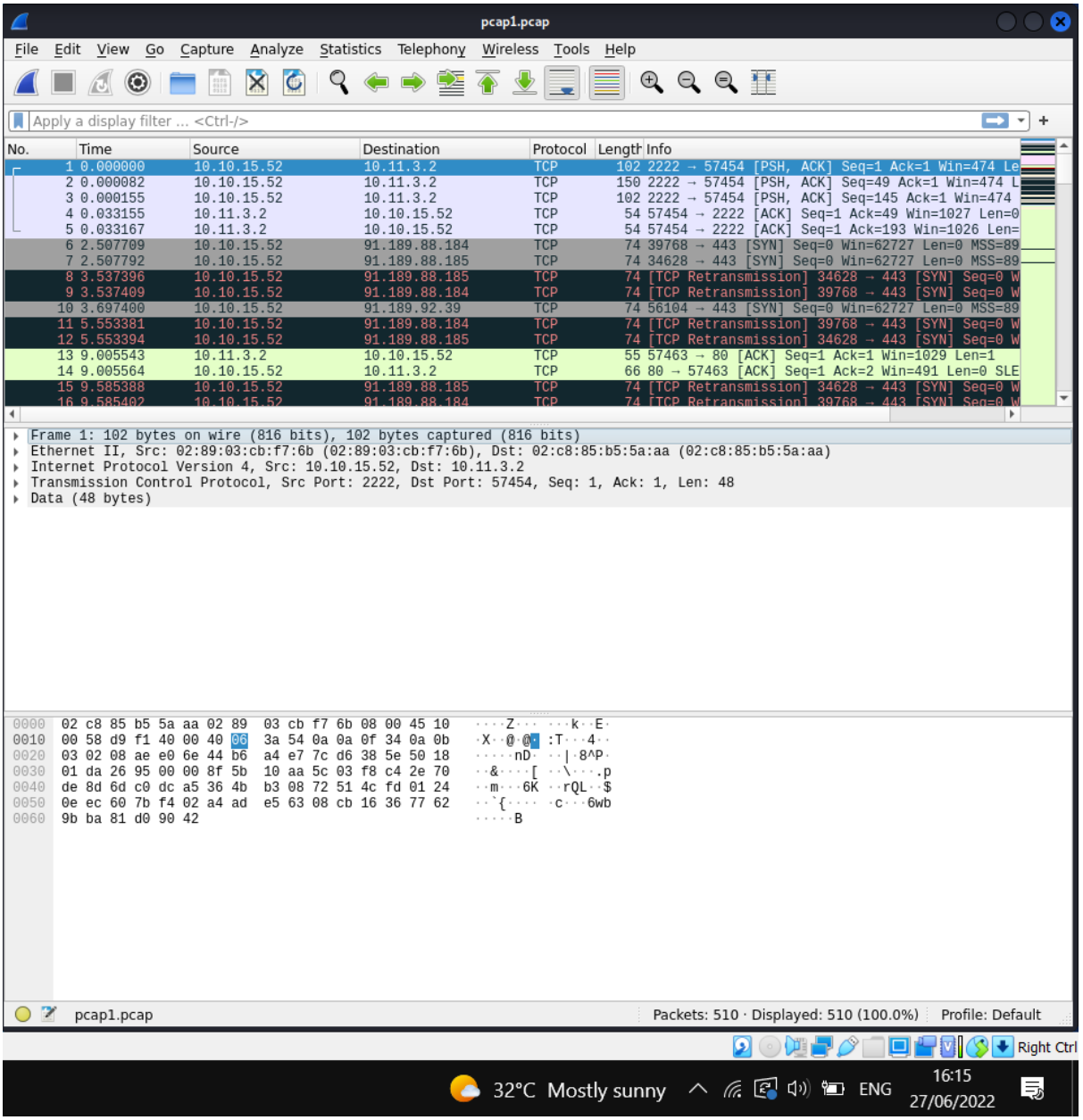
Day 7: Networking – The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Chrome

Solution/walkthrough: DarkSec

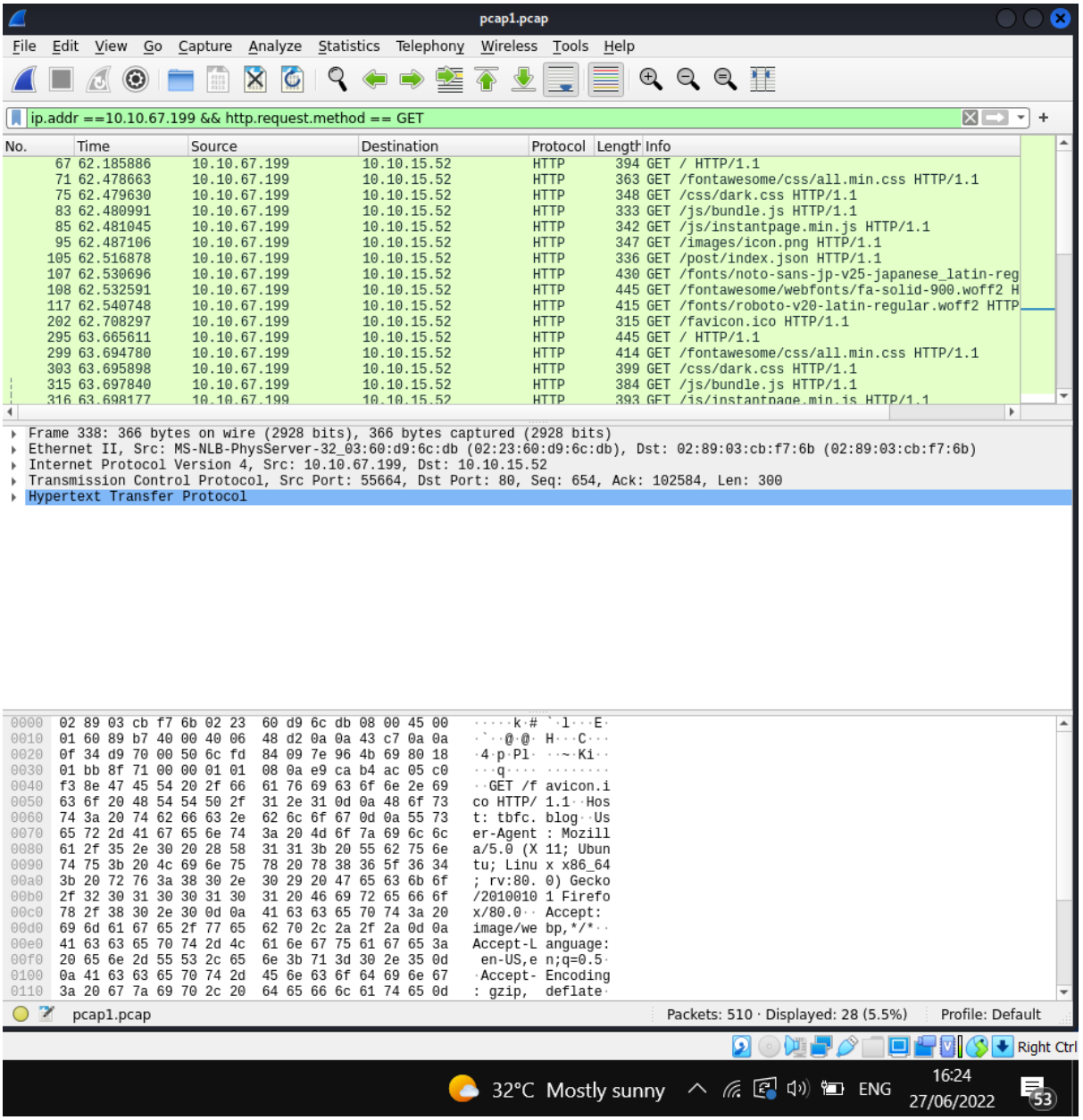
Question 1

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



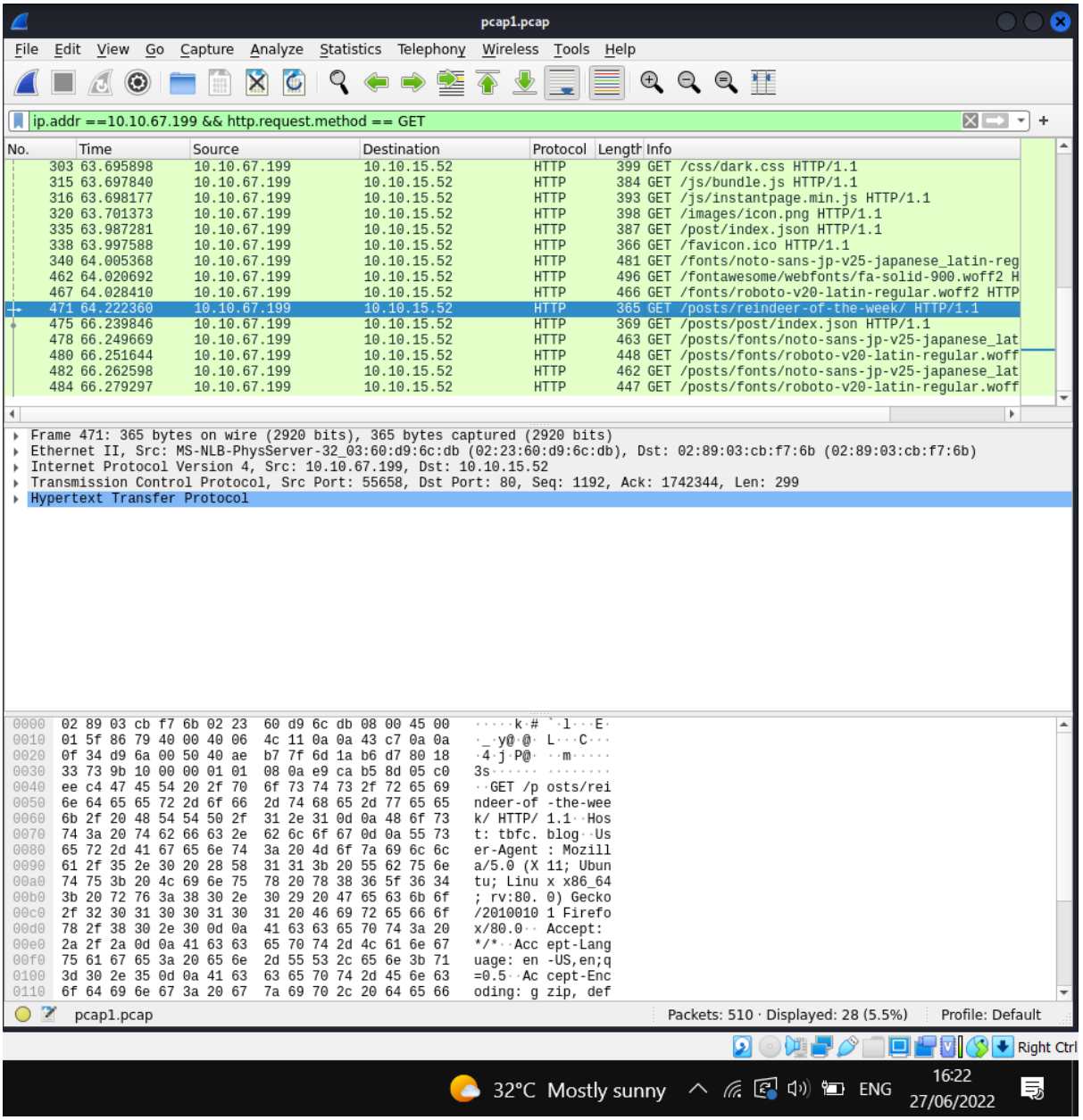
Question 2

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



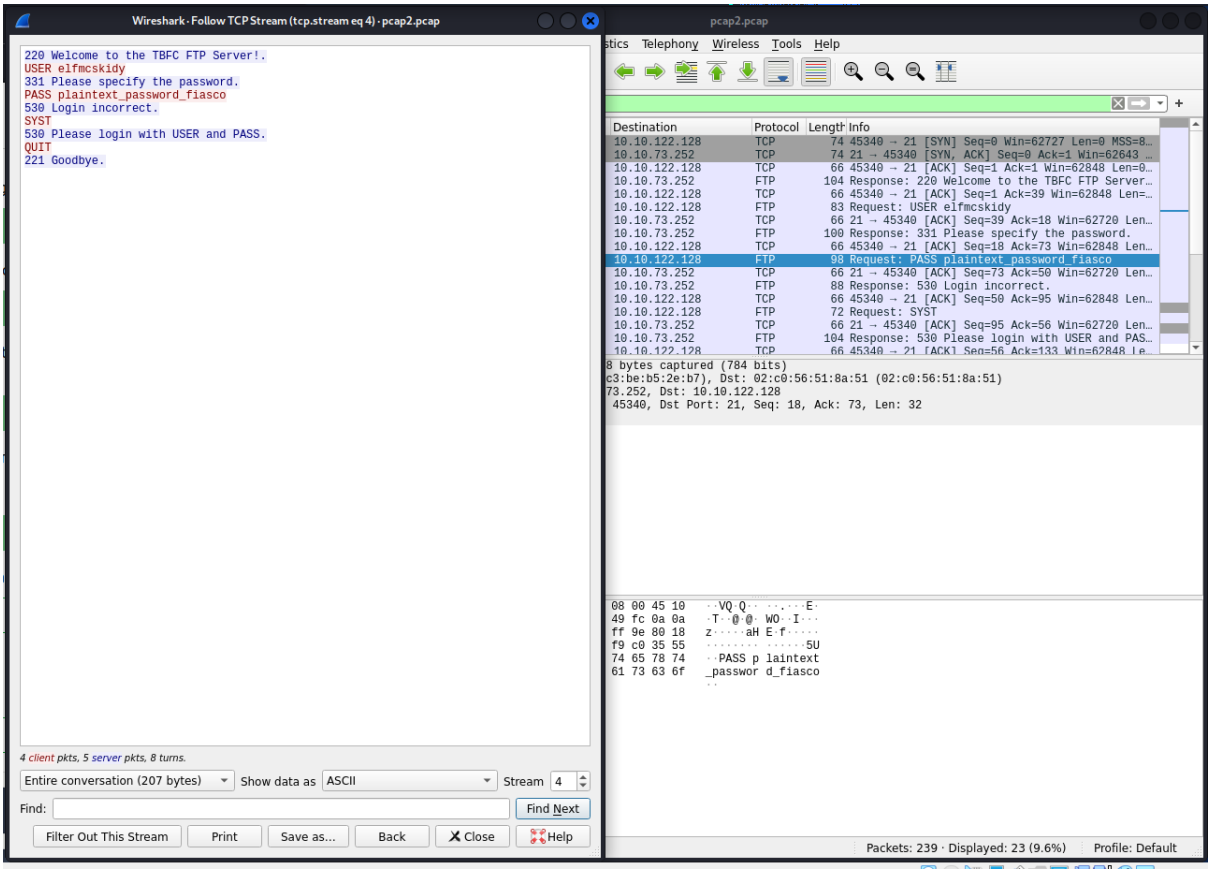
Question 3

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?



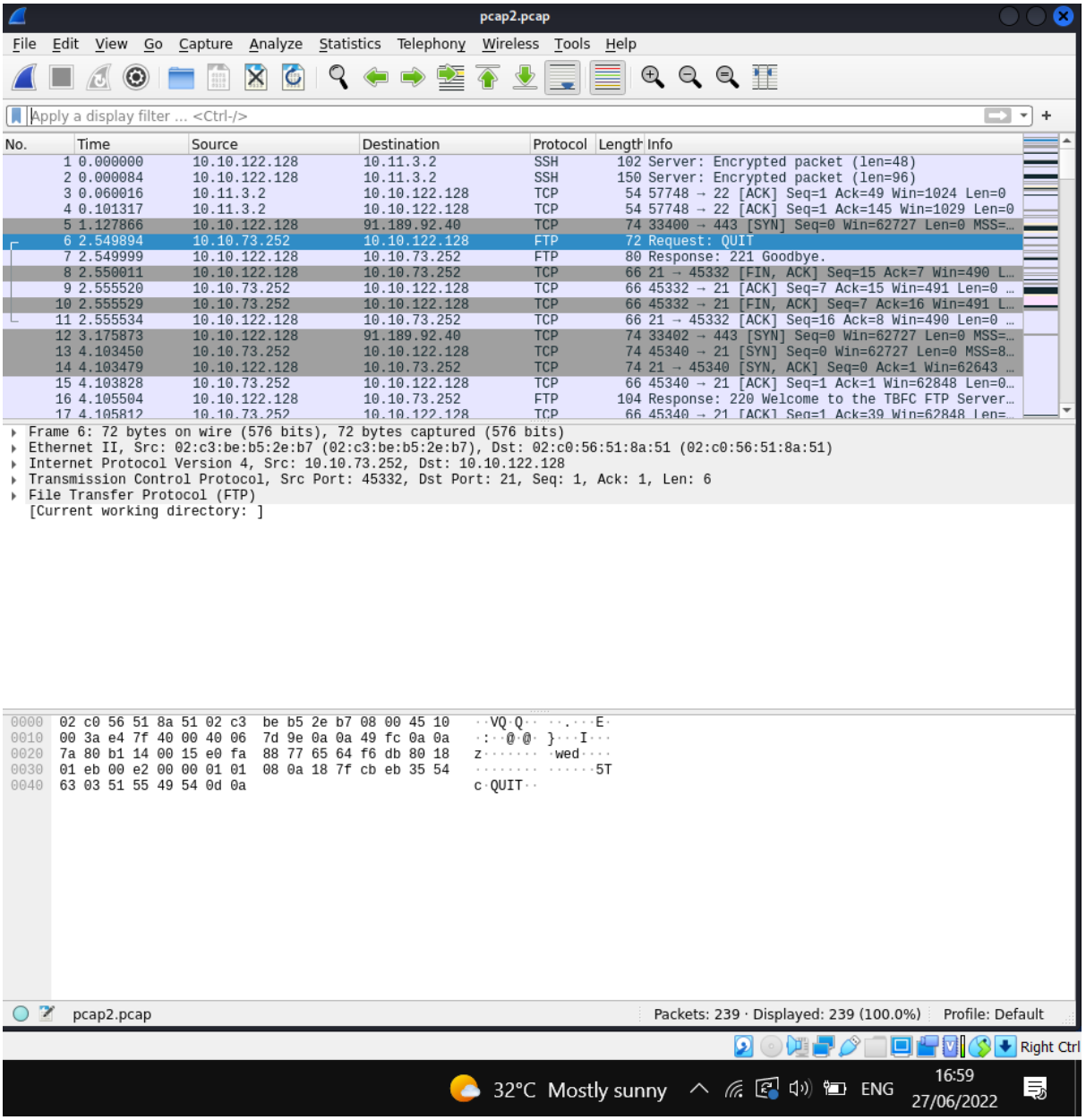
Question 4

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



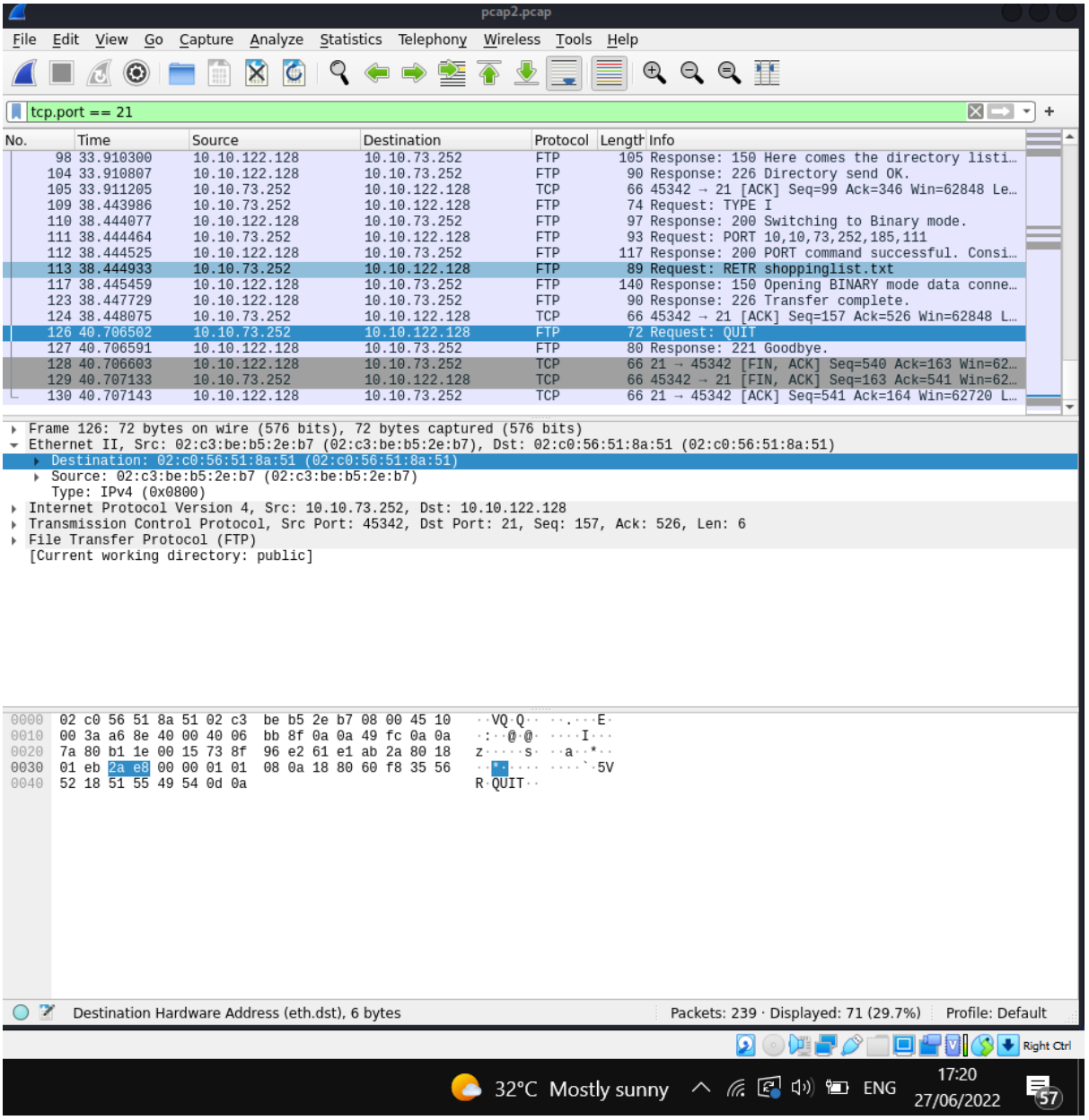
Question 5

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



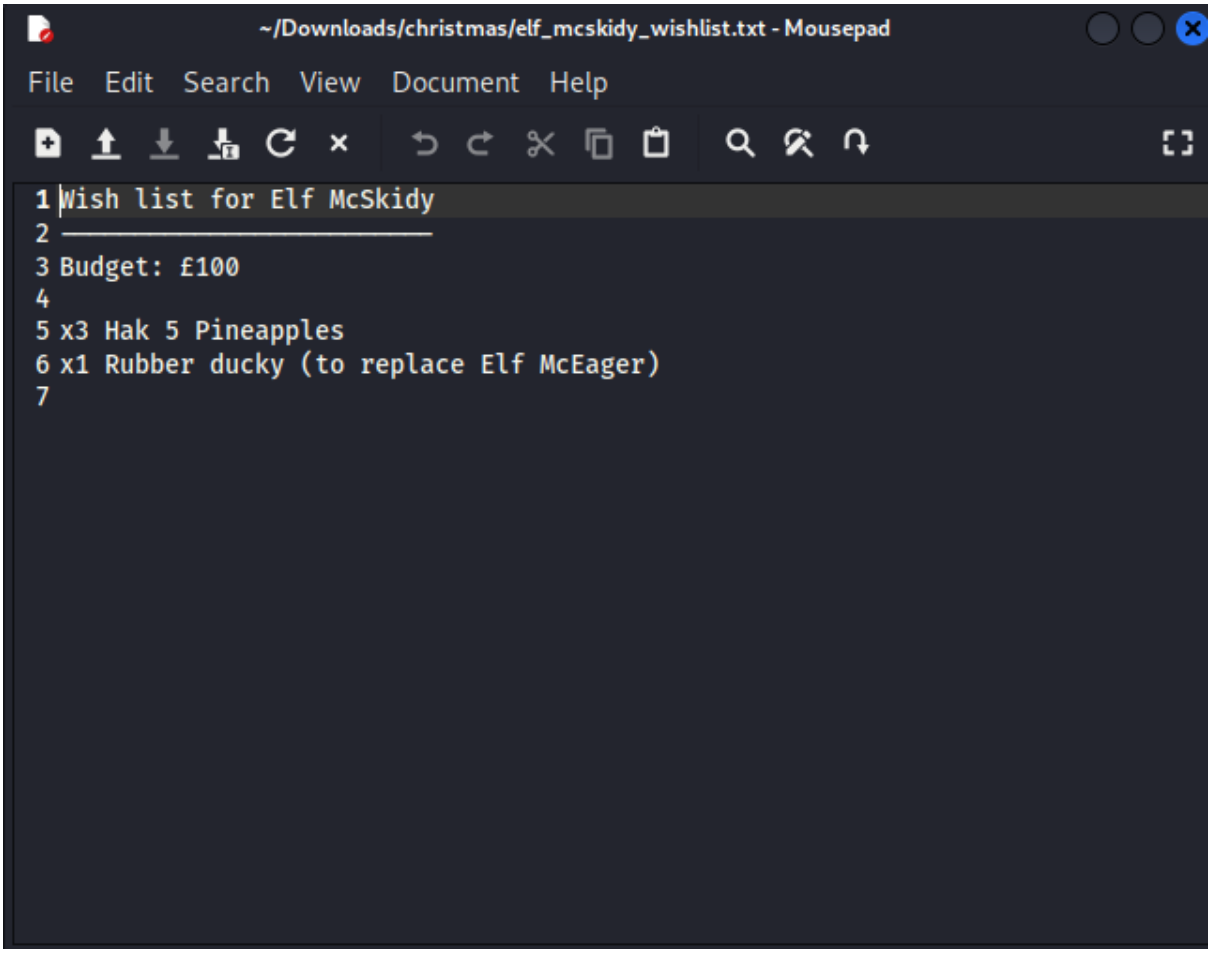
Question 6

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



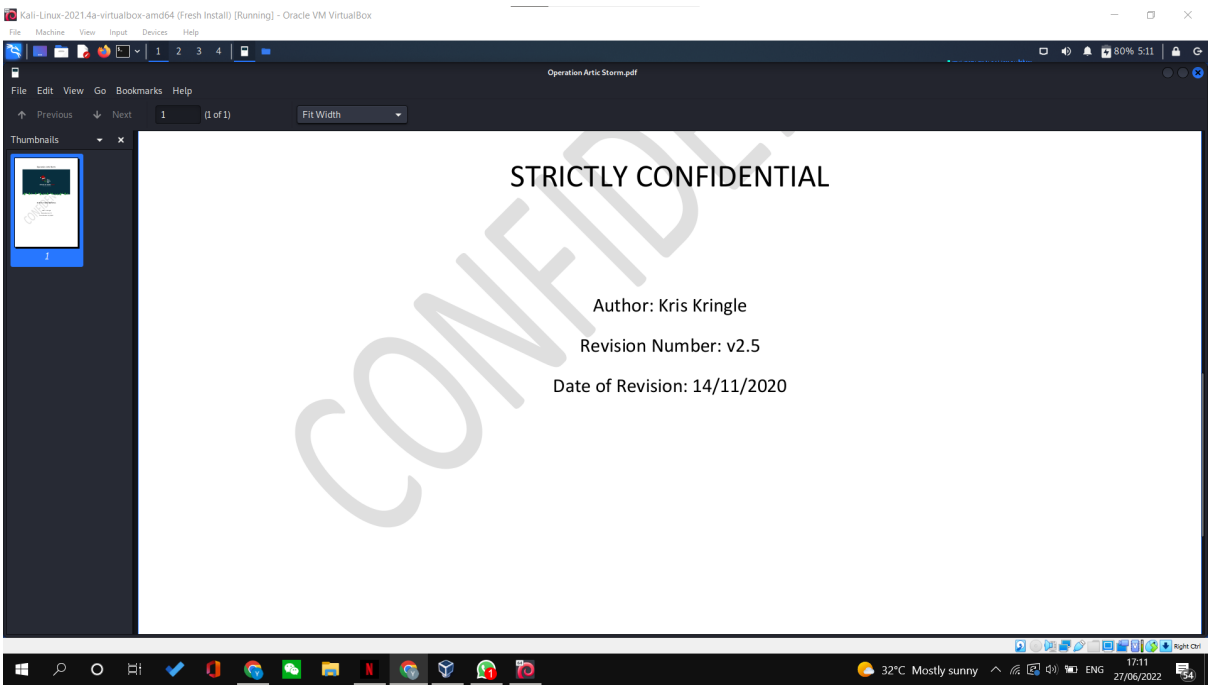
Question 7

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



Question 8

Who is the author of Operation Artic Storm?



Thought Process/Methodology:

I downloaded the zipped file and extracted it. Then, I used wireshark to open pcap1.pcap. I filtered in icmp to see the IP address. Next, I filtered in the IP address provided by TryHackMe and http.request.method == GET to see the name of the article that IP address "10.10.67.199" visited. Next, I opened the pcap2.pcap and filtered in tcp.port == 21. Then, I viewed the information needed and followed a successful login. Then, it shows the leaked password. Next, I opened pcap3.pcap to export christmas.zip and viewed the files.

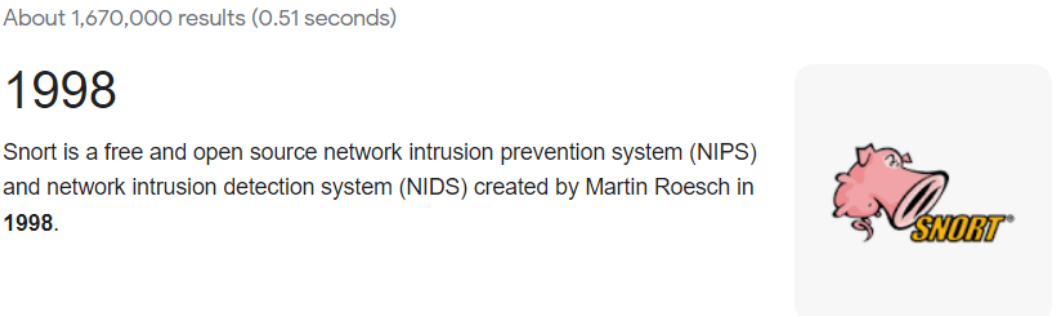
Day 8: Networking – What's Under the Christmas Tree?

Tools used: Kali Linux, Chrome

Solution/walkthrough: DarkSec

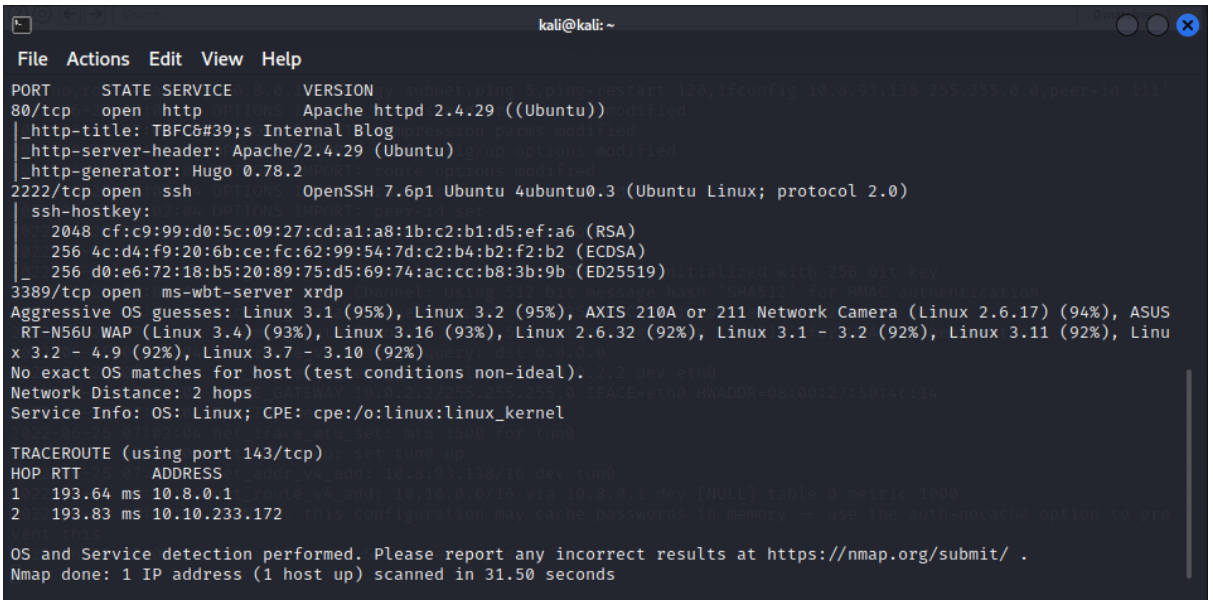
Question 1

When was Snort created?



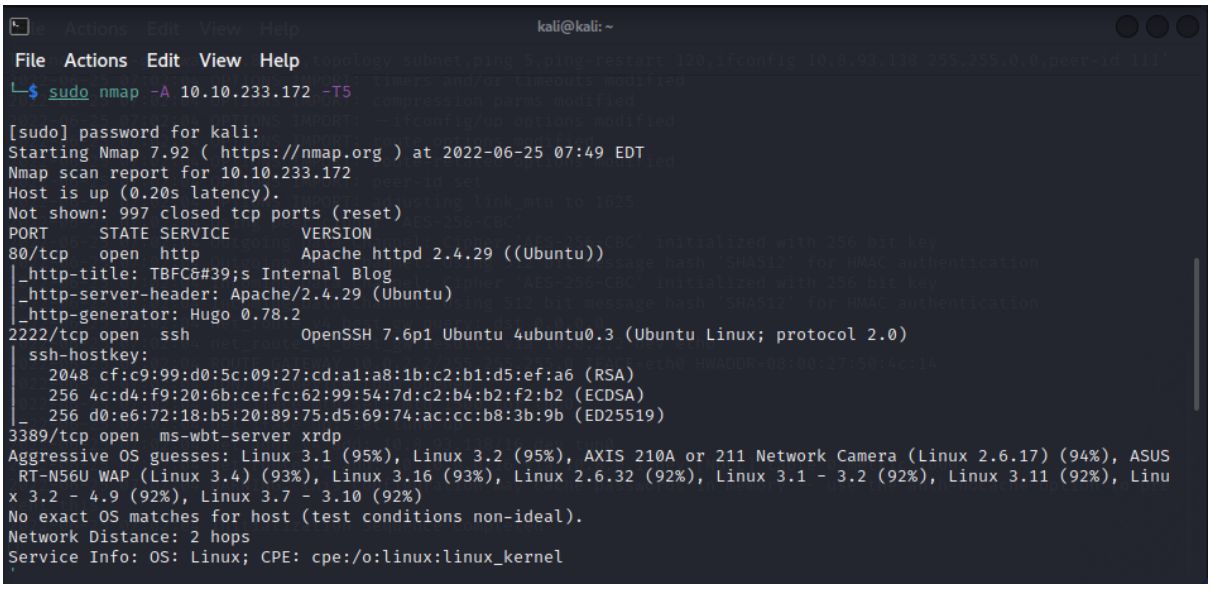
Question 2

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



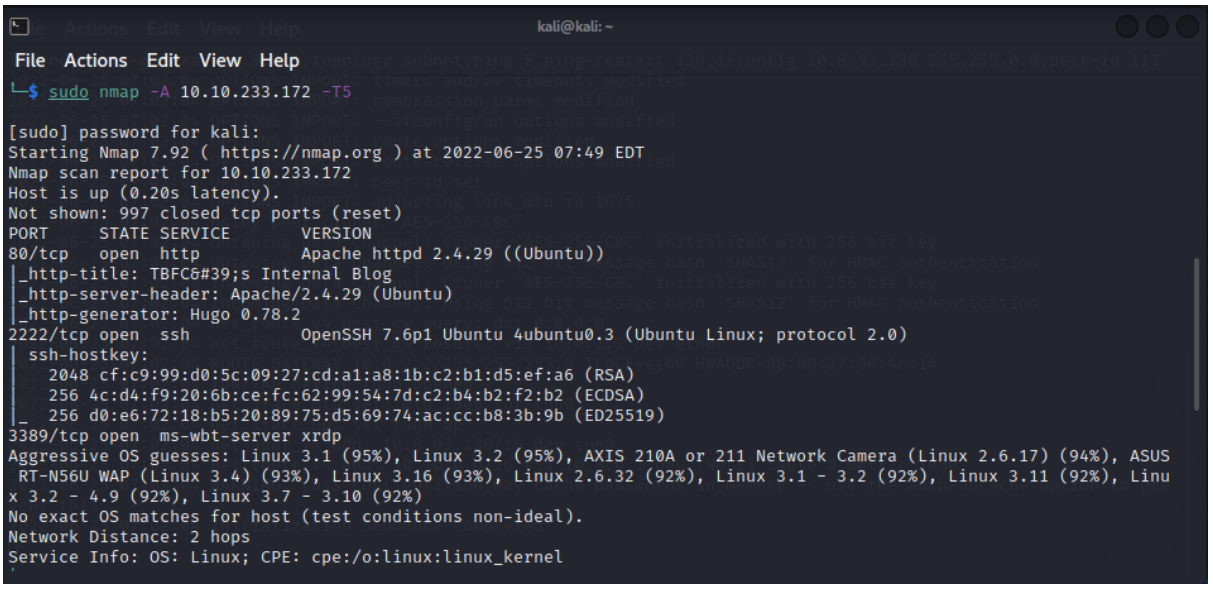
Question 3

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



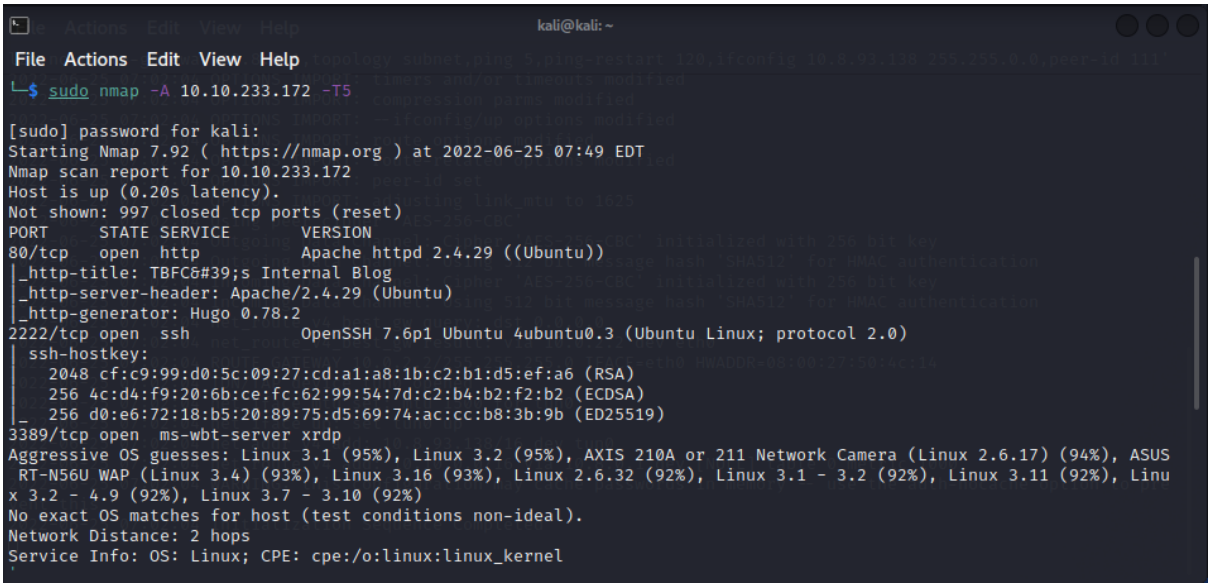
Question 4

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?

Thought Process/Methodology:

I opened the terminal and typed in 'man nmap' to view the commands. After I know which commands to use, I started nmap with my IP address and viewed the information I needed like the port numbers, the linux distribution ,the version of Apache and others. Next, I used Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver.

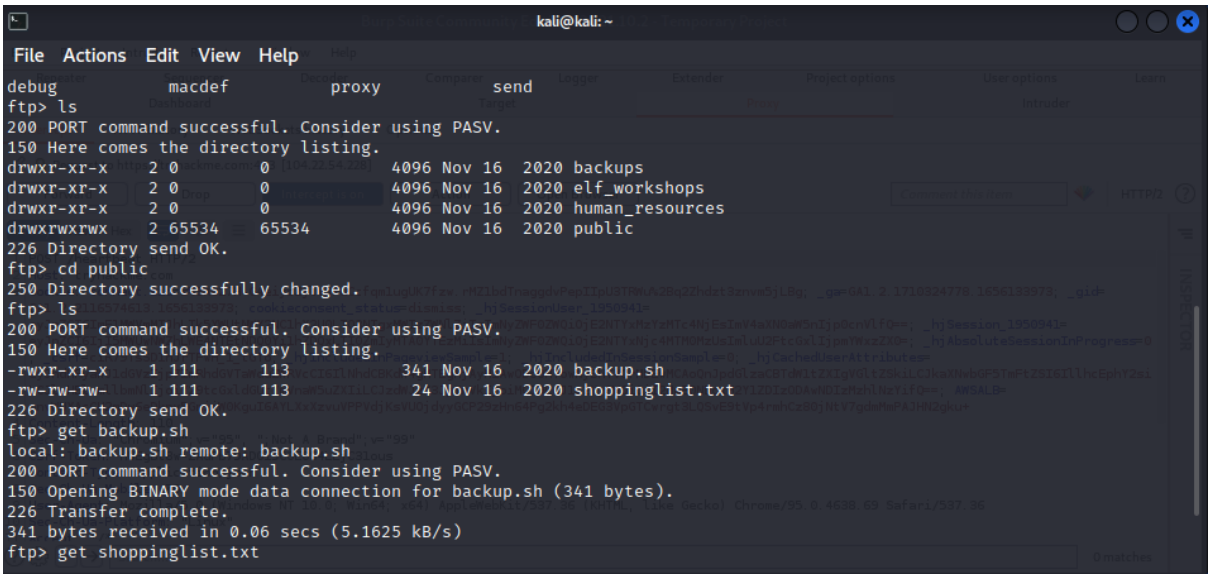
Day 9: Networking – Anyone can be Santa!

Tools used: Kali Linux, Chrome

Solution/walkthrough: DarkSec

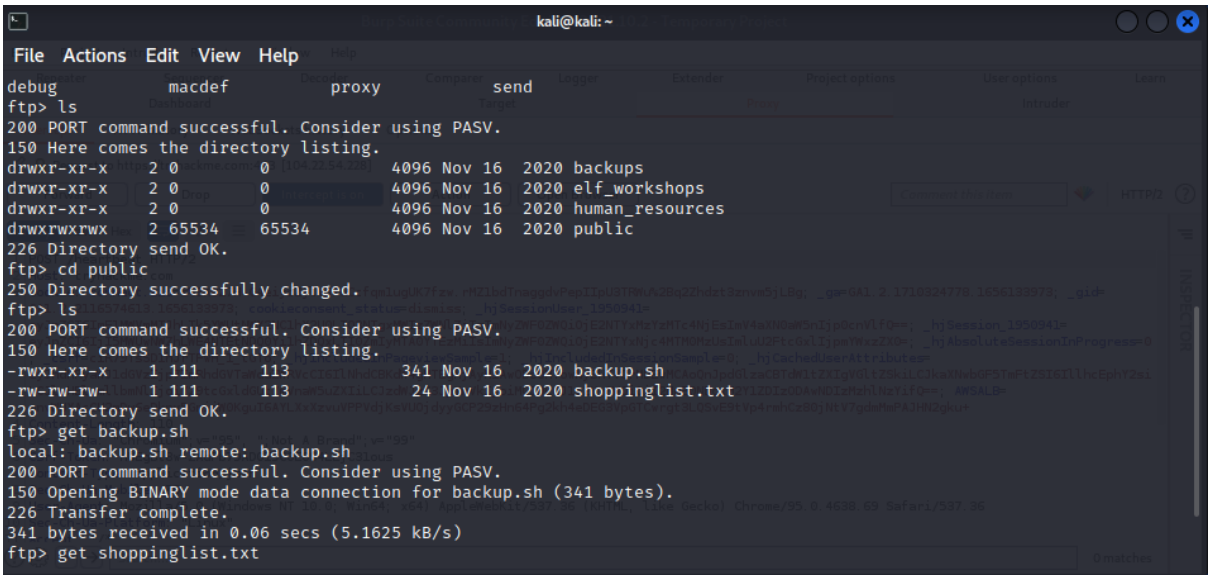
Question 1

What are the directories you found on the FTP site?



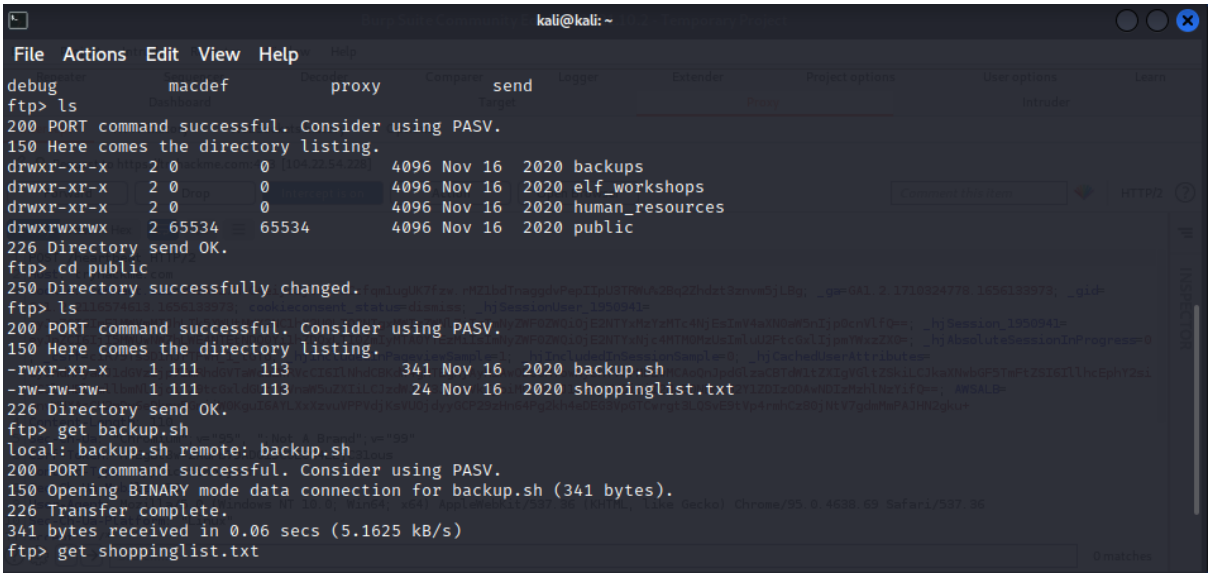
Question 2

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



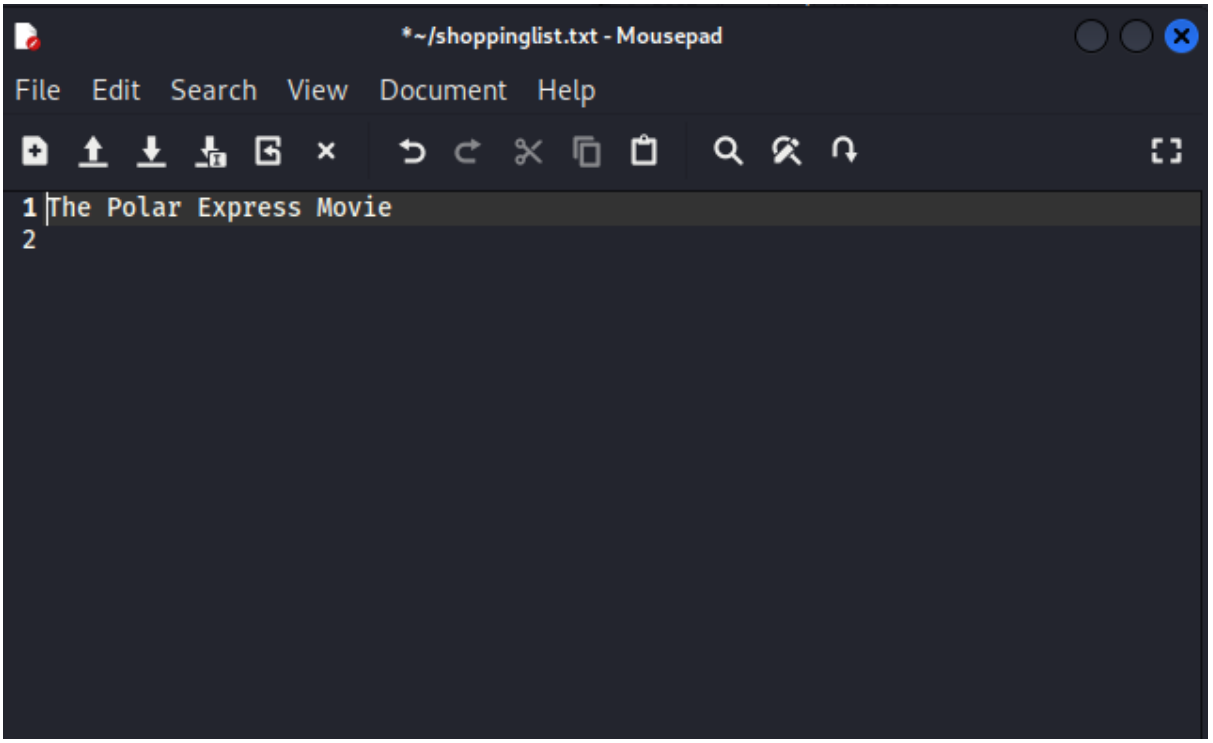
Question 3

What script gets executed within this directory?



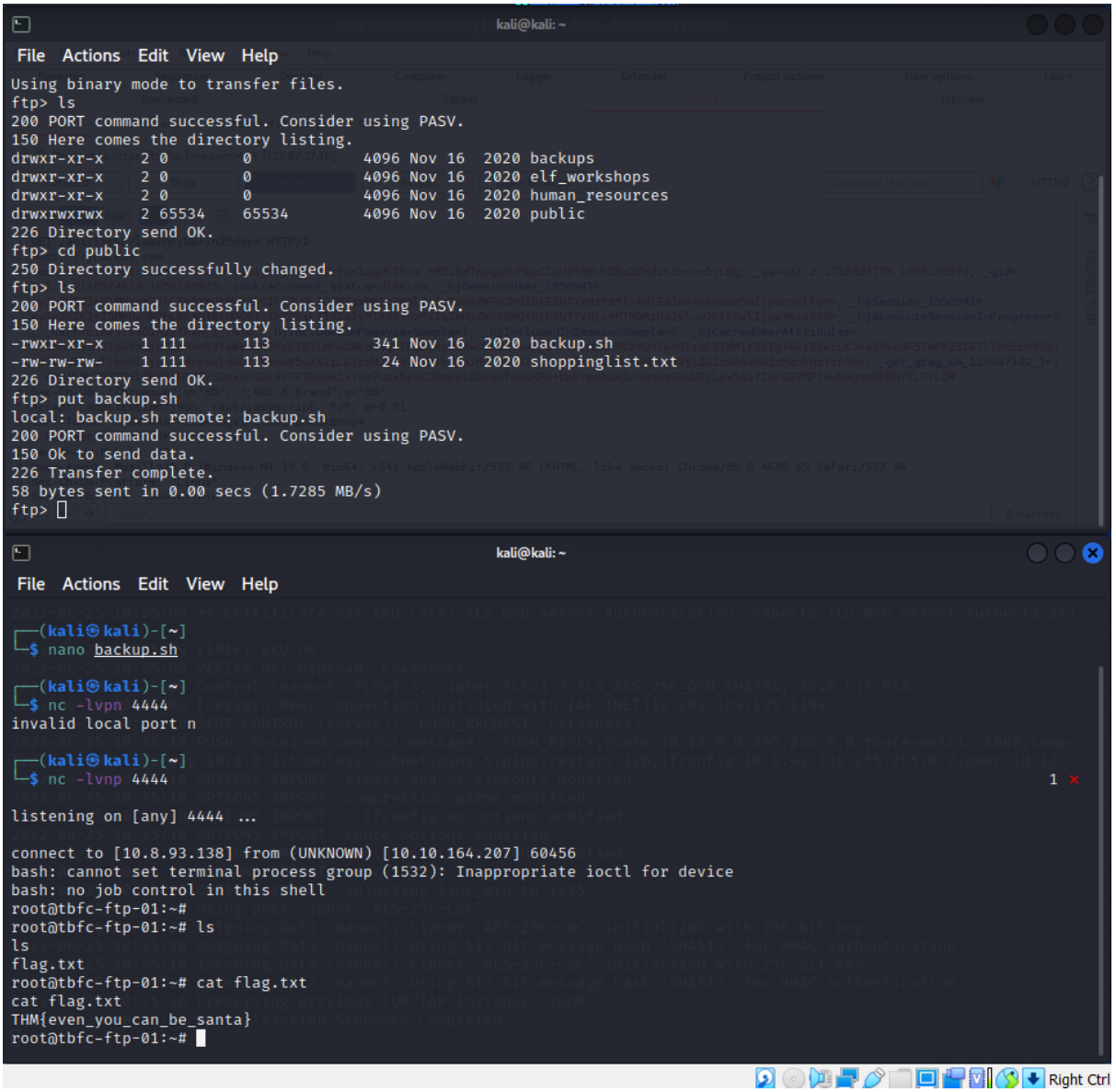
Question 4

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!



Thought Process/Methodology:

I opened the terminal and the ftp server with my ip address. When it is connected, I used the ls command to view the directories. After that, I changed to public and viewed the public directories. Then, I downloaded said directories with the get command. After it was done, I opened the script and viewed what was inside the shoppinglist.txt. Next, I altered the script with nano and put in the pentesters cheatsheet provided. Then, set up a netcat listener to catch the connection. After that, I put in in the backup.sh. When the listener is connected, I opened the flag.txt with the command (cat).

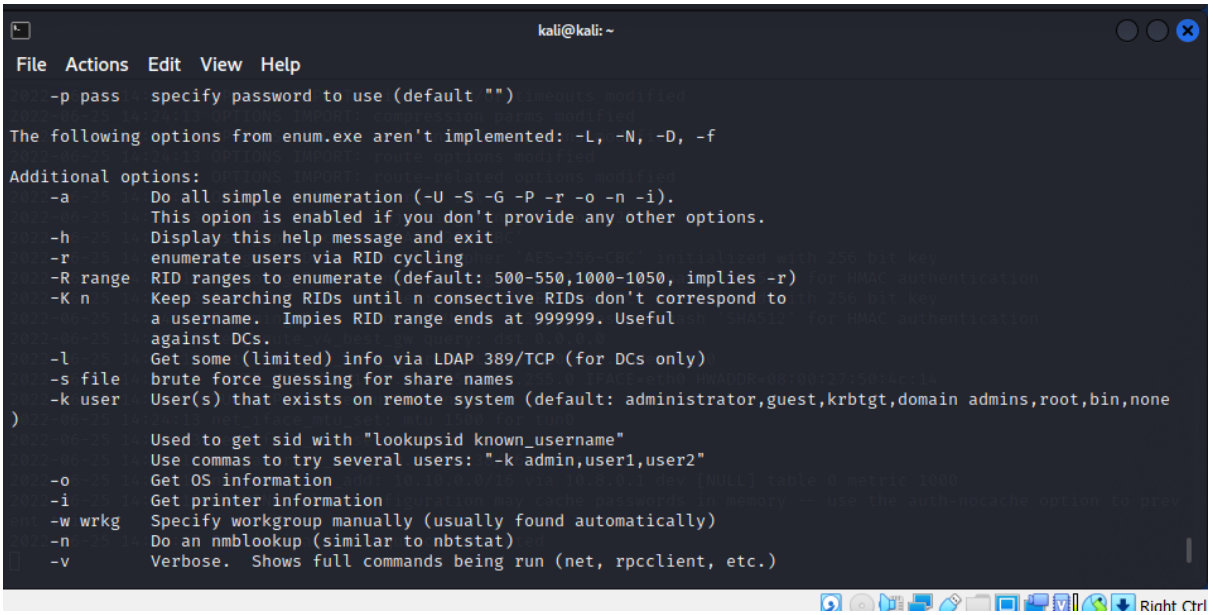
Day 10: Networking – Don't be sElfish!

Tools used: Kali Linux, Chrome

Solution/walkthrough: DarkSec

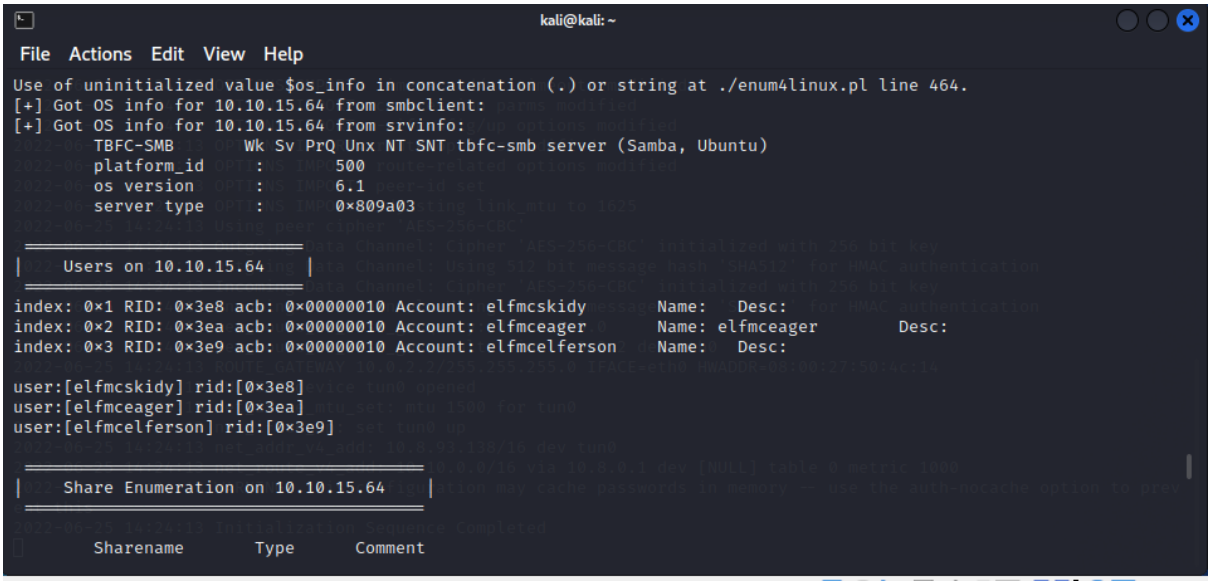
Question 1

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



Question 2

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

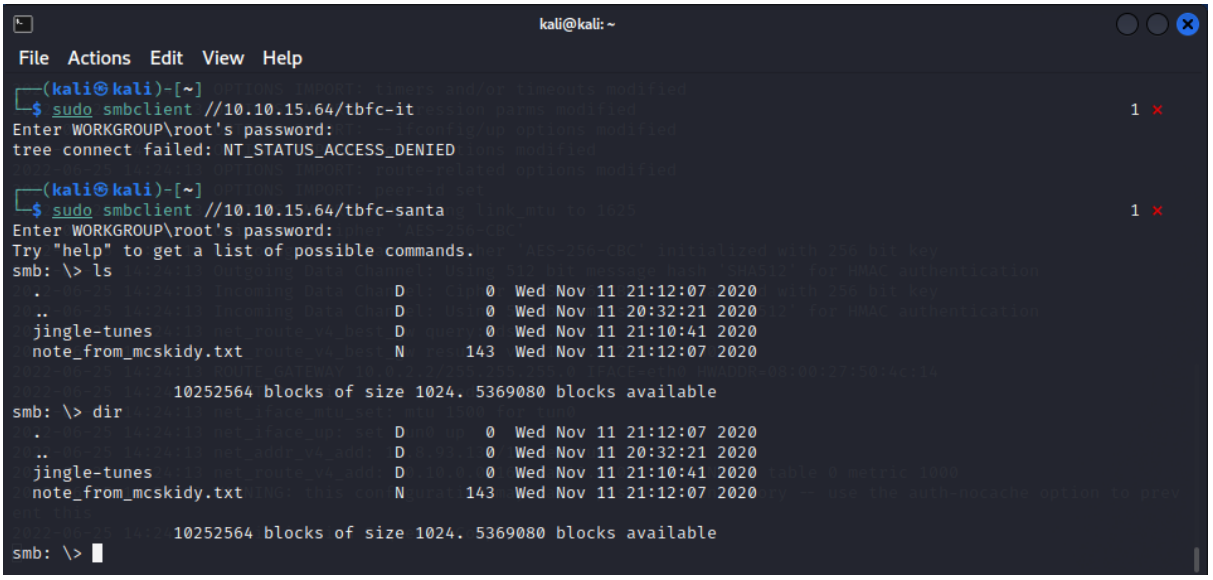


Question 3

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

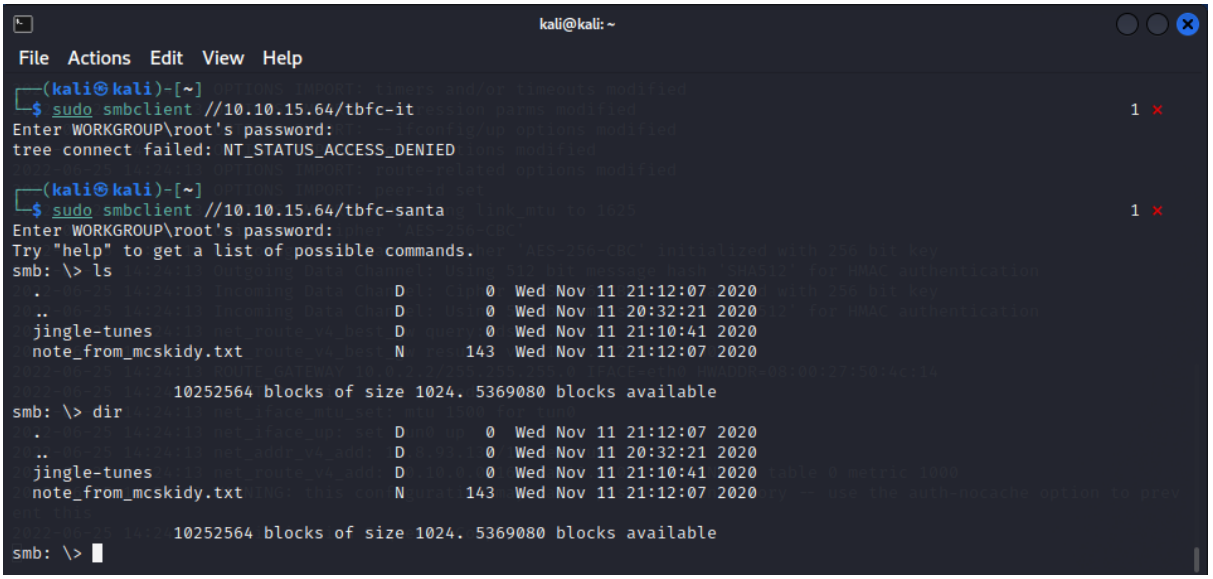
Question 4

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?



Thought Process/Methodology:

I opened the terminal and examined the help options for enum4linux. Then, I ran enum4linux with my IP address. After that, I used smbclient to try to login to the shares on the Samba server and see what share doesn't require a password. After I found out that tbfc-snata doesn't require a password, I logged into it.