PSP0201
Week 3
Report

Group Name : Cipher
Members :

ID	Name	Role
1211103064	MUHAMAD AIMAN BIN MOHD EHWAL	Leader
1211103085	MUHAMMAD FARID BIN JAYATAN	Member
1211103373	MUHAMMAD ALIF BIN KHABALI	Member
1211103451	ARIF MUHRIZ BIN SYAMSUL FOZY	Member

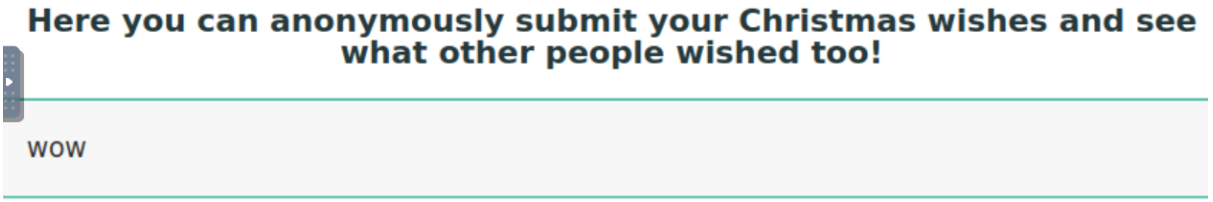
Day 6 : Web Exploitation - Be Careful With What You Wish On A Christmas Night

Tool Used : Kali Linux, Firefox
Solution / Walkthrough :

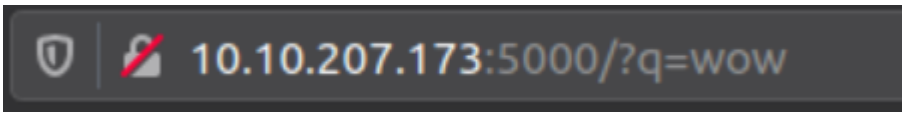
Question 1 & 2

What vulnerability type was used to exploit the application?

stored crosssite scripting | Correct Answer



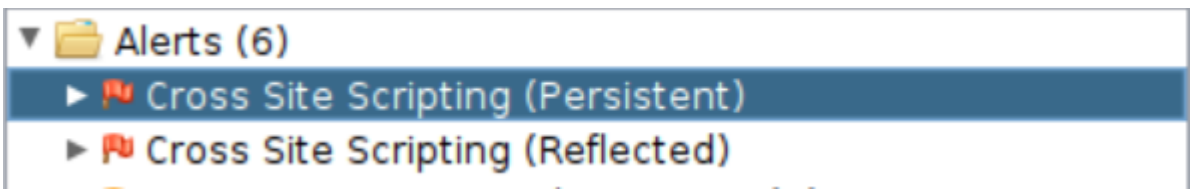
When we type anything in the query section, we will get a parameter of 'q'



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

q | Correct Answer | Hint

Question 3



There are two types of XSS scripting in the scan which are persistent and reflected

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

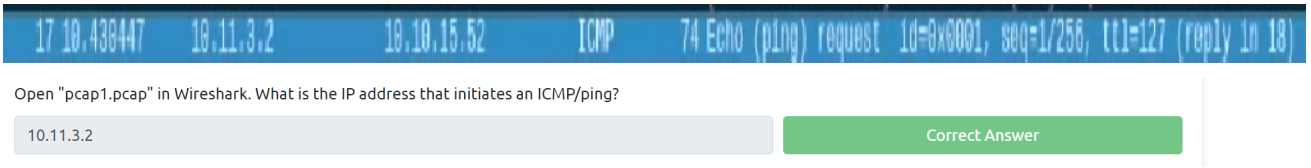
2 | Correct Answer

Thought Process / Methodology : After launching the website, we can get the query string that is abused to craft a reflected XSS by thyping something in the query section. Then, we launch the OWASP ZAP application to run a ZAP (zaproxy) automated scan on the target. It will then show the amount of XSS alerts that are in the scan.

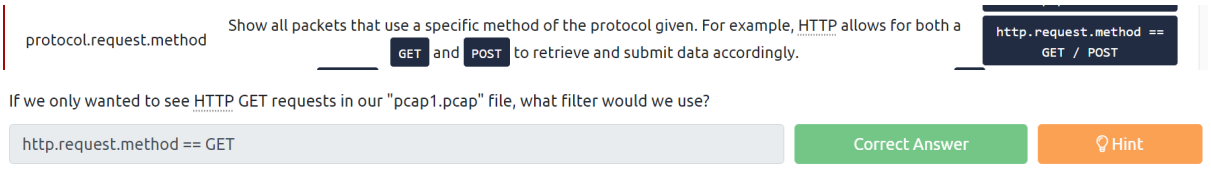
Day 7 : Networking - The Grinch Really Did Steal Christmas

Tool Used : Kali Linux, Firefox
Solution / Walkthrough :

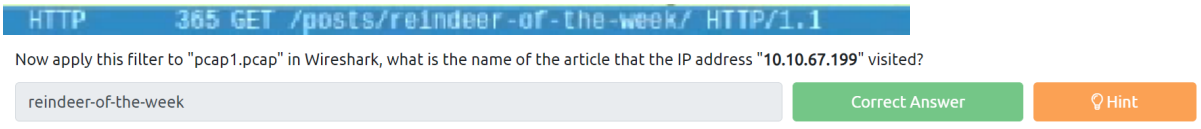
Question 1 & 2



The source is coming from 10.11.3.2



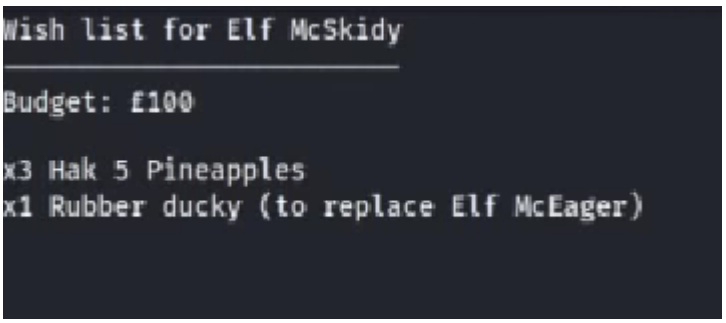
Question 3



Question 4

Question 5

Question 7

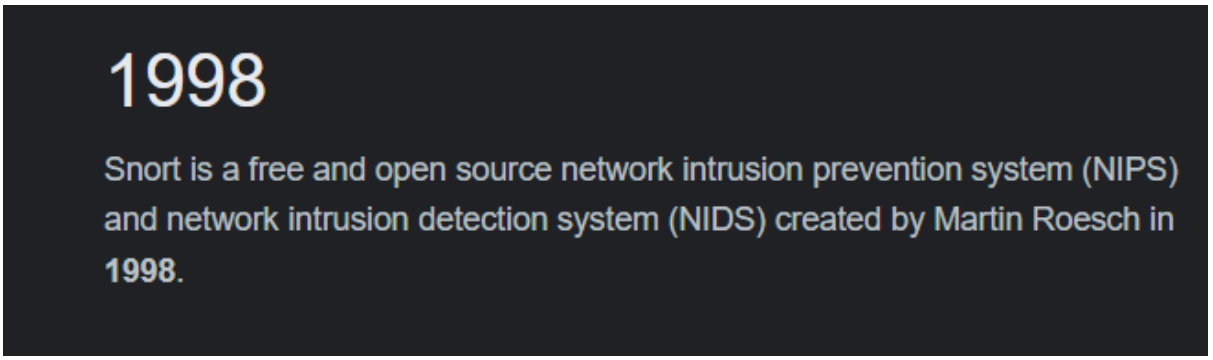


Thought Process / Methodology : After downloading the zip file, open the file “pcap1.pcap” in wireshark. It will show the IP address that initiates an ICMP/ping. We then use “http.request.method == GET” to see HTTP GET requests in our "pcap1.pcap" file. After applying the filter, we can get the name of the article that the IP address "10.10.67.199" visited. After that, we use the filter “tcp.port == 21” in the file "pcap2.pcap" to get the password that was leaked during the login process.

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

Tool Used : Kali Linux, Firefox
Solution / Walkthrough :

Question 1



Snort was created in 1998.

Question 2

```
┌──(1211103064㉿kali)-[~]
└─$ nmap 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:47 EDT
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 72.87% done; ETC: 23:48 (0:00:16 remaining)
Nmap scan report for 10.10.125.174
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 68.49 seconds
```

We got it by using the command **nmap** on the **Machine_ip**.

Question 3

```
┌──(1211103064㉿kali)-[~]
└─$ nmap -Pn 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:50 EDT
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 92.80% done; ETC: 23:51 (0:00:02 remaining)
Nmap scan report for 10.10.125.174
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 37.16 seconds
```

We use **-Pn** to determine if the host is up or not.

Question 4

```
┌──(1211103064㉿kali)-[~]
└─$ nmap -A 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:52 EDT
Nmap scan report for 10.10.125.174
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-server-header: Apache/2.4.29 (Ubuntu)
|_http-generator: Hugo 0.78.2
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_  256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (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 44.65 seconds
```

```
┌──(1211103064㉿kali)-[~]
└─$ nmap -sV 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:56 EDT
Nmap scan report for 10.10.125.174
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))
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
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 34.34 seconds
```

We experiment with different scan settings such as **-A** and **-sV** and comparing the outputs between those two scan settings.

Question 5

```
┌──(1211103064㉿kali)-[~]
└─$ nmap -sV 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:56 EDT
Nmap scan report for 10.10.125.174
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))
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
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 34.34 seconds
```

We get the name of the linux that is running through the scan that we did earlier.

Question 6

```
┌──(1211103064㉿kali)-[~]
└─$ nmap -A 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:52 EDT
Nmap scan report for 10.10.125.174
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-server-header: Apache/2.4.29 (Ubuntu)
|_http-generator: Hugo 0.78.2
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_  256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (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 44.65 seconds
```

The website is used for blog. We get it by using the nmap scan.

Question 7

```
┌──(1211103064㉿kali)-[~]
└─$ nmap --script ftp-proftpd-backdoor -p 21 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:55 EDT
Nmap scan report for 10.10.125.174
Host is up (0.22s latency).

PORT   STATE  SERVICE
21/tcp closed ftp

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

```
┌──(1211103064㉿kali)-[~]
└─$ nmap -A -sV -sC 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:45 EDT
Stats: 0:00:40 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 23:46 (0:00:12 remaining)
Nmap scan report for 10.10.125.174
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-generator: Hugo 0.78.2
|_http-title: TBFC&#39;s Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (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

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 54.41 seconds
```

We tried using different script to get more information about the server.

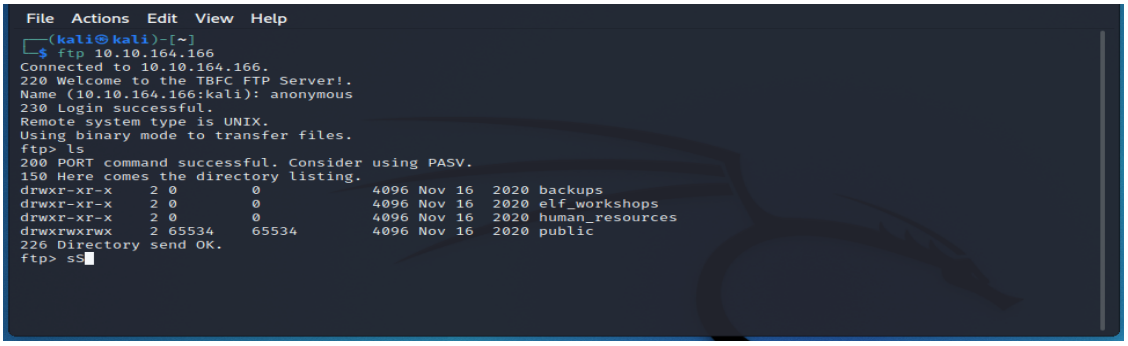
Thought Process / Methodology :

Firstly, we opened the terminal prompt and we used **nmap** to scan the **MACHINE_IP**. We got all the answers by using nmap scan except for the first question. We used **nmap** scan on the **MACHINE_IP** to get the ports number of the three services running. We used **nmap** command **-Pn** to run a scan and provided us the flag to ignore ICMP being used to determine if the host is up or not. After that we experiment with different scan settings such as -A and -Sv whilst comparing the outputs of it. We determine the name of the Linux distribution that is running by using **nmap** too. After that we used **nmap** scan to figure out what the website is used for.Lastly, we tried using different script.

Day 9 : Networking - Anyone can be Santa!

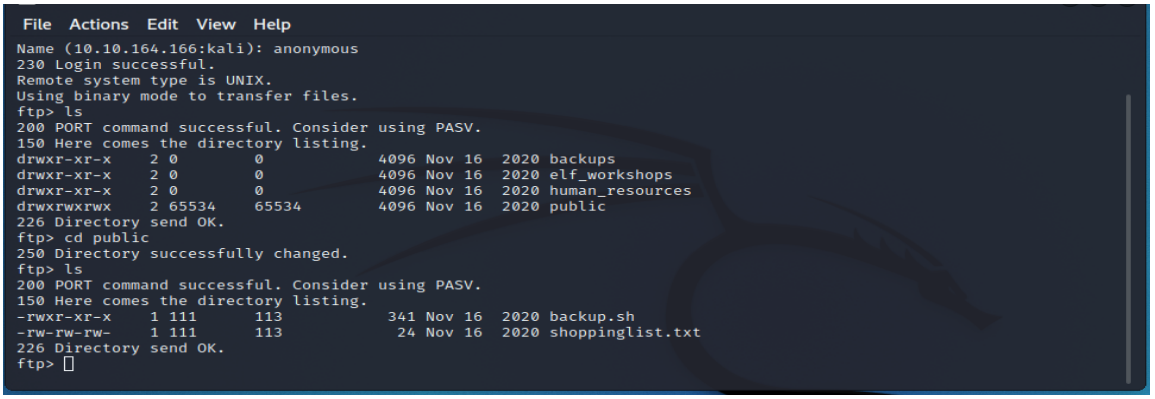
Tool Used : Kali Linux, Firefox
Solution / Walkthrough :

Question 1



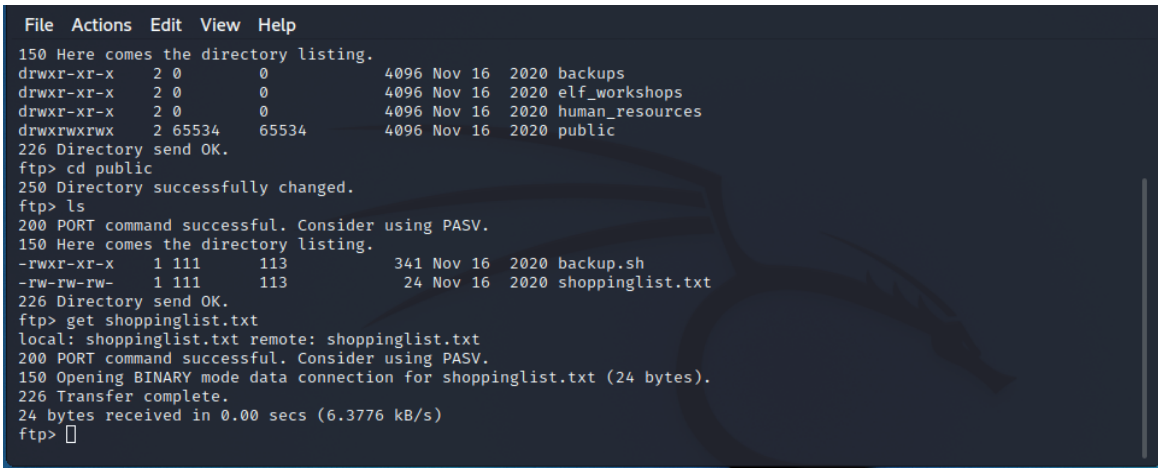
Accessible directory : “Public”

Question 2

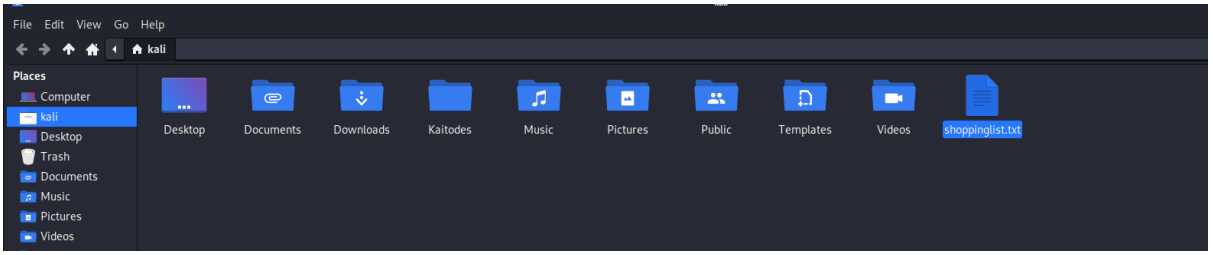


Two files were discovered. The file with “.sh” is the script found in the directory.

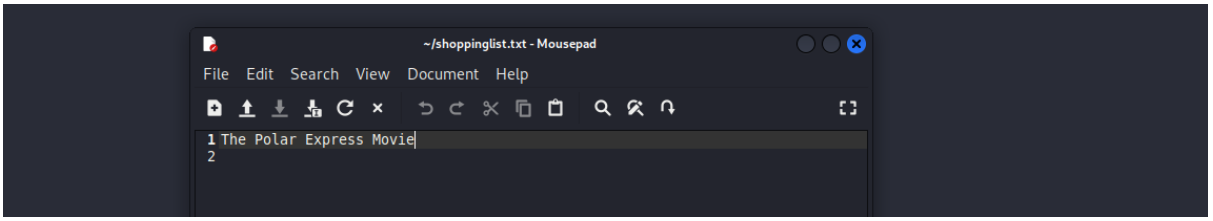
Question 3



Download the “shoppinglist.txt” .

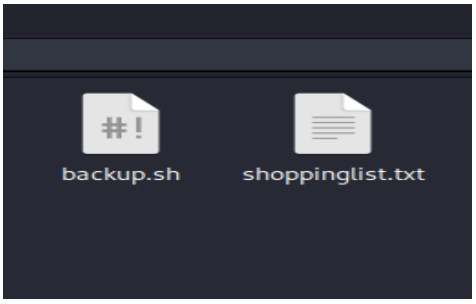


Open the file.

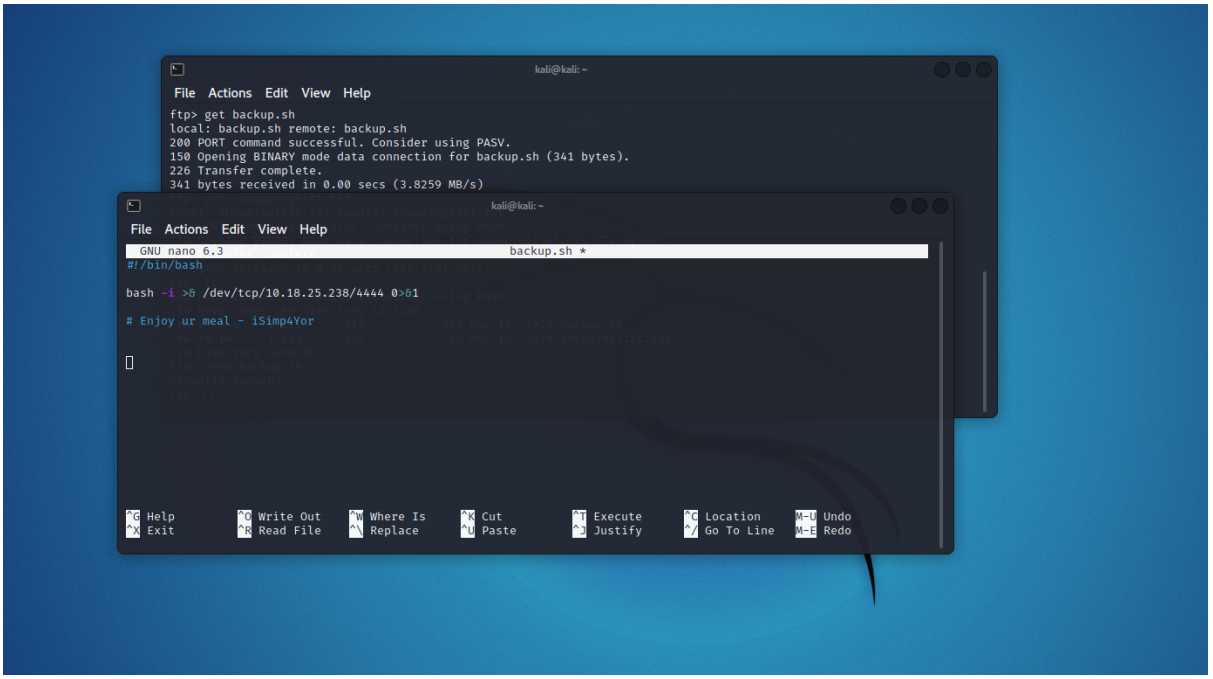


The title is “The Polar Express”

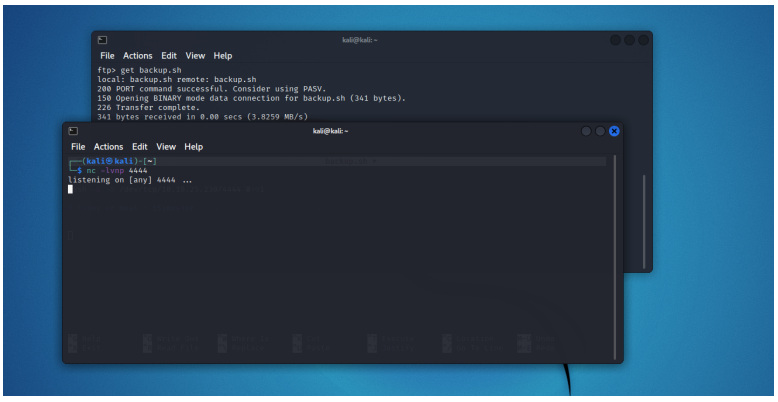
Question 4



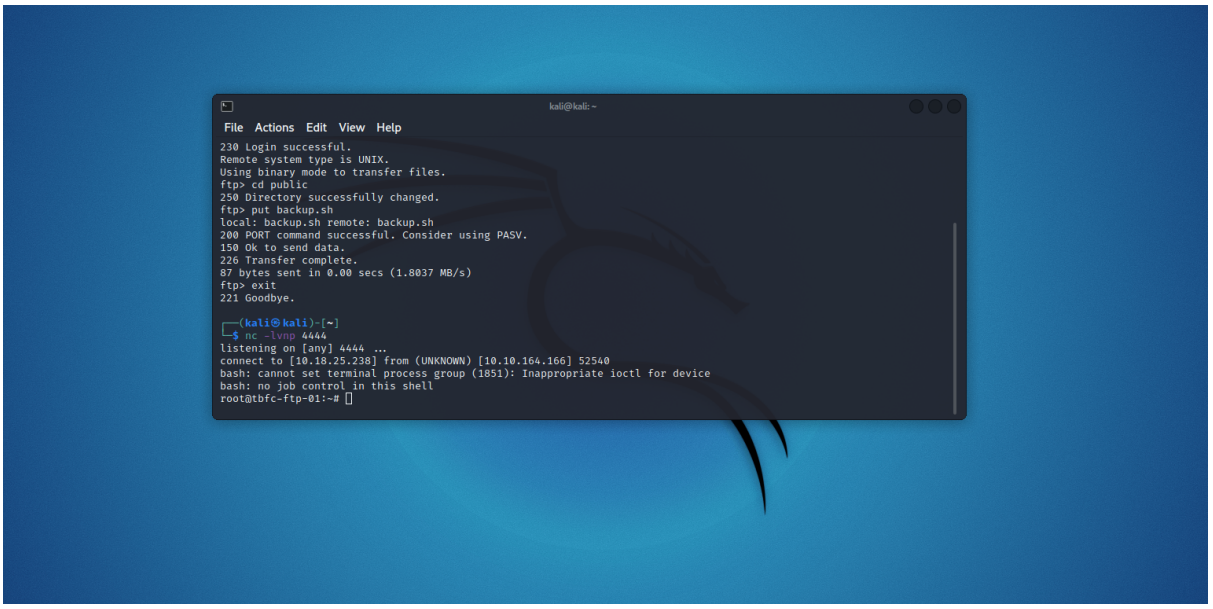
Download the backup.sh using ftp> get backup.sh



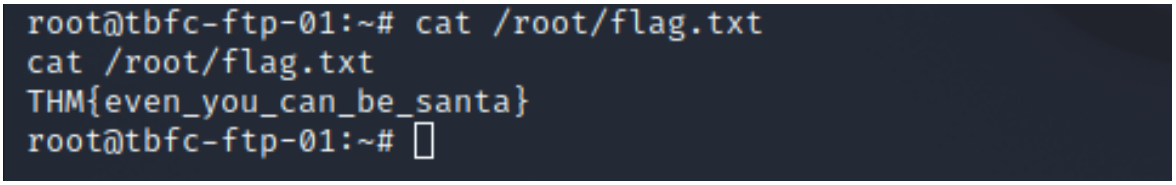
We change the content of this script to as above and use our own machine IP



Set a netcat listener and listen to any 4444



Send new script with syntax ftp> cd public , ftp> put backup.sh
Exit the ftp and listen to netcat.



Enter “cat /root/flag.txt” . Claim the flag.

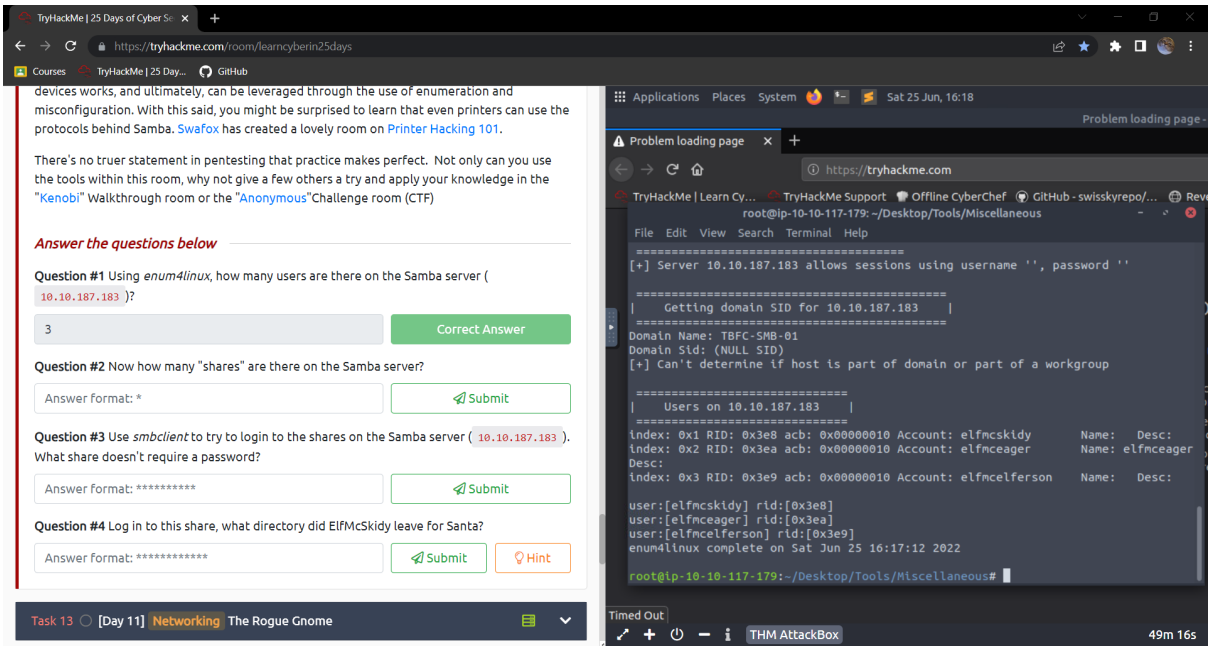
Thought Process / Methodology :

After we open the terminal on Kali Linux, we put the command “ftp” alongside IP that has been given from the THM 25 Days challenge. When asked for a name, we type “anonymous” then we can enter . After that we listed the directories using “ftp> ls” and found an anonymously-accessible directory named “Public” . We changed the directory using the command “ftp> cd public” and relisted what we could find. We found out two files which are “backup.sh” and “shoppinglist.txt”. We download them using the command “ftp> get {files name}” . We opened the shoppinglist.txt file and found a movie named “The Polar Express” . After that, we opened the terminal and type “nano backup.sh” and changed the content to as above. We setted up a netcat listener to listen to 4444 then we sent the new backup.sh to the same public directory using the commands “ftp> cd public” and “ftp> put backup.sh” . After a few minutes, netcat was connected. Lastly, we put the command “cat /root/flag.txt” and were able to claim the flag of THM{even_you_can_be_santa}.

Day 10 : Networking - Don’t Be sElfish!

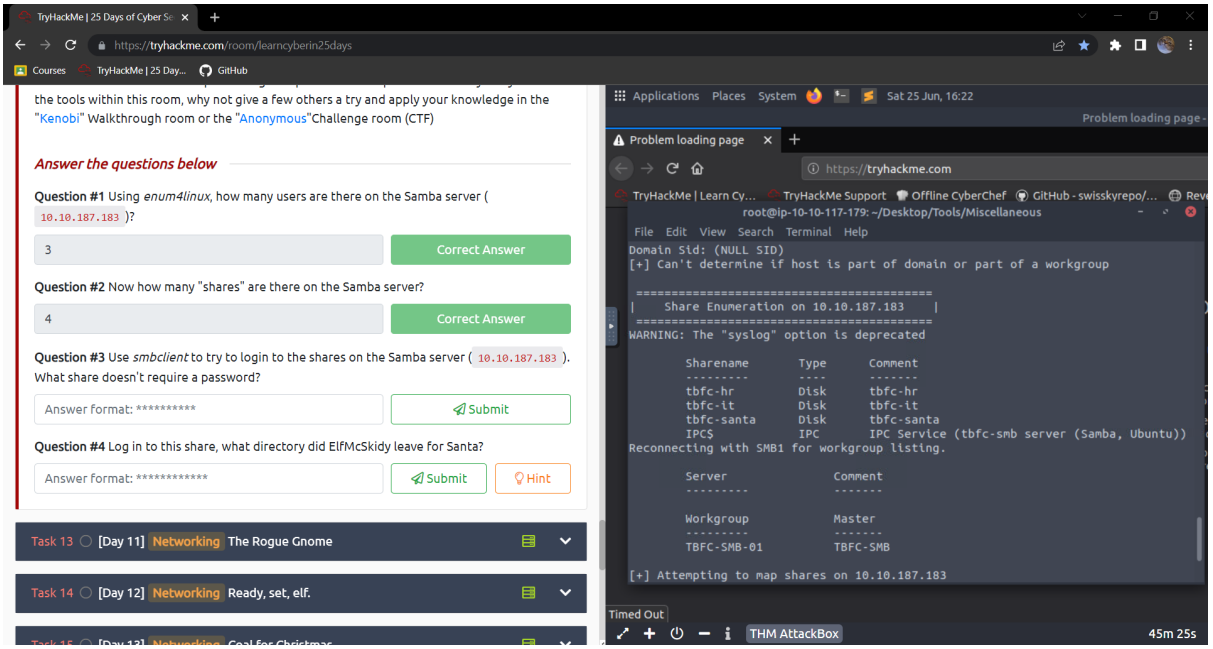
Tool Used : Kali Linux, Firefox, Attackbox
Solution / Walkthrough :

Question 1



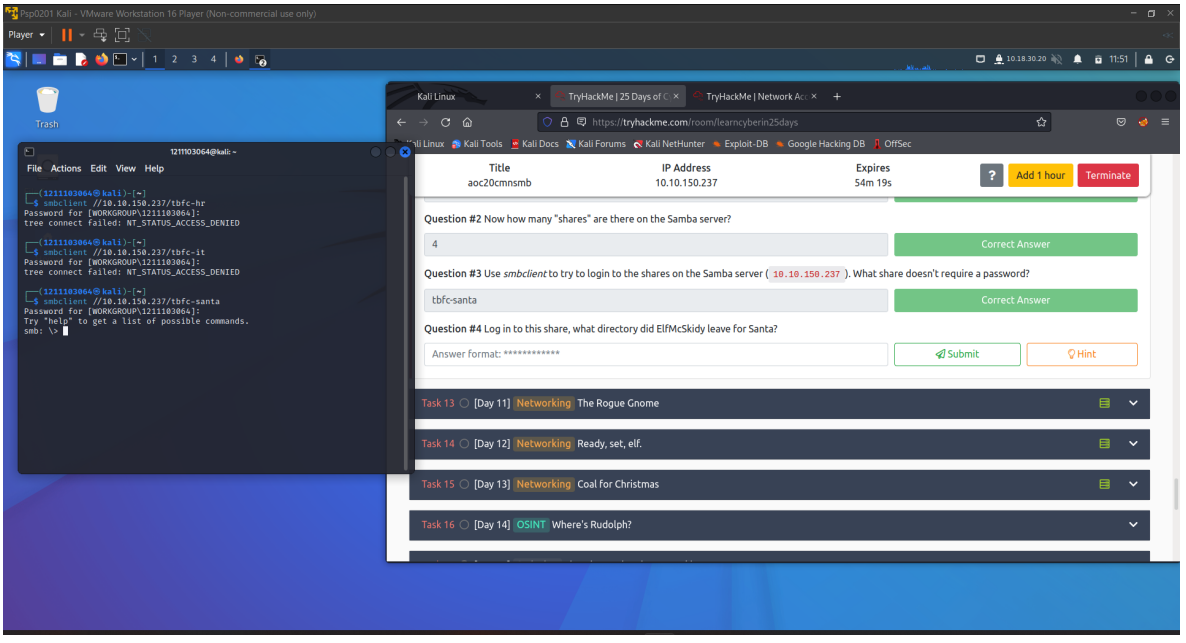
By using the enum4linux command which is **./enum4linux.pl -U MACHINE_IP** , we are able to get how many users are there on the server.

Question 2



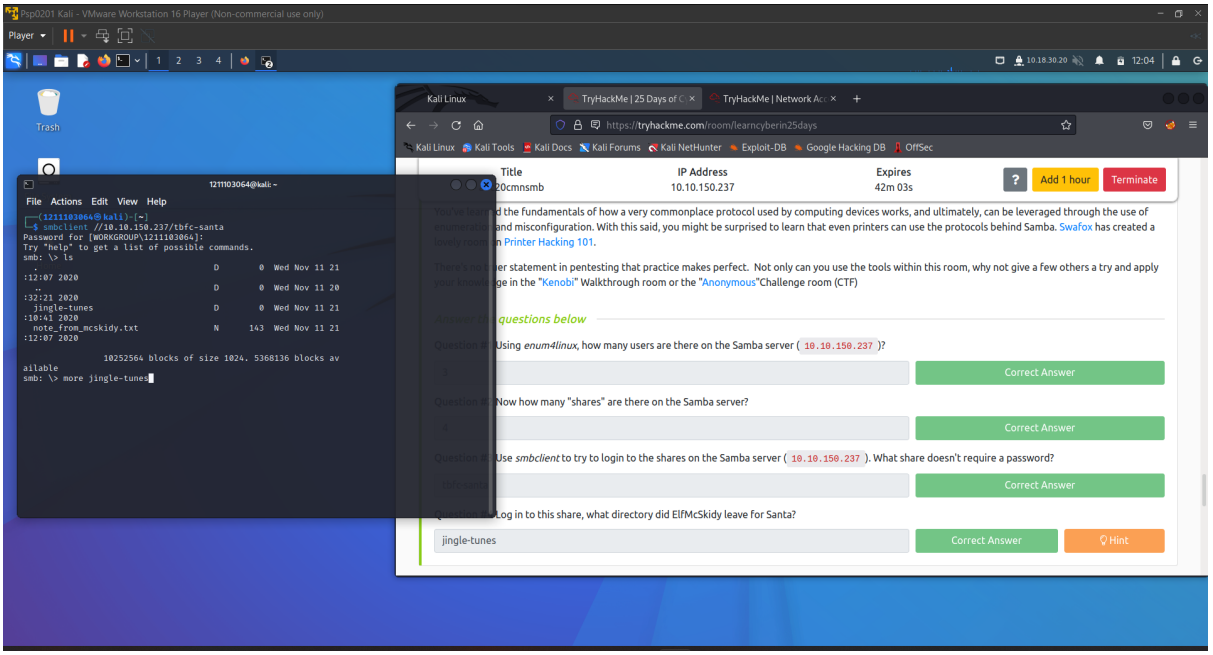
By using the enum4linux command which is **./enum4linux.pl -S MACHINE_IP** , we are able to get how many “shares” are there on the server.

Question 3



We use the smbclient tool which is **smbclient //INSTANCE_IP_ADDRESS/**sharename**** . We replace the “**sharename**” with the name of the “share” we wish to access. Share that doesn’t require a password is **tbfc-santa** .

Question 4



After log in into the “share" , we do command **ls** to get the list files and directories in the current location. The directory that ElfMcskidy left for Santa is **jingle-tunes**.

Thought Process / Methodology :

We opened the terminal prompt first and then we navigate to **enum4linux**. We run **enum4linux** and lists all the options by using the **./enum4linux.pl** . After that we used command **./enum4linux.pl -U MACHINE-IP** to get the userlist and then we used the command **./enum4linux.pl -S MACHINE_IP** to get the sharelist from the Samba server. We used smbclient tool script which is **smbclient //INSTANCE_IP_ADDRESS/**sharename**** to log in into the correct share that doesn’t require a password, we replace sharename with the “share” we wish to access and we just press “**enter”** when the system asks us for the password. The correct share will let us log in into the account without a password. After logging into the “share" which is **tbfc-santa,** we do command **ls** to get the correct directory which is **jingle-tunes**.

Extra Questions :

Day 6 :

Question 1

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

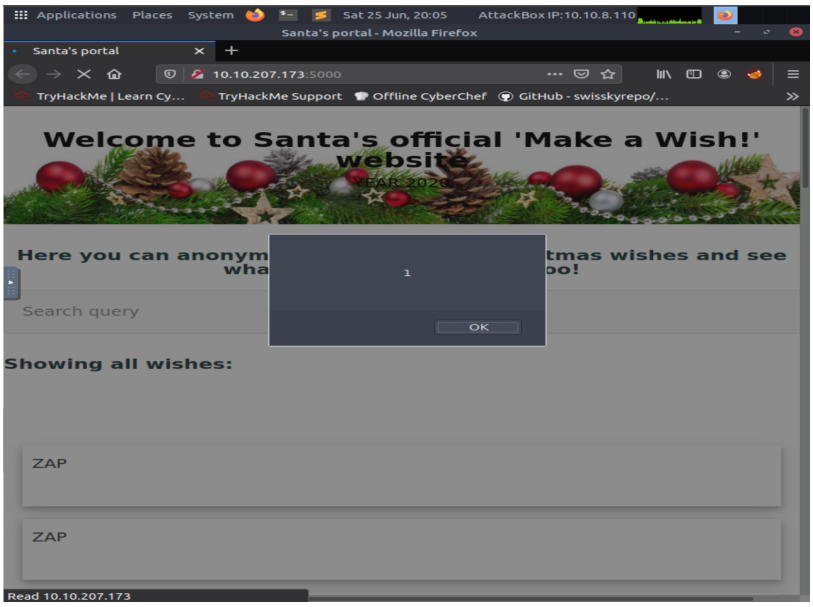
Validating a U.S. Zip Code (5 digits plus optional -4)

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

Question 6

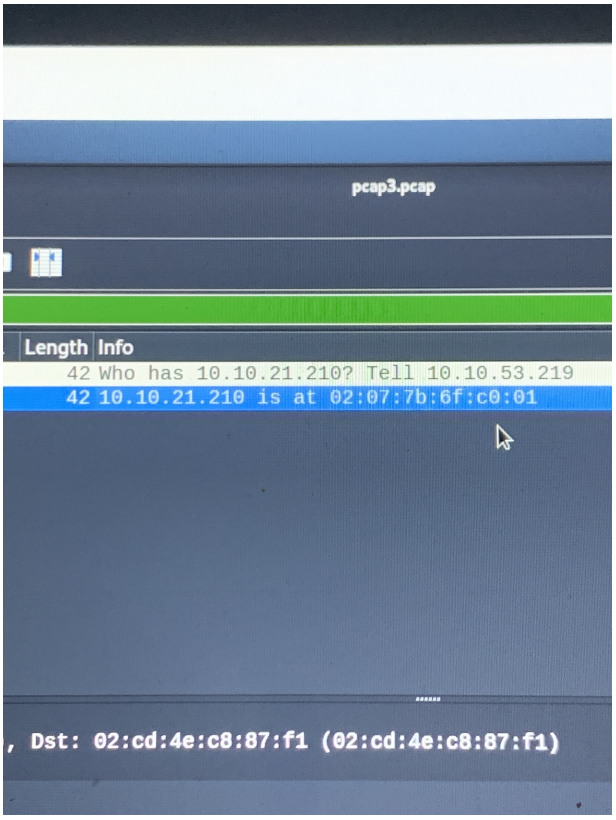
```
10.10.100.27/reflected?keyword=<script>alert(1)</script>
```

Question 7

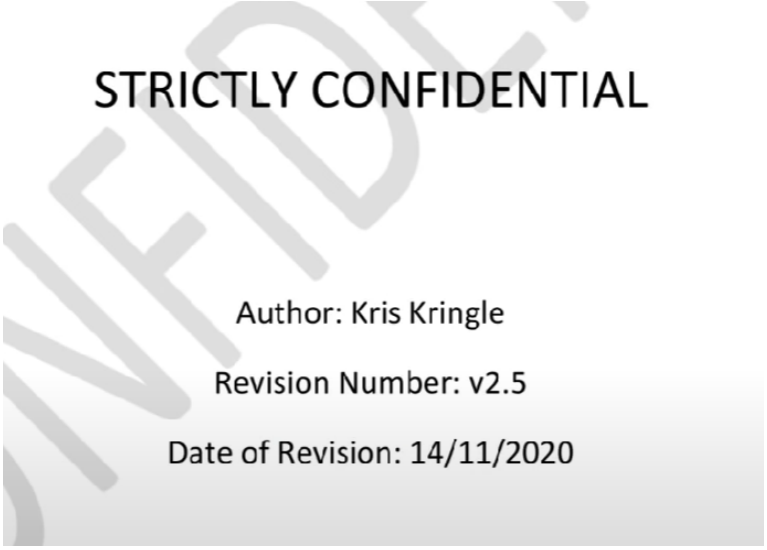


Day 7 :

Question 6



Question 8

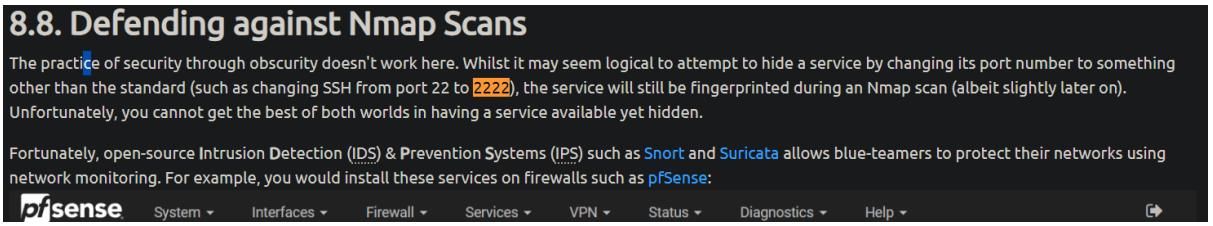


Day 8 :

Question 4

```
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&#39;s Internal Blog
```

Question 5



Day 10 :

Question 1

```
Options are (like "enum"):
    -U        get userlist
    -M        get machine list*
    -S        get sharelist
    -P        get password policy information
    -G        get group and member list
    -d        be detailed, applies to -U and -S
    -u user   specify username to use (default "")
    -p pass   specify password to use (default "")

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

Additional options:
    -a        Do all simple enumeration (-U -S -G -P -r -o -n -i).
              This option is enabled if you don't provide any other options.
    -h        Display this help message and exit
    -r        enumerate users via RID cycling
    -R range  RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
    -K n      Keep searching RIDs until n consective RIDs don't correspond to
              a username.  Impies RID range ends at 999999. Useful
              against DCs.
    -l        Get some (limited) info via LDAP 389/TCP (for DCs only)
    -s file   brute force guessing for share names
    -k user   User(s) that exists on remote system (default: administrator,guest,krbtgt,
              Used to get sid with "lookupsid known_username"
              Use commas to try several users: "-k admin,user1,user2"
    -o        Get OS information
    -i        Get printer information
    -w wrkg   Specify workgroup manually (usually found automatically)
    -n        Do an nmblookup (similar to nbtstat)
    -v        Verbose.  Shows full commands being run (net, rpcclient, etc.)
    -A        Aggressive. Do write checks on shares etc
```