PSP0201 Week 3 Writeup

Group Name: **No Entry**

Members:

ID	**Name**	**Role**
1211102976	Lee Le Xuan	Leader
1211103182	Ester Ong Xiang Lin	Member
1211102020	Jackter Un Chia Te	Member
1211102575	Pang Ding Yuan	Member

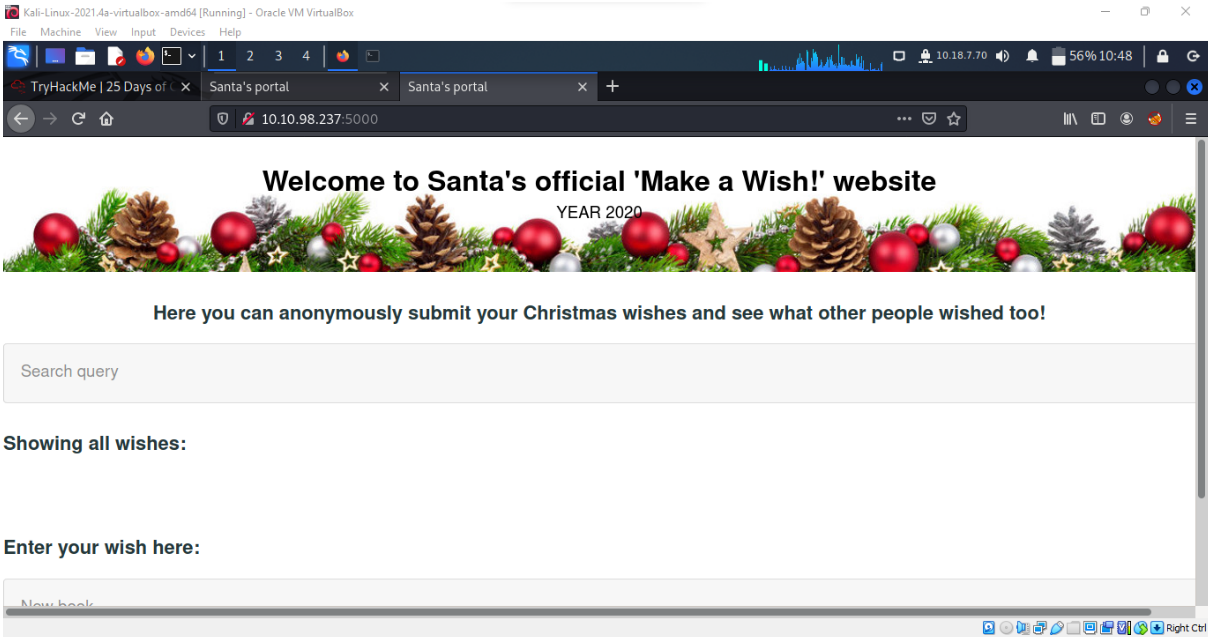
Day 6: [Exploitation] Be careful with what you wish on a Christmas Night

Tools used: Kali Linux, Firefox, OWASP ZAP

Walkthrough:

Step 1

We paste the given IP address in the browser. A page as below is shown.


Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.18.7.70
56% 10:48
TryHackMe | 25 Days of C
Santa's portal
Santa's portal
10.10.98.237:5000
Right Ctrl

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

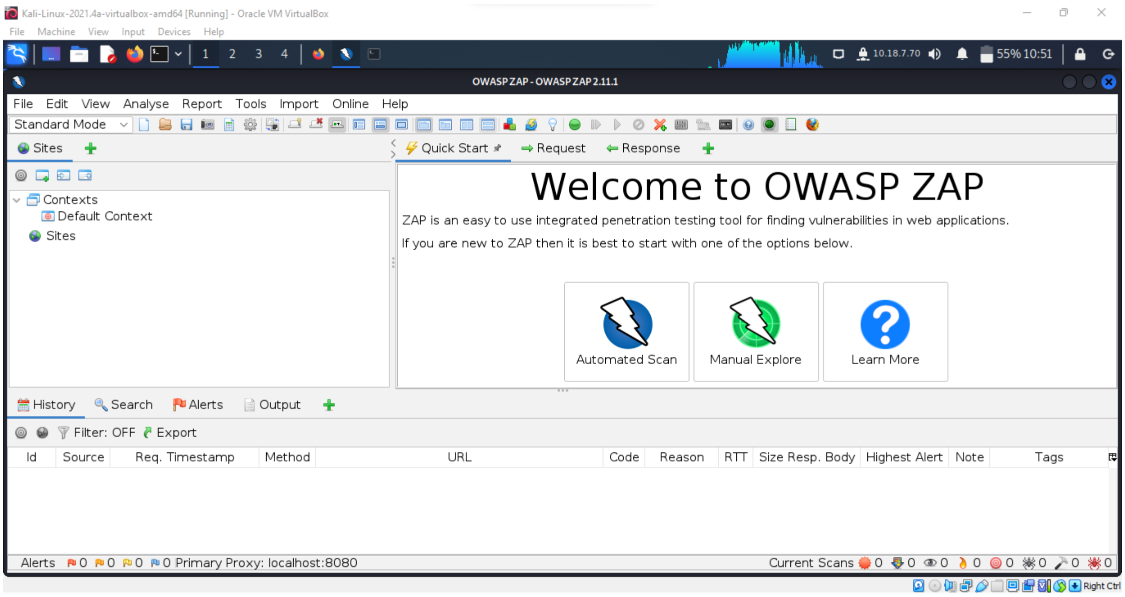
Showing all wishes:

Enter your wish here:

New book

Step 2

To detect vulnerabilities, we open OWASP ZAP in Kali Linux machine. We choose to use automated scan.


Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.18.7.70
55% 10:51
OWASP ZAP - OWASP ZAP 2.11.1
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
Automated Scan
Manual Explore
Learn More
History
Search
Alerts
Output
Filter: OFF
Export
Id Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
Alerts 0 0 0 0 Primary Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0
Right Ctrl

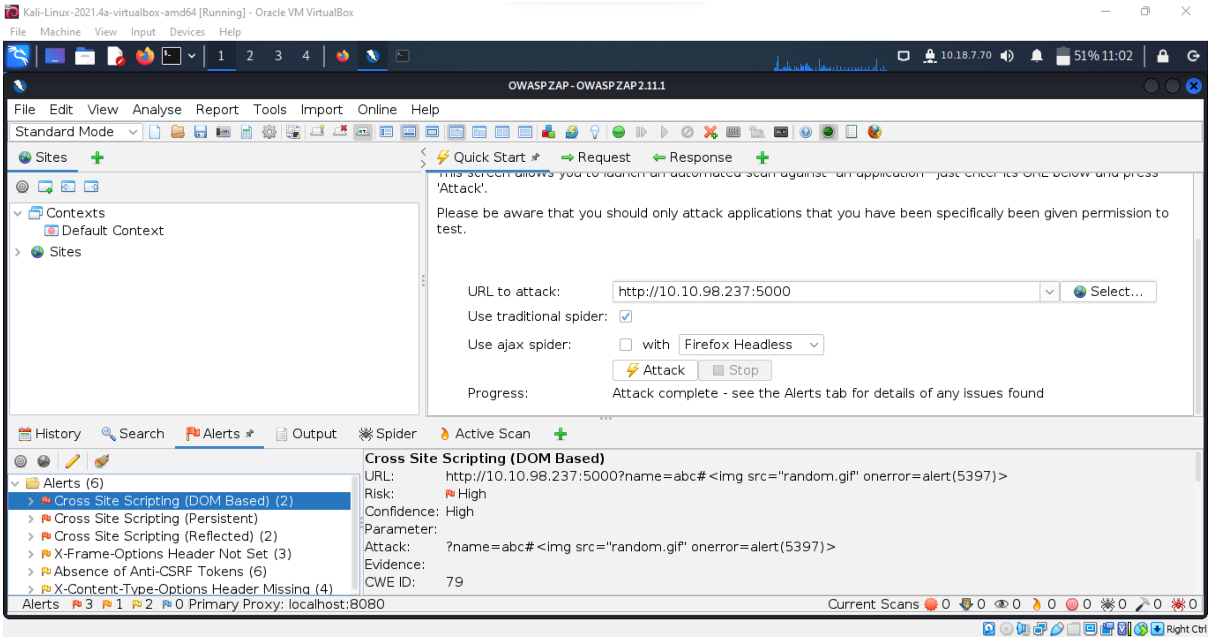
Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

Step 3

After pasting the given URL of our webpage, we start the attack. After done scanning, we saw a XSS (DOM Based) vulnerability with a malicious URL. We copy the URL.


Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
OWASP ZAP - OWASP ZAP 2.11.1
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
History Search Alerts Output Spider Active Scan
Select...
Attack
Stop
Right Ctrl

'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://10.10.98.237:5000

Use traditional spider: ☑

Use ajax spider: ☐ with Firefox Headless

Progress: Attack complete - see the Alerts tab for details of any issues found

```
Alerts (6)
  > Cross Site Scripting (DOM Based) (2)
  > Cross Site Scripting (Persistent)
  > Cross Site Scripting (Reflected) (2)
  > X-Frame-Options Header Not Set (3)
  > Absence of Anti-CSRF Tokens (6)
  > X-Content-Type-Options Header Missing (4)
```

```
Cross Site Scripting (DOM Based)
URL:        http://10.10.98.237:5000?name=abc#<img src="random.gif" onerror=alert(5397)>
Risk:       High
Confidence: High
Parameter:
Attack:     ?name=abc#<img src="random.gif" onerror=alert(5397)>
Evidence:
CWE ID:     79
```

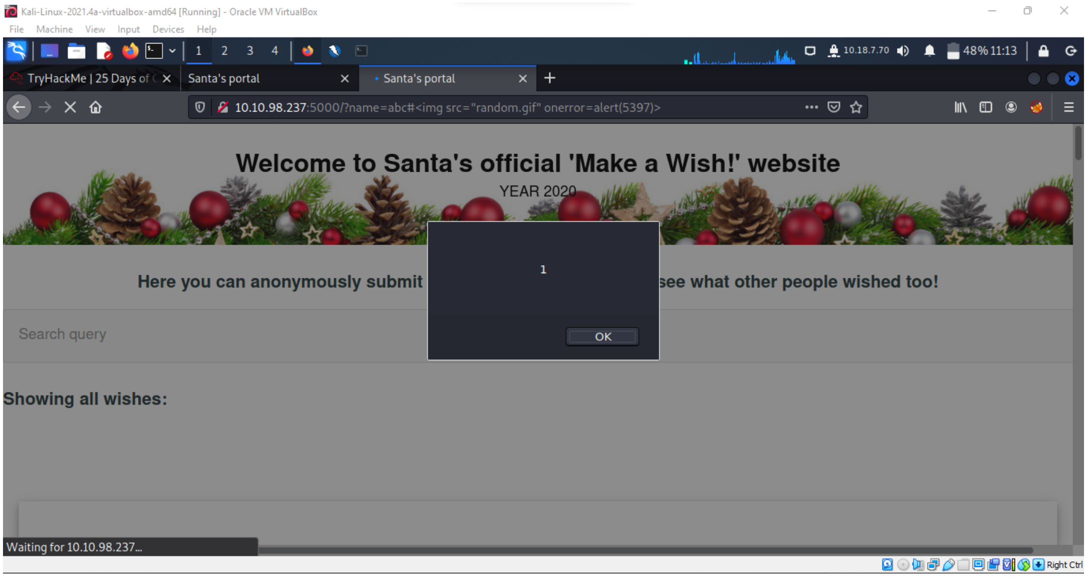
Alerts 3 1 2 0 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

Step 4

We then paste the URL in the Firefox browser. Then, several pop-ups will appear. The list of the wishes will also show some weird entries. This means that we have successfully done the attack.

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

Answer: Stored


Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
TryHackMe | 25 Days of C
Santa's portal
Santa's portal
OK
Right Ctrl

10.10.98.237:5000/?name=abc#<img src="random.gif" onerror=alert(5397)>

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

YEAR 2020

Here you can anonymously submit

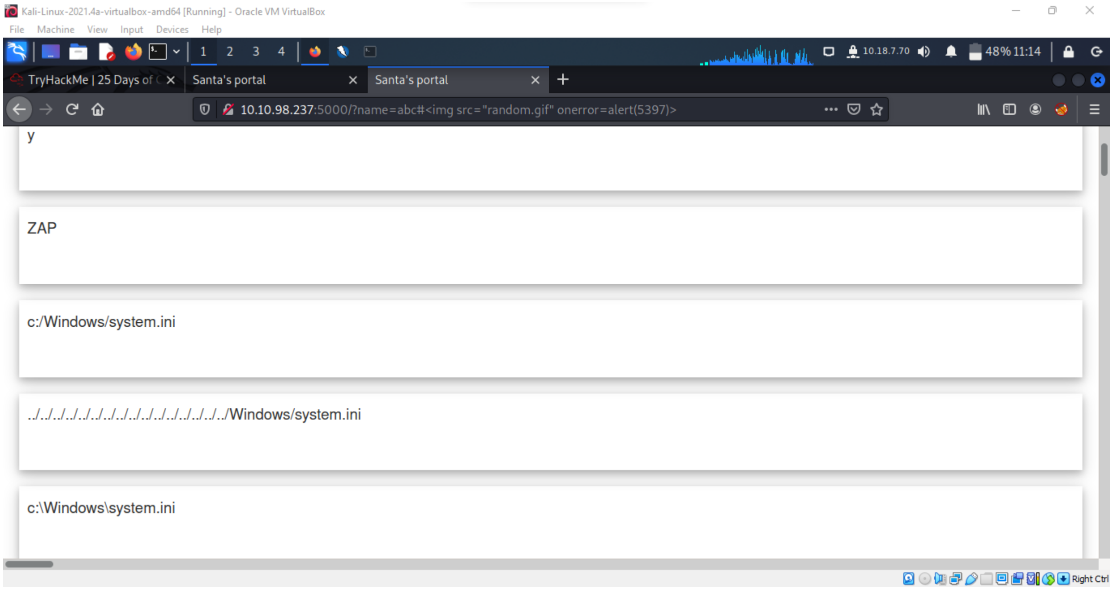
see what other people wished too!

Search query

1

Showing all wishes:

Waiting for 10.10.98.237...



Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.18.7.70
48% 11:14
TryHackMe | 25 Days of C
Santa's portal
Santa's portal
Right Ctrl

10.10.98.237:5000/?name=abc#<img src="random.gif" onerror=alert(5397)>

y

ZAP

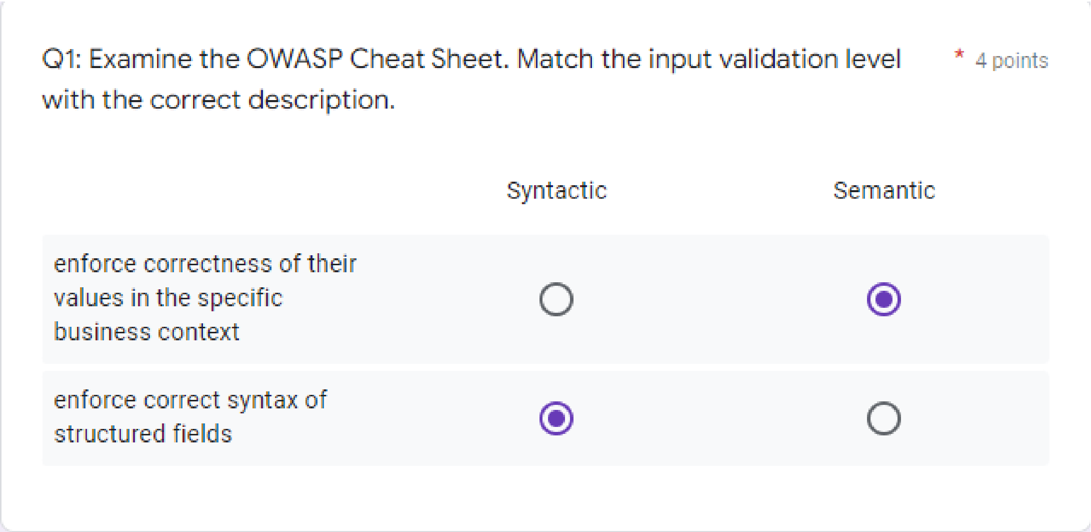
c:/Windows/system.ini

../../../../../../../../../../../../../../../../Windows/system.ini

c:\Windows\system.ini

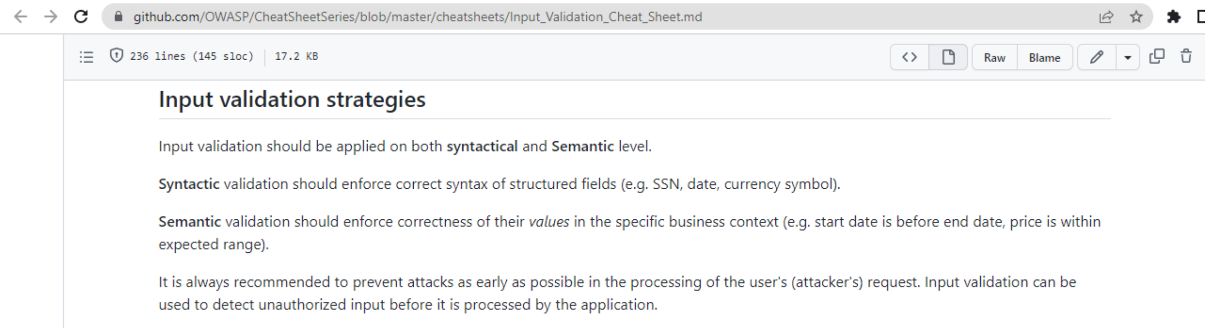
Solution:

Question 1



Q1: Examine the OWASP Cheat Sheet. Match the input validation level with the correct description. * 4 points

	Syntactic	Semantic
enforce correctness of their values in the specific business context	○	●
enforce correct syntax of structured fields	●	○



github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Input_Validation_Cheat_Sheet.md
236 lines (145 sloc) | 17.2 KB
Raw
Blame

Input validation strategies

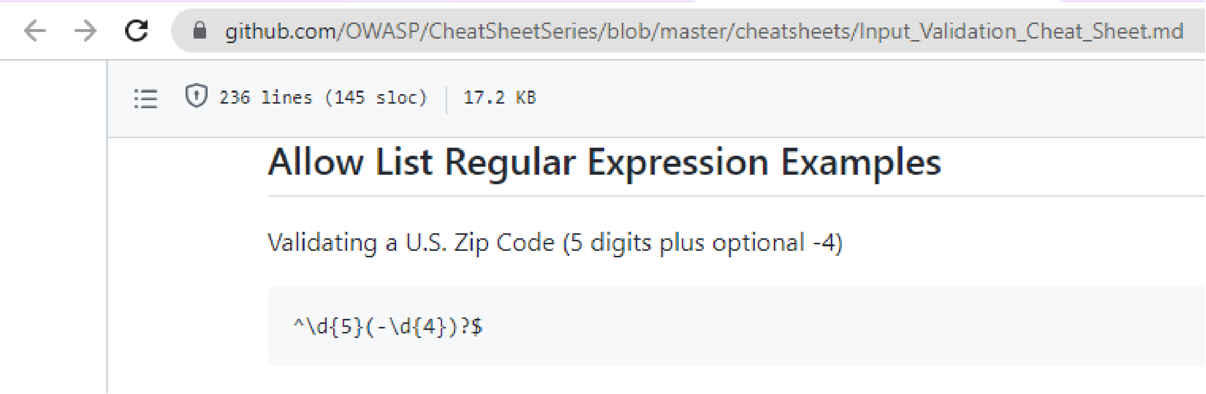
Input validation should be applied on both **syntactical** and **Semantic** level.

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.

Question 2: Examine the OWASP Cheat Sheet. What is the regular expression used to validate a US Zip code?
Answer: ^\d{5}(-\d{4})?$



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

236 lines (145 sloc) | 17.2 KB

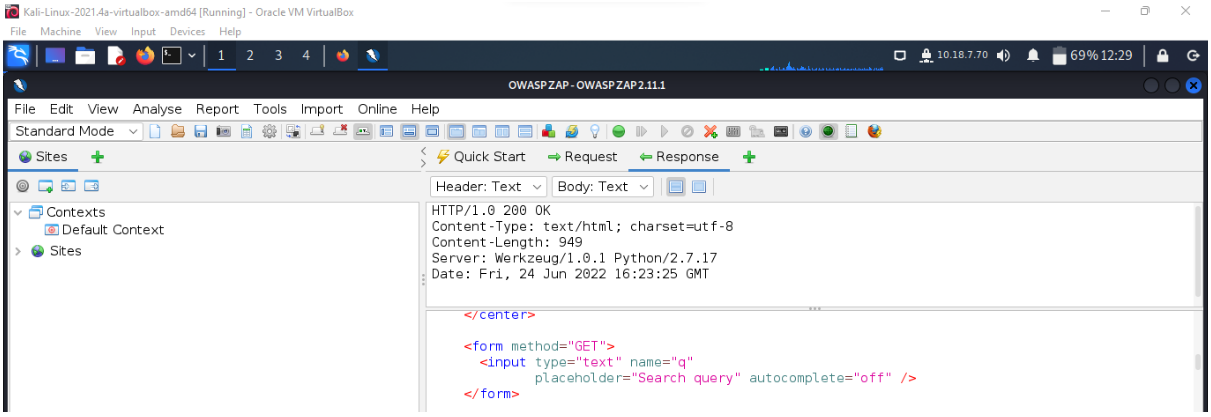
Allow List Regular Expression Examples

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

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

Question 3 has been answered in the above walkthrough.

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



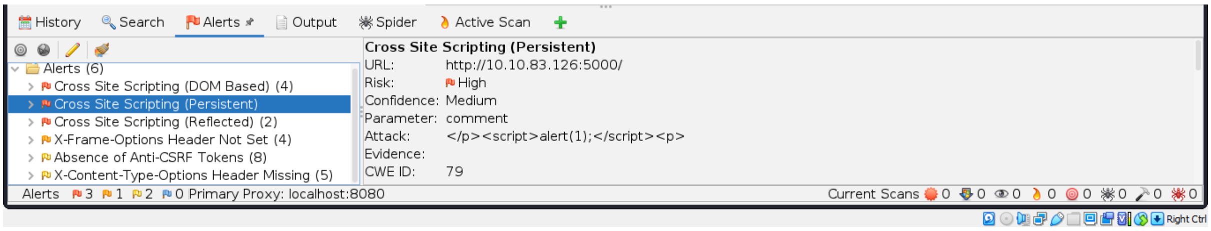
Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
OWASP ZAP - OWASP ZAP 2.11.1
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Text
Contexts
Default Context
Sites

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 949
Server: Werkzeug/1.0.1 Python/2.7.17
Date: Fri, 24 Jun 2022 16:23:25 GMT
```

```
    </center>

    <form method="GET">
      <input type="text" name="q"
             placeholder="Search query" autocomplete="off" />
    </form>
```

Question 5: Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts of high priority are in the scan?
Answer: 2

Question 6: 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>



Alerts (6)
- Cross Site Scripting (DOM Based) (4)
- Cross Site Scripting (Persistent)
- Cross Site Scripting (Reflected) (2)
- X-Frame-Options Header Not Set (4)
- Absence of Anti-CSRF Tokens (8)
- X-Content-Type-Options Header Missing (5)

Cross Site Scripting (Persistent)
URL: http://10.10.83.126:5000/
Risk: High
Confidence: Medium
Parameter: comment
Attack: </p><script>alert(1);</script><p>
Evidence:
CWE ID: 79

Alerts 3 1 2 0 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

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

Thought Process/Methodology:
Firstly, we pasted the given IP address in the browser. A website to make wishes was shown. As we were asked to figure out the way that the attacker attacked the website, we decided to scan for vulnerabilities of the website using OWASP ZAP first. We chose to use automated scan. Then, we pasted the website's IP address in the column given and clicked the attack button. We waited for a few minutes for the result. In the result, we saw a XSS (DOM Based) vulnerability. A malicious URL was there and we copied the URL as we planned to perform a stored XSS attack. To attack the website, we pasted the malicious URL in the browser. When we ran the URL, several pop-ups appeared. The list of the wishes also showed some weird entries. We had successfully done our attack.

Day 7 - [Networking] The Grinch Really Did Steal Christmas

Tools used: Kali linux, Wireshark, Terminal, Mousepad

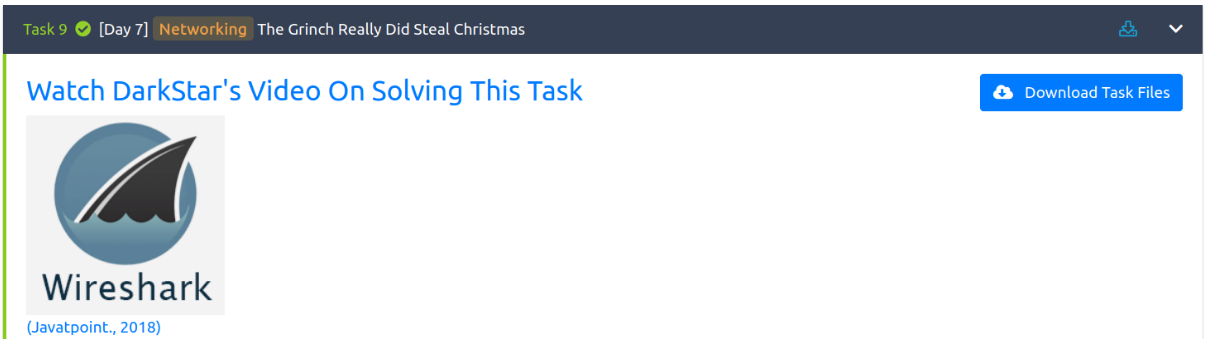
Walkthrough and Question :

Step 1

Starting by downloading the pcap files provided in THM.

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

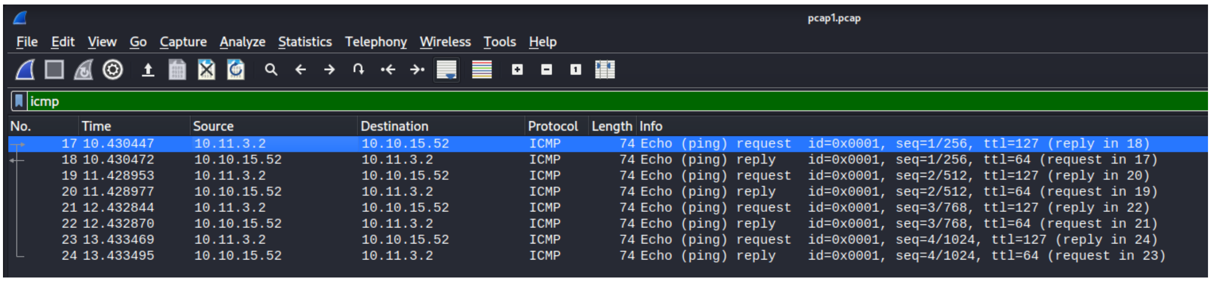
Answer: 10.11.3.2



Task 9 ✓ [Day 7] Networking The Grinch Really Did Steal Christmas

Watch DarkStar's Video On Solving This Task

(Javatpoint., 2018)



pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

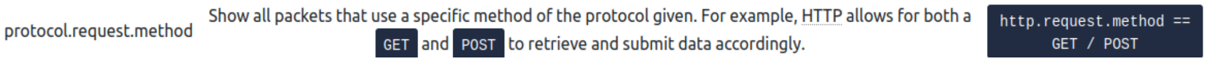
```
No.   Time        Source        Destination   Protocol Length Info
   17 10.430447   10.11.3.2     10.10.15.52   ICMP       74 Echo (ping) request  id=0x0001, seq=1/256, ttl=127 (reply in 18)
   18 10.430472   10.10.15.52   10.11.3.2     ICMP       74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=64 (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)
```

Step 2

After opening it, we can find the source of the request.

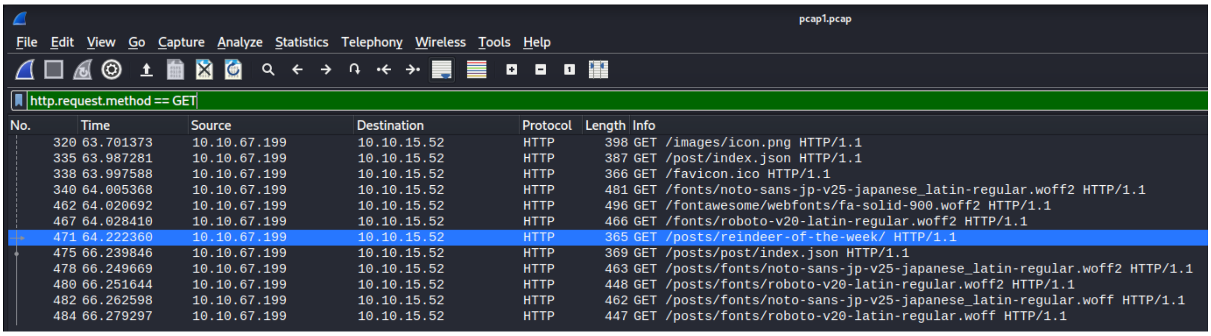
Question 2 :If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

Answer: http.request.method == GET



protocol.request.method	Show all packets that use a specific method of the protocol given. For example, HTTP allows for both a `GET` and `POST` to retrieve and submit data accordingly.	`http.request.method == GET / POST`

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.


pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

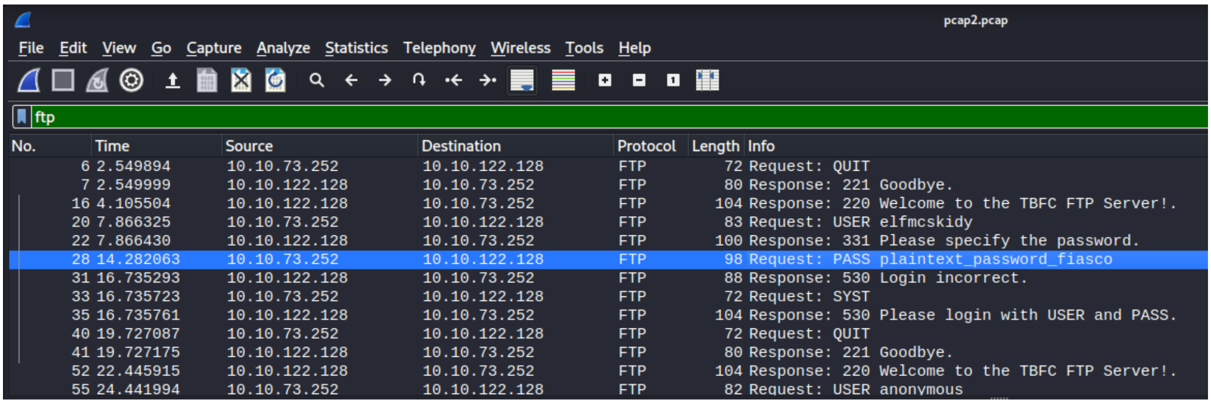
http.request.method == GET

```
No.   Time      Source        Destination  Protocol Length Info
  320 63.701373 10.10.67.199  10.10.15.52  HTTP     398 GET /images/icon.png 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
  462 64.020692 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
```

Step 3

We find the source of the ip address entering the password.

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


pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

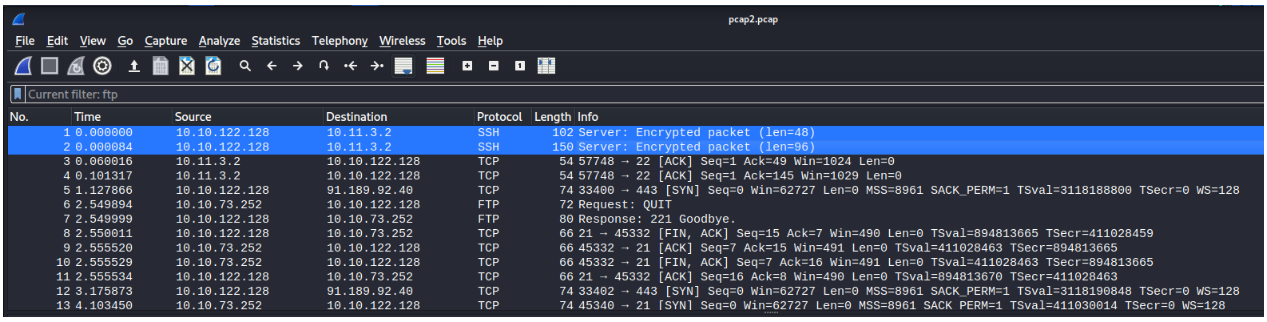
ftp

```
No.   Time      Source         Destination    Protocol Length Info
    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.
   16 4.105504  10.10.122.128  10.10.73.252   FTP      104 Response: 220 Welcome to the TBFC FTP Server!.
   20 7.866325  10.10.73.252   10.10.122.128  FTP       83 Request: USER elfmcskidy
   22 7.866430  10.10.122.128  10.10.73.252   FTP      100 Response: 331 Please specify the password.
   28 14.282063 10.10.73.252   10.10.122.128  FTP       98 Request: PASS plaintext_password_fiasco
   31 16.735293 10.10.122.128  10.10.73.252   FTP       88 Response: 530 Login incorrect.
   33 16.735723 10.10.73.252   10.10.122.128  FTP       72 Request: SYST
   35 16.735761 10.10.122.128  10.10.73.252   FTP      104 Response: 530 Please login with USER and PASS.
   40 19.727087 10.10.73.252   10.10.122.128  FTP       72 Request: QUIT
   41 19.727175 10.10.122.128  10.10.73.252   FTP       80 Response: 221 Goodbye.
   52 22.445915 10.10.122.128  10.10.73.252   FTP      104 Response: 220 Welcome to the TBFC FTP Server!.
   55 24.441994 10.10.73.252   10.10.122.128  FTP       82 Request: USER anonymous
```

Step 4

We look for the protocol that has encrypted packets.

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


pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: ftp

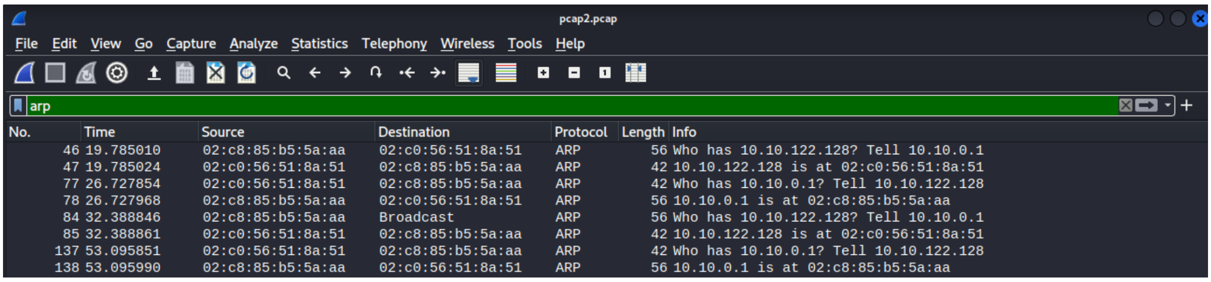
```
No.     Time       Source           Destination      Protocol  Length Info
      1 0.000000   10.10.122.128    10.11.3.2        SSH        102 Server: Encrypted packet (len=48)
      2 0.000084   10.10.122.128    10.11.3.2        SSH        150 Server: Encrypted packet (len=96)
      3 0.060016   10.11.3.2        10.10.122.128    TCP         54 57748 → 22 [ACK] Seq=1 Ack=49 Win=1024 Len=0
      4 0.101317   10.11.3.2        10.10.122.128    TCP         54 57748 → 22 [ACK] Seq=1 Ack=145 Win=1029 Len=0
      5 1.127866   10.10.122.128    91.189.92.40     TCP         74 33400 → 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 2.550011   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 2.555520   10.10.73.252     10.10.122.128    TCP         66 45332 → 21 [ACK] Seq=7 Ack=15 Win=491 Len=0 TSval=411028463 TSecr=894813665
     10 2.555529   10.10.73.252     10.10.122.128    TCP         66 45332 → 21 [FIN, ACK] Seq=7 Ack=16 Win=491 Len=0 TSval=411028463 TSecr=894813665
     11 2.555534   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    91.189.92.40     TCP         74 33402 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118190848 TSecr=0 WS=128
     13 4.103450   10.10.73.252     10.10.122.128    TCP         74 45340 → 21 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=411030014 TSecr=0 WS=128
```

Step 5

Examine the ARP communications.

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


pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

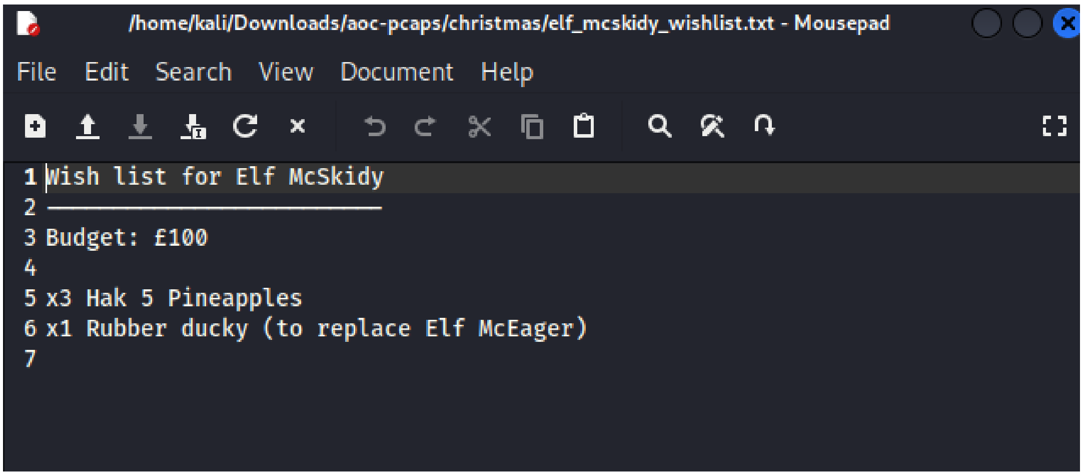
```
No.     Time        Source              Destination         Protocol  Length Info
     46 19.785010   02:c8:85:b5:5a:aa   02:c0:56:51:8a:51   ARP        56 Who has 10.10.122.128? Tell 10.10.0.1
     47 19.785024   02:c0:56:51:8a:51   02:c8:85:b5:5a:aa   ARP        42 10.10.122.128 is at 02:c0:56:51:8a:51
     77 26.727854   02:c0:56:51:8a:51   02:c8:85:b5:5a:aa   ARP        42 Who has 10.10.0.1? Tell 10.10.122.128
     78 26.727968   02:c8:85:b5:5a:aa   02:c0:56:51:8a:51   ARP        56 10.10.0.1 is at 02:c8:85:b5:5a:aa
     84 32.388846   02:c8:85:b5:5a:aa   Broadcast           ARP        56 Who has 10.10.122.128? Tell 10.10.0.1
     85 32.388861   02:c0:56:51:8a:51   02:c8:85:b5:5a:aa   ARP        42 10.10.122.128 is at 02:c0:56:51:8a:51
    137 53.095851   02:c0:56:51:8a:51   02:c8:85:b5:5a:aa   ARP        42 Who has 10.10.0.1? Tell 10.10.122.128
    138 53.095990   02:c8:85:b5:5a:aa   02:c0:56:51:8a:51   ARP        56 10.10.0.1 is at 02:c8:85:b5:5a:aa
```

Step 6

Open “pcap3.pcap” file.

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


/home/kali/Downloads/aoc-pcaps/christmas/elf_mcskidy_wishlist.txt - Mousepad
File Edit Search View Document Help

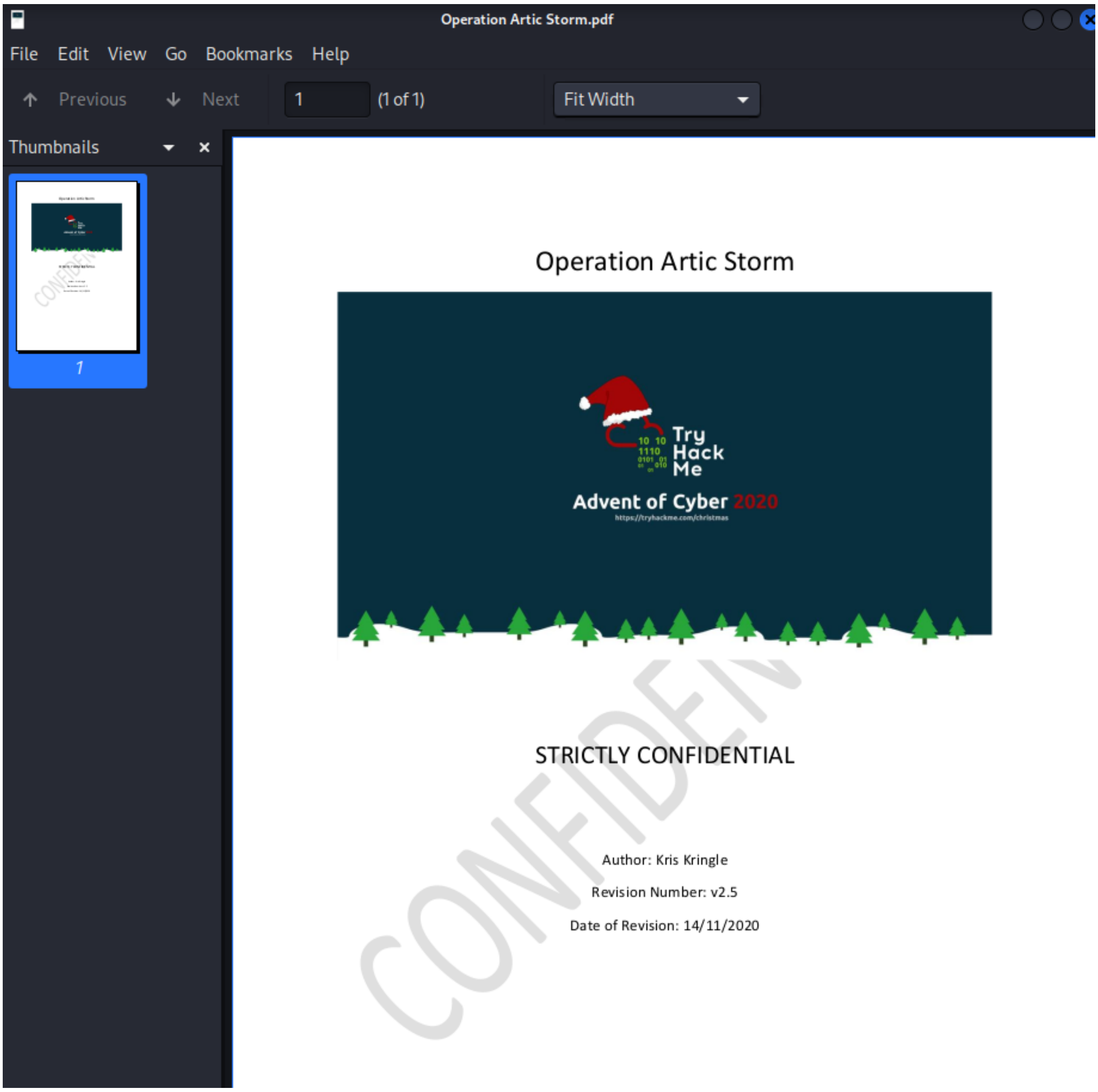
```
Wish list for Elf McSkidy
-------------------------
Budget: £100

x3 Hak 5 Pineapples
x1 Rubber ducky (to replace Elf McEager)

```

Step 7

Look for the text file from the zip downloaded and find the pdf file in the zip and look for the author.

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

Answer: Kris Kringle



Operation Artic Storm

STRICTLY CONFIDENTIAL

Author: Kris Kringle

Revision Number: v2.5

Date of Revision: 14/11/2020

Thought Process/Methodology:

Open wireshark after the task file is downloaded. First and foremost, open pcap1.pcap and filter ICMP to see what is the IP address that initiates an ICMP/ping which is the requesting IP address. After that, filter with http.request.method == GET to find the article visited by the given IP address. Other than that, we also open pcap2.pcap and apply ftp filter to find what password was used to login. We also look for the protocol that has encrypted packets. Later, we examine the ARP communications. Lastly, we open pcap3.pcap and download the christmas.zip file to check for what is used to replace Elf McEager and who is the author of Operation Artic Storm.

Day 8 - [Networking] What's Under the Christmas Tree?

Tools used: Kali Linux, Firefox, Nmap, Terminal

Walkthrough:

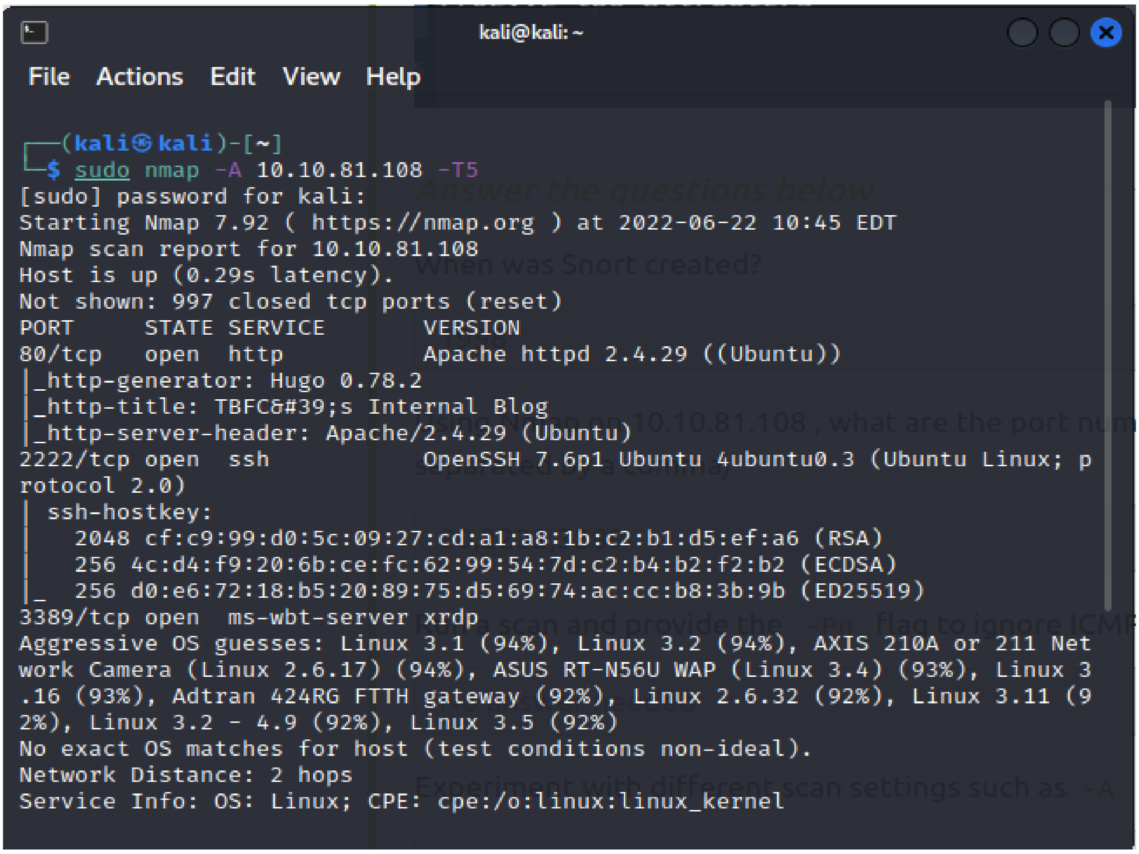
Step 1
Open terminal and type nmap with IP address command. We will then see the information as below.

Question 2: Using Nmap on MACHINE_IP , what are the port numbers of the three services running?
Answer: 80,2222,3389

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

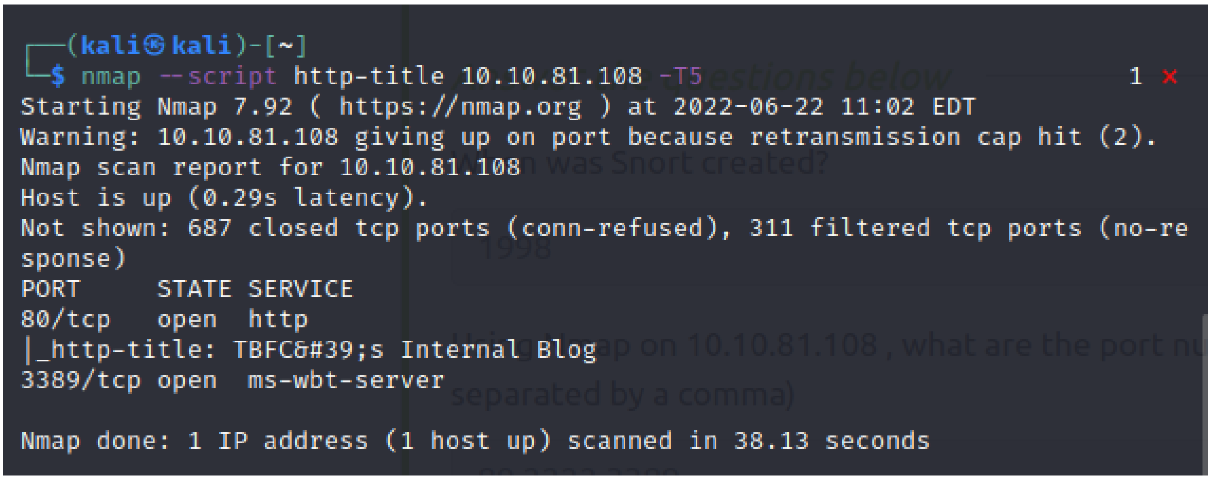
Question 5: What is running on port 2222?
Answer: SSH



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 10.10.81.108 -T5
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 10:45 EDT
Nmap scan report for 10.10.81.108
Host is up (0.29s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-title: TBFC&#39;s Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; p
rotocol 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
Aggressive OS guesses: Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Net
work Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3
.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 3.11 (9
2%), Linux 3.2 - 4.9 (92%), Linux 3.5 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Step 2:
Type nmap script command.

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



```
┌──(kali㉿kali)-[~]
└─$ nmap --script http-title 10.10.81.108 -T5                                1 ✕
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 11:02 EDT
Warning: 10.10.81.108 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.81.108
Host is up (0.29s latency).
Not shown: 687 closed tcp ports (conn-refused), 311 filtered tcp ports (no-re
sponse)
PORT     STATE SERVICE
80/tcp   open  http
|_http-title: TBFC&#39;s Internal Blog
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 38.13 seconds
```

Solution:

Question 1: When was Snort created?
Answer: 1998

Question 2,3,4,5,6 have been answered above.

Thought Process/Methodology:
Firstly, we typed the nmap open all command together with our own IP address in terminal. Then we can see some information and figure out what are the port numbers, name of the Linux distribution that is running and the version of Apache. Next, we use nmap script command to check what is the website be used for.

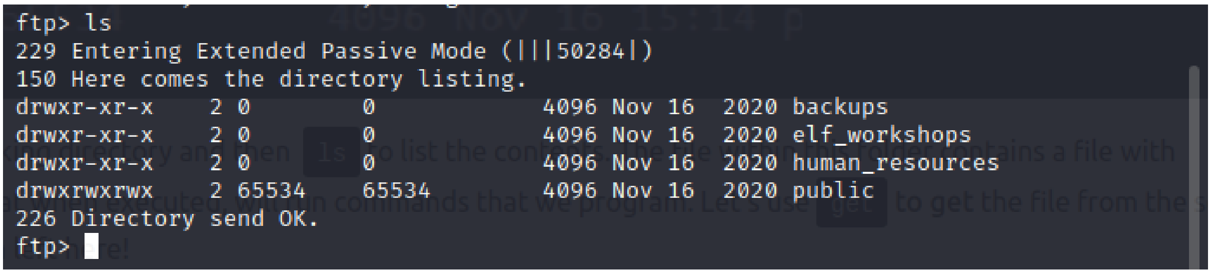
Day 9 - [Networking] Anyone can be Santa!

Tools used: Kali Linux, FTP, Terminal

Step 1

Enter the File Transfer Protocol (FTP) server of the given IP Address as anonymous and list the directories in it.

Question 1: What are the directories you found on the FTP site?
Answer: backups, elf_workshops, human_resources and public



```
ftp> ls
229 Entering Extended Passive Mode (|||50284|)
150 Here comes the directory listing.
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> 
```

Step 2

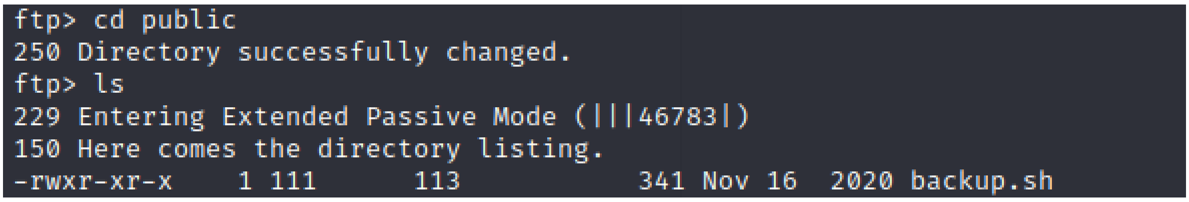
Only the directory - ‘public’ has data in it.

Question 2: Name the directory on the FTP server that has data accessible by the "anonymous" user.
Answer: public

Step 3

backup.sh is found in the directory.

Question 3: What script gets executed within this directory?
Answer: backup.sh

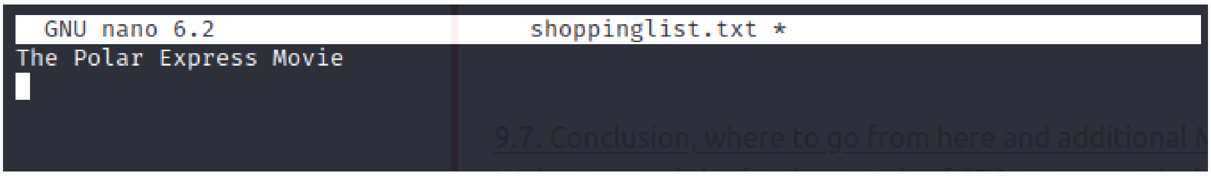


```
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||46783|)
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
```

Step 4

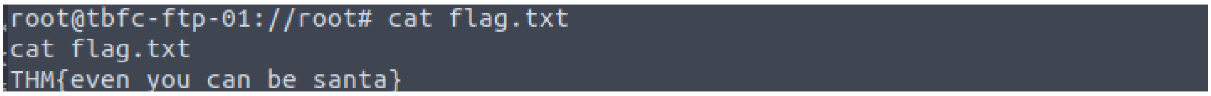
Get the shoppinglist.txt in the public directory and The Polar Express is in it. Find the flag.

Question 4: What movie did Santa have on his Christmas shopping list?
Answer: The Polar Express



```
  GNU nano 6.2                          shoppinglist.txt *
The Polar Express Movie
```

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



```
root@tbfc-ftp-01://root# cat flag.txt
cat flag.txt
THM{even_you_can_be_santa}
```

Thought Process/Methodology:

Enter the File Transfer Protocol (FTP) server of the given IP address with the terminal and login as anonymous. After logging in, we list the directories. Then, we check for the directory that has data accessible by the "anonymous" user. We are able to see the scripting language commands file that will be run to backup the server. We download the file and replace the command in the script to our own reverse shell script. After setting up a listener to catch the connection ,we upload the modified scripting language commands file. With the reverse shell, we now take over the server. We can now find the flag in the server's directory.

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

Tools used: Kali Linux, enum4linux, smbclient, Terminal

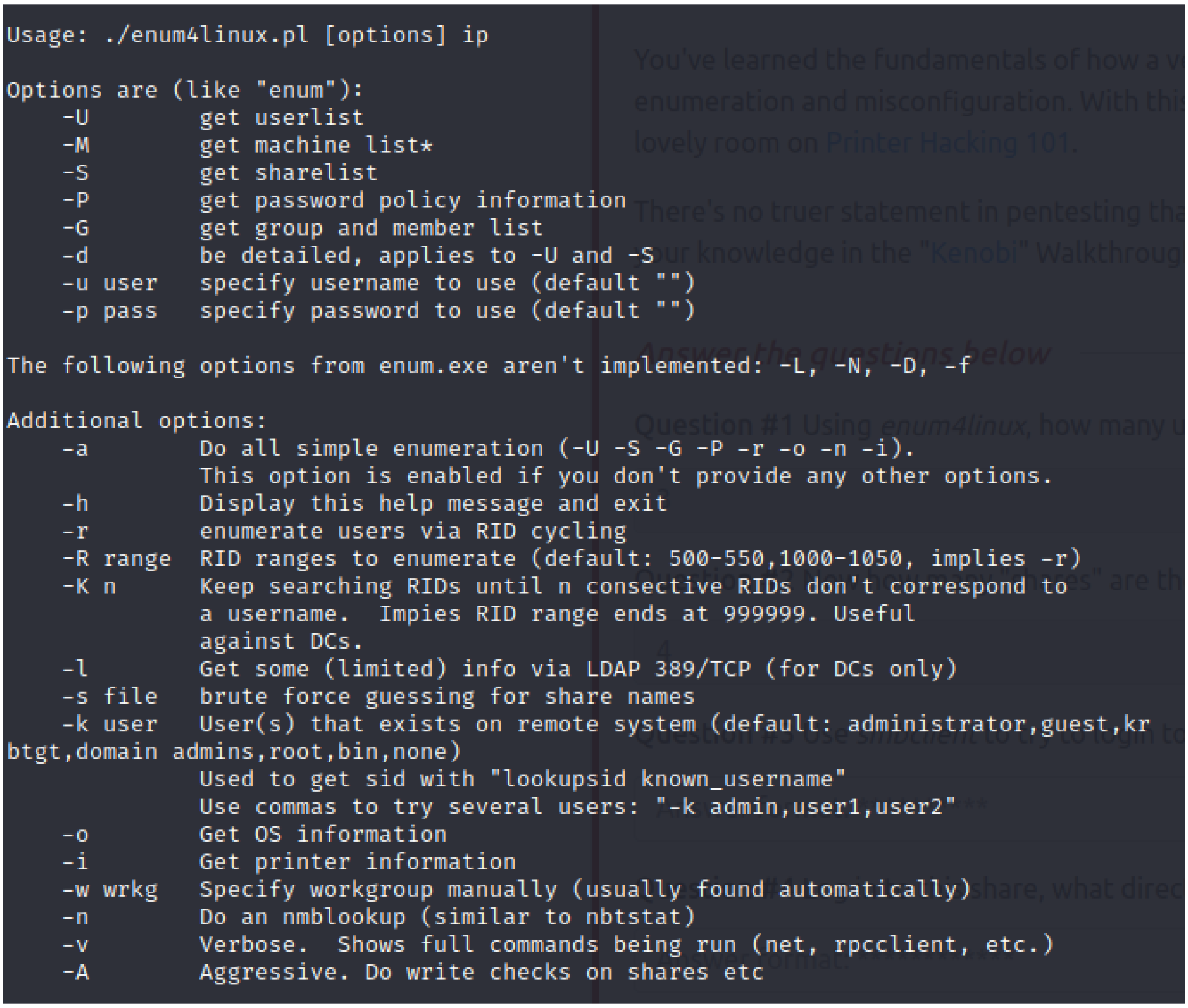
Walkthrough and Question:

Step 1

Examine the help options for enum4linux.

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

Answer: -h Display help message -a Do all simple enumeration
-S Get share list -o Get OS information

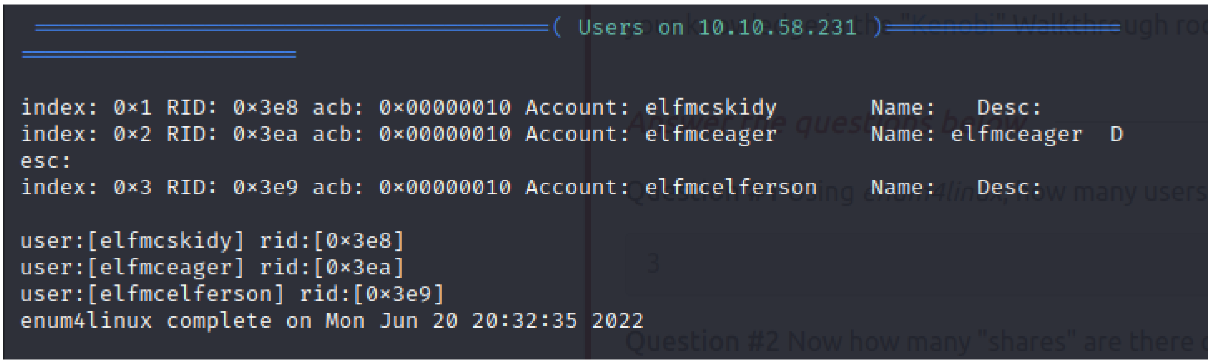


```
Usage: ./enum4linux.pl [options] ip

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 consective 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,kr
btgt,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
```

Step 2

Use command ./enum4linux.pl -U MACHINE_IP to check for the number of users on the server.

Question 2: Using enum4linux, how many users are there on the Samba server?
Answer: 3

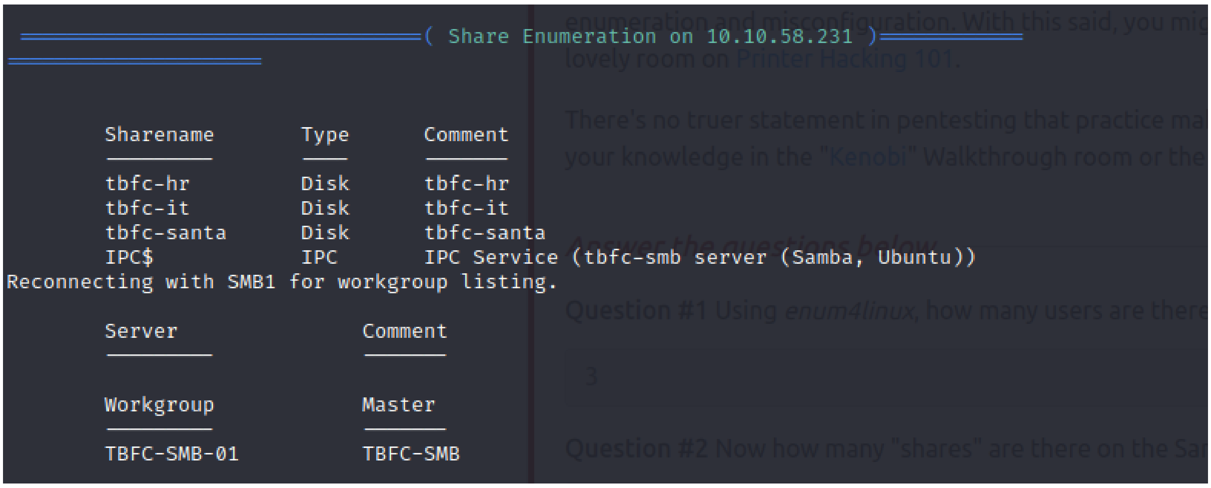


```
 ================================( Users on 10.10.58.231 )================
 ================

index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: elfmcskidy       Name:   Desc:
index: 0×2 RID: 0×3ea acb: 0×00000010 Account: elfmceager       Name: elfmceager  D
esc:
index: 0×3 RID: 0×3e9 acb: 0×00000010 Account: elfmcelferson    Name:   Desc:

user:[elfmcskidy] rid:[0×3e8]
user:[elfmceager] rid:[0×3ea]
user:[elfmcelferson] rid:[0×3e9]
enum4linux complete on Mon Jun 20 20:32:35 2022
```

Step 3

Use command ./enum4linux.pl -S MACHINE_IP to check for the number of shares on the server.

Question 3: Now how many "shares" are there on the Samba server?
Answer: 4



```
 ===========================( Share Enumeration on 10.10.58.231 )=========
 =================


        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
```

Step 4

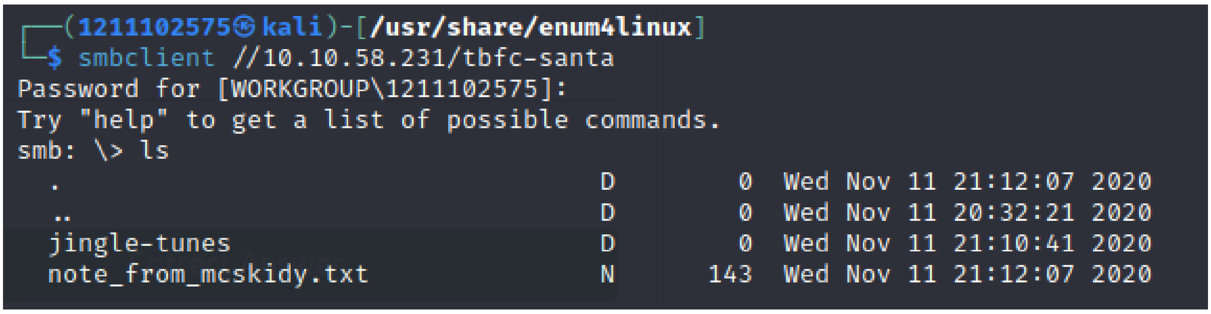
Login in to each share found on the server and find which share can be login successfully without password.

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

Step 5

We can find two directories in the tbfc-santa share.

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



```
┌──(1211102575㉿kali)-[/usr/share/enum4linux]
└─$ smbclient //10.10.58.231/tbfc-santa
Password for [WORKGROUP\1211102575]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   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
```

Thought Process/Methodology:

After navigating to enum4linux, we use enum4linux to check for the users and shares on the given server. Then, we find the share that we can access without a password. Next, we list the directory in the share and download and read through the note_from_mcskidy.txt. Lastly,we find the directory ElfMcSkidy leaves for Santa.