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 |

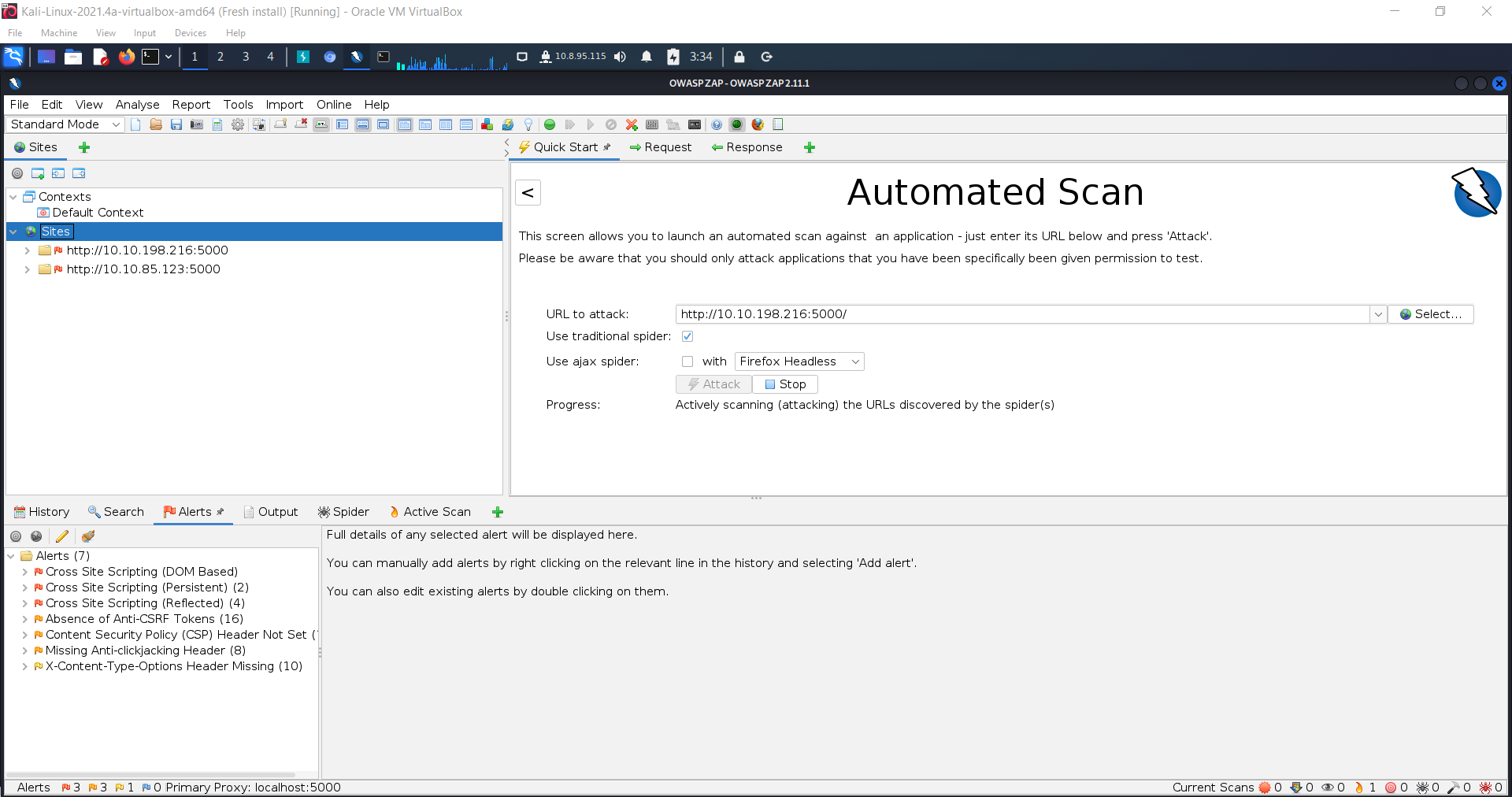
**Day 6: Web Exploitation - Be careful with what you wish on a Christmas night**

**Tools used:** Kali Linux, Chrome

**Solution/walkthrough:**

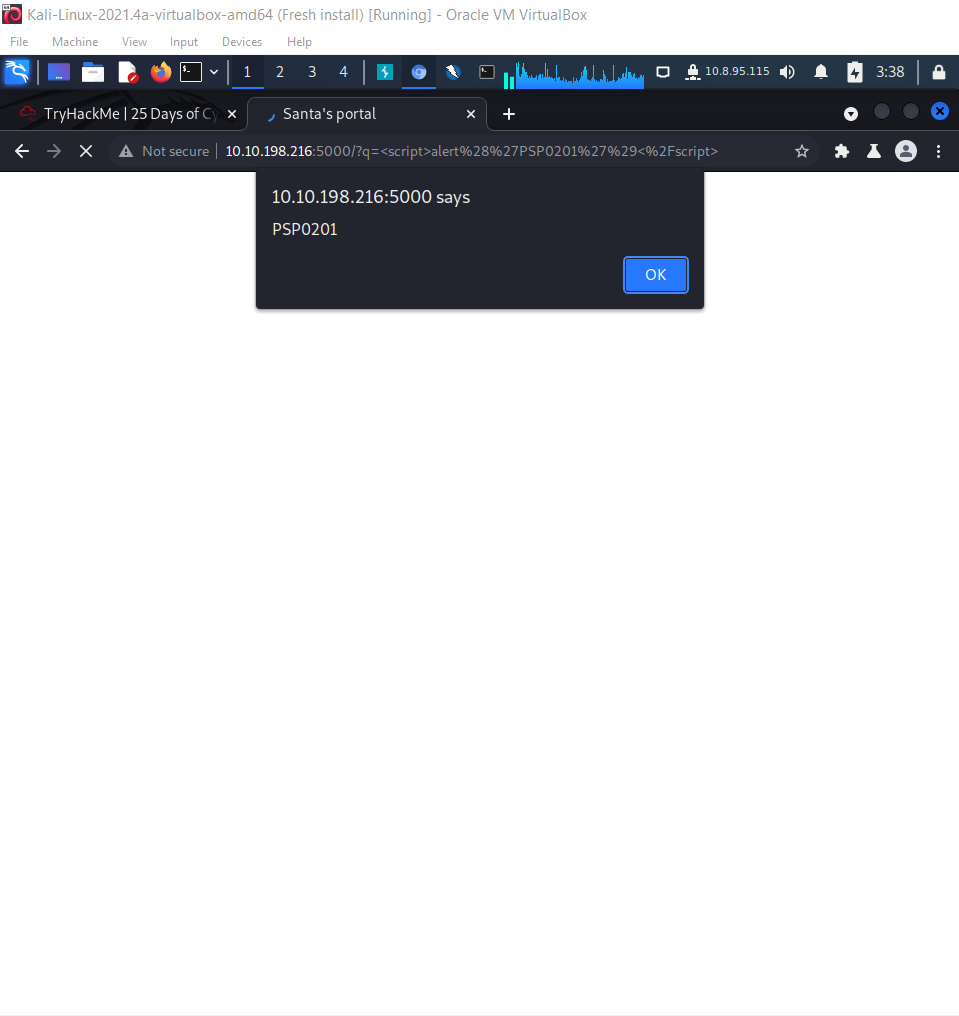
Q5: Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts of high priority are in the scan?

A5: 2



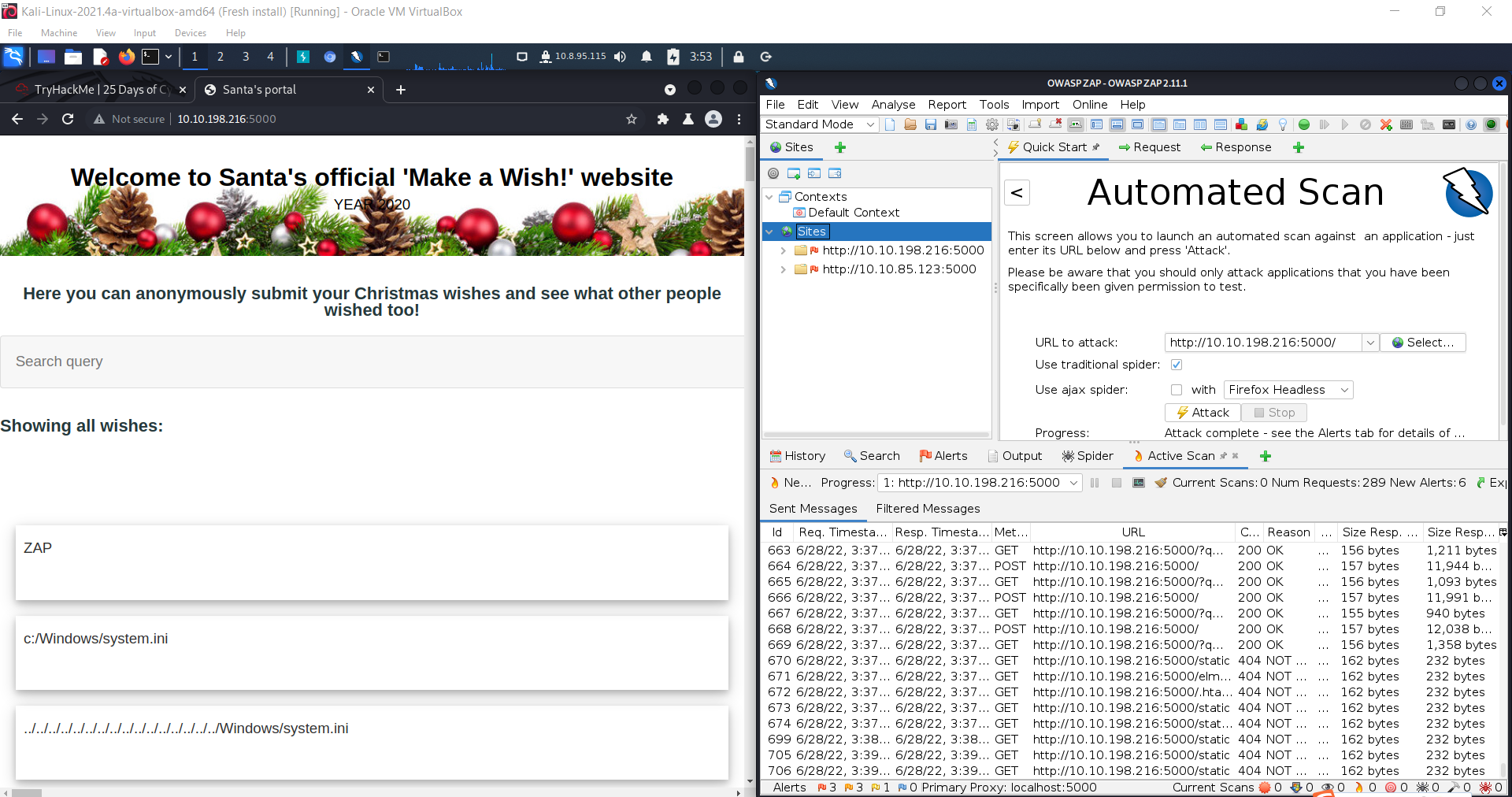
Q6: What Javascript code should you put in the wish text box if you want to show an alert saying "PSP0201"?

A6: <script>alert('PSP0201')</script>



Q7: Close your browser and revisit the site MACHINE-IP:5000 again. Does your XSS attack persist?

A7: No



**Thought Process/Methodology:**

First, I access the OWASP cheatsheet series and check the regular expression used to validate a US Zip code. Then, I go to the back-up server to key in random words in the query box to check what query string can be abused to craft a reflected XSS. Afterwards, I open ZAP and start automated scan to check how many XSS alerts of high priority are in the scan. Next, I know that the command for showing alert is <script>alert()</script>. Therefore, I key in <script>alert(‘PSP0201’)</script> to show an alert saying ‘PSP0201’. Then, I close my browser and revisit the site MACHINE-IP:5000 again, the XSS attack is not persisting anymore.

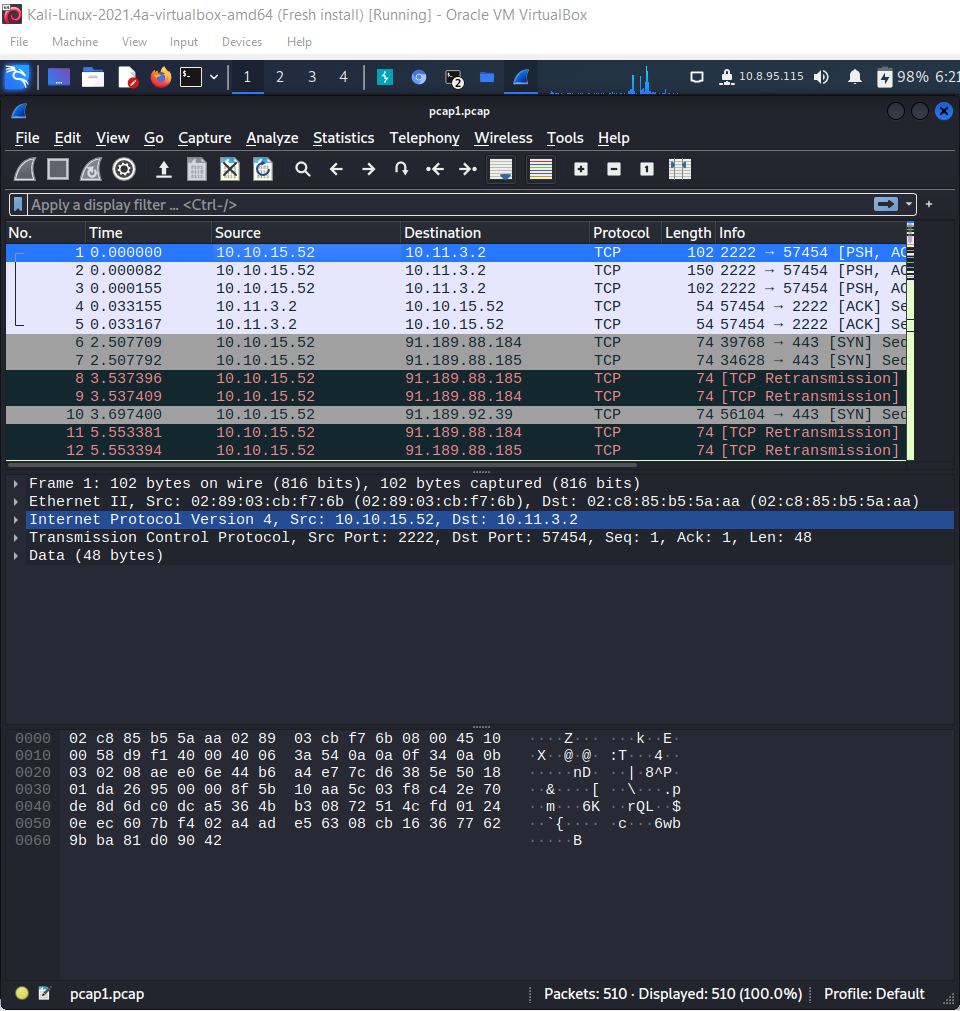
**Day 7: Networking The Grinch Really Did Steal Christmas**

**Tools used:** Kali Linux, Chrome

**Solution/walkthrough:**

Q1: Open "pcap1.pcap" in Wireshark. What is the IP address that initiates an ICMP/ping?

A1: 10.11.3.2

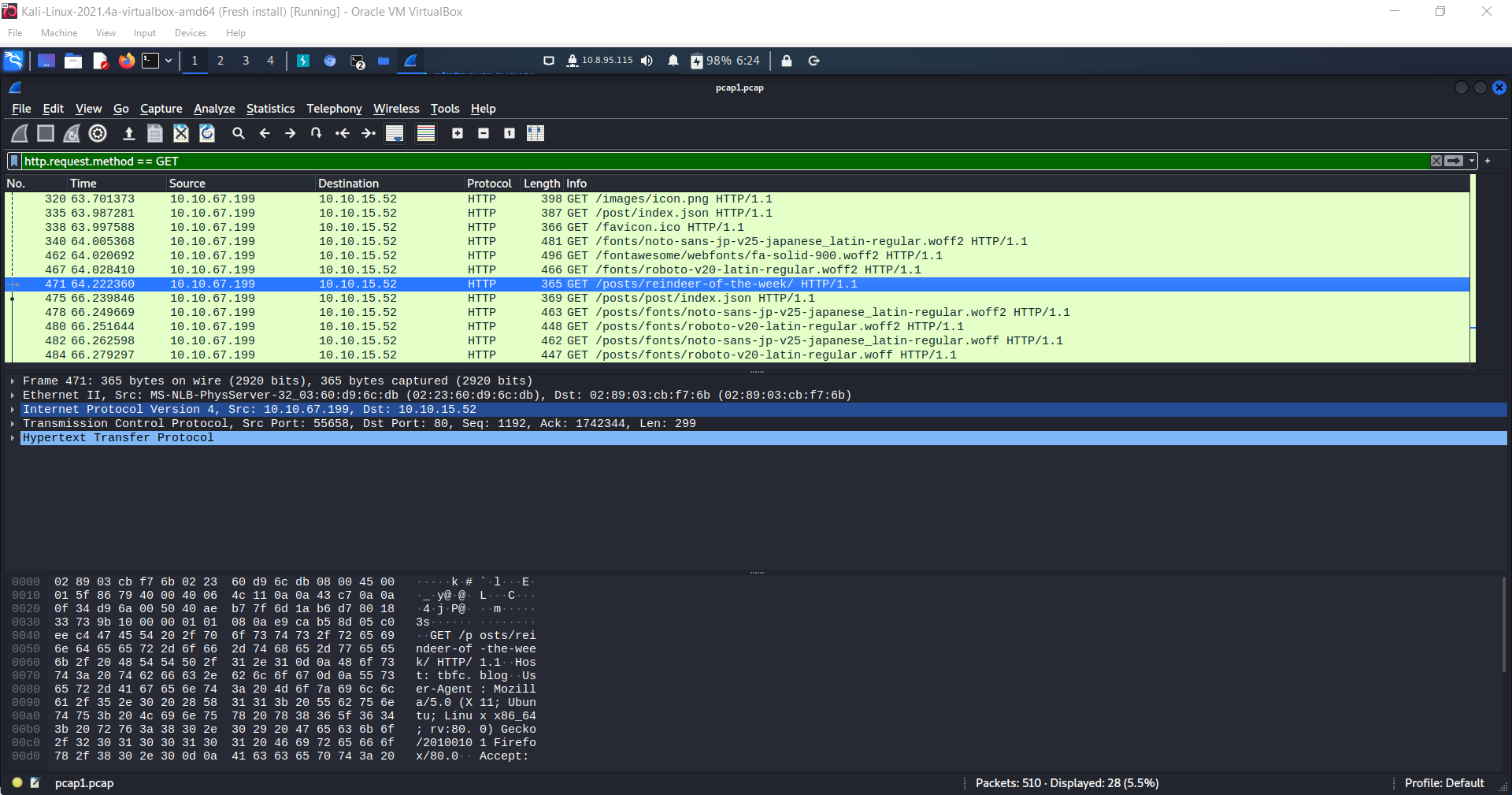


Q2: If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

A2: http.request.method == GET

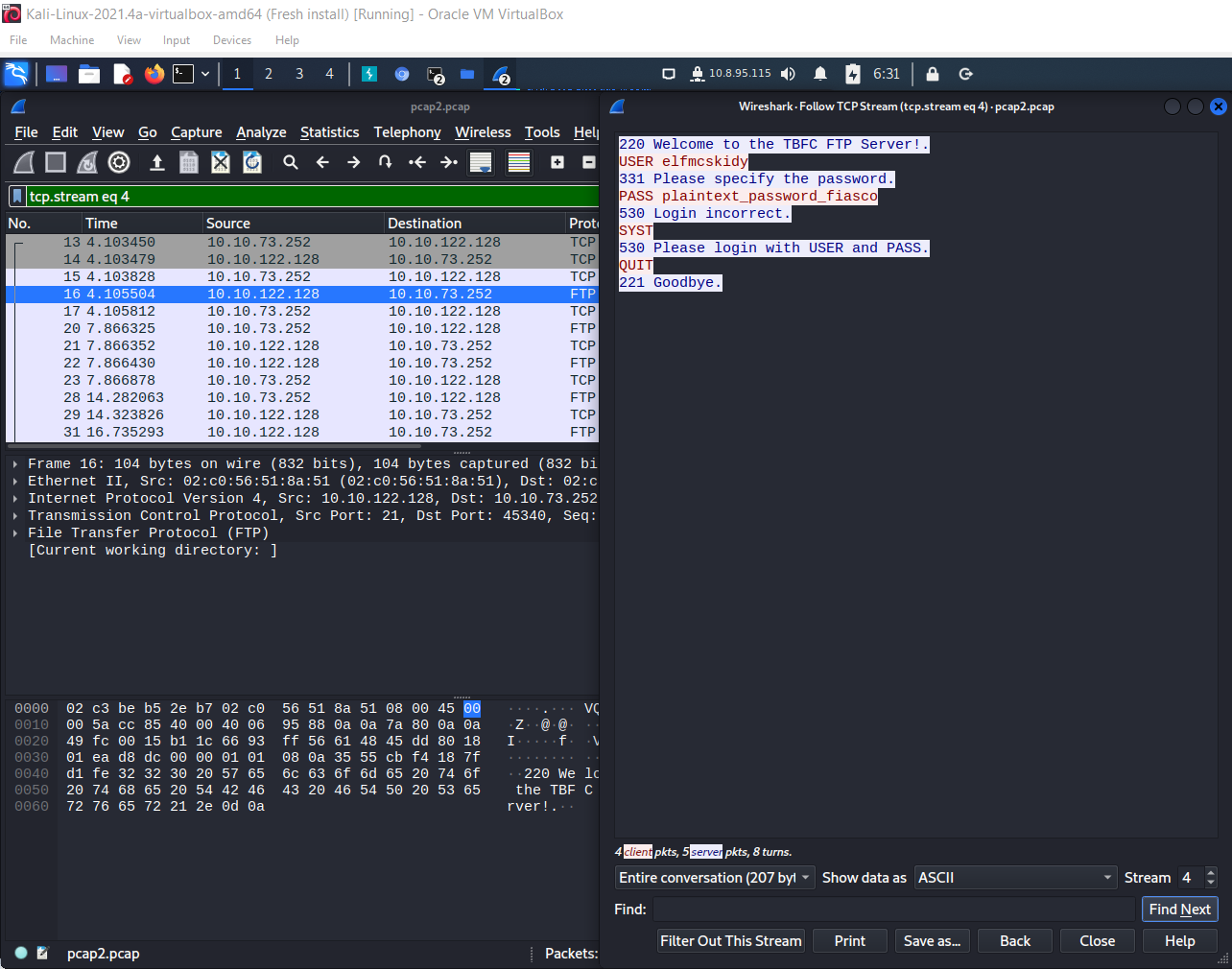
Q3: Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "10.10.67.199" visited?

A3: reindeer-of-the-week



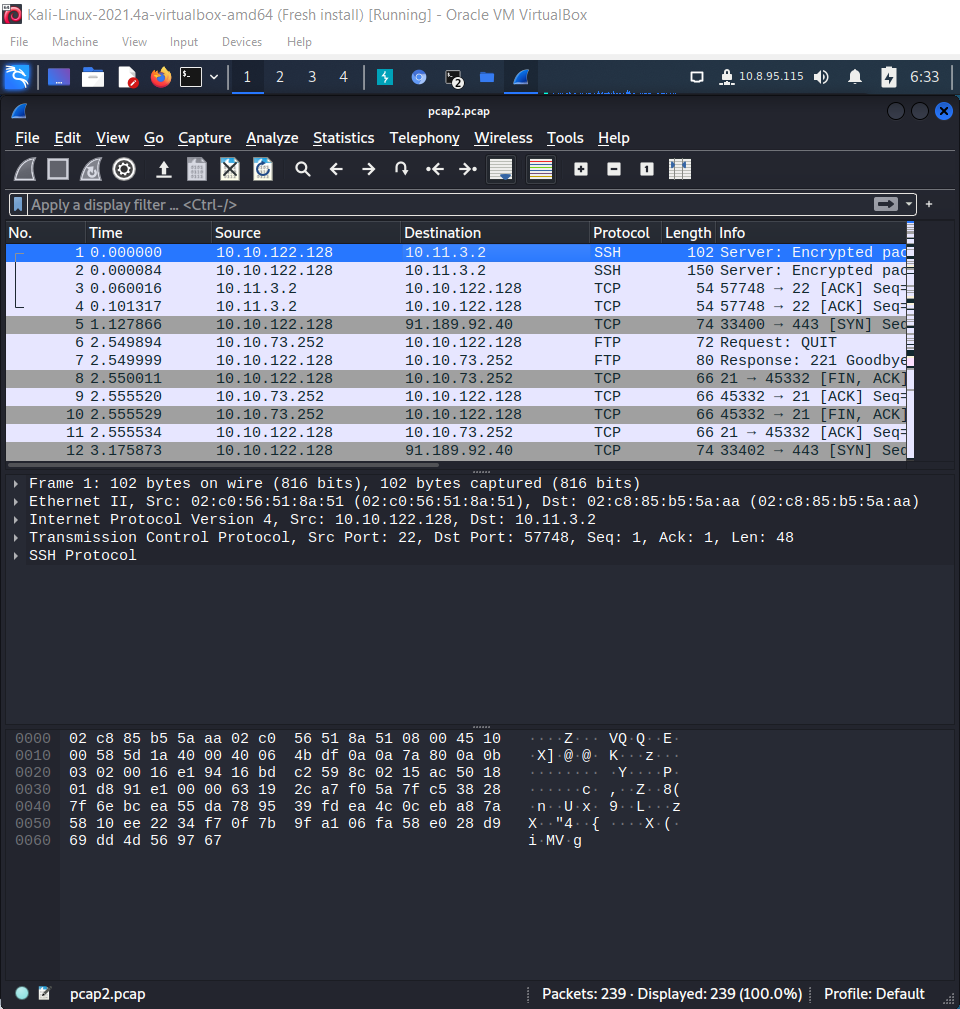
Q4: Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process?

A4: paintext\_password\_fiasco



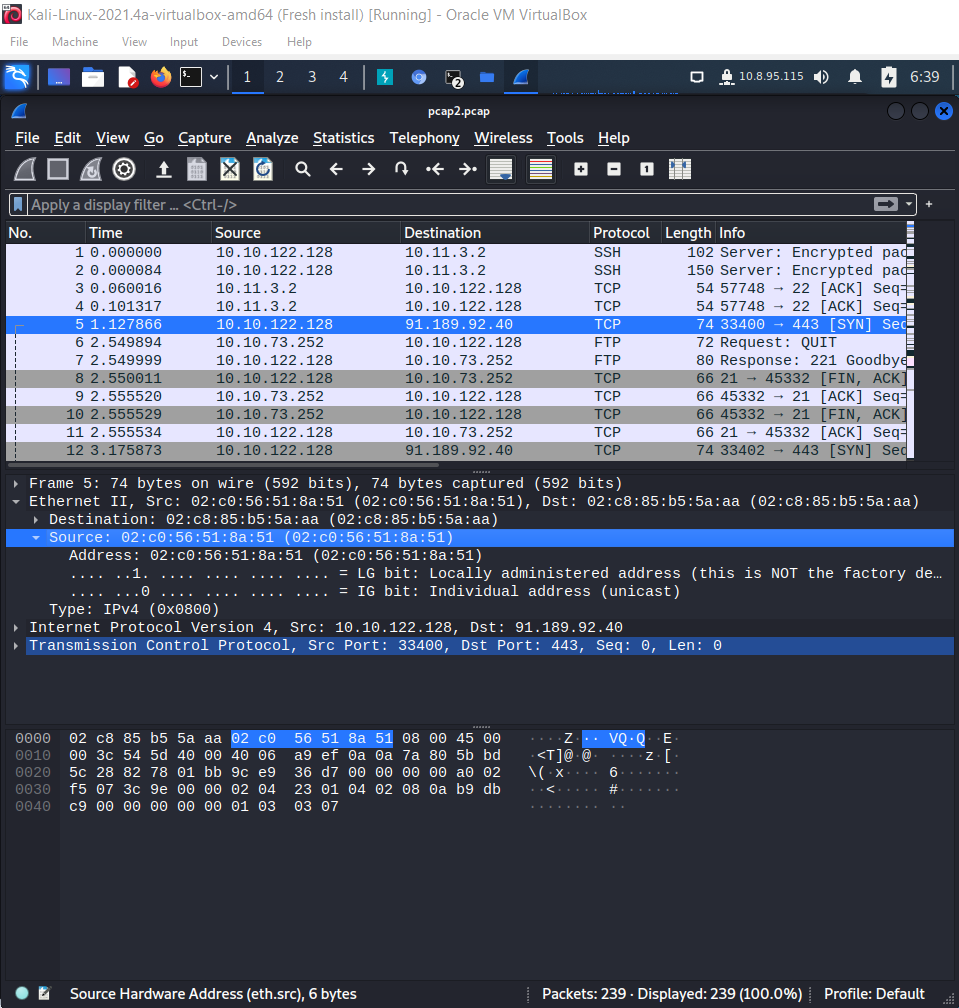
Q5: Continuing with our analysis of "pcap2.pcap", what is the name of the protocol that is encrypted?

A5: SSH



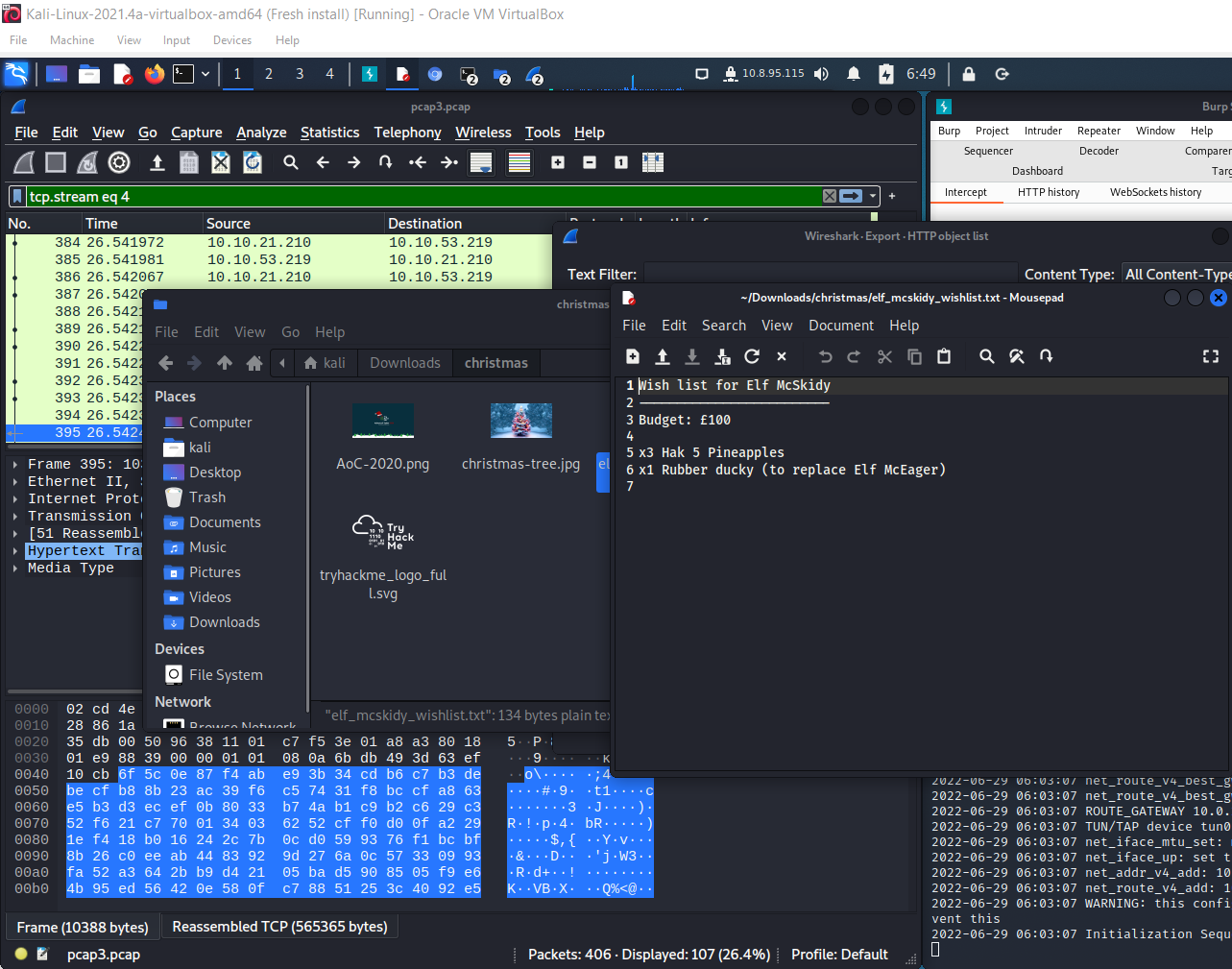
Q6: Examine the ARP communications. Who has 10.10.122.128? Tell 10.10.10.1. Answer: 10.10.122.128 is at

A6: 02:c0:56:51:8a:51



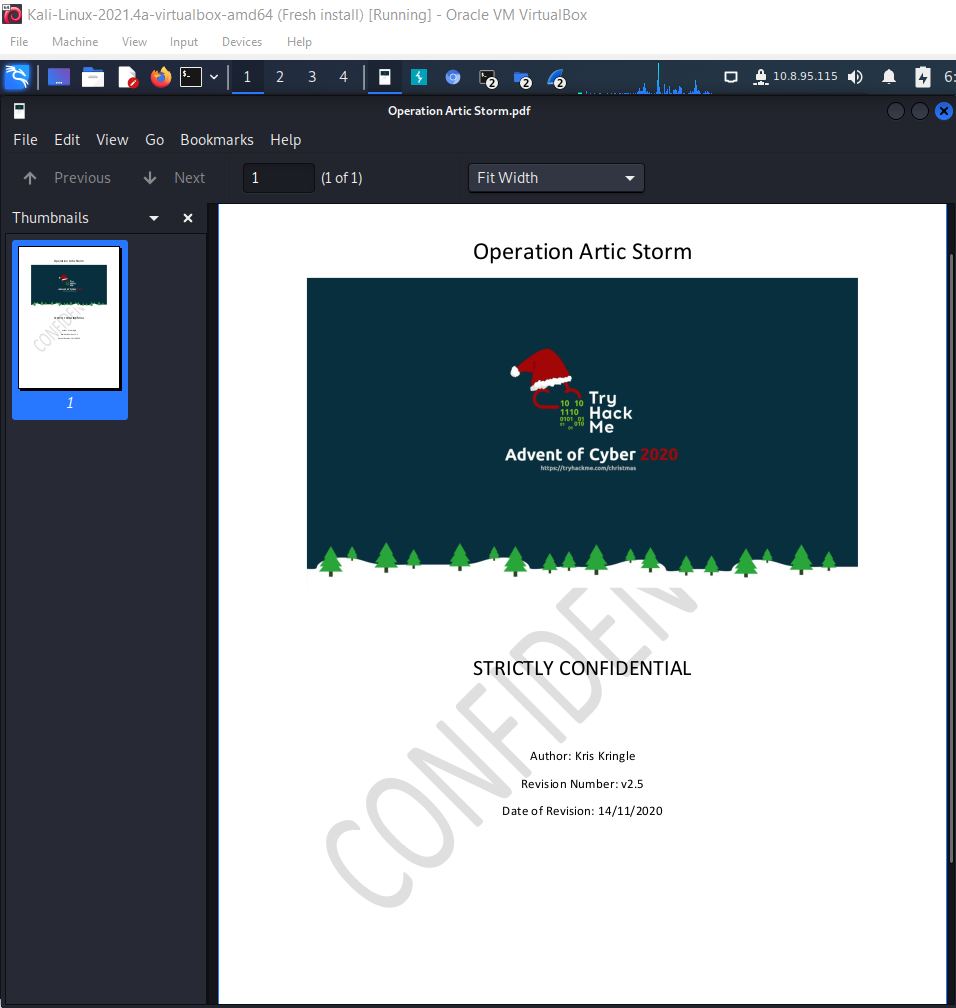
Q7: Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

A7: rubber ducky



Q8: Who is the author of Operation Artic Storm?

A8: Kris Kringle



**Thought Process/Methodology:**

First, I download the zip file from TryHackMe website and unzip it. I get pcap1, 2, 3 file. Then, I install Wireshark and use it to open pcap 1 file. And I see the IP address that initiates an ICMP/ping. Then, I apply a display filter ‘http.request.method == GET’ to get the name of the article that the IP address ’10.10.67.199’. Next, I open pcap 2 file, apply the display filter ‘tcp.port == 21’ to get the password leaked during the login process. Next, I open pcap 3 file to export christmas.zip and unzip it to get Elf McSkidy's wishlist that will be used to replace Elf McEager.

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

**Tools used:** Kali Linux, Chrome

**Solution/walkthrough:**

Q2: Using Nmap on MACHINE\_IP , what are the port numbers of the three services running?

80, 2222, 3389

Q3: 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

Q4: What is the version of Apache?

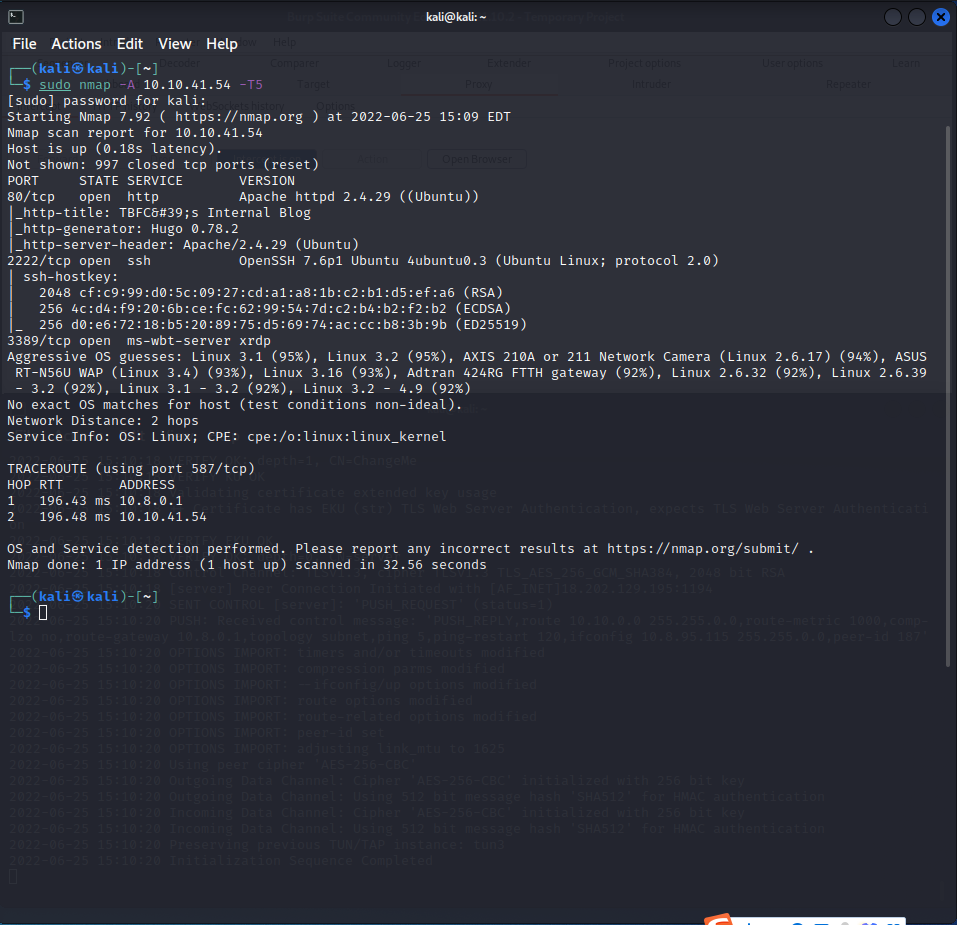
2.4.29

Q5: What is running on port 2222?

SSH

Q6: 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



**Thought Process/Methodology:**

First, I open the terminal and key in ‘sudo nmap –A [MACHINE-IP] –T5’, and it shows everything to me.

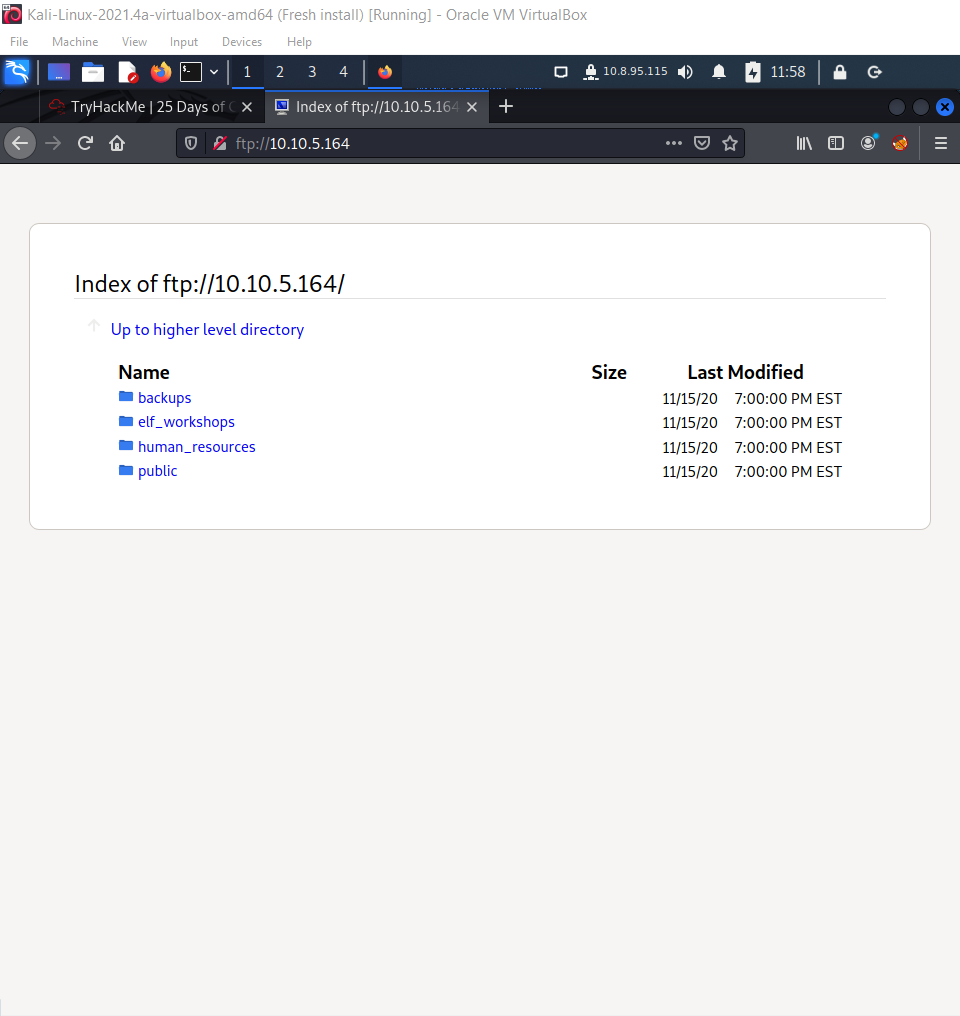
**Day 9: Networking - Anyone can be Santa!**

**Tools used:** Kali Linux, Chrome

**Solution/walkthrough:**

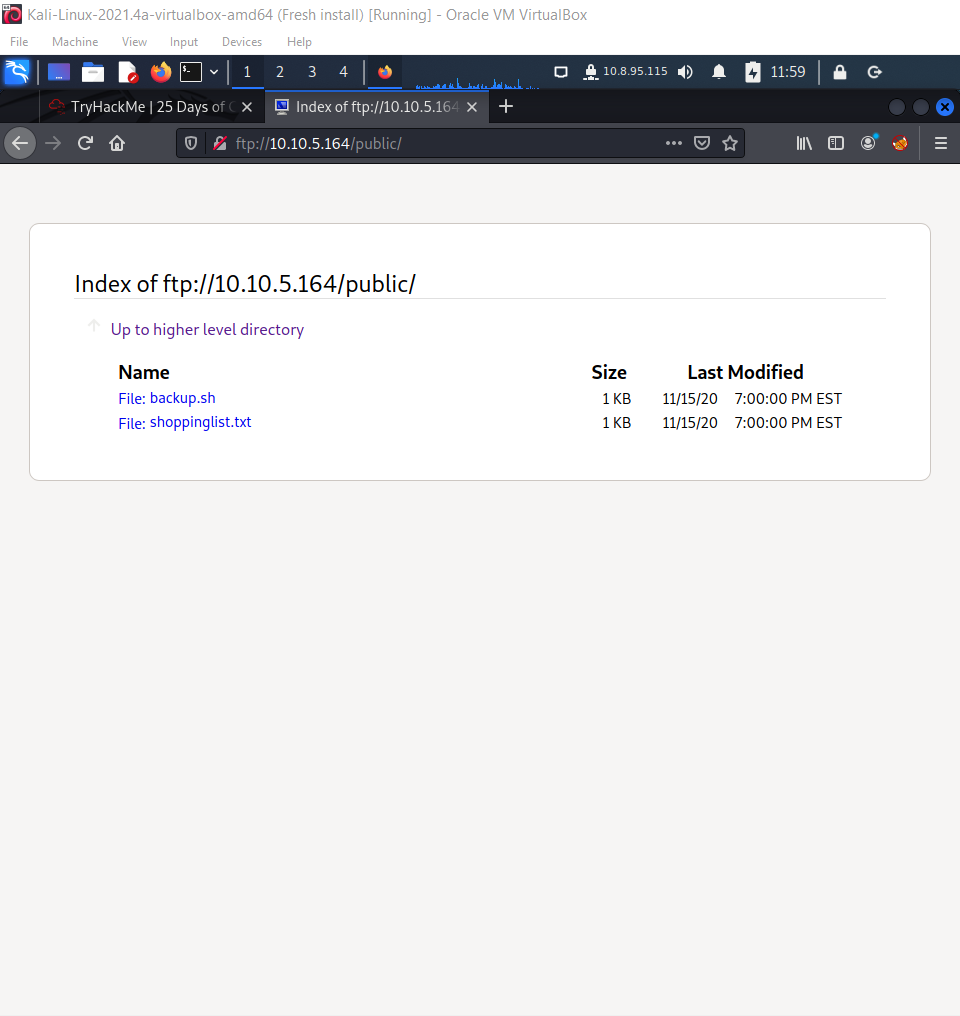
Q1: What are the directories you found on the FTP site?

A1: backups, elf\_workshops, human\_resources, public

****

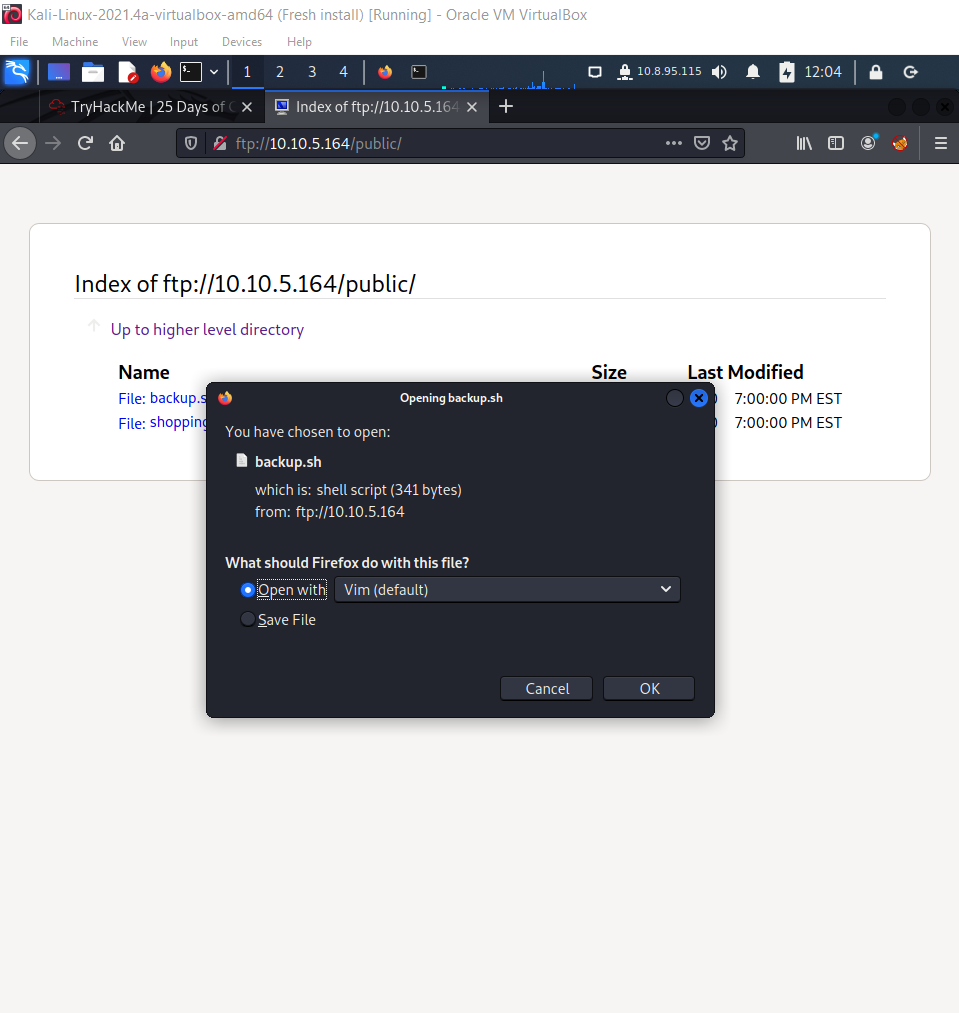
Q2: Name the directory on the FTP server that has data accessible by the "anonymous" user

A2: public

****

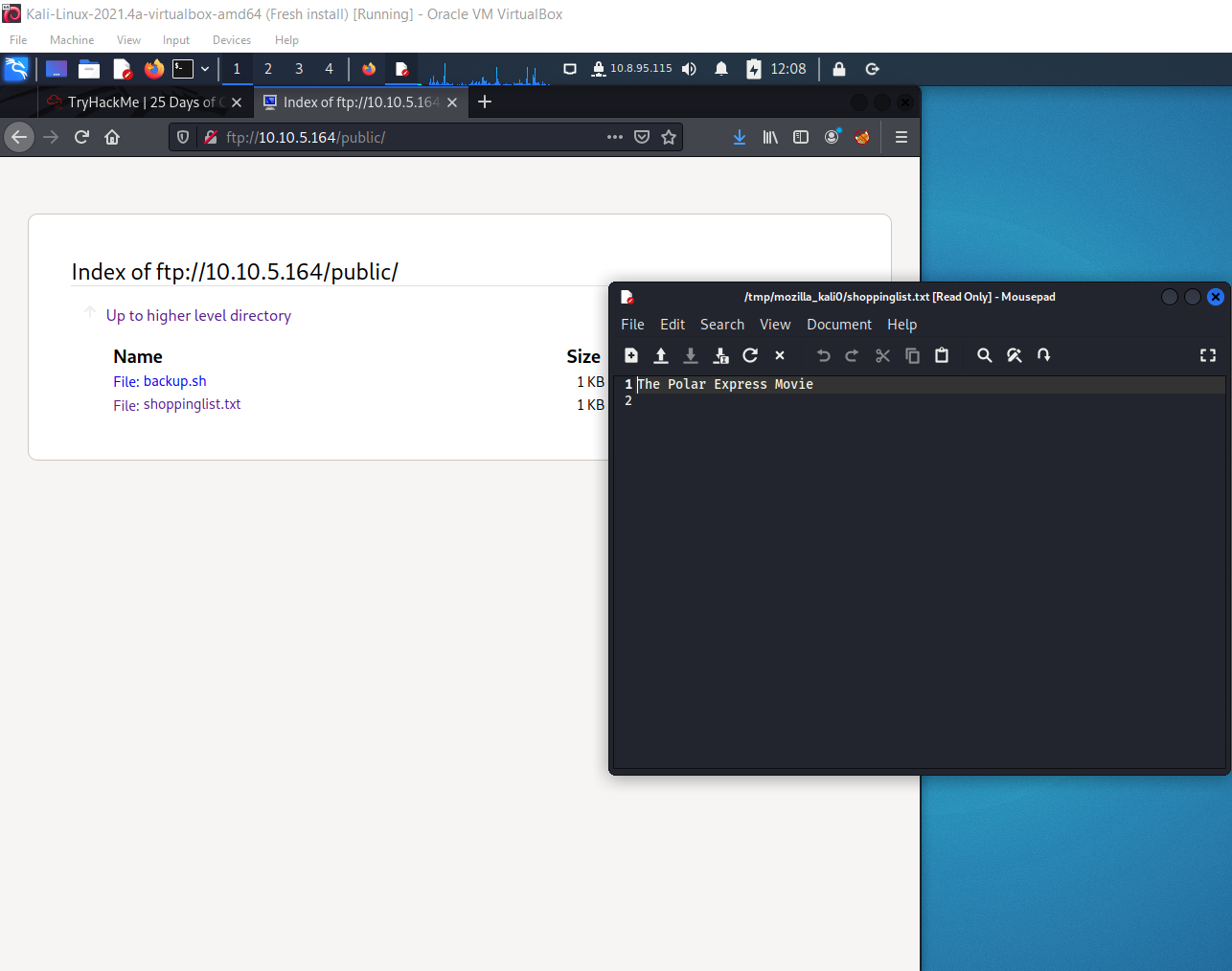
Q3: What script gets executed within this directory?

A3: backup.sh



Q4: What movie did Santa have on his Christmas shopping list?

A4: The Polar Express Movie



Q5: Re-upload this script to contain malicious data (just like we did in section 9.6. Output the contents of /root/flag.txt!

A5: THM{even\_you\_can\_be\_santa}



**Thought Process/Methodology:**

First, I key in <ftp://[MACHINE-IP>] to check the information I need. Afterwards, I open first terminal and key in ftp [MACHINE-IP], change directory into ‘public’ and get backup.sh. Then, I use the command ‘nano’ to change the content of backup.sh. Then, I open second terminal and key in ‘nc –lvnp 4444’. Later, I put back the backup.sh into the ‘public’. After a while, the second terminal shows the flag.txt. I use the command ‘cat’ to check what the content inside the flag.txt is.

**Day 10: Networking - Don't be sElfish!**

**Tools used:** Kali Linux, Chrome

**Solution/walkthrough:**

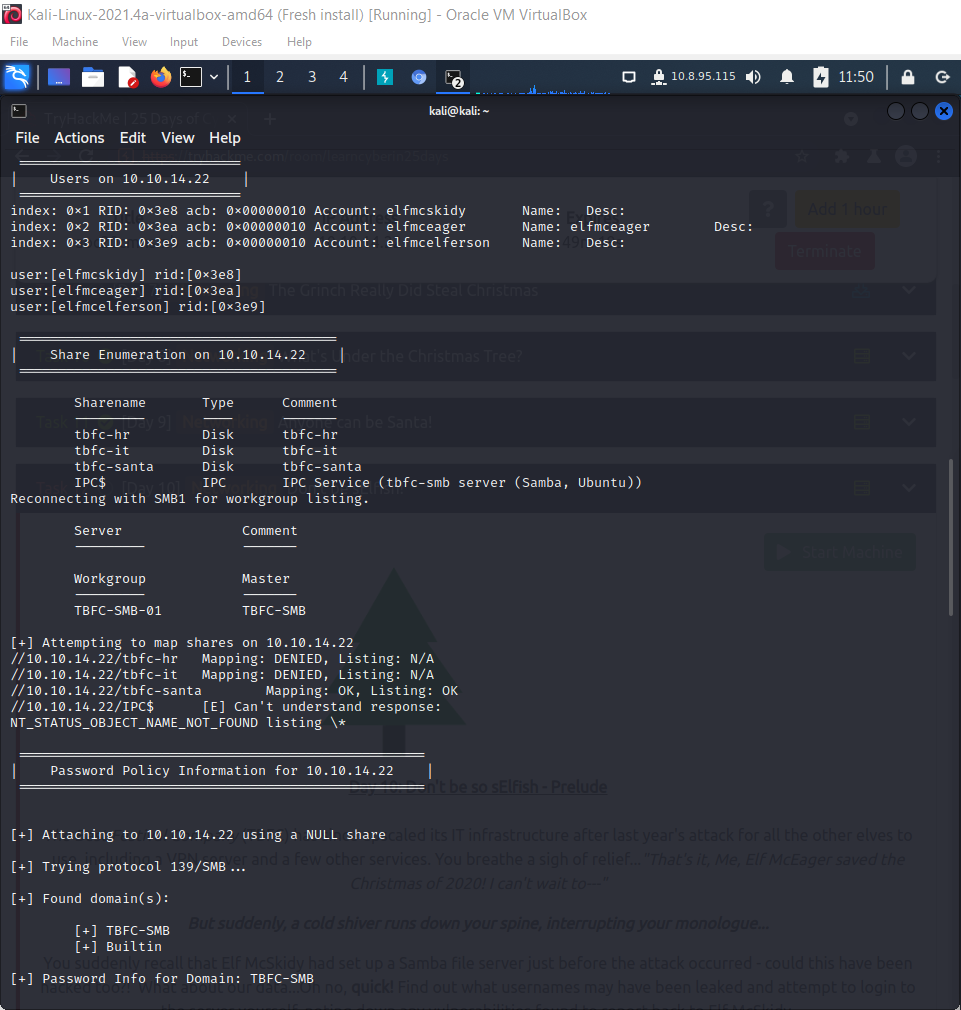
Q1: Examine the help options for enum4linux. Match the following flags with the descriptions.

A1:



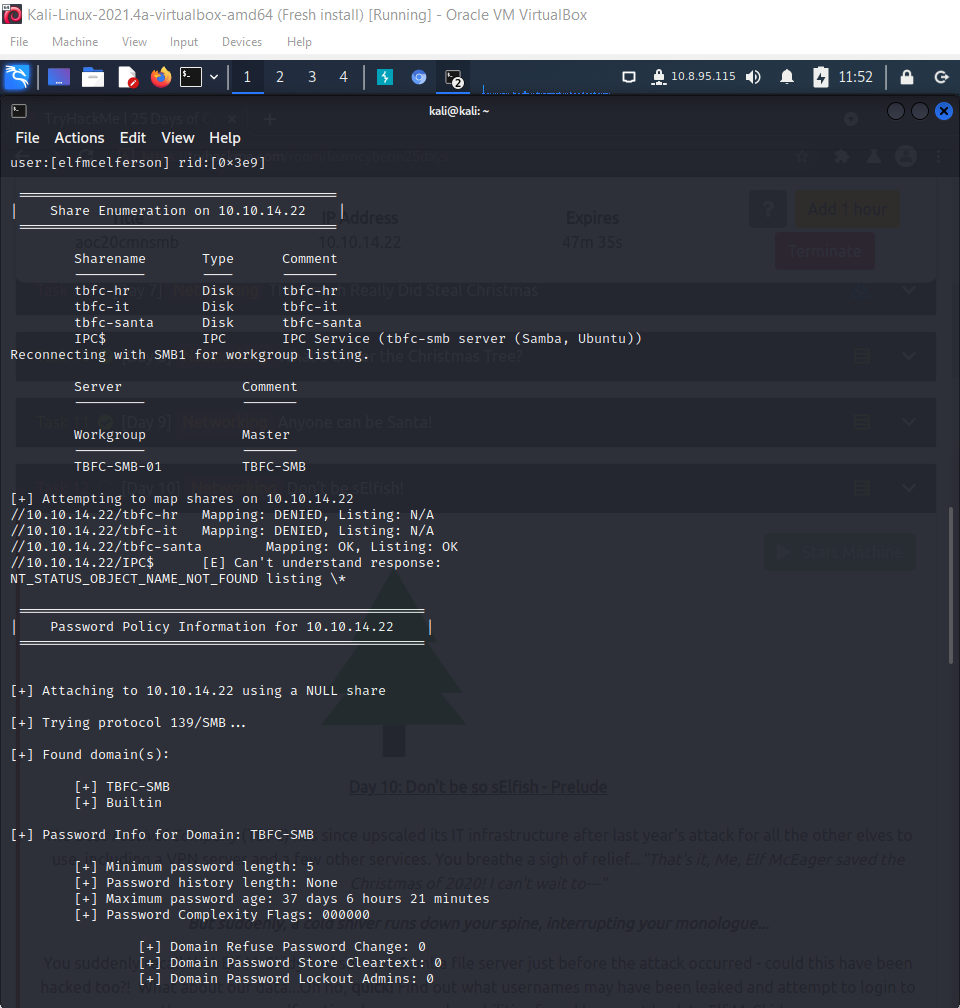
Q2: Using enum4linux, how many users are there on the Samba server?

A2: 3



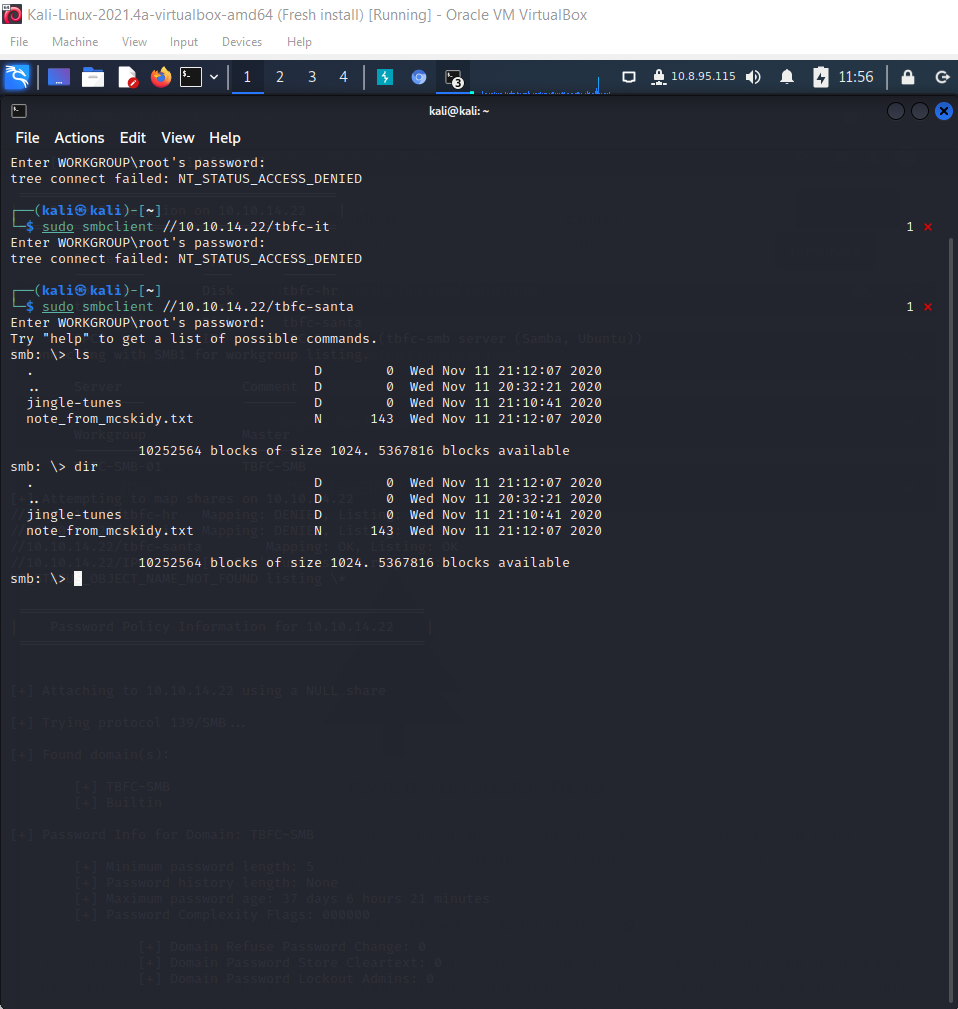
Q3: Now how many "shares" are there on the Samba server?

A3: 4



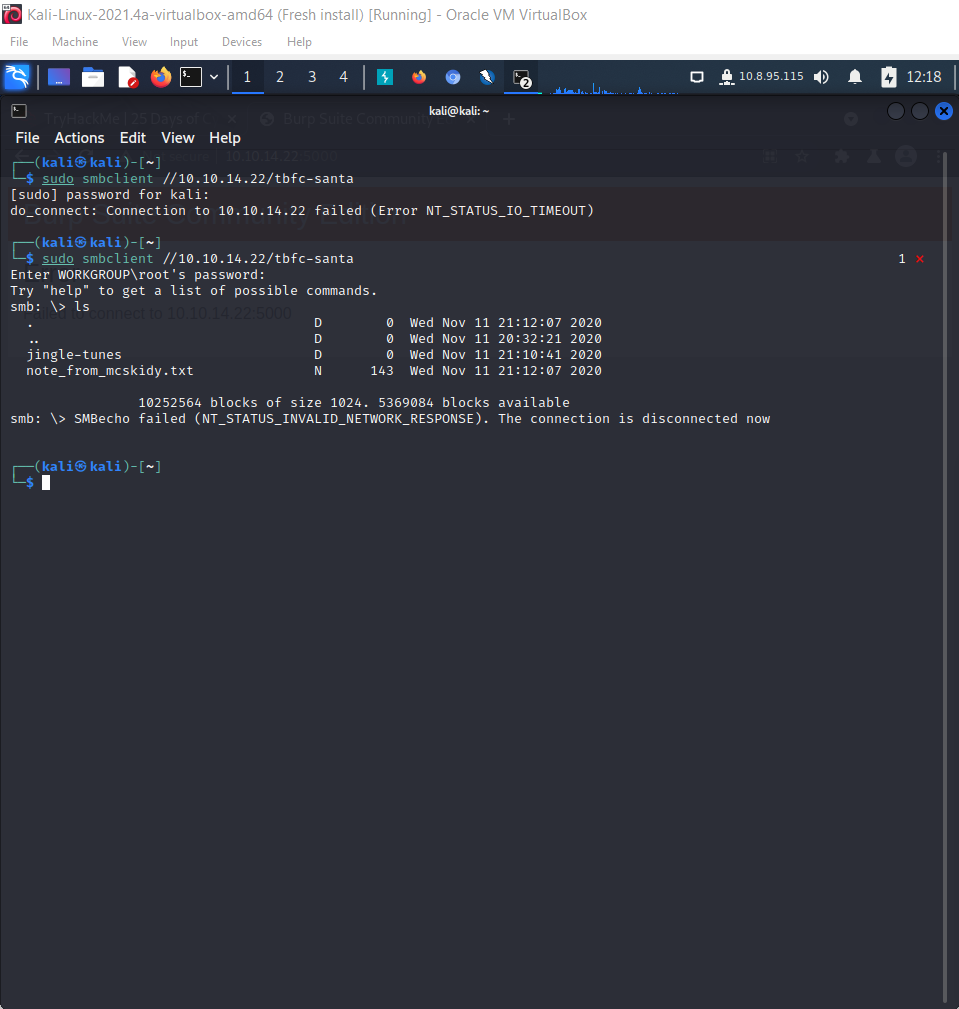
Q4: Use smbclient to try to login to the shares on the Samba server. What share doesn't require a password?

A4: tbfc-santa



Q5: Log in to this share, what directory did ElfMcSkidy leave for Santa?

A5: jingle-tunes

****

**Thought Process/Methodology:**

First, I open the terminal and key in ‘sudo enum4linux’ and it shows the help message and the information I need. Then, I key in ‘sudo smbclient //[MACHINE-IP]/[SHARENAME]’ by using different sharenames showed in the terminal one by one. I find that tbfc-santa doesn’t require a password to login to the shares on the Samba server. After logging into this share, I found jingle-tunes did ElfMcSkidy leave for Santa.