

PSP0201

Week 3

Writeup

Group Name: Woohoo

Members

ID	Name	Role
1211100312	CHAN HAO YANG	Leader
1211101506	LEONG JIA YI	Member
1211101961	CHAI DI SHENG	Member
1211101726	TAI JIN PEI	Member

Day 6: Web Exploitation – Be careful with what you wish on a Christmas night

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

Solution/walkthrough:

Input validation strategies

Input validation should be applied on both **syntactical** and **Semantic** level.

Syntactic validation should enforce correct syntax of structured fields (e.g. SSN, date, currency symbol).

Semantic validation should enforce correctness of their *values* in the specific business context (e.g. start date is before end date, price is within expected range).

It is always recommended to prevent attacks as early as possible in the processing of the user's (attacker's) request. Input validation can be used to detect unauthorized input before it is processed by the application.

Open the link and find the description of syntactic and semantic:

https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Input_Validation_Cheat_Sheet.md

Question 1: Examine the OWASP Cheat Sheet. Match the input validation level with the correct description.

Answer: Syntactic : enforce correct syntax of structured fields

Semantic : enforce correctness of their values in the specific business context

Allow List Regular Expression Examples

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

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

Look for validating a U.S. zip code in the link.

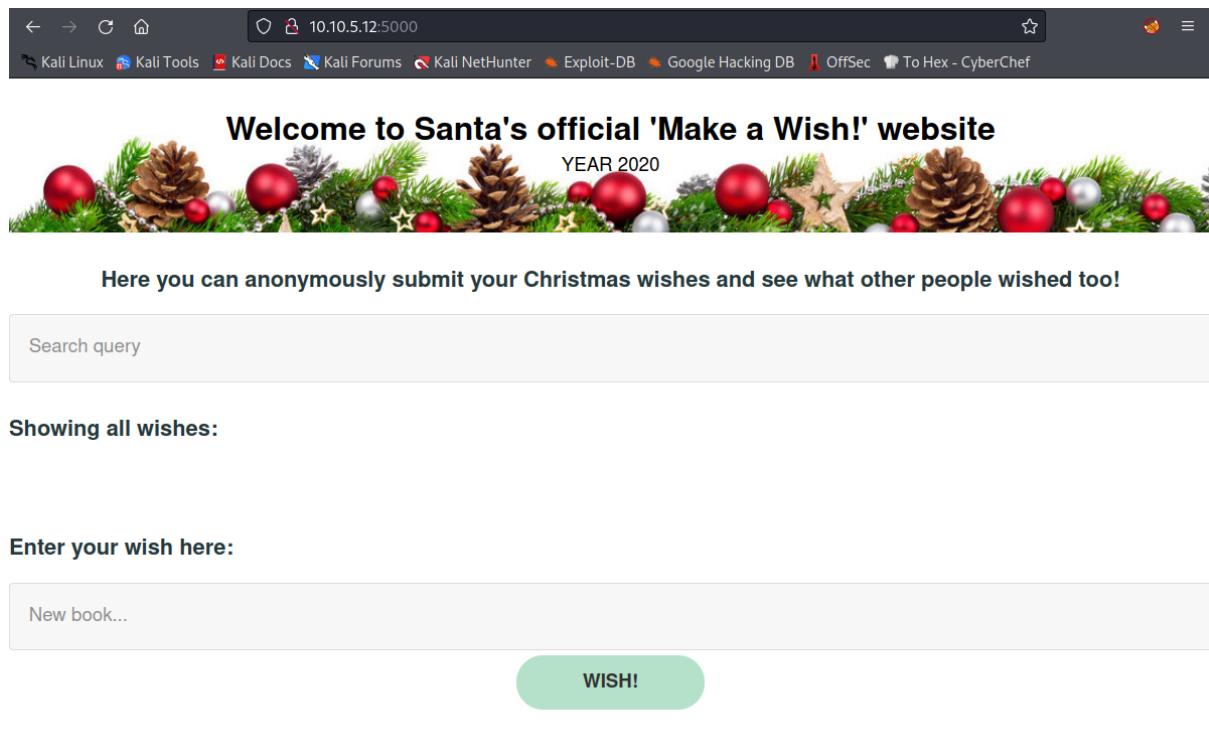
Question 2: Examine the OWASP Cheat Sheet. What is the regular expression used to validate a US Zip code?

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

Cross-site scripting (XSS) is a web vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, and carry out any actions that the user is able to perform. If the victim user has privileged access within the application (i.e admin), then the attacker might be able to gain full control over all of the application's functionality and data. Even if a user is a low privileged one, XSS can still allow an attacker to obtain a lot of sensitive information.

Question 3: What vulnerability type was used to exploit the application?

Answer: Stored cross-site scripting



Welcome to Santa's official 'Make a Wish!' website

YEAR 2020

Here you can anonymously submit your Christmas wishes and see what other people wished too!

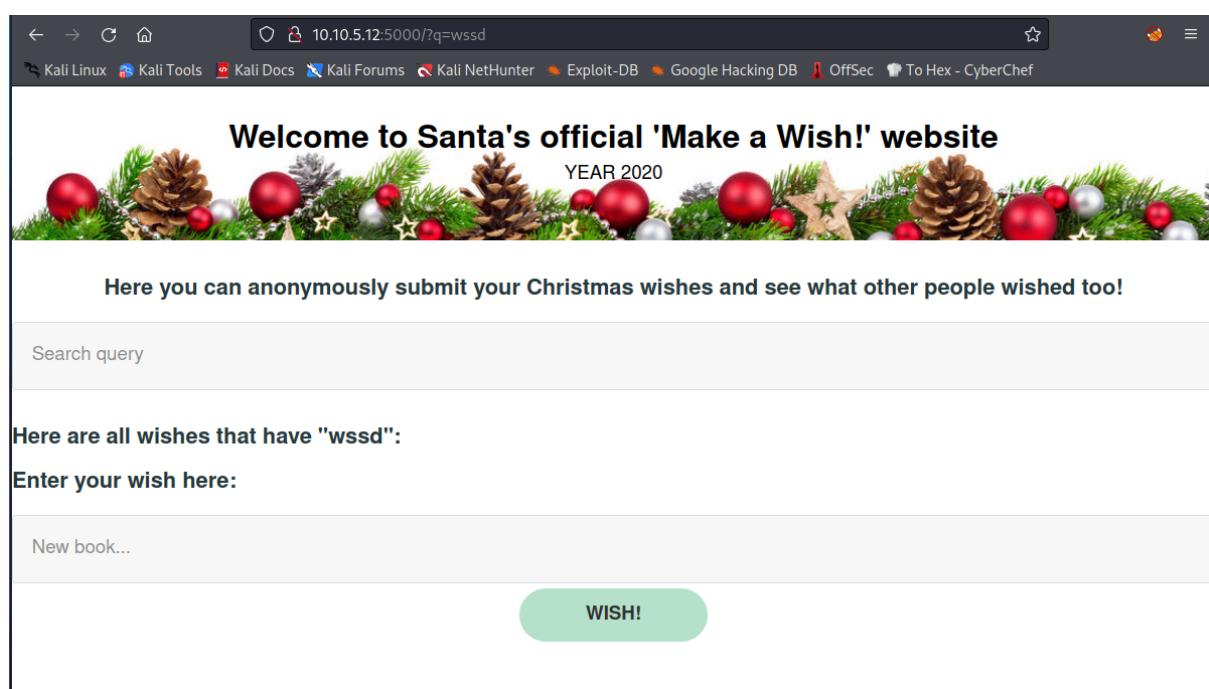
Search query

Showing all wishes:

Enter your wish here:

New book...

WISH!



Welcome to Santa's official 'Make a Wish!' website

YEAR 2020

Here you can anonymously submit your Christmas wishes and see what other people wished too!

Search query

Here are all wishes that have "wssd":

Enter your wish here:

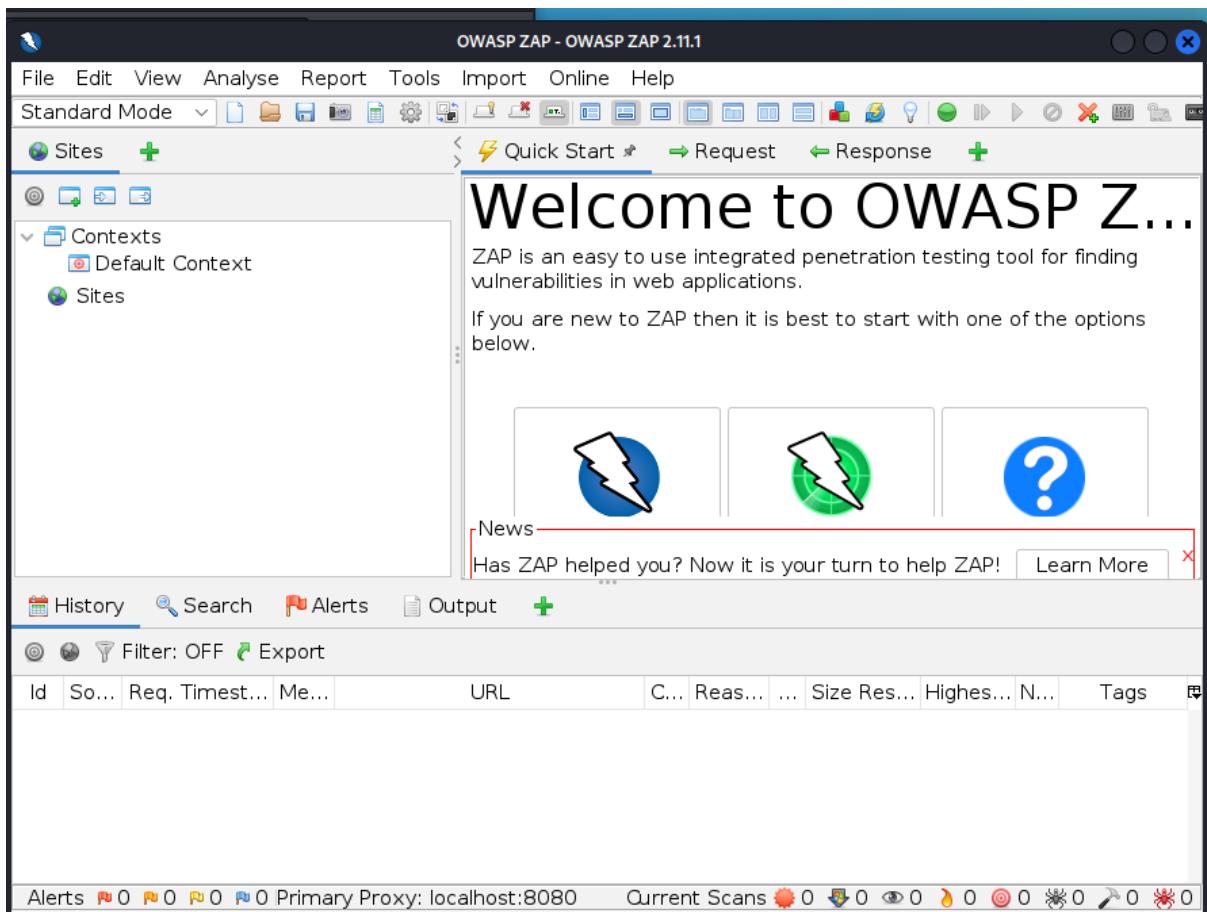
New book...

WISH!

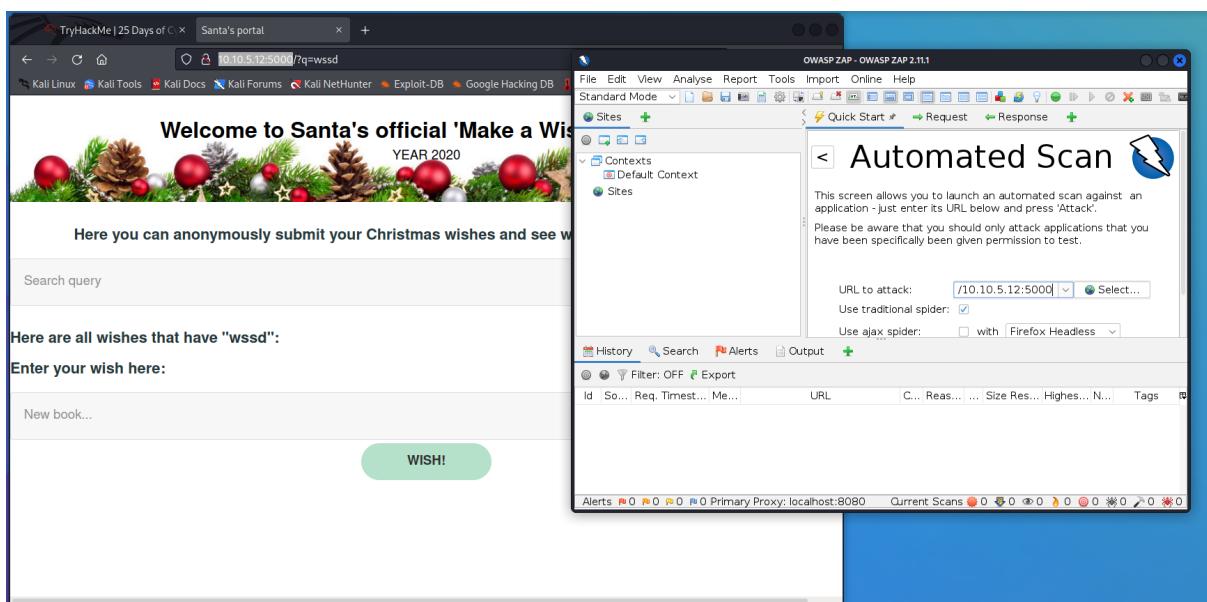
Key in something and press "WISH", the link will appear as a query string.

Question 4: What query string can be abused to craft a reflected XSS?

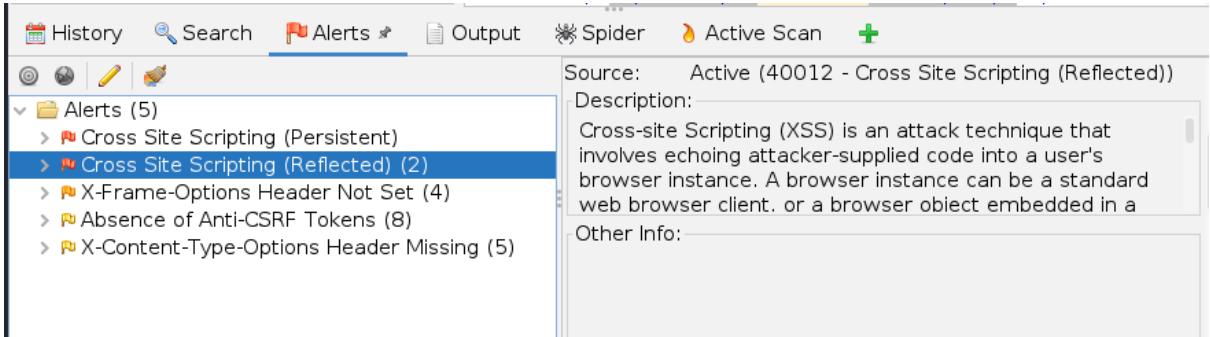
Answer: q



Open OWASP.



Copy MACHINE_IP and paste it in Automated Scan and click attack.



The screenshot shows the OWASP ZAP interface with the 'Alerts' tab selected. A single alert is highlighted: 'Cross Site Scripting (Reflected) (2)'. The alert details are as follows:

- Source: Active (40012 - Cross Site Scripting (Reflected))
- Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a
- Other Info: (empty)

Go to Alerts to get the number of alerts.

Cross Site Scripting (DOM Based)

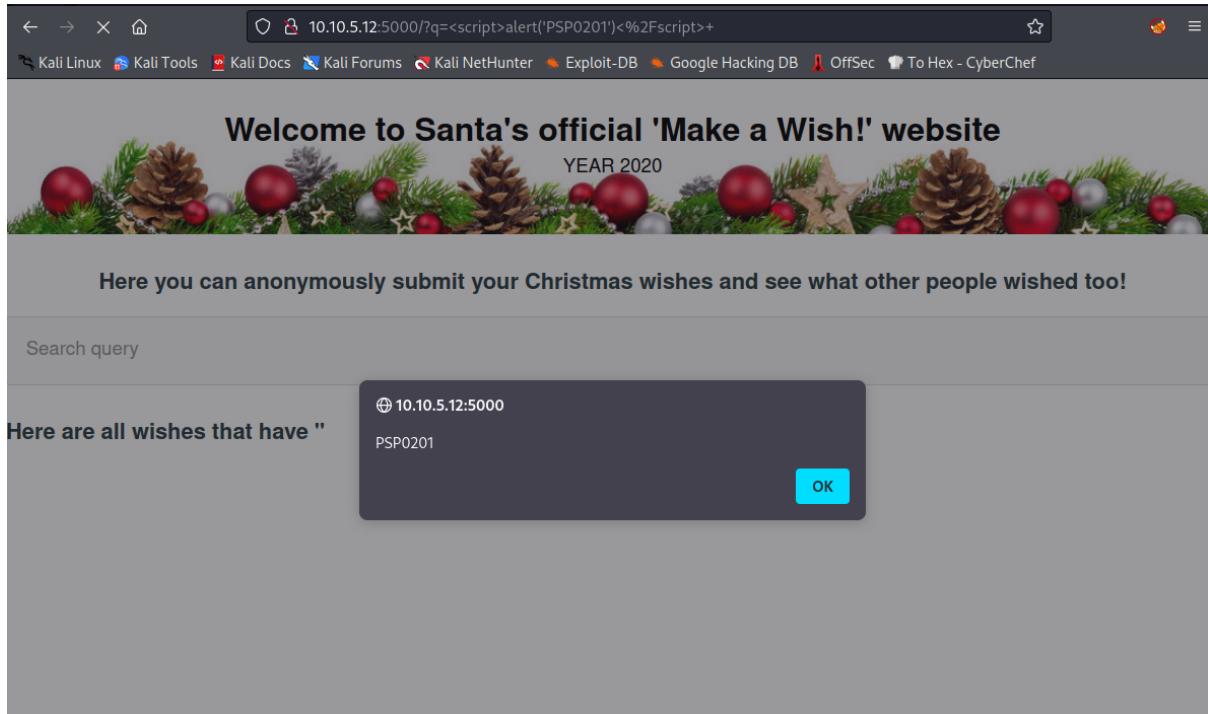
URL:	http://10.10.5.12:5000/
Risk:	High
Confidence:	High
Parameter:	
Attack:	>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence:	
CWE ID:	79
WASC ID:	8
Description:	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object

Cross Site Scripting (Reflected)

URL:	http://10.10.5.12:5000/
Risk:	High
Confidence:	Medium
Parameter:	comment
Attack:	</p><script>alert(1);</scRipt><p>
Evidence:	</p><script>alert(1);</scRipt><p>
CWE ID:	79
WASC ID:	8
Description:	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object

Question 5: Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts of high priority are in the scan?

Answers: 2



Type `<script>alert('PSP0201')</script>` in the wish text box and press “WISH”.

Q6: What Javascript code should you put in the wish text box if you want to show an alert saying “PSP0201”?

Answer: `<script>alert('PSP0201')</script>`

Question 7: Close your browser and revisit the site MACHINE-IP:5000 again. Does your XSS attack persist?

Answer: Yes

Thought Process/Methodology:

Open the link and find the description of syntactic and semantic:

https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Input_Validation_Cheat_Sheet.md and also look for validating a U.S. zip code in the link. Copy IP address and paste in a new tab. Key in something and press “WISH”, the link will appear as a query string. Open OWASP and copy MACHINE_IP and paste it in Automated Scan and click attack. Go to Alerts to get the number of alerts. Type `<script>alert('PSP0201')</script>` in the wish text box and press “WISH”.

Day 7: Networking – The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

Solution/walkthrough:

No.	Time	Source	Destination	Protocol	Length	Info
10	62.697400	10.10.15.52	91.189.92.39	TCP	74	56184 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TStamp=827256410 TSectr=0 WS=128
11	5.553381	10.10.15.52	91.189.88.184	TCP	74	[TCP Retransmission] 39768 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TStamp=1776
12	5.553394	10.10.15.52	91.189.88.185	TCP	74	[TCP Retransmission] 34628 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TStamp=5226
13	9.005543	10.11.3.2	10.10.15.52	TCP	55	57463 → 80 [ACK] Seq=1 Ack=1 Win=1029 Len=1
14	9.005564	10.10.15.52	10.11.3.2	TCP	66	80 → 57468 [ACK] Seq=1 Ack=2 Win=491 Len=0 SLE=1 SRE=2
15	9.585388	10.10.15.52	91.189.88.185	TCP	74	[TCP Retransmission] 34628 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TStamp=5226
16	9.585402	10.10.15.52	91.189.88.184	TCP	74	[TCP Retransmission] 39768 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TStamp=1776
17	16.436447	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=127 (reply in 18)
18	18.438472	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)

Open pcap1.pcap and search for ICMP/PING.

Question 1: Open "pcap1.pcap" in Wireshark. What is the IP address that initiates an ICMP/ping?

Answer: 10.11.3.2

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	62.481945	10.10.67.199	10.10.15.52	HTTP	342	GET /js/instantpage.min.js HTTP/1.1
95	62.487186	10.10.67.199	10.10.15.52	HTTP	347	GET /images/icon.png HTTP/1.1
185	62.516878	10.10.67.199	10.10.15.52	HTTP	336	GET /post/index.json HTTP/1.1
187	62.536694	10.10.67.199	10.10.15.52	HTTP	436	GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
188	62.532591	10.10.67.199	10.10.15.52	HTTP	445	GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
117	62.546748	10.10.67.199	10.10.15.52	HTTP	415	GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
282	62.788297	10.10.67.199	10.10.15.52	HTTP	415	GET /favicon.ico HTTP/1.1

Key in "http.request.method == GET" and press enter.

Question 2: If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

Answer: http.request.method == GET

No.	Time	Source	Destination	Protocol	Length	Info
338	63.997588	10.10.67.199	10.10.15.52	HTTP	366	GET /favicon.ico HTTP/1.1
340	64.005363	10.10.67.199	10.10.15.52	HTTP	481	GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
462	64.028692	10.10.67.199	10.10.15.52	HTTP	496	GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
467	64.028410	10.10.67.199	10.10.15.52	HTTP	466	GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
471	64.222360	10.10.67.199	10.10.15.52	HTTP	365	GET /posts/reindeer-of-the-week/ 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
480	66.251644	10.10.67.199	10.10.15.52	HTTP	448	GET /posts/fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
482	66.262598	10.10.67.199	10.10.15.52	HTTP	462	GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff HTTP/1.1
484	66.279297	10.10.67.199	10.10.15.52	HTTP	447	GET /posts/fonts/roboto-v20-latin-regular.woff HTTP/1.1

Look for the difference between them and get the answer.

Question 3: Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "10.10.67.199" visited?

Answer: reindeer-of-the-week

No.	Time	Source	Destination	Protocol	Length	Info
13	4.103450	10.10.73.25	10.10.122.1	FTP	220	Welcome to the TBFC FTP Server!
14	4.103479	10.10.122.1	10.10.73.25	FTP	321	Please specify the password.
15	4.103828	10.10.73.25	10.10.122.1	FTP	530	530 Login incorrect.
16	4.105594	10.10.122.1	10.10.73.25	FTP	530	530 Please login with USER and PASS.
17	4.105812	10.10.73.25	10.10.122.1	FTP	530	530 Please login with USER and PASS.
20	7.866325	10.10.73.25	10.10.122.1	FTP	530	530 Please login with USER and PASS.
21	7.866352	10.10.73.25	10.10.122.1	FTP	530	530 Please login with USER and PASS.
22	7.866438	10.10.73.25	10.10.122.1	FTP	530	530 Please login with USER and PASS.
23	7.866878	10.10.73.25	10.10.122.1	FTP	530	530 Please login with USER and PASS.
24	14.282663	10.10.73.25	10.10.122.1	FTP	530	530 Please login with USER and PASS.
29	14.323826	10.10.73.25	10.10.122.1	FTP	530	530 Please login with USER and PASS.
31	16.357293	10.10.73.25	10.10.122.1	FTP	530	530 Please login with USER and PASS.
41	16.184 bytes on wire (83 bytes on wire)					Find

Now open pcap2.pcap. Look for the most requested FTP and click follow and the answer will be shown.

Question 4: Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process?

Answer: plaintext_password_fiasco

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	150	Server: Encrypted packet (len=96)

Question 5: Continuing with our analysis of "pcap2.pcap", what is the name of the protocol that is encrypted?

Answer: SSH

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	150	Server: Encrypted packet (len=96)
3	0.000016	10.10.122.128	10.10.122.128	TCP	54	57480 - 22 [ACK] Seq=1 Ack=49 Win=1024 Len=0
4	0.101317	10.10.122.128	10.10.122.128	TCP	54	57480 - 23 [ACK] Seq=1 Ack=49 Win=1024 Len=0
5	1.127866	10.10.122.128	91.189.92.49	TCP	74	33469 - 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118188800 TSecr=0 WS=128
6	2.549894	10.10.73.252	10.10.122.128	FTP	72	Request: QUIT
7	2.549999	10.10.122.128	10.10.73.252	FTP	80	Response: 221 Goodbye.
8	2.558011	10.10.122.128	10.10.73.252	TCP	66	21 - 45332 [FIN, ACK] Seq=15 Ack=7 Win=490 Len=0 TSval=894813665 TSecr=411028459
9	2.558520	10.10.73.252	10.10.122.128	TCP	66	45332 - 21 [ACK] Seq=15 Win=491 Len=0 TSval=411028463 TSecr=894813665
10	2.558529	10.10.73.252	10.10.122.128	TCP	66	45332 - 21 [FIN, ACK] Seq=16 Ack=491 Win=0 TSval=411028463 TSecr=894813665
11	2.558534	10.10.122.128	10.10.73.252	TCP	66	21 - 45332 [ACK] Seq=16 Ack=8 Win=490 Len=0 TSval=894813670 TSecr=411028463
12	3.175873	10.10.122.128	91.189.92.49	TCP	74	33469 - 443 [SYN] Seq=0 Win=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=31181890848 TSecr=0 WS=128
13	4.1092450	10.10.73.252	10.10.122.128	TCP	74	15240 - 24 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=31181890844 TSecr=0 WS=128

Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
 Ethernet II, Src: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa), Dst: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51)
 Internet Protocol Version 4, Src: 10.11.3.2, Dst: 10.10.122.128
 Transmission Control Protocol, Src Port: 57748, Dst Port: 22, Seq: 1, Ack: 49, Len: 0

Click it and the answer is shown.

Question 6: Examine the ARP communications. Who has 10.10.122.128? Tell 10.10.10.1. Answer: 10.10.122.128 is at

Answer: 02:c0:56:51:8a:51

No.	Time	Source	Destination	Protocol	Length	Info
286	26.536504	10.10.53.219	10.10.21.210	TCP	74	88 - 80 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=1676611782 TSecr=0 WS=128
289	26.536965	10.10.21.210	10.10.53.219	TCP	74	89 - 38456 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM=1 TSval=1809533241 TSecr=1809533241
290	26.536993	10.10.53.219	10.10.21.210	TCP	66	38456 - 80 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=1676611782 TSecr=1809533241
291	26.537049	10.10.53.219	10.10.21.210	HTTP	215	GET /christmas.zip HTTP/1.1
294	26.537385	10.10.21.210	10.10.53.219	TCP	66	89 - 38456 [ACK] Seq=1 Ack=159 Win=62592 Len=0 TSval=1809533241 TSecr=1676611782
295	26.537729	10.10.21.210	10.10.53.219	TCP	9015	89 - 38456 [ACK] Seq=1 Ack=159 Win=62592 Len=8949 TSval=1809533241 TSecr=1676611782 [TCP seg1]
296	26.537746	10.10.53.219	10.10.21.210	TCP	66	38456 - 89 [ACK] Seq=159 Ack=8950 Win=56784 Len=0 TSval=1676611783 TSecr=1809533241
297	26.537842	10.10.21.210	10.10.53.219	TCP	35862	89 - 38456 [ACK] Seq=8950 Ack=150 Win=62592 Len=35796 TSval=1809533241 TSecr=1676611782 [TCP seg1]
298	26.537863	10.10.53.219	10.10.21.210	TCP	66	38456 - 89 [ACK] Seq=159 Ack=44746 Win=33024 Len=0 TSval=1676611783 TSecr=1809533241
300	26.537872	10.10.21.210	10.10.53.219	TCP	9015	89 - 38456 [PSH, ACK] Seq=44746 Ack=150 Win=62592 Len=8944 TSval=1809533241 TSecr=1676611782
301	26.537878	10.10.53.219	10.10.21.210	TCP	66	38456 - 89 [ACK] Seq=159 Ack=3695 Win=26368 Len=0 TSval=1676611783 TSecr=1809533241
302	26.537882	10.10.21.210	10.10.53.219	TCP	9228	89 - 38456 [ACK] Seq=159 Ack=159 Win=62592 Len=9154 TSval=1809533241 TSecr=1676611782 [TCP seg1]
304	26.538054	10.10.53.219	10.10.21.210	TCP	66	38456 - 80 [ACK] Seq=159 Ack=62849 Win=17536 Len=0 TSval=1676611783 TSecr=1809533241

christmas.zip

elf_mcskidy_wishlist.txt

~/.cache/lfr-GRAD3/elf_mcskidy_wishlist.txt - Mousepad

```
1 Wish list For Elf McSkidy
2
3 Budget: £100
4
5 x3 Hak 5 Pineapples
6 x1 Rubber ducky (to replace Elf McEager)
7
```

Find the christmas.zip and open the elf_mcskidy_wishlist.txt.

Question 7: Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

Answer: rubber ducky



STRICTLY CONFIDENTIAL

Author: Kris Kringle

Revision Number: v2.5

Date of Revision: 14/11/2020

Open the Operation Artic Storm.pdf from christmas.zip.

Question 8: Who is the author of Operation Artic Storm?

Answer: Kris Kringle

Thought Process/Methodology:

Open pcap1.pcap and search for ICMP/PING. Key in “http.request.method == GET” and press enter and look for the difference between them and get the answer. Now open pcap2.pcap and look for the most requested FTP and click follow and the answer will be shown. Click it and the answer is shown. Find the christmas.zip and open the elf_mcskidy_wishlist.txt. Open the Operation Artic Storm.pdf from christmas.zip.

Day 8: Networking – What's Under the Christmas Tree?

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

Solution/walkthrough:

About 1,580,000 results (0.45 seconds)

1998

Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) created by Martin Roesch in **1998**.



<https://digital.ai/technology/snort> ::

Snort - Digital.ai

Question 1: When was Snort created?

Answer: 1998

```
└─(1211101961㉿kali)-[~]
$ nmap 10.10.101.186
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 05:34 EDT
Nmap scan report for 10.10.101.186
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 19.59 seconds
```

Open terminal and use nmap on MACHINE_IP.

Question 2: Using nmap on MACHINE_IP , what are the port numbers of the three services running?

Answer: 80,2222,3389

```
└─(1211101961㉿kali)-[~]
$ nmap -sV 10.10.101.186
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 05:38 EDT
Nmap scan report for 10.10.101.186
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
2222/tcp  open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu
tu Linux; protocol 2.0)
3389/tcp  open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results a
t https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.14 seconds
```

Key in nmap -sV and MACHINE_IP.

Question 3: Use Nmap to determine the name of the Linux distribution that is running, what is reported as the most likely distribution to be running?

Answer: Ubuntu

Question 4: What is the version of Apache?

Answer: 2.4.29

Question 5: What is running on port 2222?

Answer: SSH

```
(1211101961㉿kali)-[~]
$ nmap -A 10.10.101.186
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 05:39 EDT
Nmap scan report for 10.10.101.186
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-title: TBFC's Internal Blog
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp  open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_  256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
3389/tcp  open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.24 seconds
```

Key in nmap -A and MACHINE_IP.

Question 6: Use Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. Based on the value returned, what do we think this website might be used for?

Answer: blog

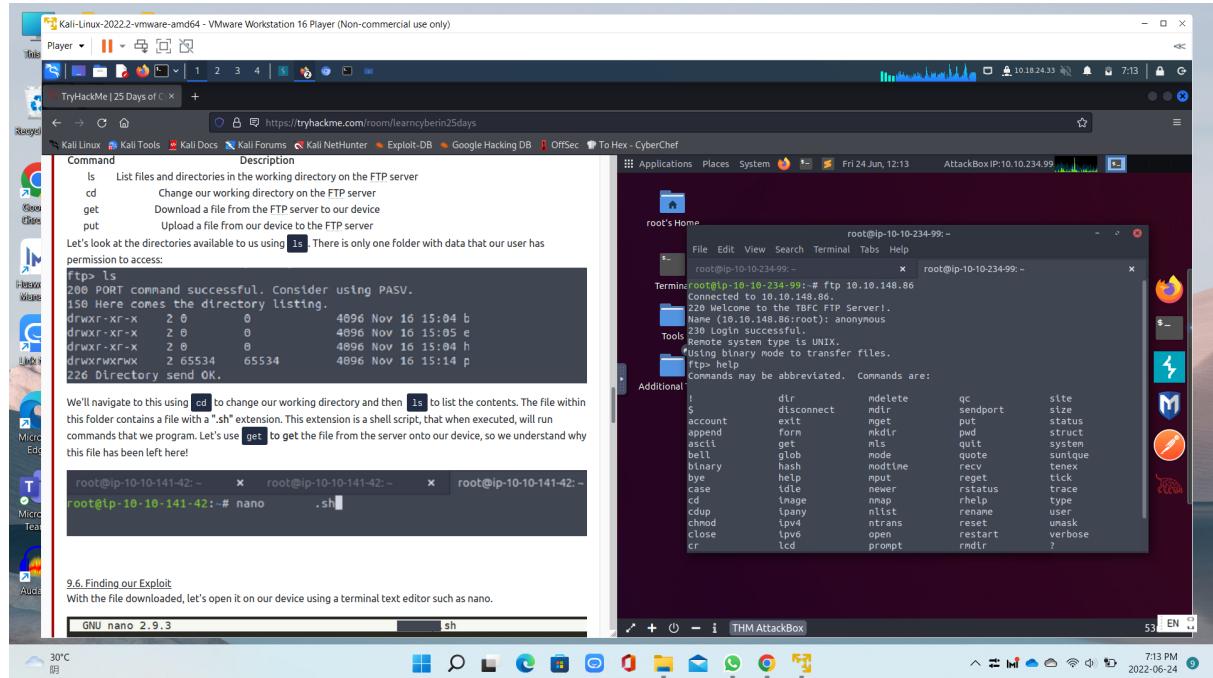
Thought Process/Methodology:

Open terminal and use nmap on MACHINE_IP. After that, key in nmap -sV and MACHINE_IP. Last, key in nmap -A and MACHINE_IP.

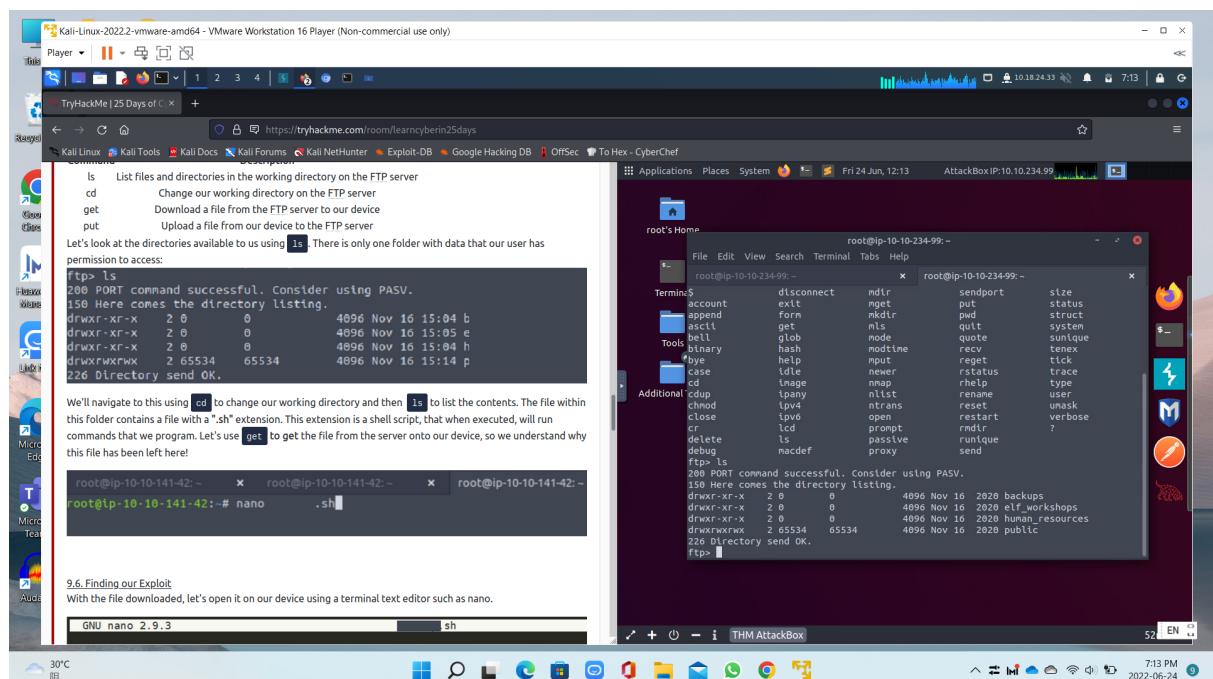
Day 9: Networking – Anyone can be Santa!

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

Solution/walkthrough:



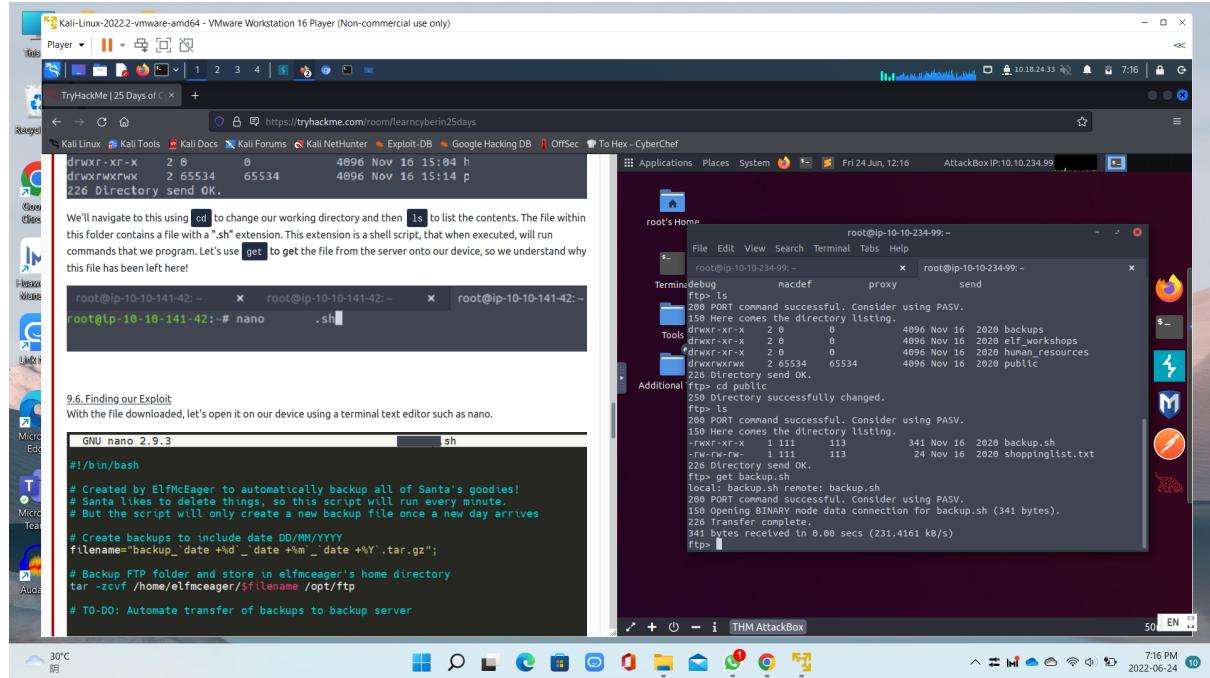
First, press Start Machine and Start AttackBox. After that, open the terminal in AttackBox and type in `ftp_MACHINE IP` which is `10.10.148.86`. Enter `anonymous` for the name. Enter “help” to list out some commands.



Enter “ls” to look at the directories which are available.

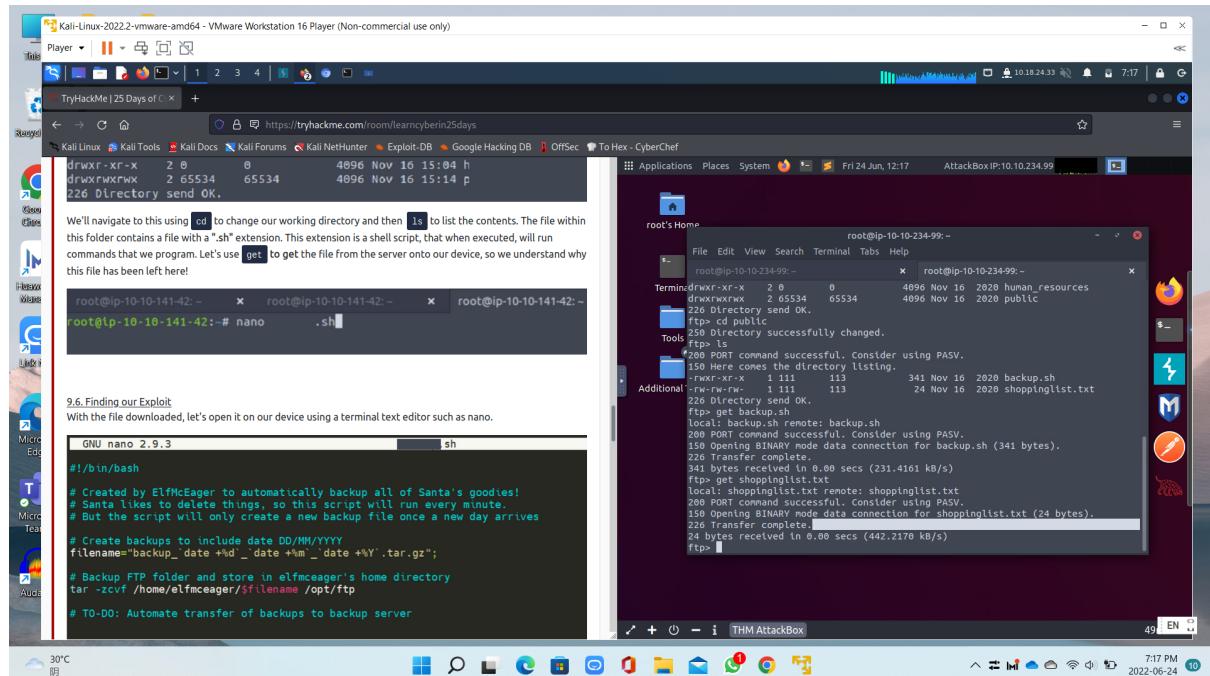
Question 1: What are the directories you found on FTP site?

Answer: backups, elf_workshop, human_resources, and public.



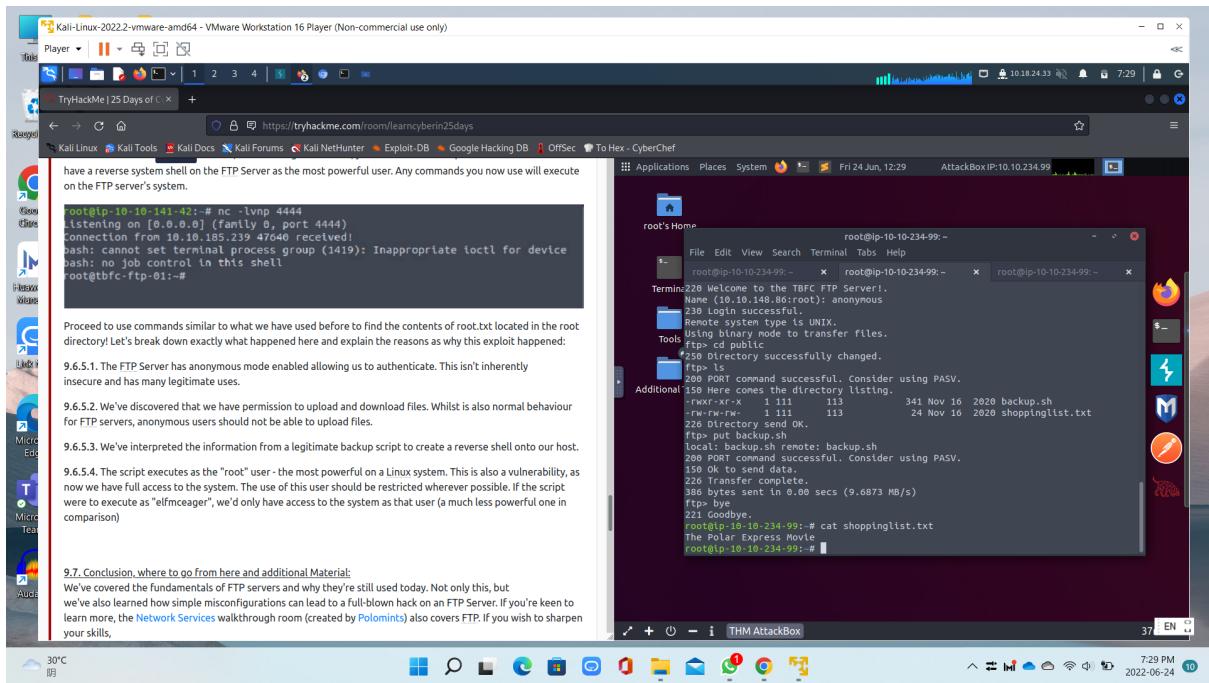
Question 2: Name the directories on the FTP server that has data accessible by the “anonymous” user.

Answer: public



Question 3: What script gets executed within this directory?

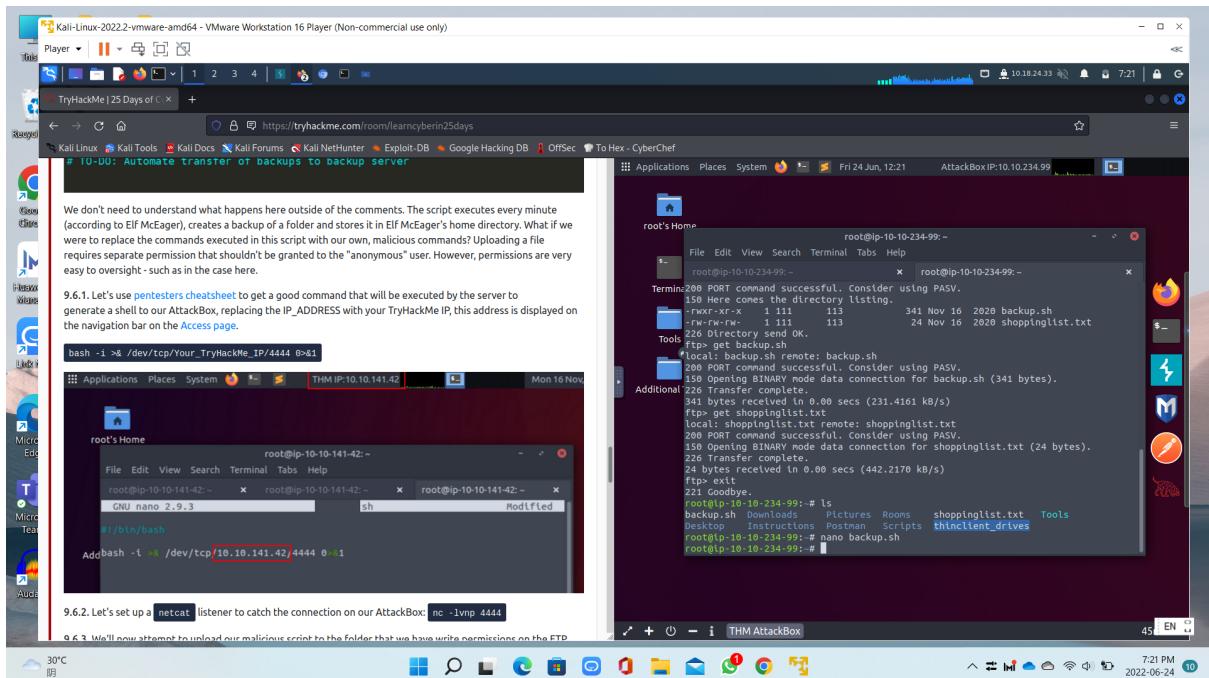
Answer: backup.sh



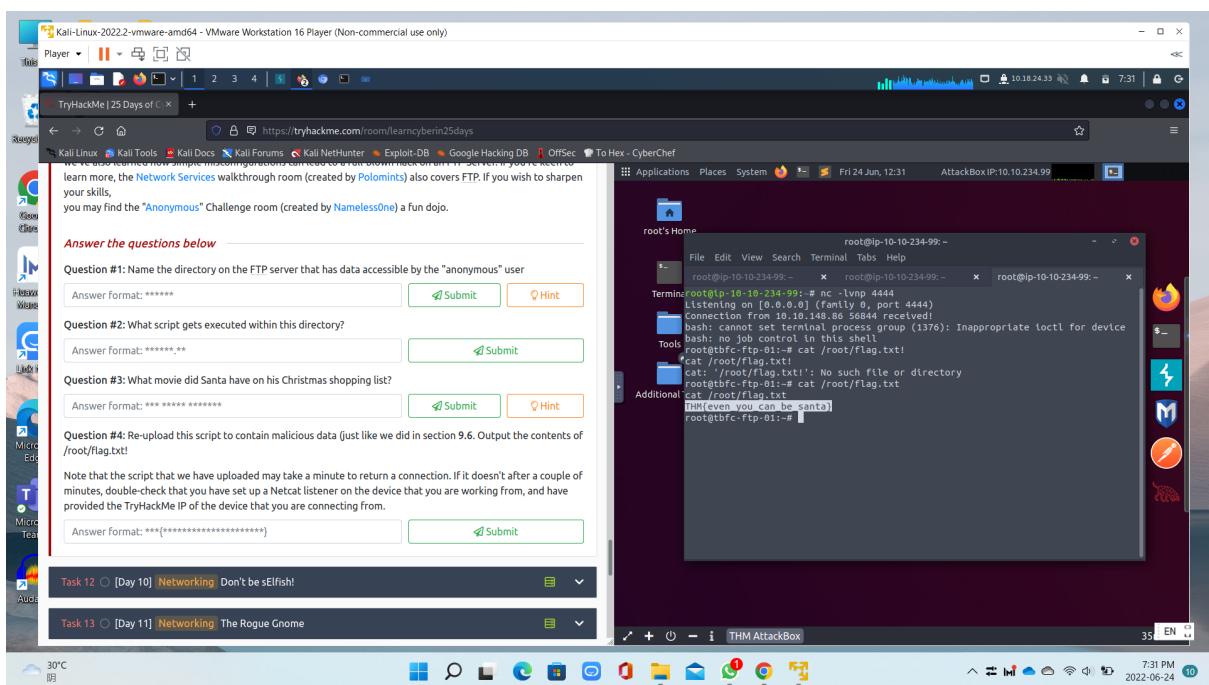
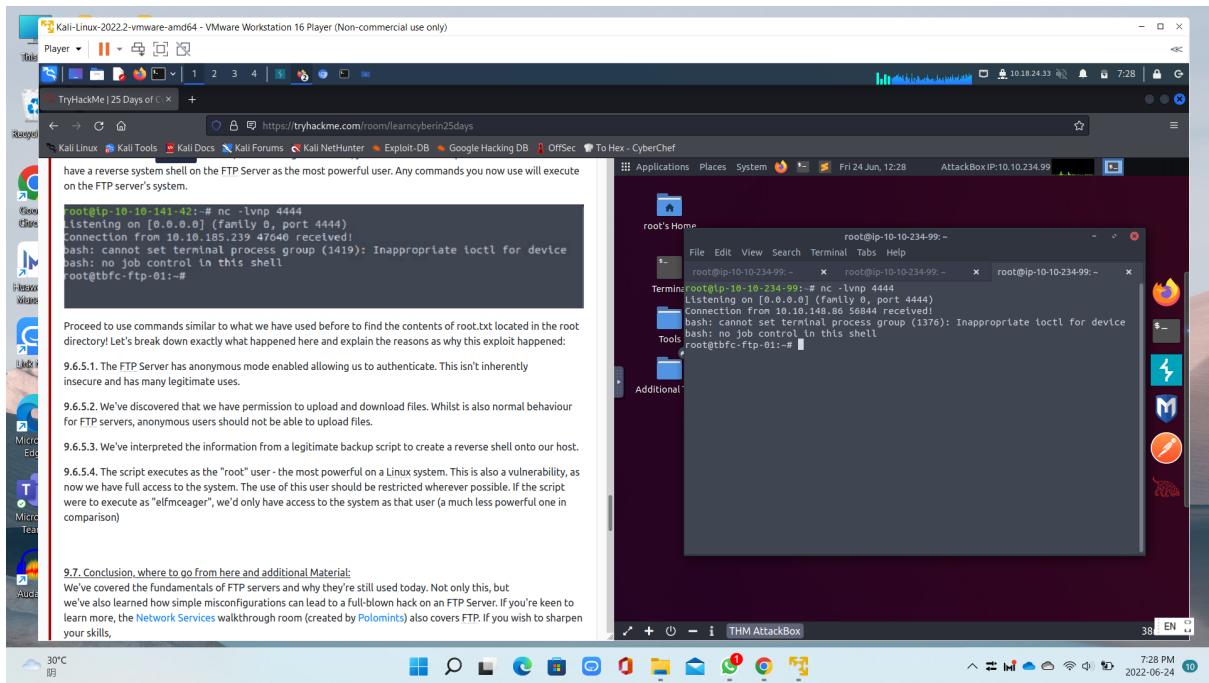
Enter “cat shoppinglist.txt” to get the answer.

Question 4: What movie did Santa have on his Christmas shopping list?

Answer: The Polar Express Movie



Key in nano backup.sh to add in command.



Enter “nc -lvp 4444” and press “Enter”, it will show “connection from IP-address received!” after a few minutes. After that, key in “cat /root/flag.txt” and press “Enter” and it will show a flag.

Question 5: Re-upload this script to contain malicious data (just like we did in section 9.6. Output the content of /root/flag.txt!

Answer: THM{even_you_can_be_santa}

Thought Process/Methodology:

First, press Start Machine and Start AttackBox. After that, open the terminal in AttackBox and type in ftp_MACHINE IP which is 10.10.148.86. Enter anonymous for the name. Enter “help” to list out some commands. Enter “ls” to look at the directories which are available. Enter “cat shoppinglist.txt” to get the answer. Key in nano backup.sh to add in command. Enter “nc -lvp 4444” and press “Enter”, it will show “connection from IP-address received!” after a few minutes. After that, key in “cat /root/flag.txt” and press “Enter” and it will show a flag.

Day 10: Networking – Don’t be sElfish!

Tools used: Kali Linux, Firefox

Solution/walkthrough:

```
1211101961@kali: ~
File Actions Edit View Help
1211101961@kali: ~ x 1211101961@kali: ~ x

└──(1211101961@kali)-[~]
$ enum4linux -h
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

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 -i).
        This option is enabled if you don't provide any other options.
-h      Display this help message and exit
-r      enumerate users via RID cycling
-R range RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
-K n    Keep searching RIDs until n 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,gues
t,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
-i      Get printer information
-w wrkg  Specify workgroup manually (usually found automatically)
-n      Do an nmblookup (similar to nbtstat)
-v      Verbose. Shows full commands being run (net, rpcclient, etc.)
-A      Aggressive. Do write checks on shares etc
```

Enter “enum4linux -h” to get the flags with descriptions in the terminal.

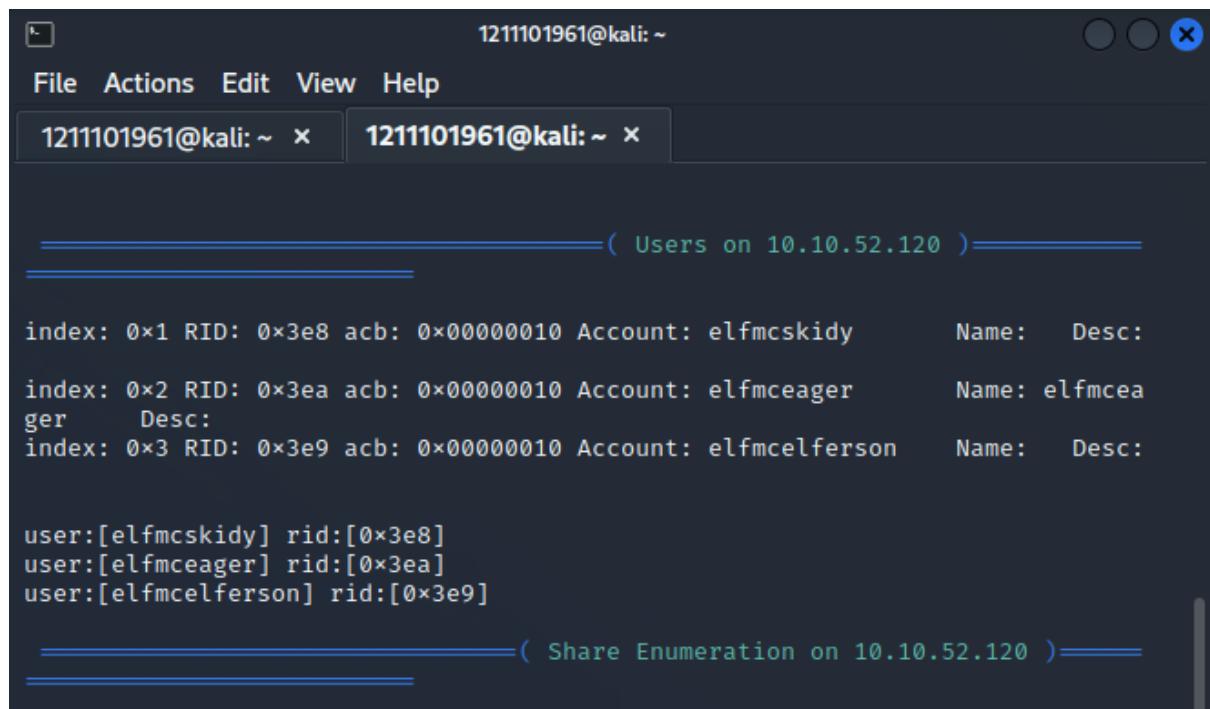
Question 1: Examine the help options for enum4linux. Match the following flags with the descriptions.

Answer: -h : Display help messages

-a : Do all simple enumeration

-S : Get sharelist

-o : Get OS information



```
1211101961@kali: ~
1211101961@kali: ~

=====
( Users on 10.10.52.120 )
=====

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

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

=====
( Share Enumeration on 10.10.52.120 )
=====
```

Enter “enum4linux -U IP Address(10.10.52.120)” to get the number of users.

Question 2: Using enum4linux, how many users are there on the Samba server?

Answer: 3

```
1211101961@kali: ~
File Actions Edit View Help
1211101961@kali: ~ x 1211101961@kali: ~ x

[ (1211101961@kali)-[~]
$ enum4linux -S 10.10.52.120
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linu
x/ ) on Fri Jun 24 12:36:21 2022

===== ( Target Information ) =====

Target ..... 10.10.52.120
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.10.52.120 ) =====

[+] Got domain/workgroup name: TBFC-SMB-01

===== ( Session Check on 10.10.52.120 ) =====

[+] Server 10.10.52.120 allows sessions using username '', password ''

===== ( Getting domain SID for 10.10.52.120 ) =====

Domain Name: TBFC-SMB-01
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

===== ( Share Enumeration on 10.10.52.120 ) =====

Sharename      Type      Comment
```

Enter “enum4linux -S IP Address(10.10.52.120)” to get the sharelist.

```
1211101961@kali: ~
File Actions Edit View Help
1211101961@kali: ~ x 1211101961@kali: ~ x

[+] Got domain/workgroup name: TBFC-SMB-01
=====
[+] Server 10.10.52.120 allows sessions using username '', password ''
=====
Domain Name: TBFC-SMB-01
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
=====
[+] Share Enumeration on 10.10.52.120
=====



| Sharename  | Type | Comment                                       |
|------------|------|-----------------------------------------------|
| tbfc-hr    | Disk | tbfc-hr                                       |
| tbfc-it    | Disk | tbfc-it                                       |
| tbfc-santa | Disk | tbfc-santa                                    |
| IPC\$      | IPC  | IPC Service (tbfc-smb server (Samba, Ubuntu)) |


Reconnecting with SMB1 for workgroup listing.



| Server      | Comment  |
|-------------|----------|
| Workgroup   | Master   |
| TBFC-SMB-01 | TBFC-SMB |


[+] Attempting to map shares on 10.10.52.120
//10.10.52.120/tbfc-hr  Mapping: DENIED Listing: N/A Writing: N/A
//10.10.52.120/tbfc-it  Mapping: DENIED Listing: N/A Writing: N/A
//10.10.52.120/tbfc-santa  Mapping: OK Listing: OK Writing: N/A
```

Question 3: Now how many “shares” are there on the Samba server?

Answer: 4

```
1211101961@kali: ~
File Actions Edit View Help
1211101961@kali: ~ x 1211101961@kali: ~ x
[+] Server 10.10.52.120 allows sessions using username '', password ''

===== ( Getting domain SID for 10.10.52.120 ) =====

Domain Name: TBFC-SMB-01
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

===== ( Share Enumeration on 10.10.52.120 ) =====



| Sharename  | Type | Comment                                       |
|------------|------|-----------------------------------------------|
| tbfc-hr    | Disk | tbfc-hr                                       |
| tbfc-it    | Disk | tbfc-it                                       |
| tbfc-santa | Disk | tbfc-santa                                    |
| IPC\$      | IPC  | IPC Service (tbfc-smb server (Samba, Ubuntu)) |


Reconnecting with SMB1 for workgroup listing.



| Server      | Comment  |
|-------------|----------|
| Workgroup   | Master   |
| TBFC-SMB-01 | TBFC-SMB |

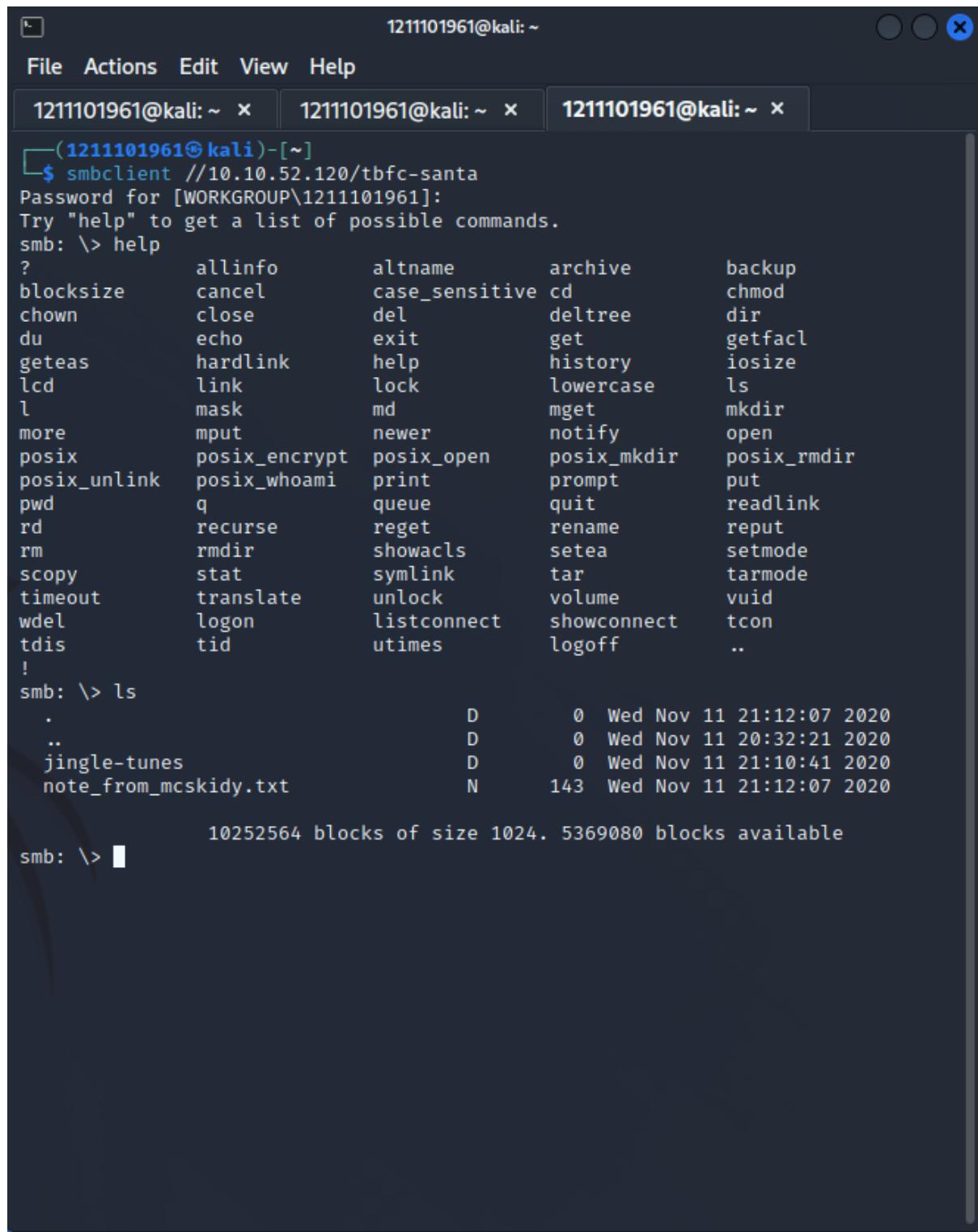

[+] Attempting to map shares on 10.10.52.120

//10.10.52.120/tbfc-hr  Mapping: DENIED Listing: N/A Writing: N/A
//10.10.52.120/tbfc-it  Mapping: DENIED Listing: N/A Writing: N/A
//10.10.52.120/tbfc-santa  Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.10.52.120/IPC$  Mapping: N/A Listing: N/A Writing: N/A
enum4linux complete on Fri Jun 24 12:36:45 2022

———(1211101961@kali)-[~]
```



1211101961@kali: ~

File Actions Edit View Help

1211101961@kali: ~ x 1211101961@kali: ~ x 1211101961@kali: ~ x

```
└─(1211101961㉿kali)-[~]
$ smbclient //10.10.52.120/tbfc-santa
Password for [WORKGROUP\1211101961]:
Try "help" to get a list of possible commands.
smb: \> help
?
allinfo      altname      archive      backup
blocksize    cancel       case_sensitive cd        chmod
chown       close        del           deltree    dir
du          echo         exit          get        getfacl
geteas      hardlink    help          history    iosize
lcd         link         lock          lowercase ls
l            mask         md            mget      mkdir
more        mput        newer         notify    open
posix       posix_encrypt posix_open    posix_mkdir posix_rmdir
posix_unlink posix_whoami  print        prompt   put
pwd          q           queue        quit     readlink
rd           recurse     reget        rename   reput
rm           rmdir       showacls    setea    setmode
scopy      stat         symlink     tar      tarmode
timeout    translate    unlock      volume   vuid
wdel       logon       listconnect showconnect tcon
tdis        tid         utimes     logoff   ..
!
smb: \> ls
.
..
jingle-tunes
note_from_mcskidy.txt
10252564 blocks of size 1024. 5369080 blocks available
smb: \> █
```

Enter “smbclient //IP Address(10.10.52.120)/sharename(tbfc-santa)” and press enter. After that, simply type in the password.

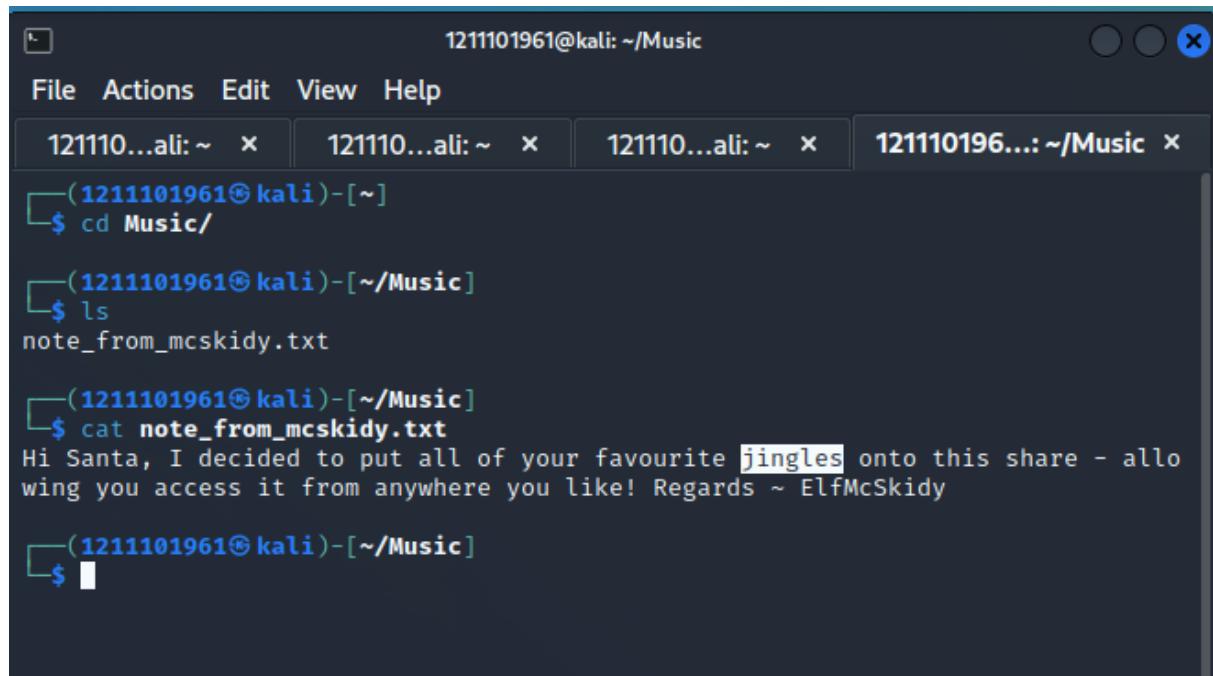
Question 4: Use smbclient to try to login to the shares on the Samba server. What share doesn't not require a password?

Answer: tbfc-santa

```
1211101961@kali: ~
File Actions Edit View Help
121110...ali: ~ x 121110...ali: ~ x 121110...ali: ~ x 121110196...: ~/Music x
(1211101961@kali)-[~]
$ smbclient //10.10.52.120/tbfc-santa
Password for [WORKGROUP\1211101961]:
Try "help" to get a list of possible commands.
smb: \> help
?           allinfo      altname      archive      backup
blocksize    cancel       case_sensitive cd          chmod
chown       close        del          deltreetree  dir
du          echo         exit         get          getfacl
geteas      hardlink    help         history      iosize
lcd         link         lock         lowercase   ls
l           mask         md          mget        mkdir
more        mput        newer        notify      open
posix       posix_encrypt  posix_open   posix_mkdir posix_rmdir
posix_unlink posix_whoami  print       prompt      put
pwd         q            queue      quit        readlink
rd          recurse     reget      rename      reput
rm          rmdir       showacls   setea      setmode
scopy      stat         symlink   tar        tarmode
timeout    translate   unlock     volume     vuid
wdel       logon       listconnect  showconnect tcon
tdis        tid         utimes    logoff    ..
!
smb: \> ls
.
..
jingle-tunes
note_from_mcskidy.txt
D      0  Wed Nov 11 21:12:07 2020
D      0  Wed Nov 11 20:32:21 2020
D      0  Wed Nov 11 21:10:41 2020
N      143 Wed Nov 11 21:12:07 2020

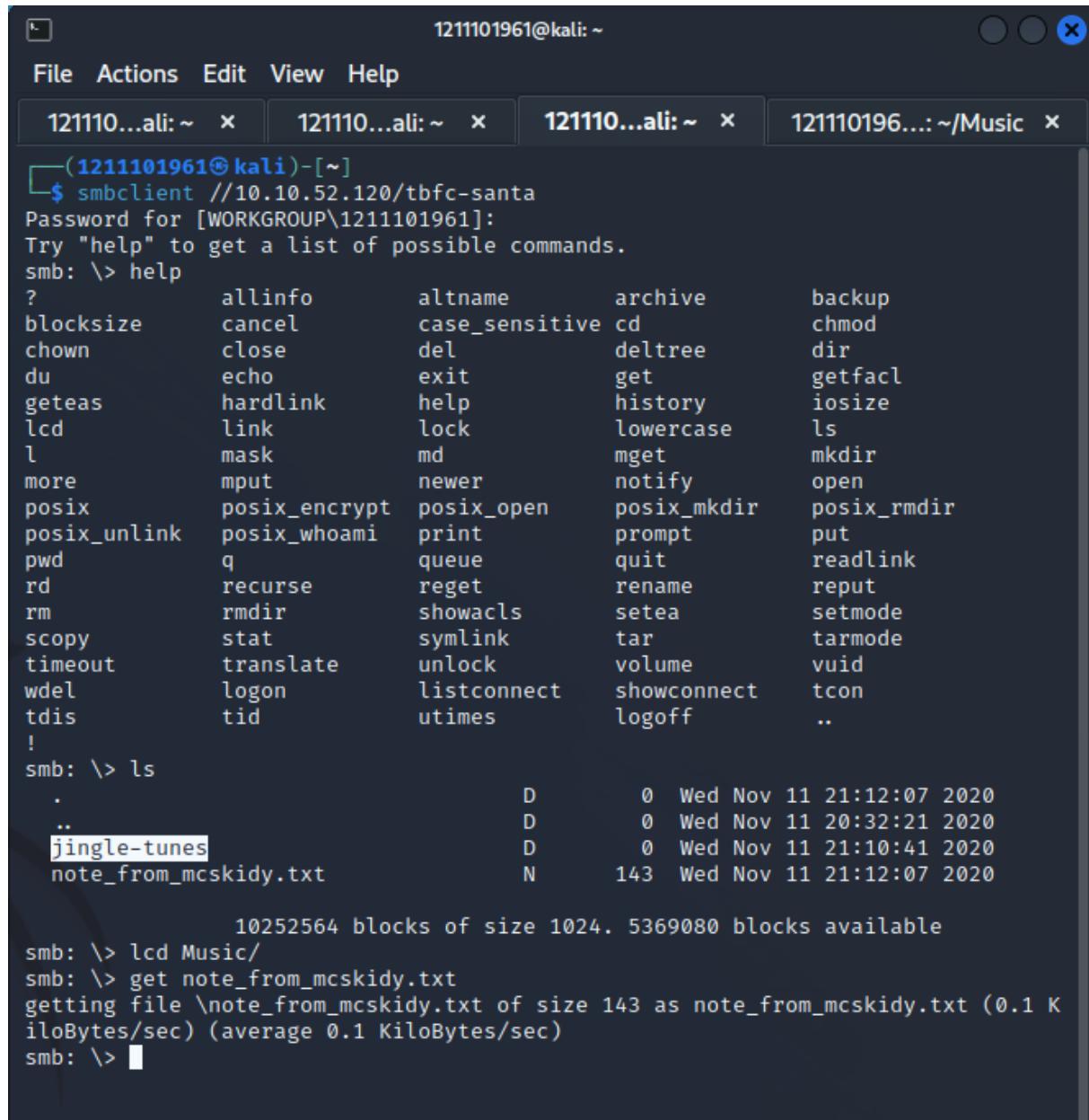
10252564 blocks of size 1024. 5369080 blocks available
smb: \> lcd Music/
smb: \> get note_from_mcskidy.txt
getting file \note_from_mcskidy.txt of size 143 as note_from_mcskidy.txt (0.1 K
iloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \> [
```

Enter “ls” to get the filelist. Enter “lcd (filename)” to create a file and key in “get note_from_mcskidy.txt”.



```
1211101961@kali: ~/Music
File Actions Edit View Help
1211101961@kali: ~ x 1211101961@kali: ~ x 1211101961@kali: ~ x 1211101961@kali: ~/Music x
└─(1211101961㉿kali)-[~]
$ cd Music/
└─(1211101961㉿kali)-[~/Music]
$ ls
note_from_mcskidy.txt
└─(1211101961㉿kali)-[~/Music]
$ cat note_from_mcskidy.txt
Hi Santa, I decided to put all of your favourite jingles onto this share - allowing you access it from anywhere you like! Regards ~ ElfMcSkidy
└─(1211101961㉿kali)-[~/Music]
$ █
```

Key in “cd (filename)” and press enter. After that, key in “ls” to check the file. Finally, enter “cat note_from_mcskidy.txt” and it shows ElfMcSkidy leaving something to Santa which is jingles.



1211101961@kali: ~

File Actions Edit View Help

121110...ali: ~ x 121110...ali: ~ x 121110...ali: ~ x 121110196...: ~/Music x

```
└─(1211101961㉿kali)-[~]
$ smbclient //10.10.52.120/tbfc-santa
Password for [WORKGROUP\1211101961]:
Try "help" to get a list of possible commands.
smb: \> help
?
blocksize      allinfo      altname      archive      backup
chown         cancel       case_sensitive cd          chmod
du            close        del          deltree      dir
getreas       hardlink    help          history      getfacl
lcd            link         lock         lowercase   ls
l              mask        md           mget        mkdir
more          mput        newer        notify      open
posix         posix_encrypt posix_open   posix_mkdir posix_rmdir
posix_unlink  posix_whoami  print       prompt      put
pwd            q           queue      quit        readlink
rd              recurse    reget       rename     reput
rm              rmdir      showacls   setea      setmode
scopy         stat        symlink    tar        tarmode
timeout       translate  unlock     volume     vuid
wdel          logon      listconnect showconnect tcon
tdis          tid        utimes    logoff     ..
!
smb: \> ls
.
..
jingle-tunes
note_from_mcskidy.txt
```

.		D	0	Wed Nov 11	21:12:07	2020		
..		D	0	Wed Nov 11	20:32:21	2020		
jingle-tunes		D	0	Wed Nov 11	21:10:41	2020		
note_from_mcskidy.txt		N	143	Wed Nov 11	21:12:07	2020		

10252564 blocks of size 1024. 5369080 blocks available

```
smb: \> lcd Music/
smb: \> get note_from_mcskidy.txt
getting file \note_from_mcskidy.txt of size 143 as note_from_mcskidy.txt (0.1 K
iloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \> █
```

Question 5: Log in to this share, what directory did ElfMcSkidy leave for Santa?

Answer: jingle-tunes

Thought Process/Methodology:

Enter “enum4linux -h” to get the flags with descriptions in the terminal. Enter “enum4linux -U IP Address(10.10.52.120)” to get the number of users. Enter “enum4linux -S IP Address(10.10.52.120)” to get the sharelist. Enter “smbclient //IP Address(10.10.52.120)/sharename(tbfc-santa)” and press enter. After that, simply type in the password. Enter “ls” to get the filelist. Enter “lcd (filename)” to create a file and key in “get note_from_mcskidy.txt”. Key in “cd (filename)” and press enter. After that, key in “ls” to check the file. Finally, enter “cat note_from_mcskidy.txt” and it shows ElfMcSkidy leaving something to Santa which is jingles.