PSP0201

Week 3

Writeup

Group Name: Woohoo

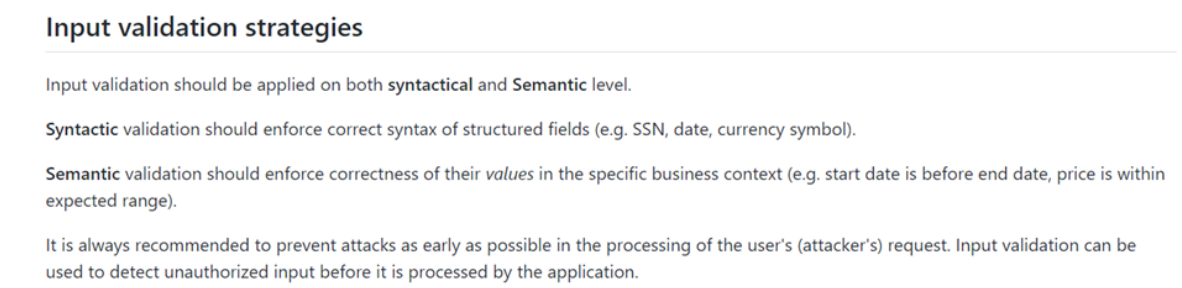
Members

ID	Name	Role
1211100312	CHAN HAO YANG	Leader
1211101506	LEONG JIA YI	Member
1211101961	CHAI DI SHENG	Member
1211101726	TAI JIN PEI	Member

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

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

Solution/walkthrough:



Input validation strategies

Input validation should be applied on both **syntactical** and **Semantic** level.

Syntactic validation should enforce correct syntax of structured fields (e.g. SSN, date, currency symbol).

Semantic validation should enforce correctness of their *values* in the specific business context (e.g. start date is before end date, price is within expected range).

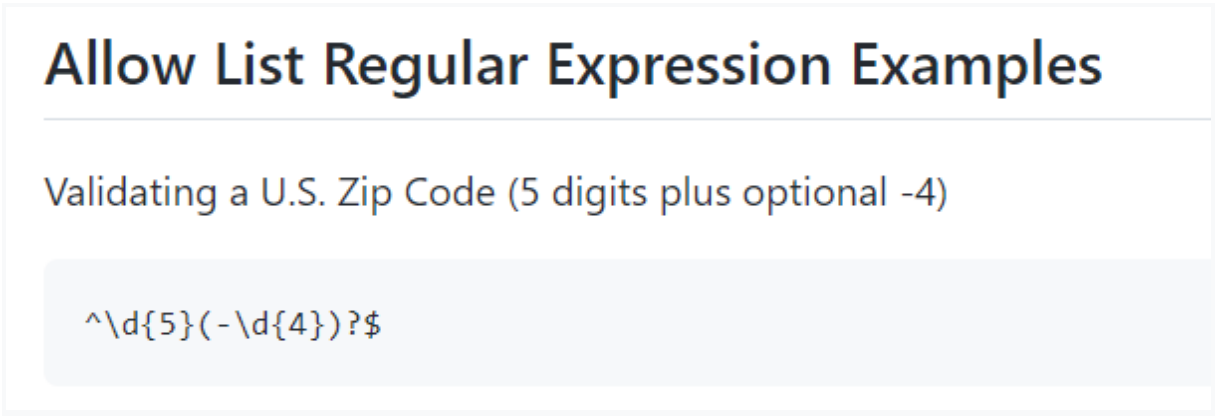
It is always recommended to prevent attacks as early as possible in the processing of the user's (attacker's) request. Input validation can be used to detect unauthorized input before it is processed by the application.

Open the link and find the description of syntactic and semantic:
https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Input_Validation_Cheat_Sheet.md

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

Answer: Syntactic : enforce correct syntax of structured fields

Semantic : enforce correctness of their values in the specific business context



Allow List Regular Expression Examples

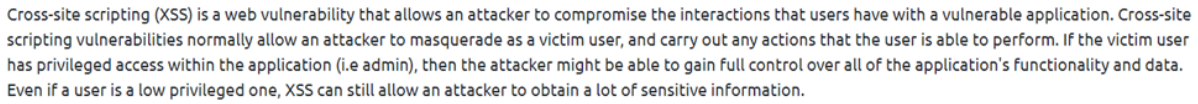
Validating a U.S. Zip Code (5 digits plus optional -4)

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

Look for validating a U.S. zip code in the link.

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

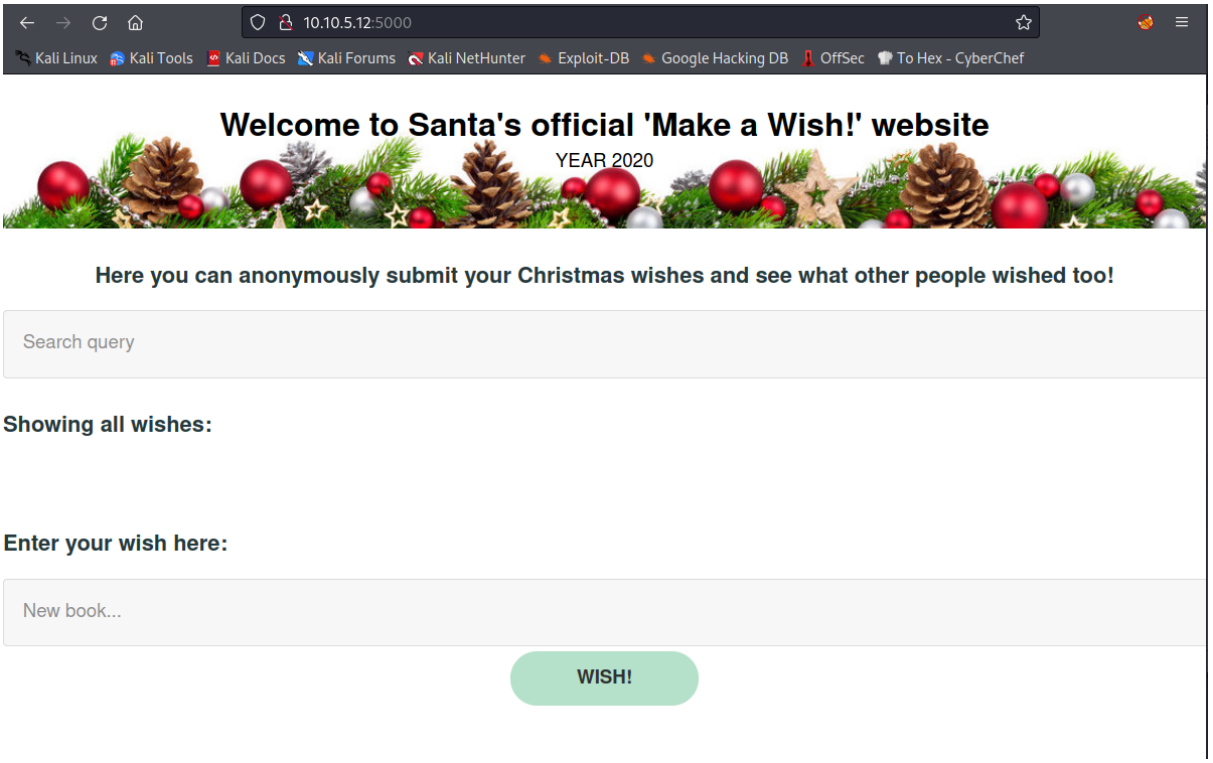
Answer: ^\d{5}(-\d{4})?$

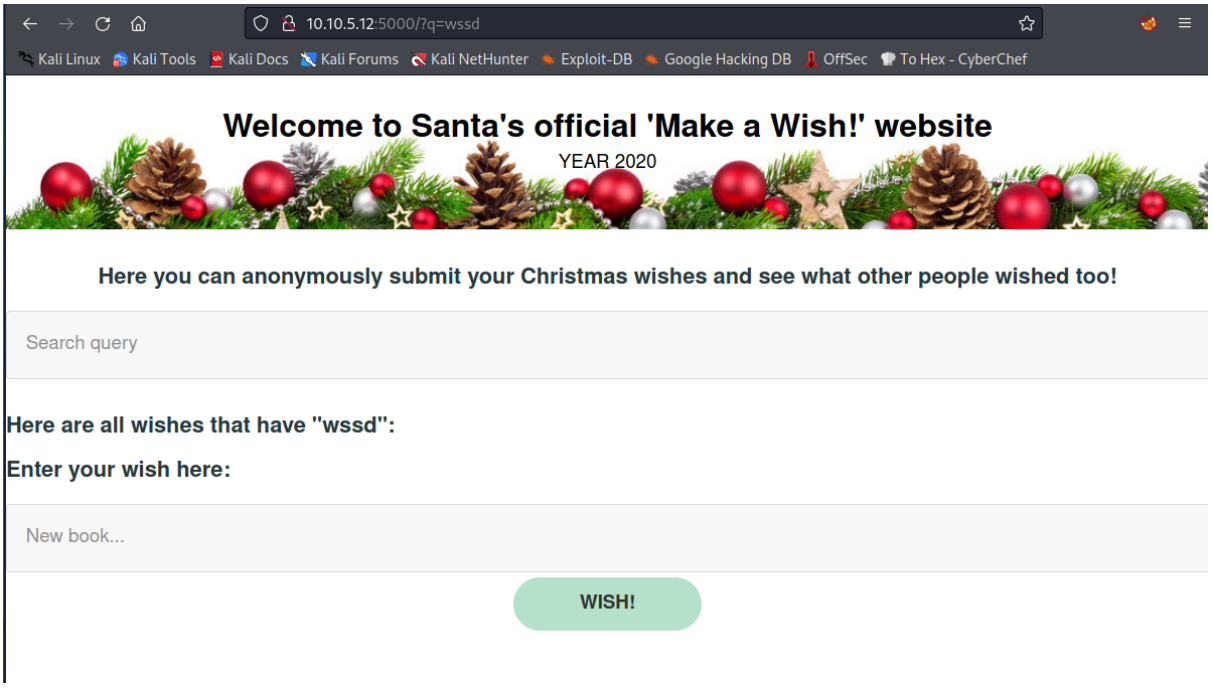


Cross-site scripting (XSS) is a web vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, and carry out any actions that the user is able to perform. If the victim user has privileged access within the application (i.e admin), then the attacker might be able to gain full control over all of the application's functionality and data. Even if a user is a low privileged one, XSS can still allow an attacker to obtain a lot of sensitive information.

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

Answer: Stored cross-site scripting

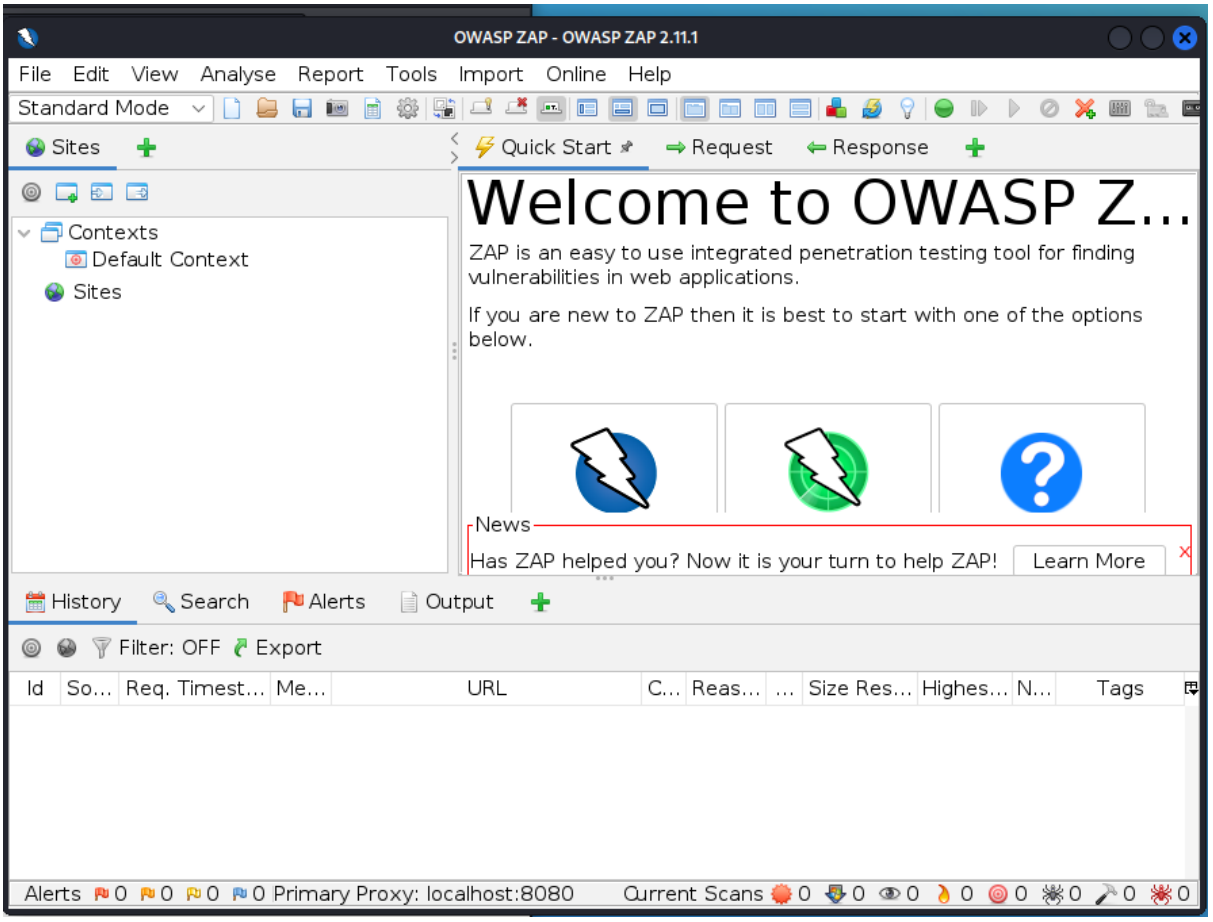




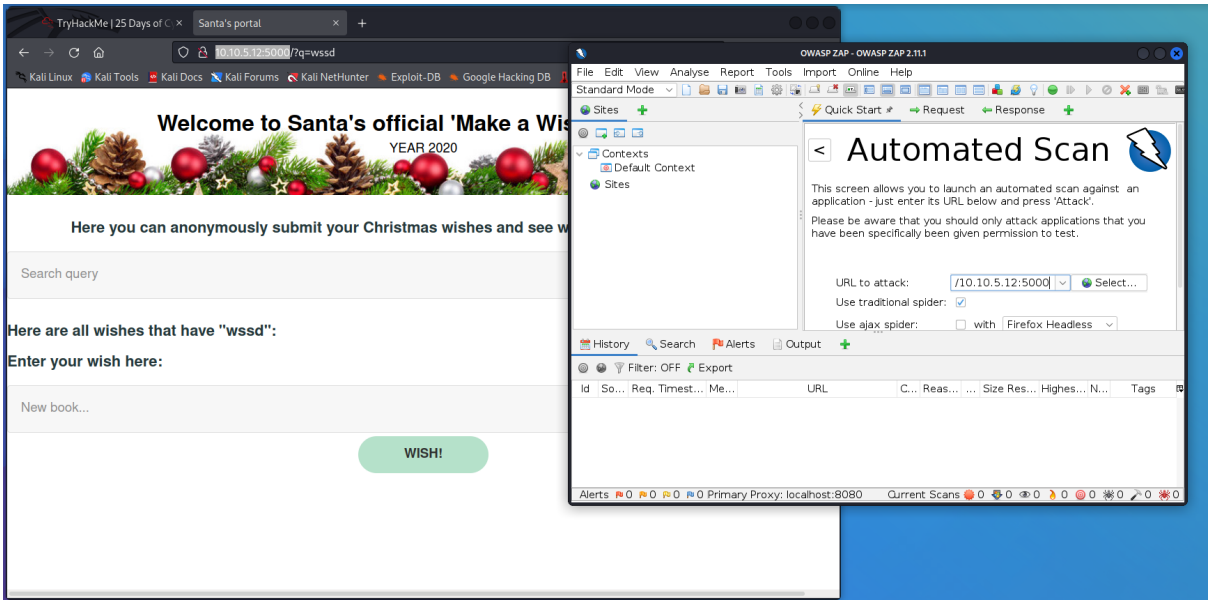
Key in something and press “WISH”, the link will appear as a query string.

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

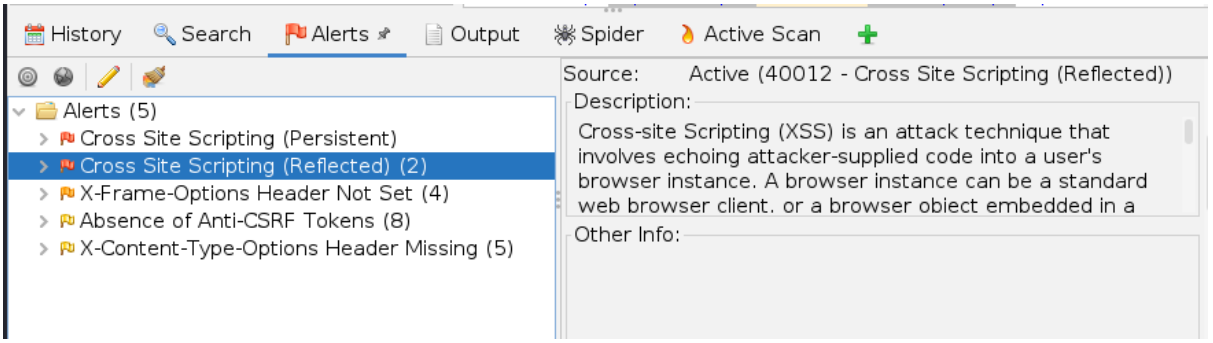
Answer: q



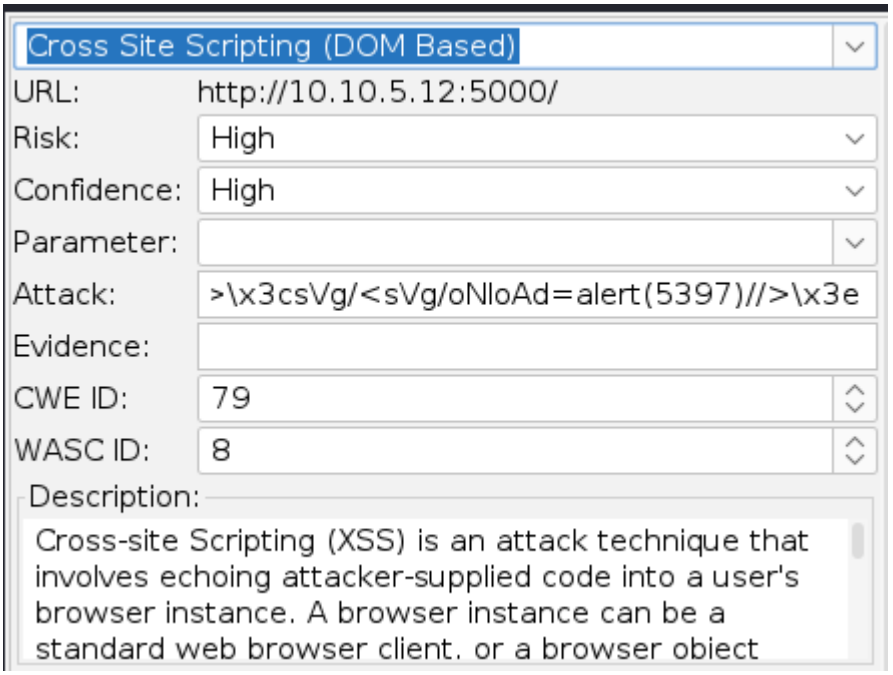
Open OWASP.

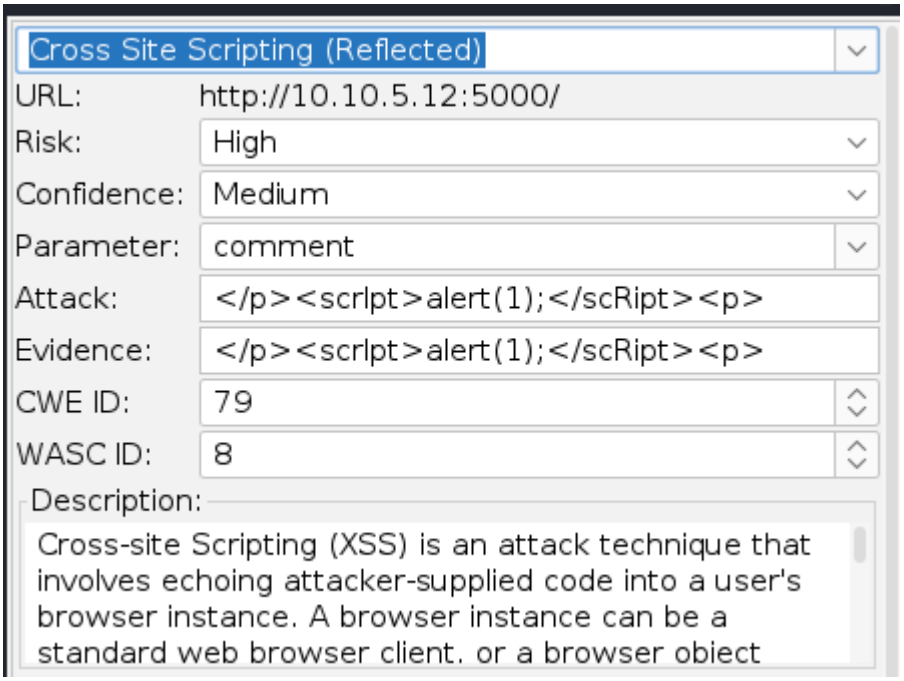


Copy MACHINE_IP and paste it in Automated Scan and click attack.



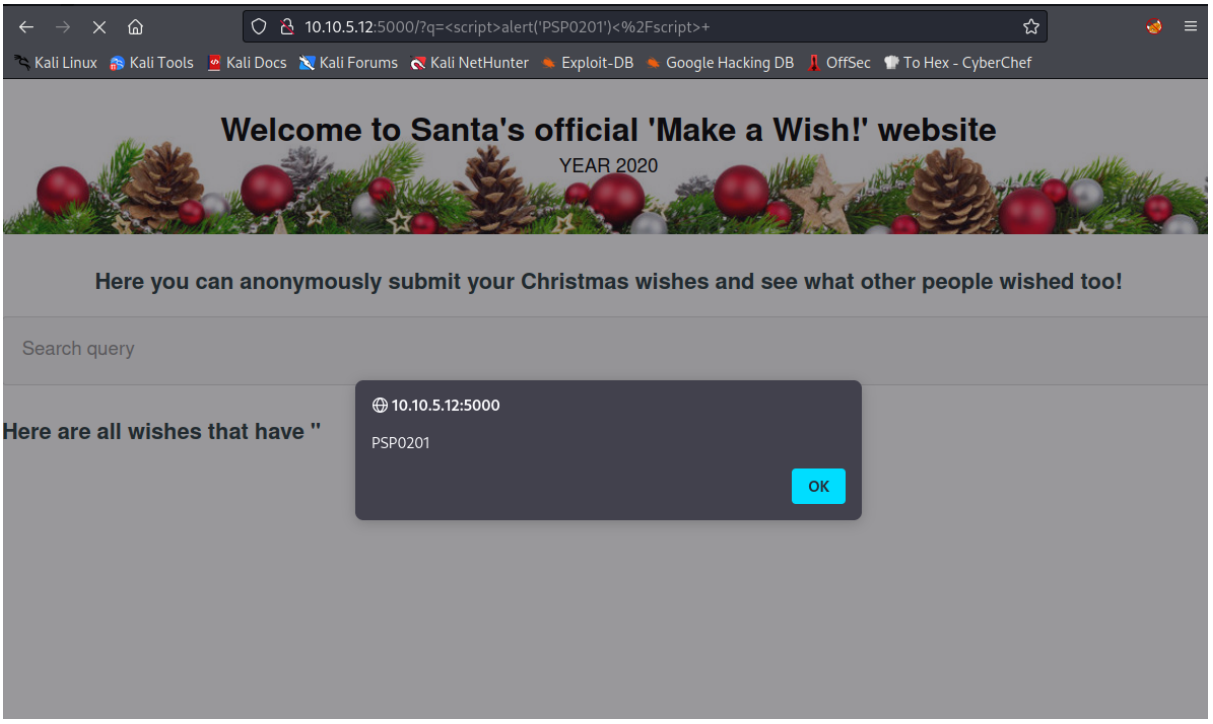
Go to Alerts to get the number of alerts.





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

Answers: 2



Type <script>alert('PSP0201')</script> in the wish text box and press “WISH”.

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

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

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

Answer: Yes

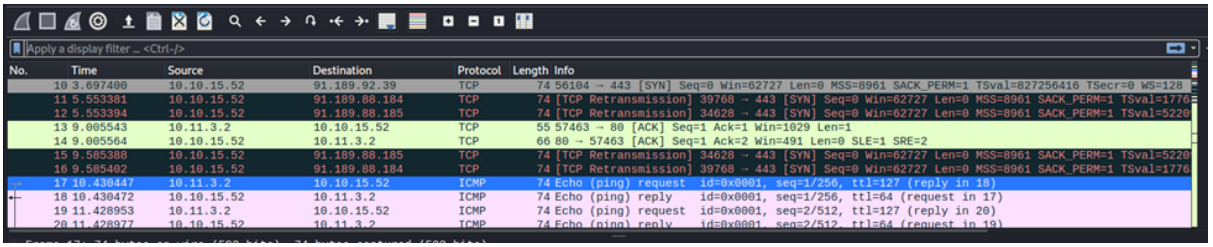
Thought Process/Methodology:

Open the link and find the description of syntactic and semantic: https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Input_Validation_Cheat_Sheet.md and also look for validating a U.S. zip code in the link. Copy IP address and paste in a new tab. Key in something and press “WISH”, the link will appear as a query string. Open OWASP and copy MACHINE_IP and paste it in Automated Scan and click attack. Go to Alerts to get the number of alerts. Type <script>alert('PSP0201')</script> in the wish text box and press “WISH”.

Day 7: Networking – The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

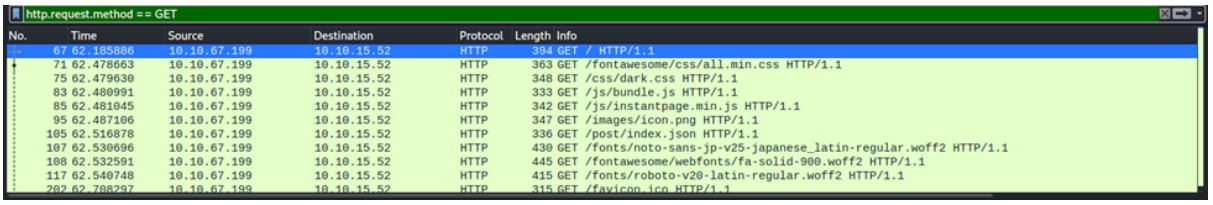
Solution/walkthrough:



Open pcap1.pcap and search for ICMP/PING.

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

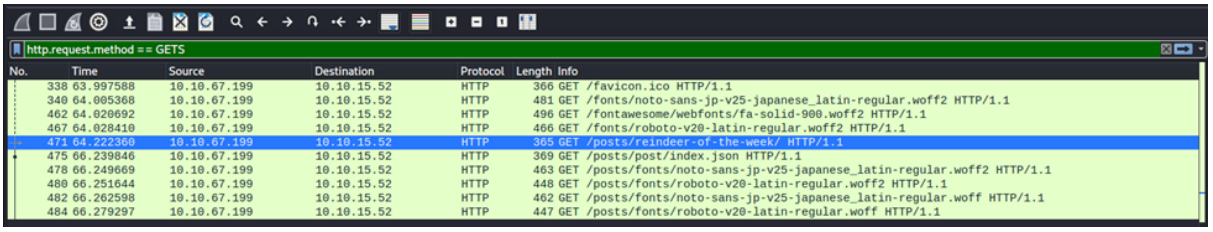
Answer: 10.11.3.2



Key in “http.request.method == GET” and press enter.

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

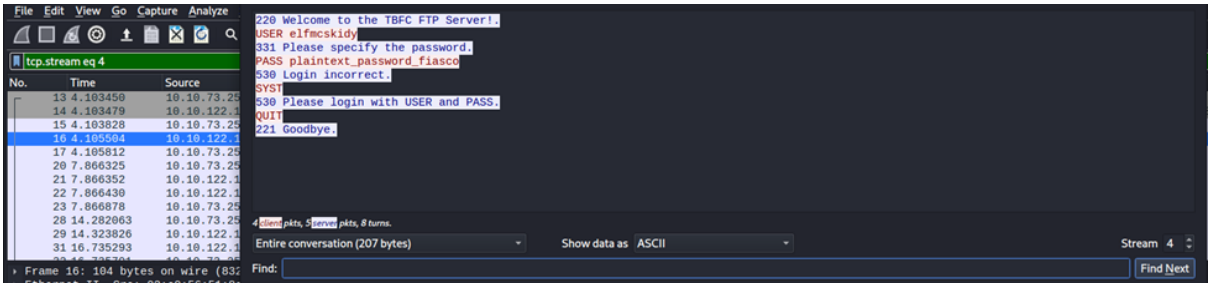
Answer: http.request.method == GET



Look for the difference between them and get the answer.

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: reinder-of-the-week



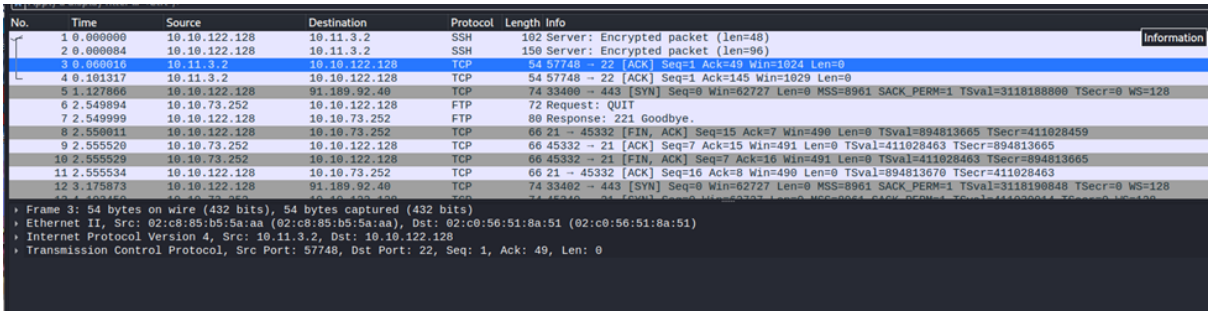
Now open pcap2.pcap. Look for the most requested FTP and click follow and the answer will be shown.

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

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

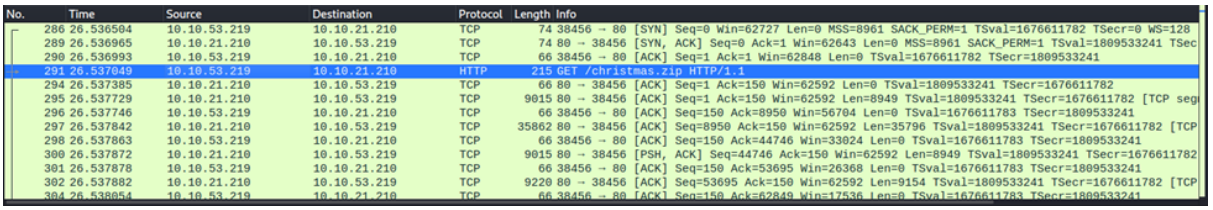
Answer: SSH

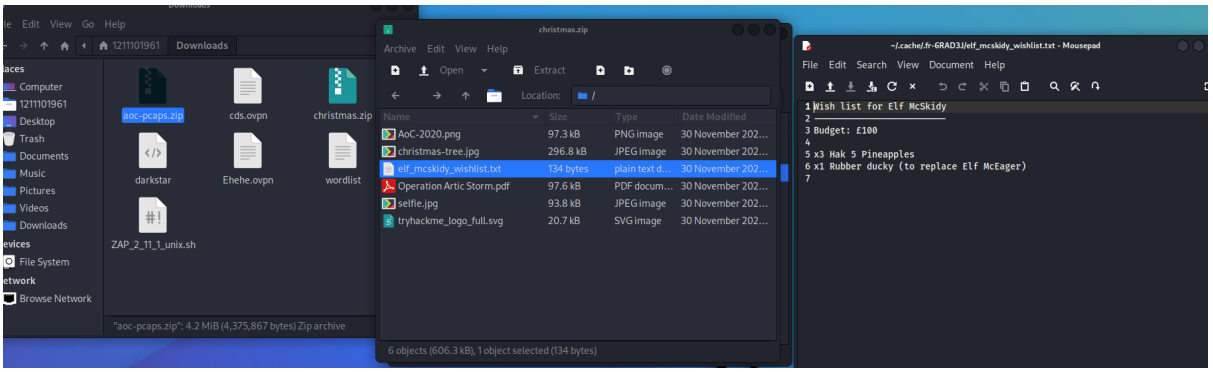


Click it and the answer is shown.

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





Find the christmas.zip and open the elf_mcskidy_wishlist.txt.

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

STRICTLY CONFIDENTIAL

Author: Kris Kringle

Revision Number: v2.5

Date of Revision: 14/11/2020

Open the Operation Artic Storm.pdf from christmas.zip.

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

Answer: Kris Kringle

Thought Process/Methodology:

Open pcap1.pcap and search for ICMP/PING. Key in "http.request.method == GET" and press enter and look for the difference between them and get the answer. Now open pcap2.pcap and look for the most requested FTP and click follow and the answer will be shown. Click it and the answer is shown. Find the christmas.zip and open the elf_mcskidy_wishlist.txt. Open the Operation Artic Storm.pdf from christmas.zip.

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

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

Solution/walkthrough:

About 1,580,000 results (0.45 seconds)

1998

Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) created by Martin Roesch in **1998**.

https://digital.ai › technology › snort

Snort - Digital.ai

Question 1: When was Snort created?

Answer: 1998

```
┌──(1211101961㉿kali)-[~]
└─$ nmap 10.10.101.186
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 05:34 EDT
Nmap scan report for 10.10.101.186
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
80/tcp   open  http
2222/tcp open  EtherNetIP-1
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 19.59 seconds
```

Open terminal and use nmap on MACHINE_IP.

Question 2: Using nmap on MACHINE_IP , what are the port numbers of the three services running?

Answer: 80,2222,3389

```
┌──(1211101961㉿kali)-[~]
└─$ nmap -sV 10.10.101.186
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 05:38 EDT
Nmap scan report for 10.10.101.186
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubun
tu Linux; protocol 2.0)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results a
t https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.14 seconds
```

Key in nmap -sV and MACHINE_IP.

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?

Answer: Ubuntu

Question 4: What is the version of Apache?

Answer: 2.4.29

Question 5: What is running on port 2222?

Answer: SSH

```
┌──(1211101961㉿kali)-[~]
└─$ nmap -A 10.10.101.186
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 05:39 EDT
Nmap scan report for 10.10.101.186
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-title: TBFC&#39;s Internal Blog
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubun
tu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_  256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results a
t https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.24 seconds
```

Key in nmap -A and MACHINE_IP.

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?

Answer: blog

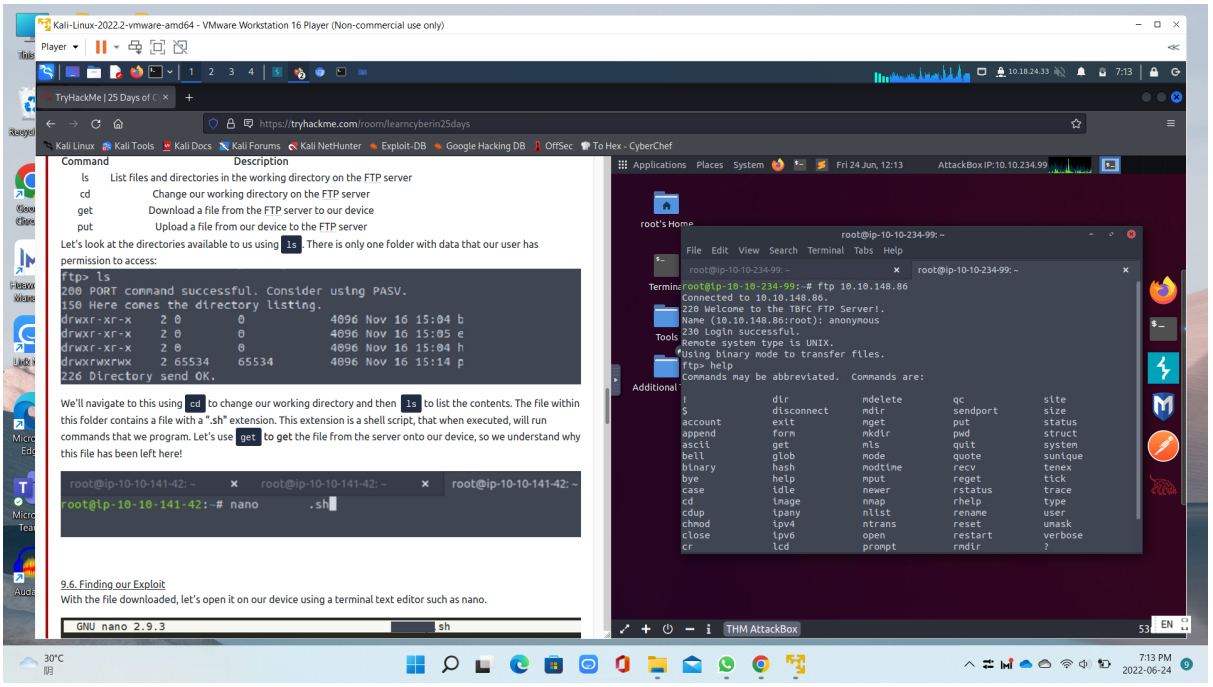
Thought Process/Methodology:

Open terminal and use nmap on MACHINE_IP. After that, key in nmap -sV and MACHINE_IP. Last, key in nmap -A and MACHINE_IP.

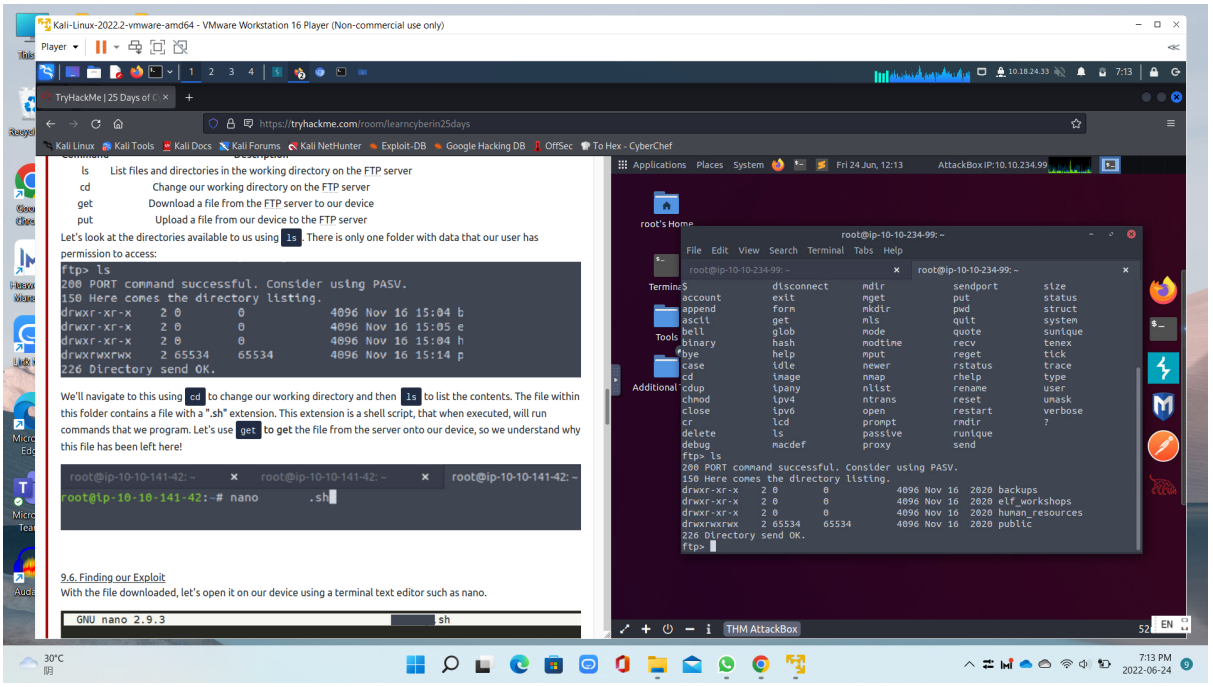
Day 9: Networking – Anyone can be Santa!

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

Solution/walkthrough:



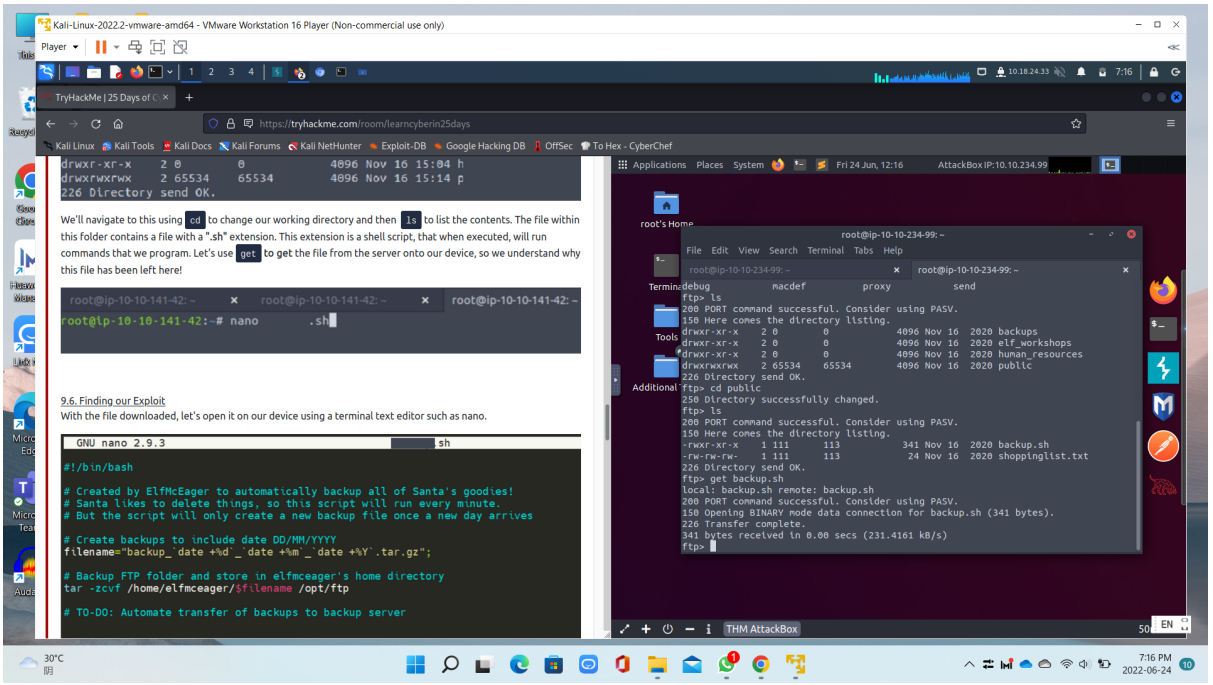
First, press Start Machine and Start AttackBox. After that, open the terminal in AttackBox and type in ftp_MACHINE IP which is 10.10.148.86. Enter anonymous for the name. Enter “help” to list out some commands.



Enter “ls” to look at the directories which are available.

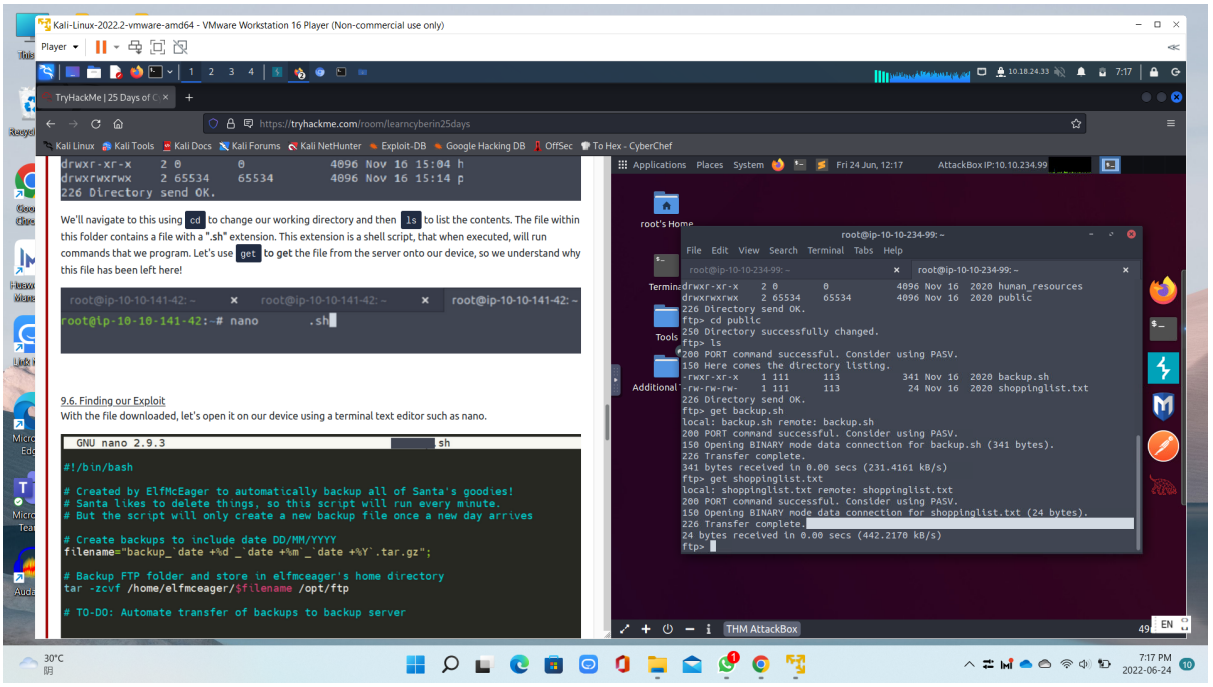
Question 1: What are the directories you found on FTP site?

Answer: backups, elf_workshop, human_resources, and public.



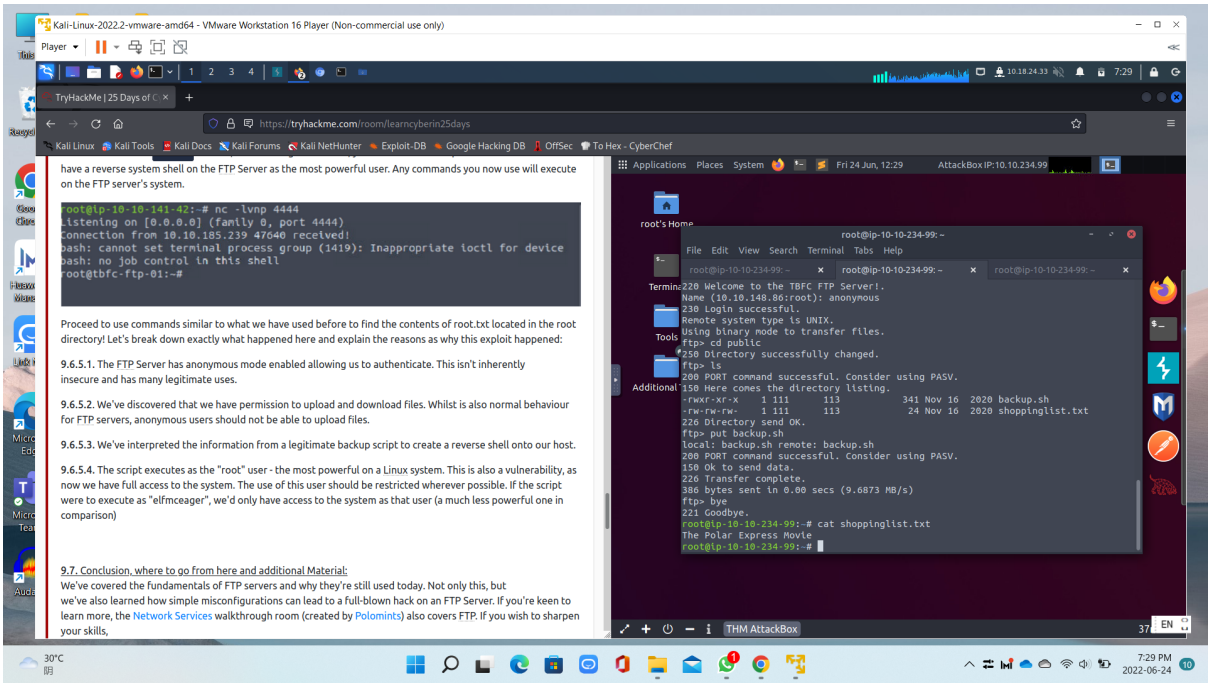
Question 2: Name the directories on the FTP server that has data accessible by the “anonymous” user.

Answer: public



Question 3: What script gets executed within this directory?

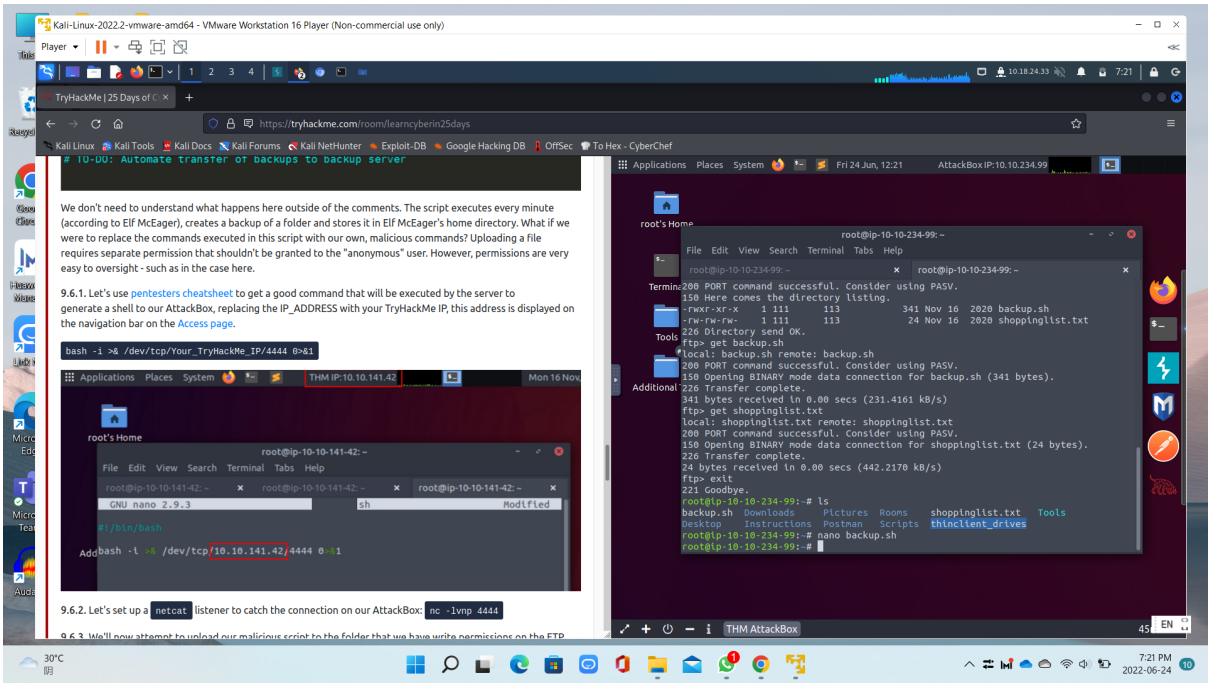
Answer: backup.sh



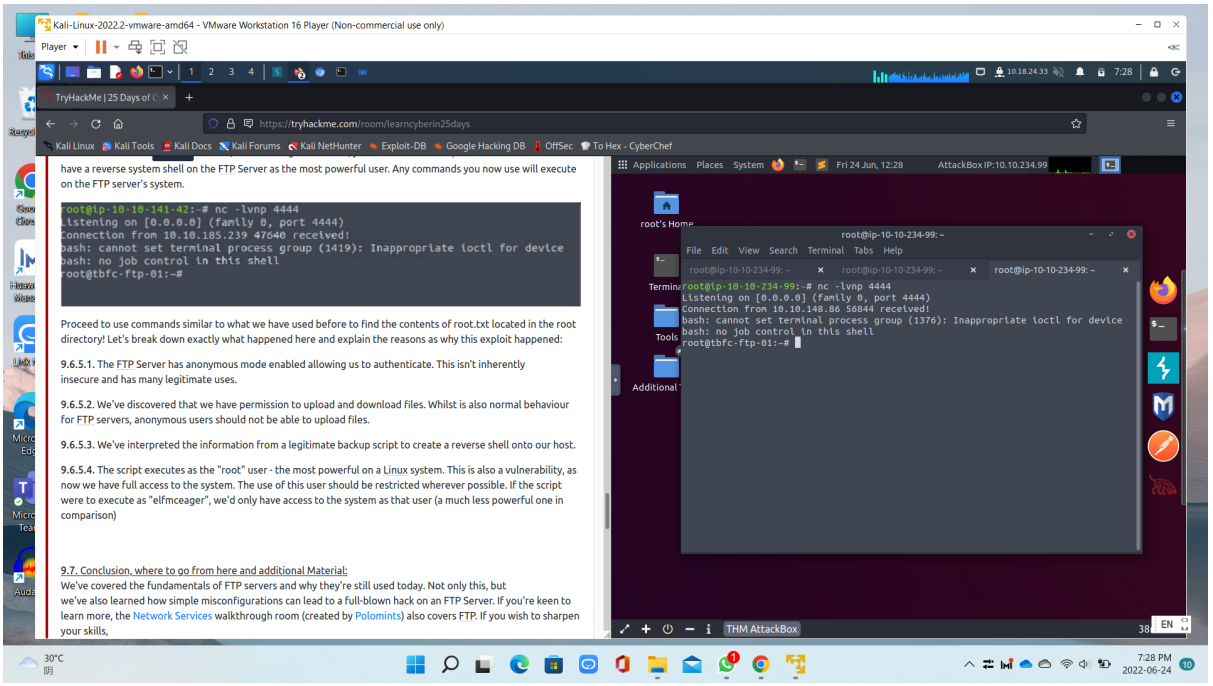
Enter “cat shoppinglist.txt” to get the answer.

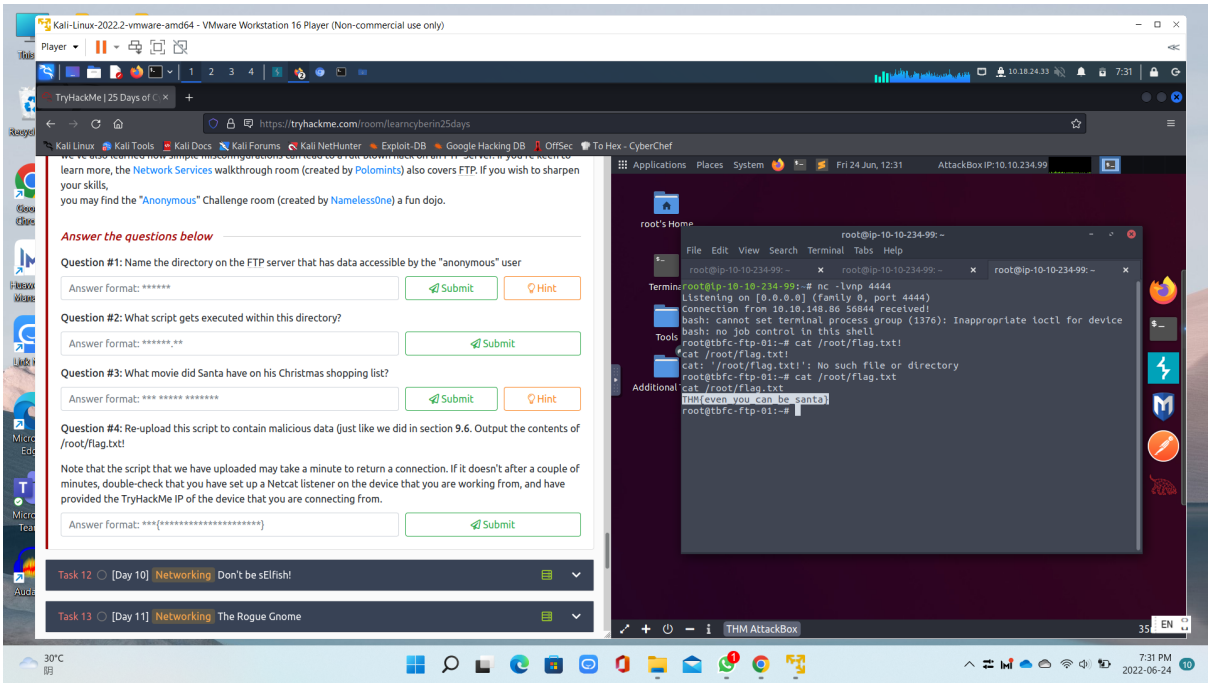
Question 4: What movie did Santa have on his Christmas shopping list?

Answer: The Polar Express Movie



Key in nano backup.sh to add in command.





Enter “nc -lvnp 4444” and press “Enter”, it will show “connection from IP-address received!” after a few minutes. After that, key in “cat /root/flag.txt” and press “Enter” and it will show a flag.

Question 5: Re-upload this script to contain malicious data (just like we did in section 9.6. Output the content of /root/flag.txt!

Answer: THM{even_you_can_be_santa}

Thought Process/Methodology:

First, press Start Machine and Start AttackBox. After that, open the terminal in AttackBox and type in ftp_MACHINE IP which is 10.10.148.86. Enter anonymous for the name. Enter “help” to list out some commands. Enter “ls” to look at the directories which are available. Enter “cat shoppinglist.txt” to get the answer. Key in nano backup.sh to add in command. Enter “nc -lvnp 4444” and press “Enter”, it will show “connection from IP-address received!” after a few minutes. After that, key in “cat /root/flag.txt” and press “Enter” and it will show a flag.

Day 10: Networking – Don’t be sElfish!

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Enter “enum4linux -h” to get the flags with descriptions in the terminal.

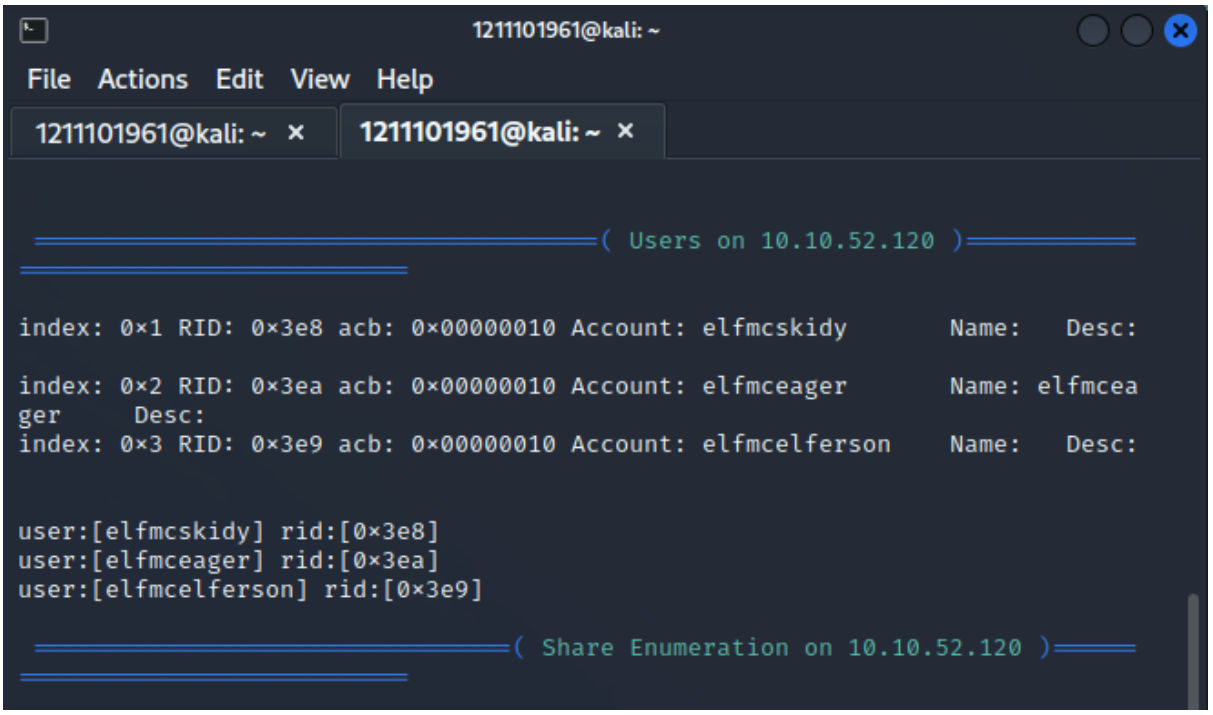
Question 1: Examine the help options for enum4linux. Match the following flags with the descriptions.

Answer: -h : Display help messages

-a : Do all simple enumeration

-S : Get sharelist

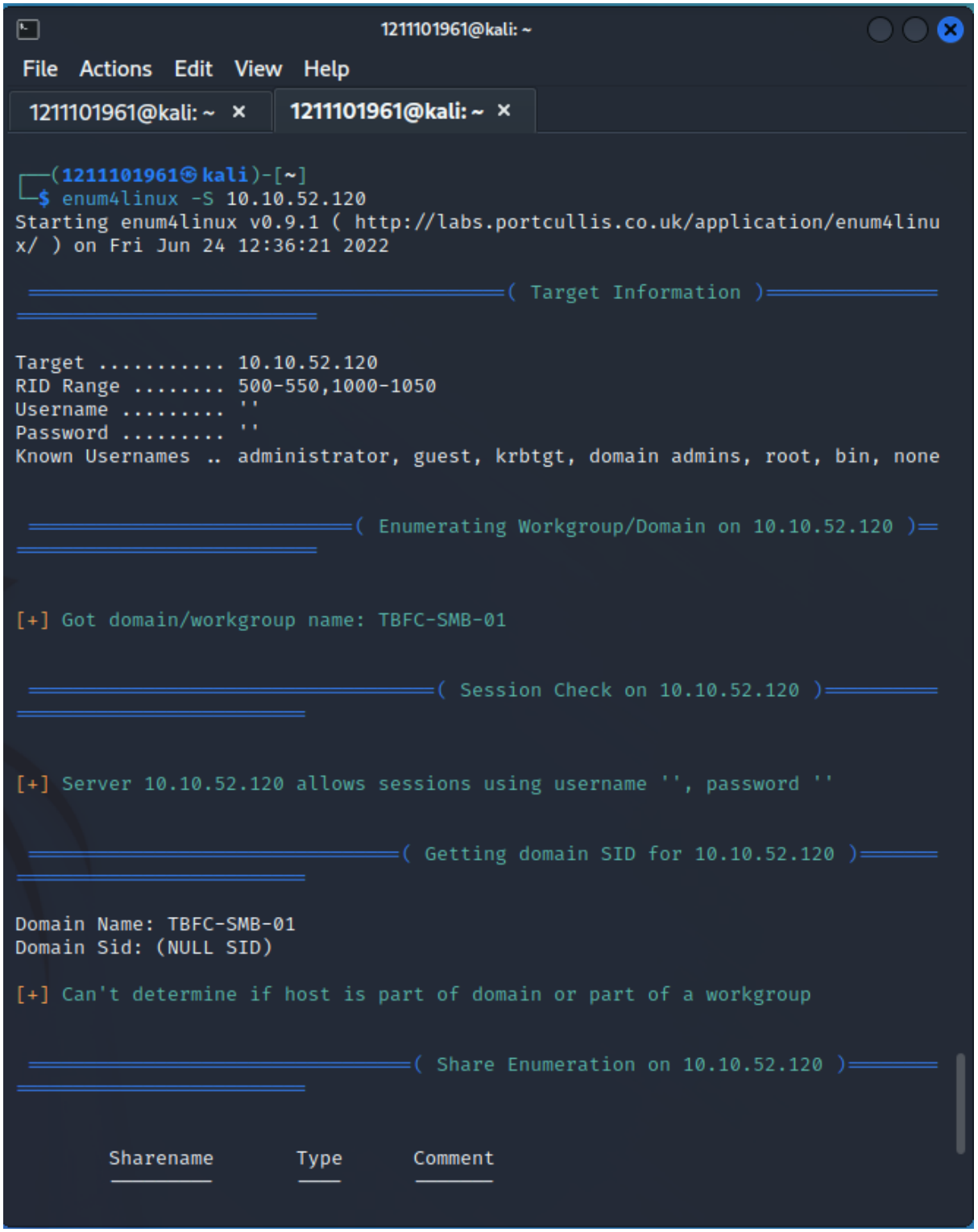
-o : Get OS information



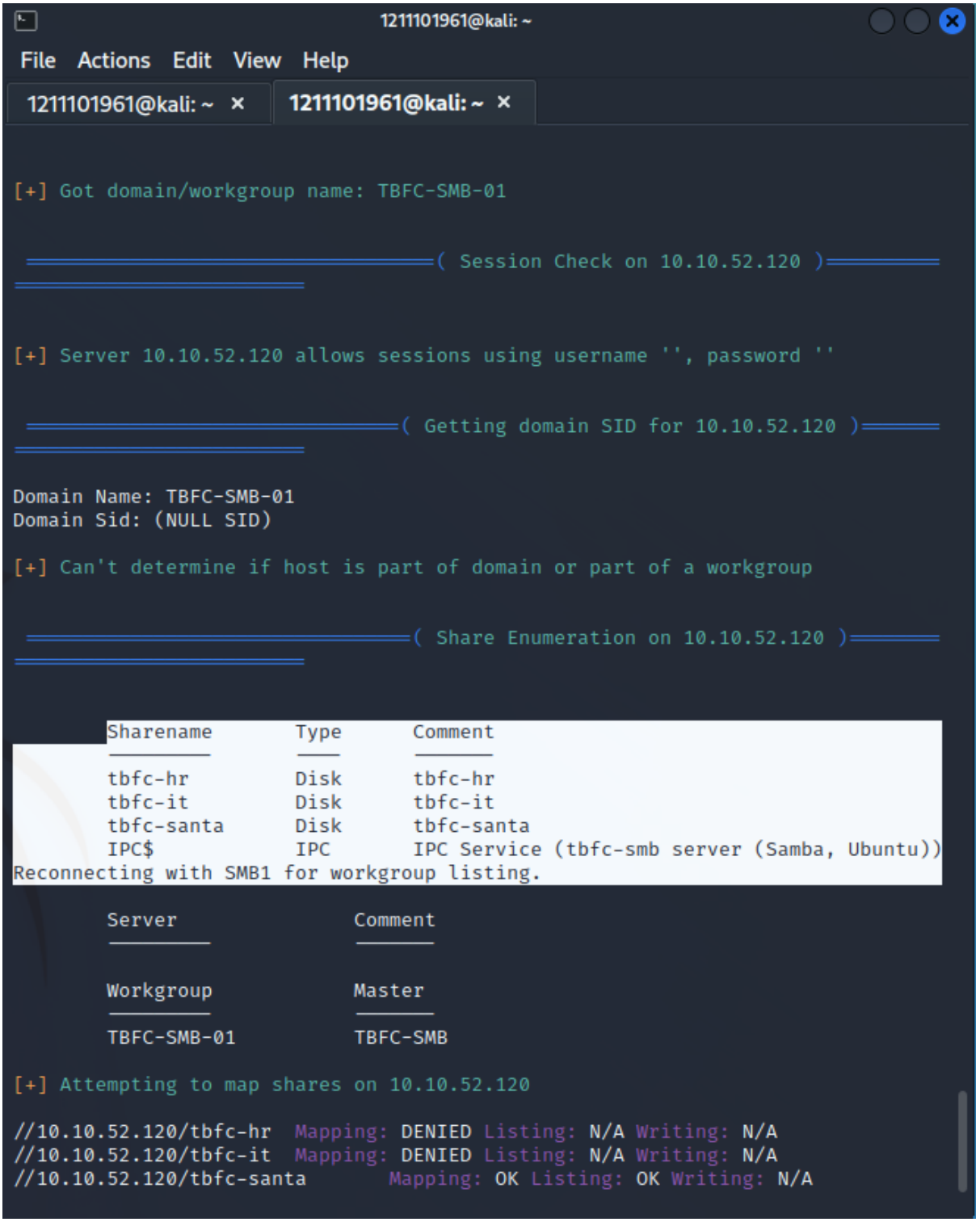
Enter “enum4linux -U IP Address(10.10.52.120)” to get the number of users.

Question 2: Using enum4linux, how many users are there on the Samba server?

Answer: 3



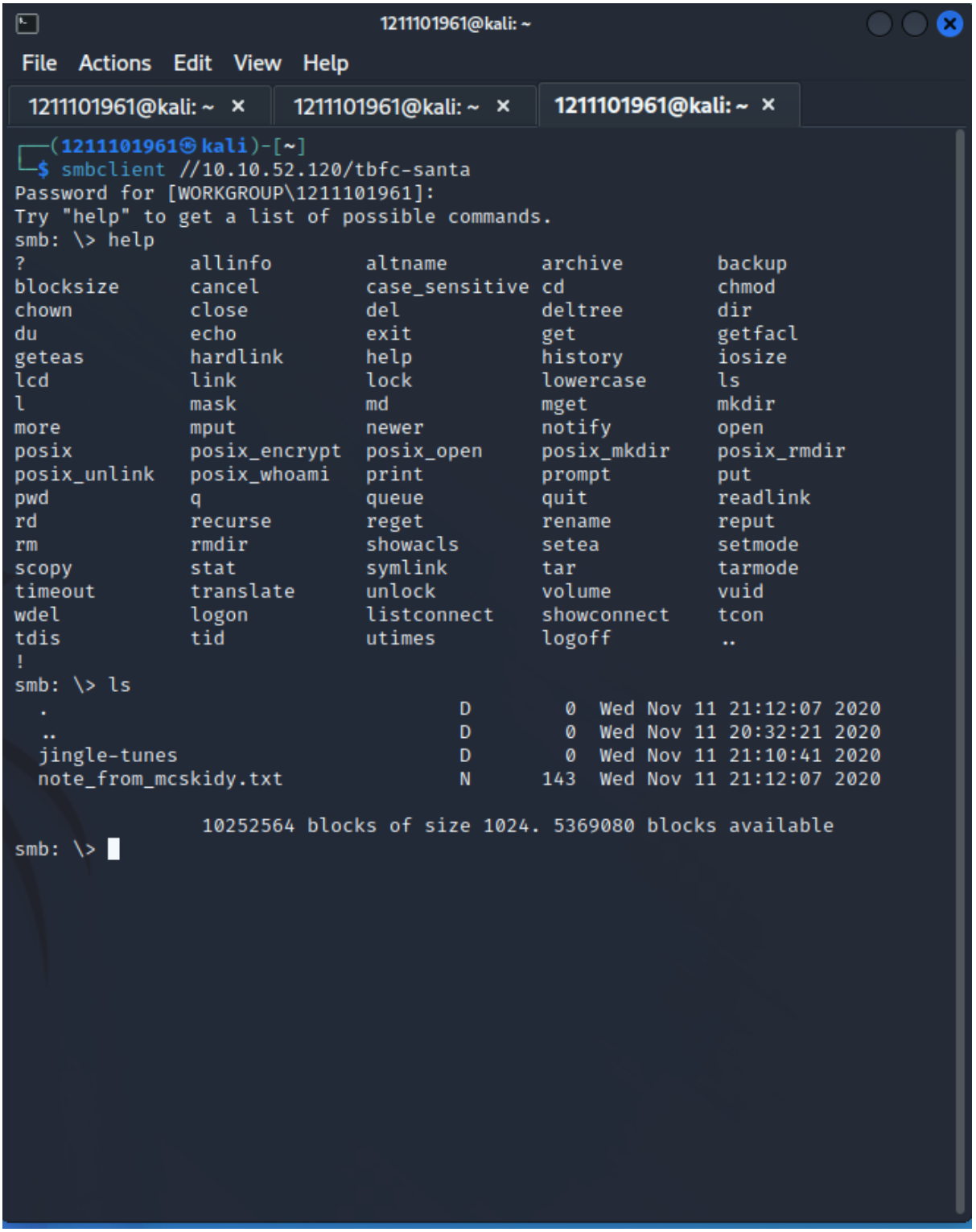
Enter “enum4linux -S IP Address(10.10.52.120)” to get the sharelist.



Question 3: Now how many “shares” are there on the Samba server?

Answer: 4

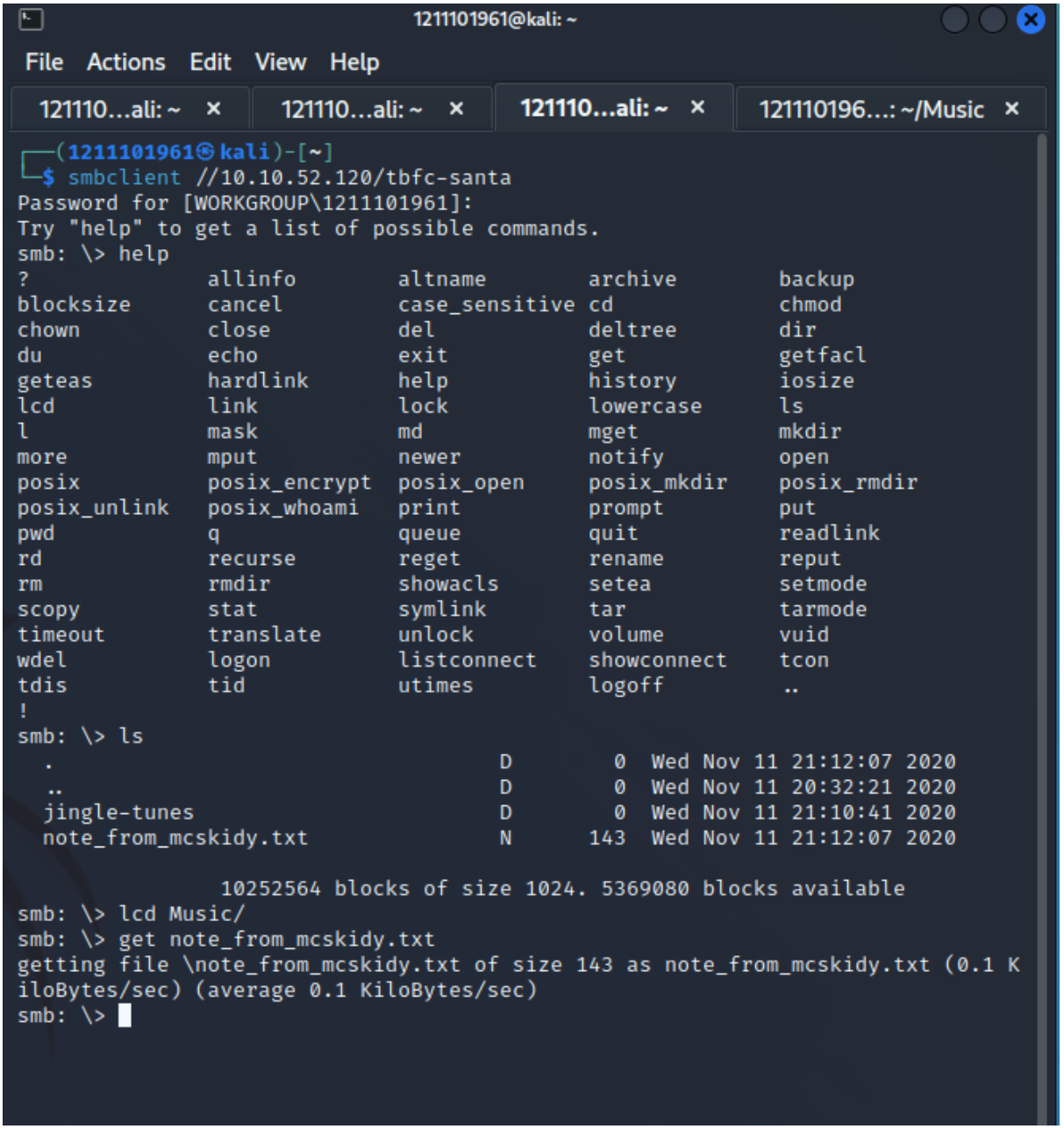

1211101961@kali: ~
File Actions Edit View Help
1211101961@kali: ~ ×
1211101961@kali: ~ ×
[+] Server 10.10.52.120 allows sessions using username '', password ''
(Getting domain SID for 10.10.52.120)
Domain Name: TBFC-SMB-01
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
(Share Enumeration on 10.10.52.120)
Sharename Type Comment
tbfc-hr Disk tbfc-hr
tbfc-it Disk tbfc-it
tbfc-santa Disk tbfc-santa
IPC$ IPC IPC Service (tbfc-smb server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
Server Comment
Workgroup Master
TBFC-SMB-01 TBFC-SMB
[+] Attempting to map shares on 10.10.52.120
//10.10.52.120/tbfc-hr Mapping: DENIED Listing: N/A Writing: N/A
//10.10.52.120/tbfc-it Mapping: DENIED Listing: N/A Writing: N/A
//10.10.52.120/tbfc-santa Mapping: OK Listing: OK Writing: N/A
[E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing *
//10.10.52.120/IPC$ Mapping: N/A Listing: N/A Writing: N/A
enum4linux complete on Fri Jun 24 12:36:45 2022
┌──(1211101961㉿kali)-[~]



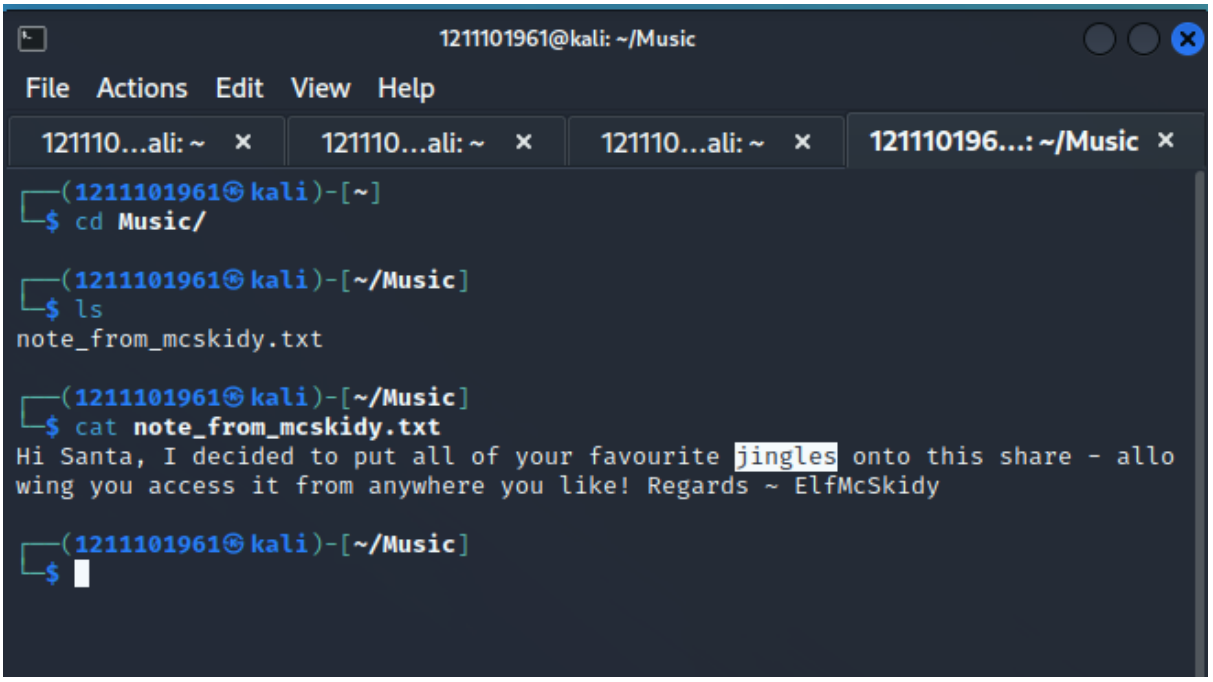
Enter “smbclient //IP Address(10.10.52.120)/sharename(tbfc-santa)” and press enter. After that, simply type in the password.

Question 4: Use smbclient to try to login to the shares on the Samba server. What share doesn’t not require a password?

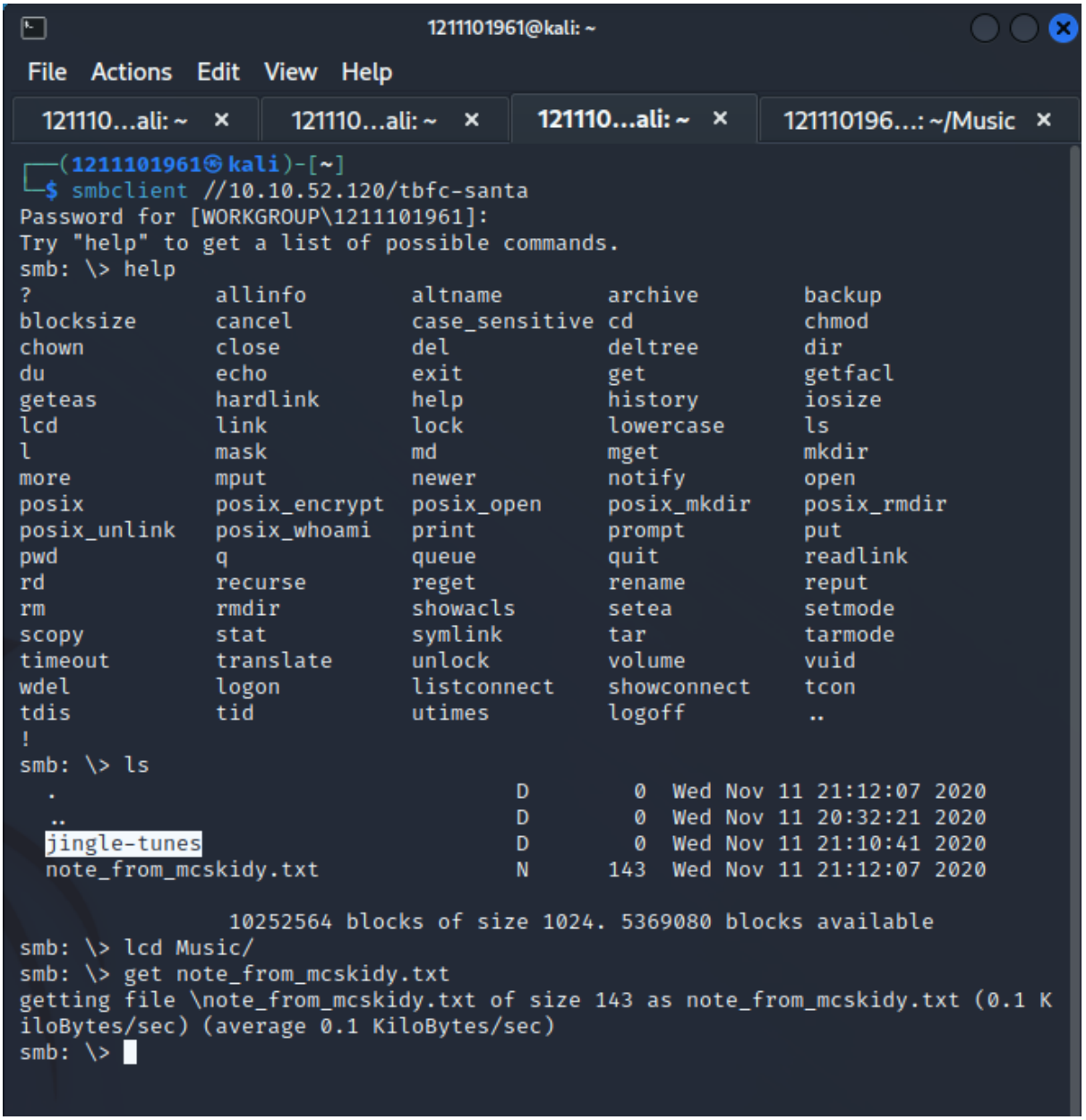
Answer: tbfc-santa



Enter “ls” to get the filelist. Enter “lcd (filename)” to create a file and key in “get note_from_mcskidy.txt”.



Key in “cd (filename)” and press enter. After that, key in “ls” to check the file. Finally, enter “cat note_from_mcskidy.txt” and it shows ElfMcSkidy leaving something to Santa which is jingles.



Question 5: Log in to this share, what directory did ElfMcSkidy leave for Santa?

Answer: jingle-tunes

Thought Process/Methodology:

Enter “enum4linux -h” to get the flags with descriptions in the terminal. Enter “enum4linux -U IP Address(10.10.52.120)” to get the number of users. Enter “enum4linux -S IP Address(10.10.52.120)” to get the sharelist. Enter “smbclient //IP Address(10.10.52.120)/sharename(tbfc-santa)” and press enter. After that, simply type in the password. Enter “ls” to get the filelist. Enter “lcd (filename)” to create a file and key in “get note_from_mcskidy.txt”. Key in “cd (filename)” and press enter. After that, key in “ls” to check the file. Finally, enter “cat note_from_mcskidy.txt” and it shows ElfMcSkidy leaving something to Santa which is jingles.