

# PSP0201

## Week 3

# Writeup

Group Name: SupremeChickens

Members

ID	Name	Role
1211103024	Yap Jack	Leader
1211102425	Ang Hui Yee	Member
1211101198	Fam YI Qi	Member
1211103978	Dlckshen	Member

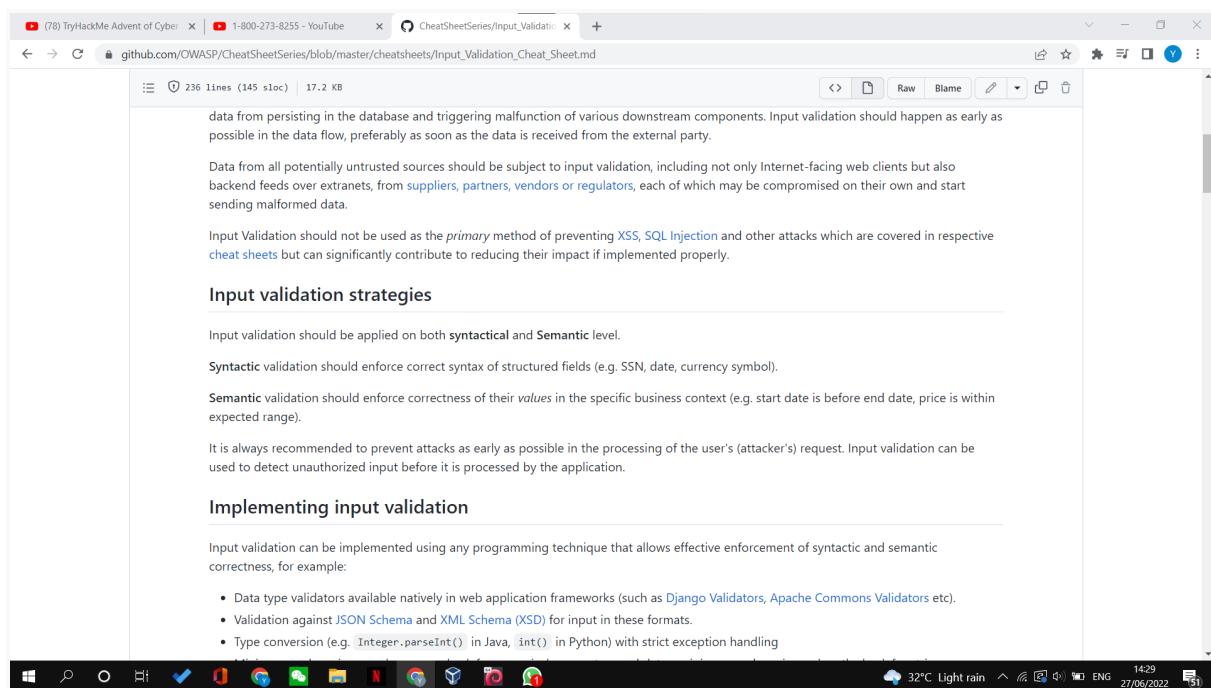
## **Day 6: Networking – Be careful with what you wish on a Christmas night**

**Tools used:** Kali Linux, Chrome

**Solution/walkthrough:** DarkSec

### **Question 1**

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



The screenshot shows a Microsoft Edge browser window with the URL [github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Input\\_Validation\\_Cheat\\_Sheet.md](https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Input_Validation_Cheat_Sheet.md). The page content is as follows:

data from persisting in the database and triggering malfunction of various downstream components. Input validation should happen as early as possible in the data flow, preferably as soon as the data is received from the external party.

Data from all potentially untrusted sources should be subject to input validation, including not only Internet-facing web clients but also backend feeds over extranets, from **suppliers**, **partners**, **vendors** or **regulators**, each of which may be compromised on their own and start sending malformed data.

Input Validation should not be used as the *primary* method of preventing [XSS](#), [SQL Injection](#) and other attacks which are covered in respective [cheat sheets](#) but can significantly contribute to reducing their impact if implemented properly.

#### **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.

#### **Implementing input validation**

Input validation can be implemented using any programming technique that allows effective enforcement of syntactic and semantic correctness, for example:

- Data type validators available natively in web application frameworks (such as [Django Validators](#), [Apache Commons Validators](#) etc).
- Validation against [JSON Schema](#) and [XML Schema \(XSD\)](#) for input in these formats.
- Type conversion (e.g. `Integer.parseInt()` in Java, `int()` in Python) with strict exception handling

### **Question 2**

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

The screenshot shows a browser window with several tabs open. The active tab is a GitHub page titled 'Input\_Validation\_Cheat\_Sheet.md'. The page content includes a list of US states and a Java Regex example for validating zip codes.

**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|NE|MH|MD|MA|MI|MN|HS|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|WV)$
```

**Java Regex Usage Example:**

Example validating the parameter 'zip' using a regular expression.

```
private static final Pattern zipPattern = Pattern.compile("^\\d{5}(-\\d{4})?");  
  
public void doPost( HttpServletRequest request, HttpServletResponse response ) {  
    try {  
        String zipCode = request.getParameter( "zip" );  
        if ( !zipPattern.matcher( zipCode ).matches() ) {  
            throw new YourValidationException( "Improper zipcode format." );  
        }  
        // do what you want here, after its been validated ..  
    } catch(YourValidationException e) {  
        response.sendError( response.SC_BAD_REQUEST, e.getMessage() );  
    }  
}
```

Some Allow list validators have also been predefined in various open source packages that you can leverage. For example:

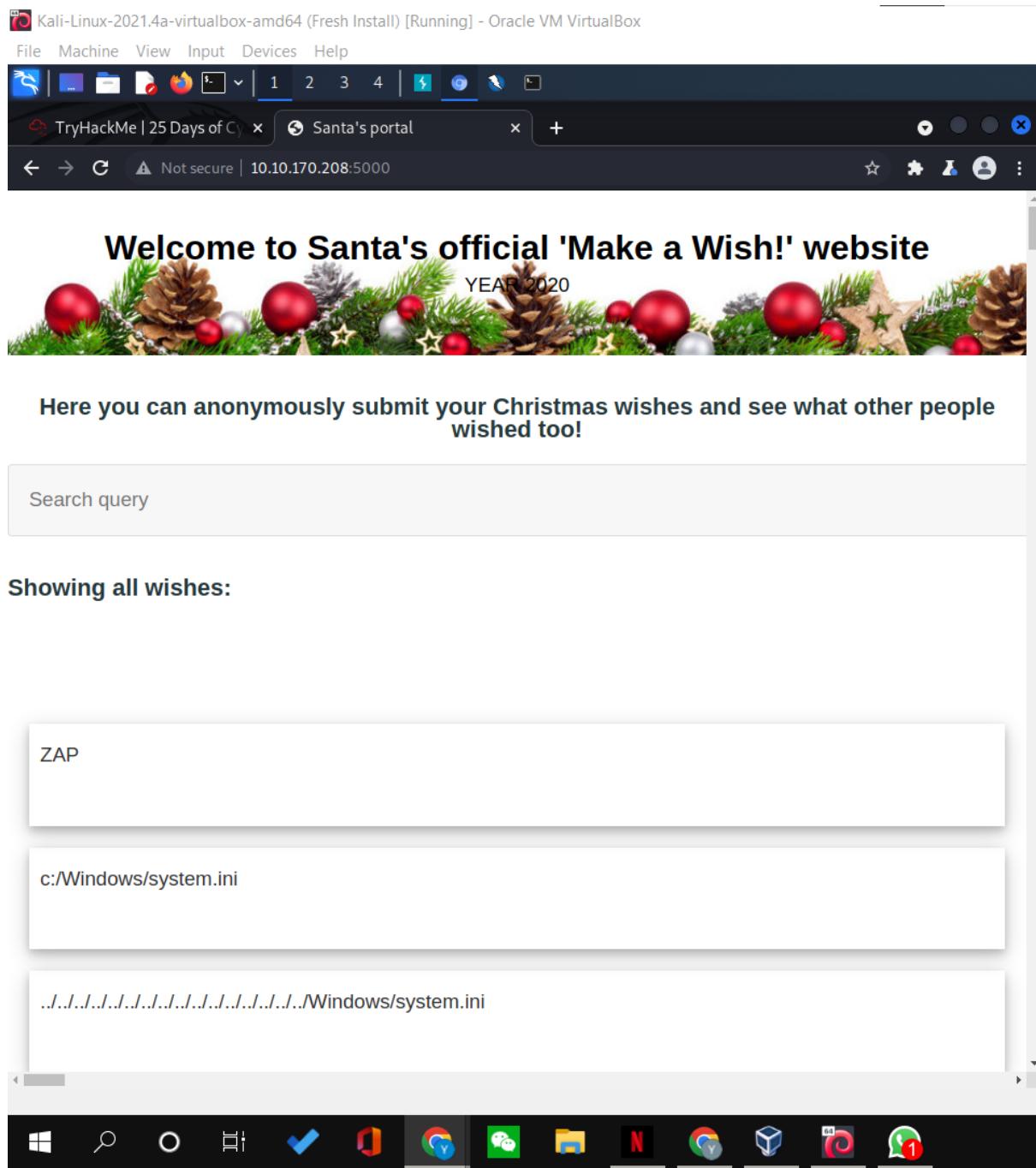
- [Apache Commons Validator](#)

**Client Side vs Server Side Validation**

Be aware that any JavaScript input validation performed on the client can be bypassed by an attacker that disables JavaScript or uses a Web

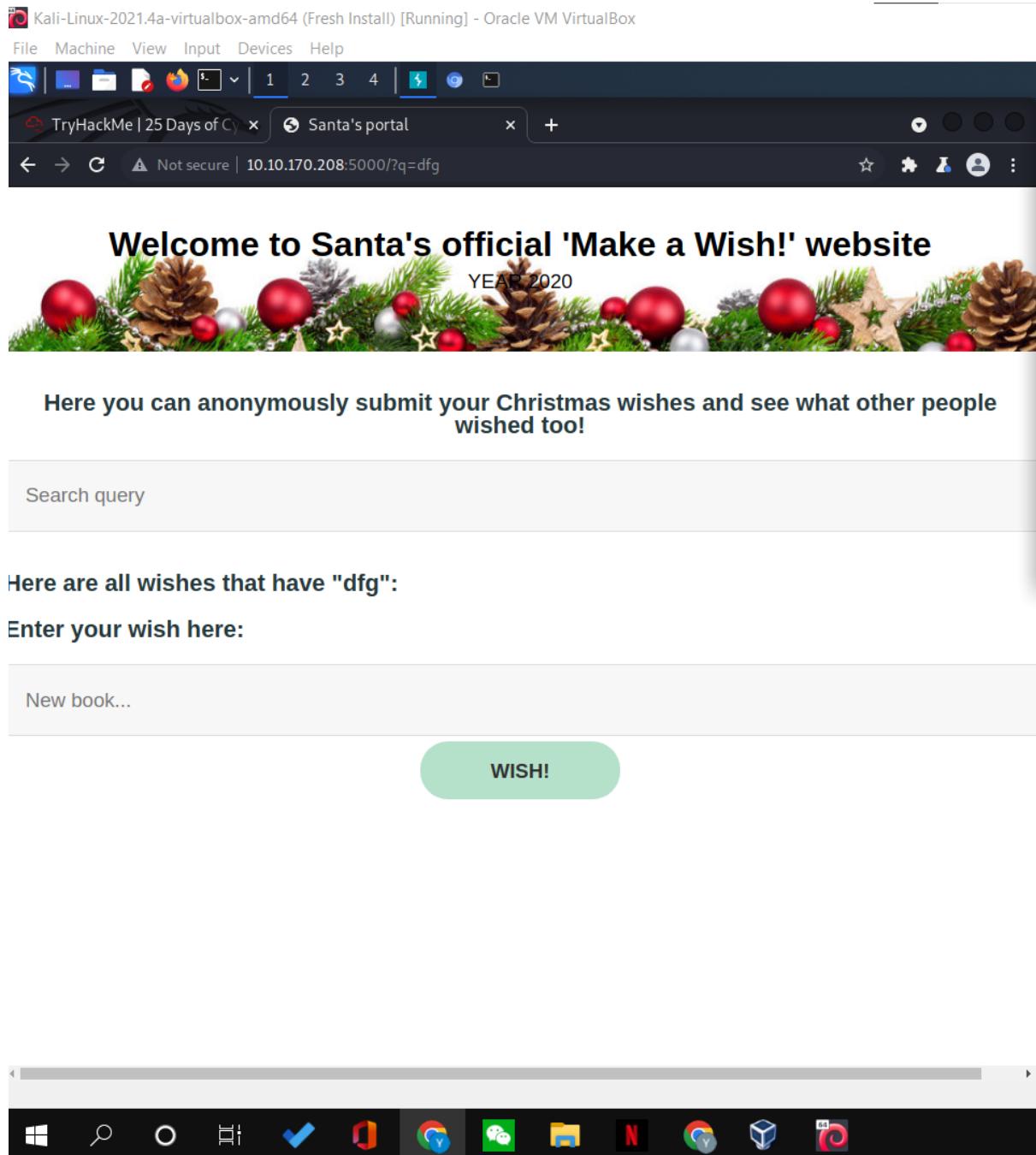
### Question 3

What vulnerability type was used to exploit the application?



### Question 4

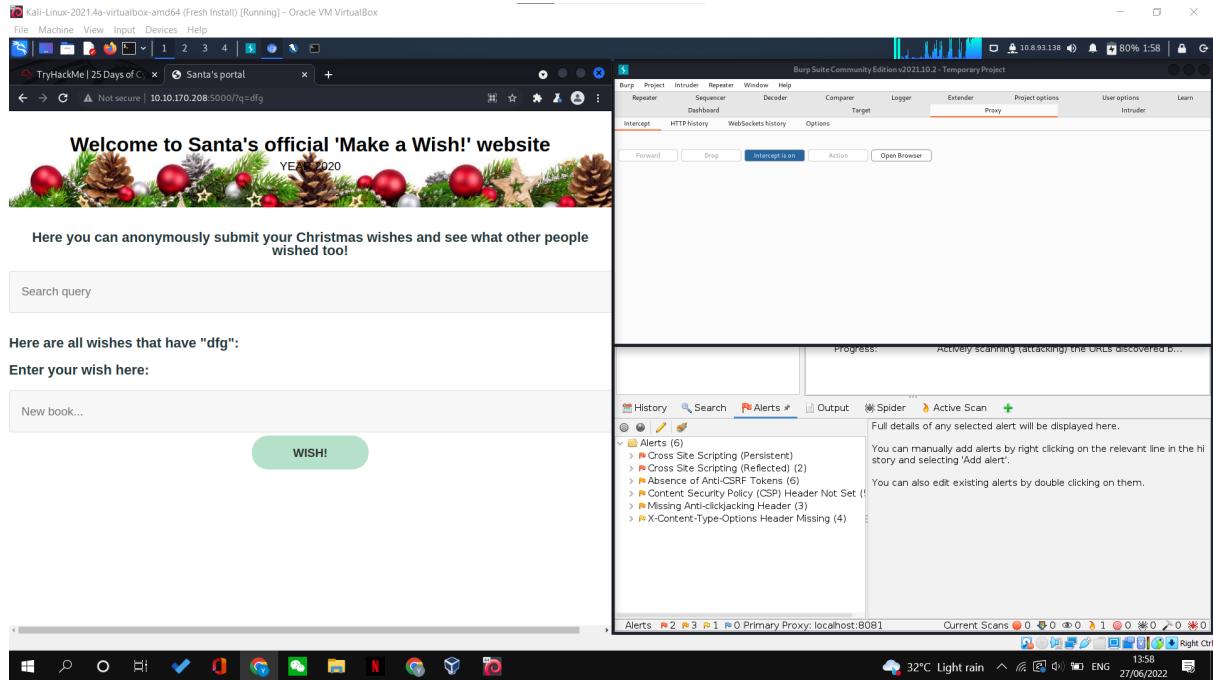
What query string can be abused to craft a reflected XSS?



### Question 5

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

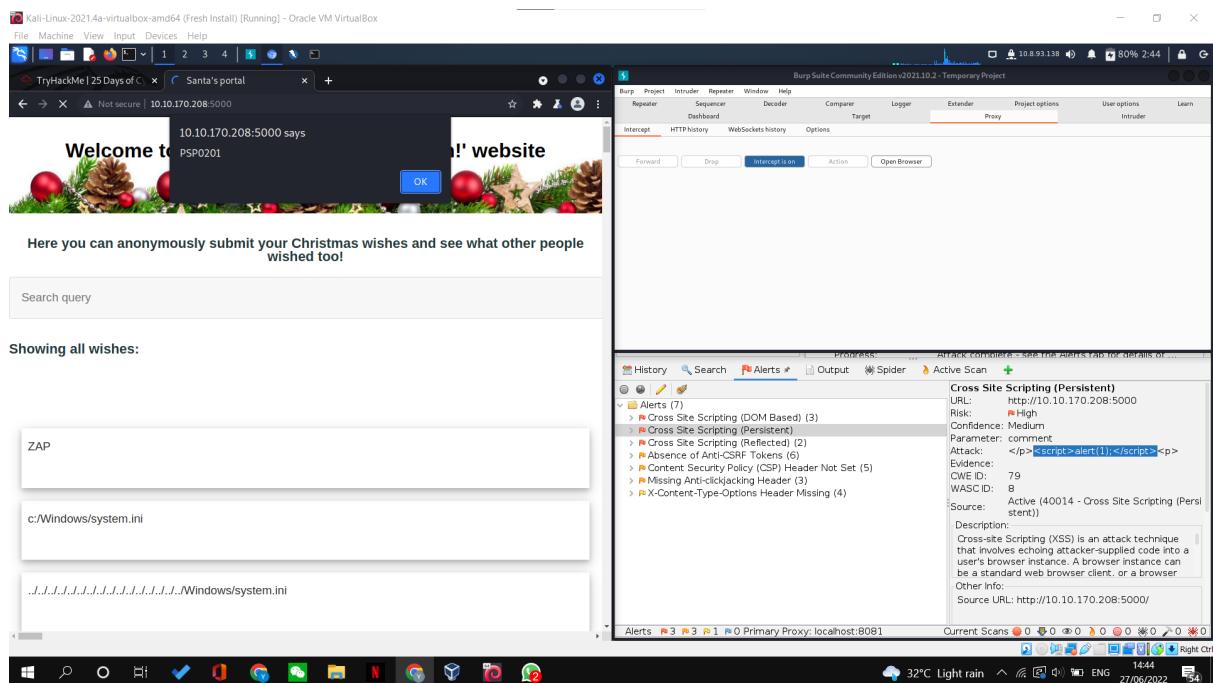
Use the AttackBox's Zap 2.9.0 or Kali's 2.11.1, otherwise you may get different answers



## Question 6

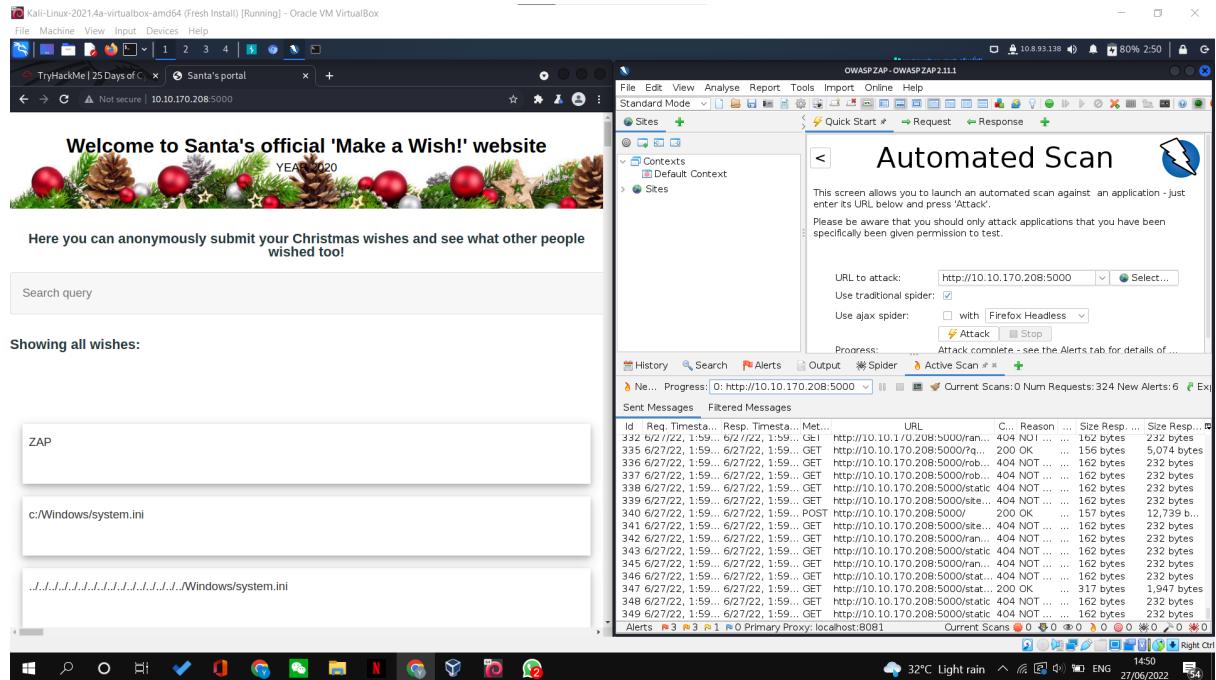
What Javascript code should you put in the wish text box if you want to show an alert saying "PSP0201"?

Answer hint: <script>xxxxxx</script> <--insert your answer TOGETHER with the script tags.



## Question 7

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



### Thought Process/Methodology:

I went into the OWASP cheatsheet series and viewed the needed information. Next, I went into the back-up server and keyed in random words in the query box to see what query string can be abused to craft a reflected XSS. Then, I opened up ZAP. After that, I keyed in the url and clicked attack to view the alerts.

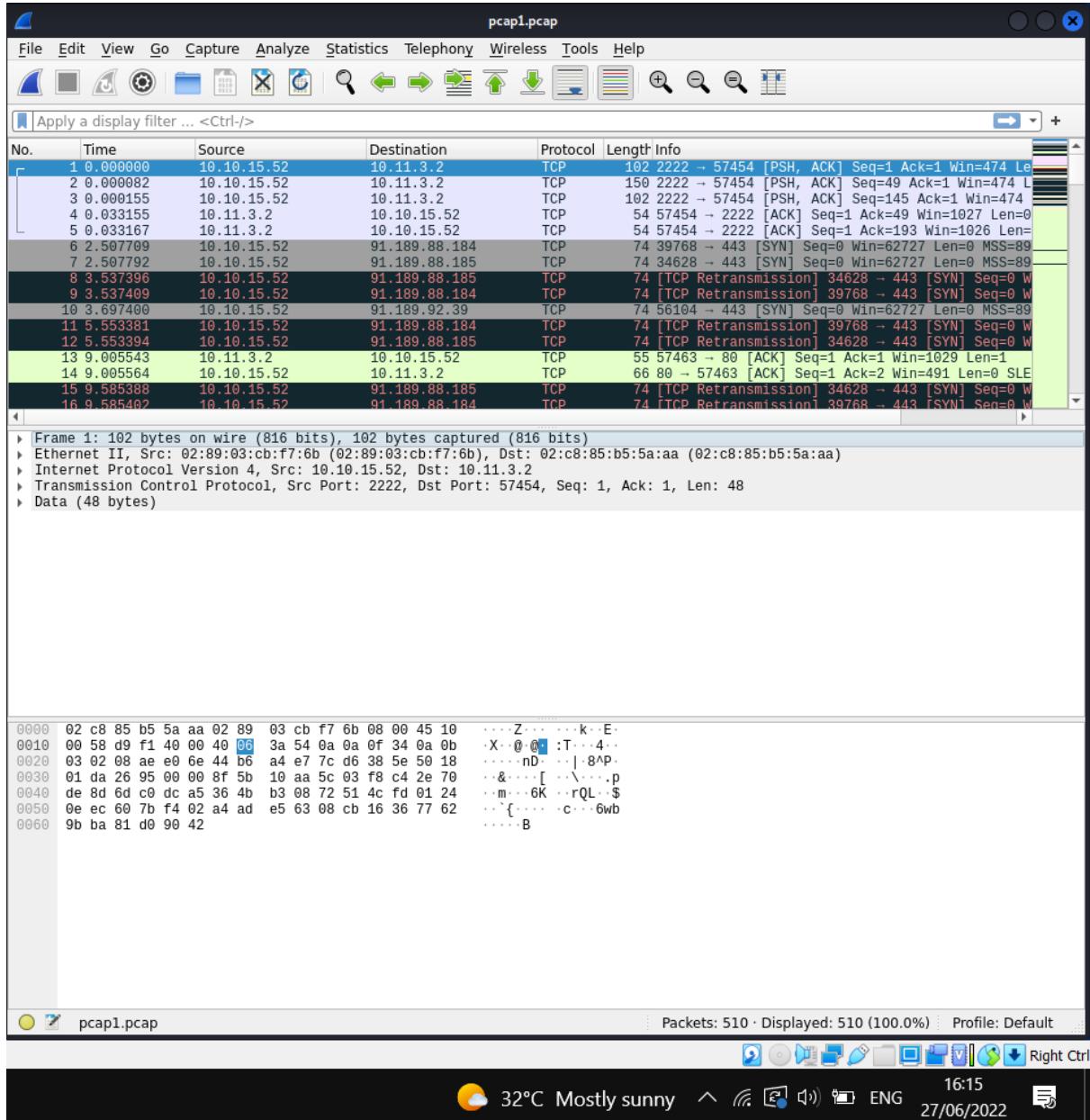
### Day 7: Networking – The Grinch Really Did Steal Christmas

**Tools used:** Kali Linux, Chrome

**Solution/walkthrough:** DarkSec

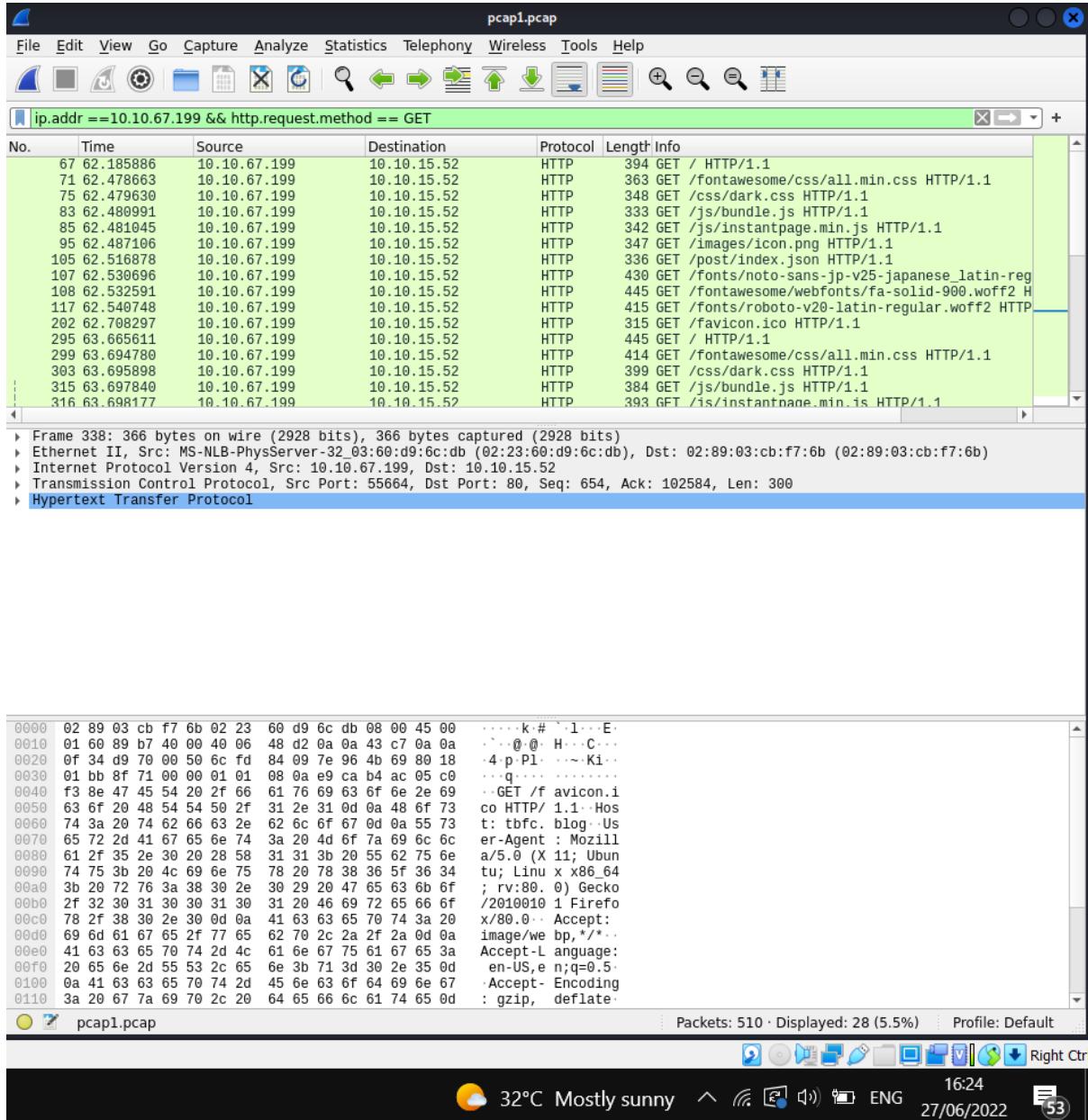
### Question 1

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



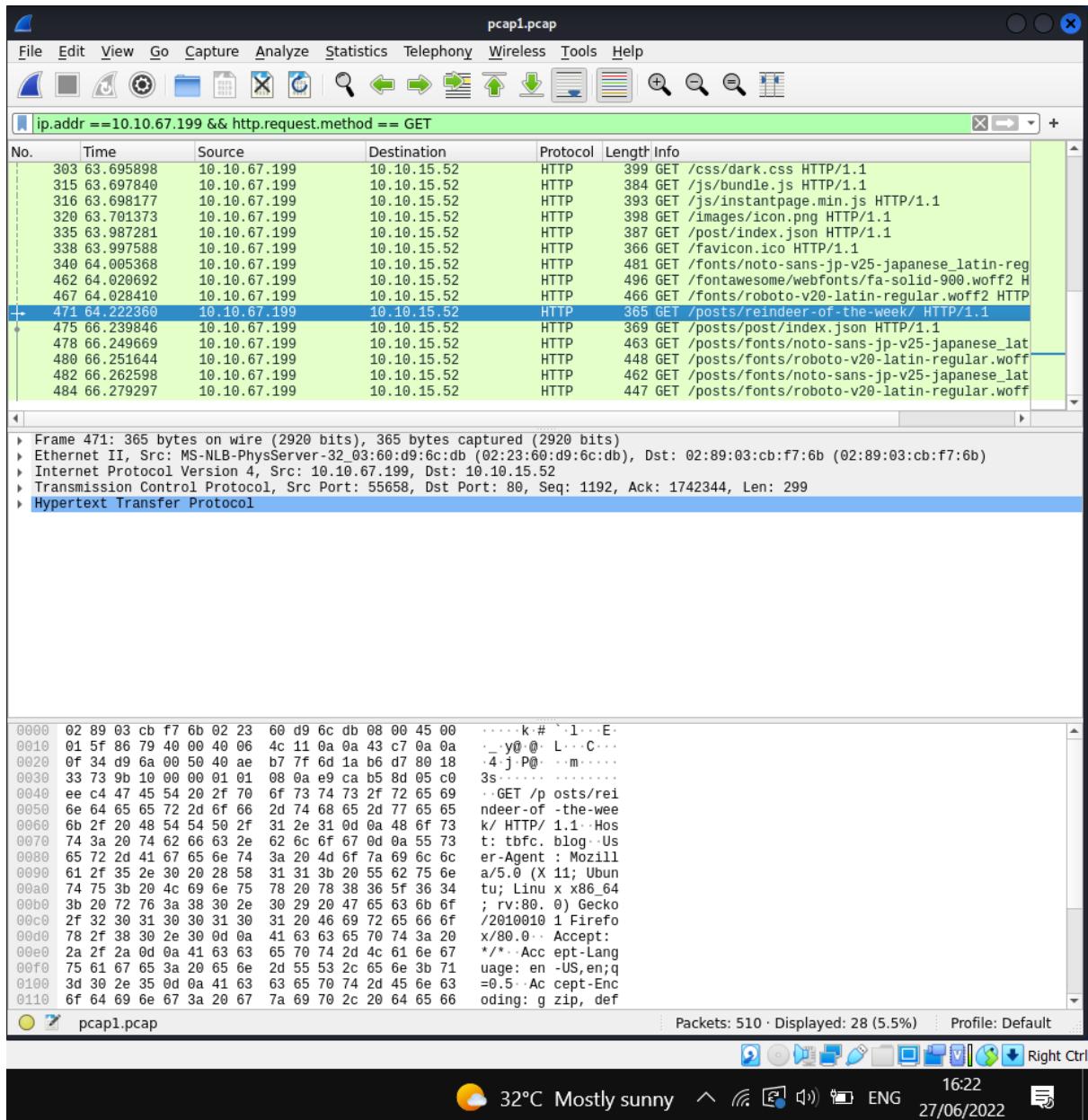
## Question 2

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



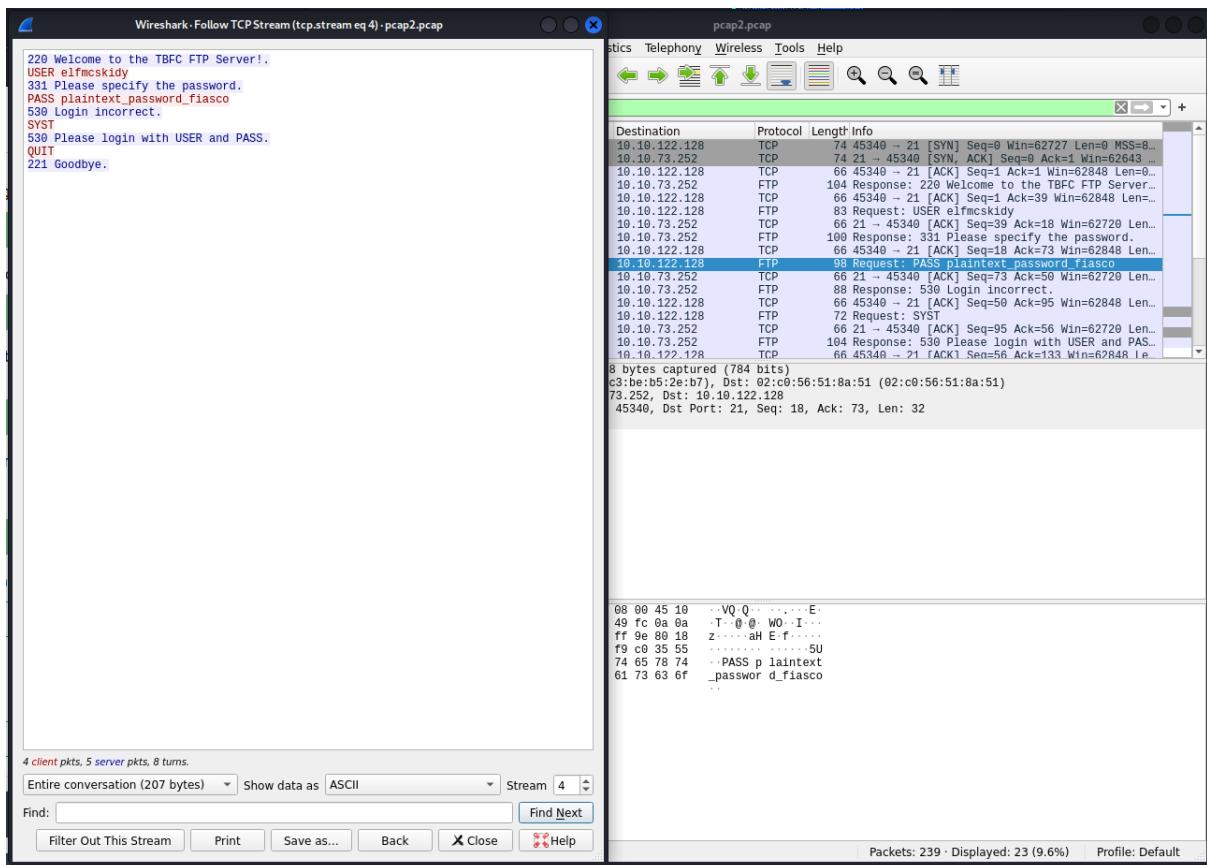
### Question 3

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?



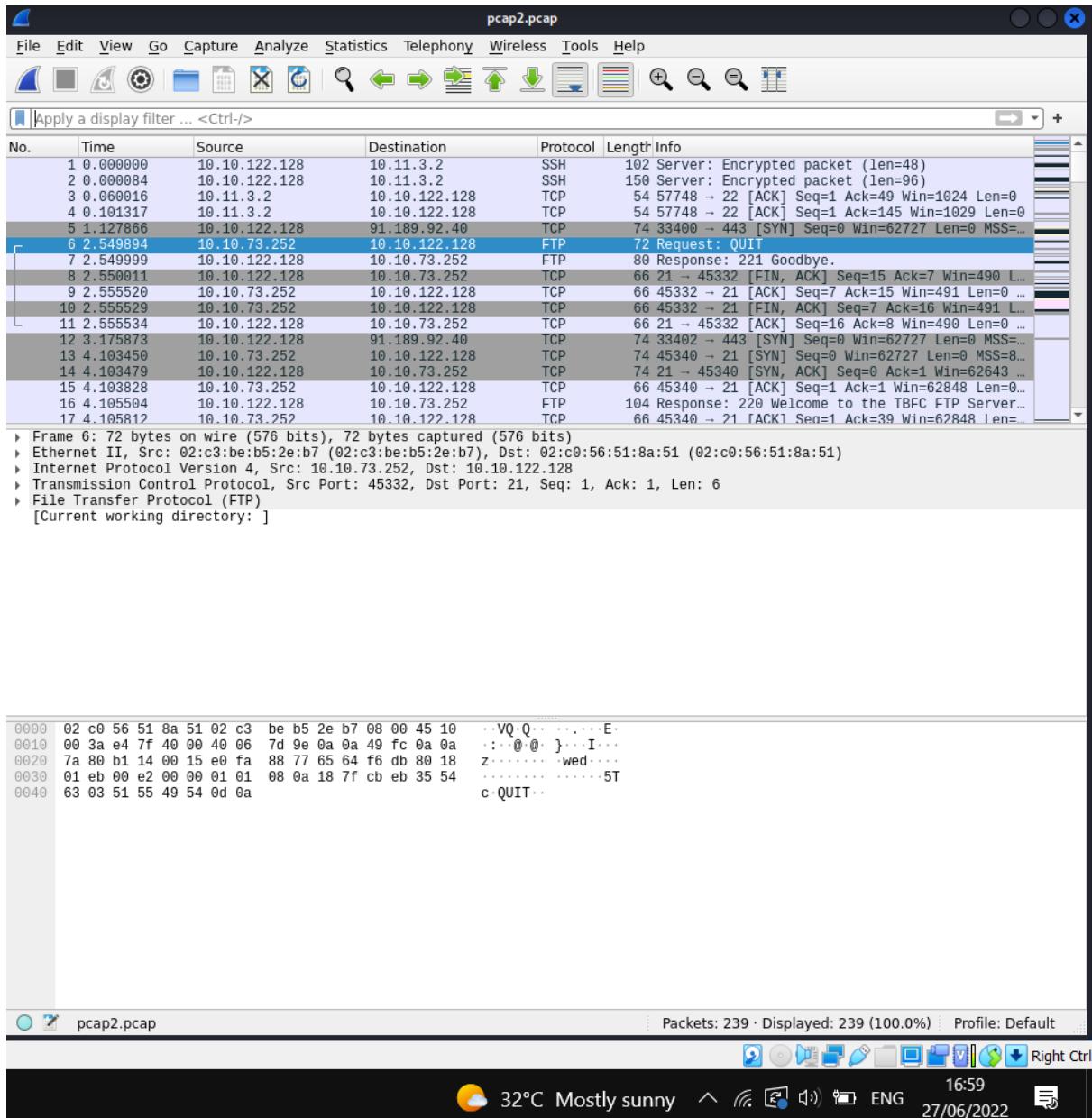
#### Question 4

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



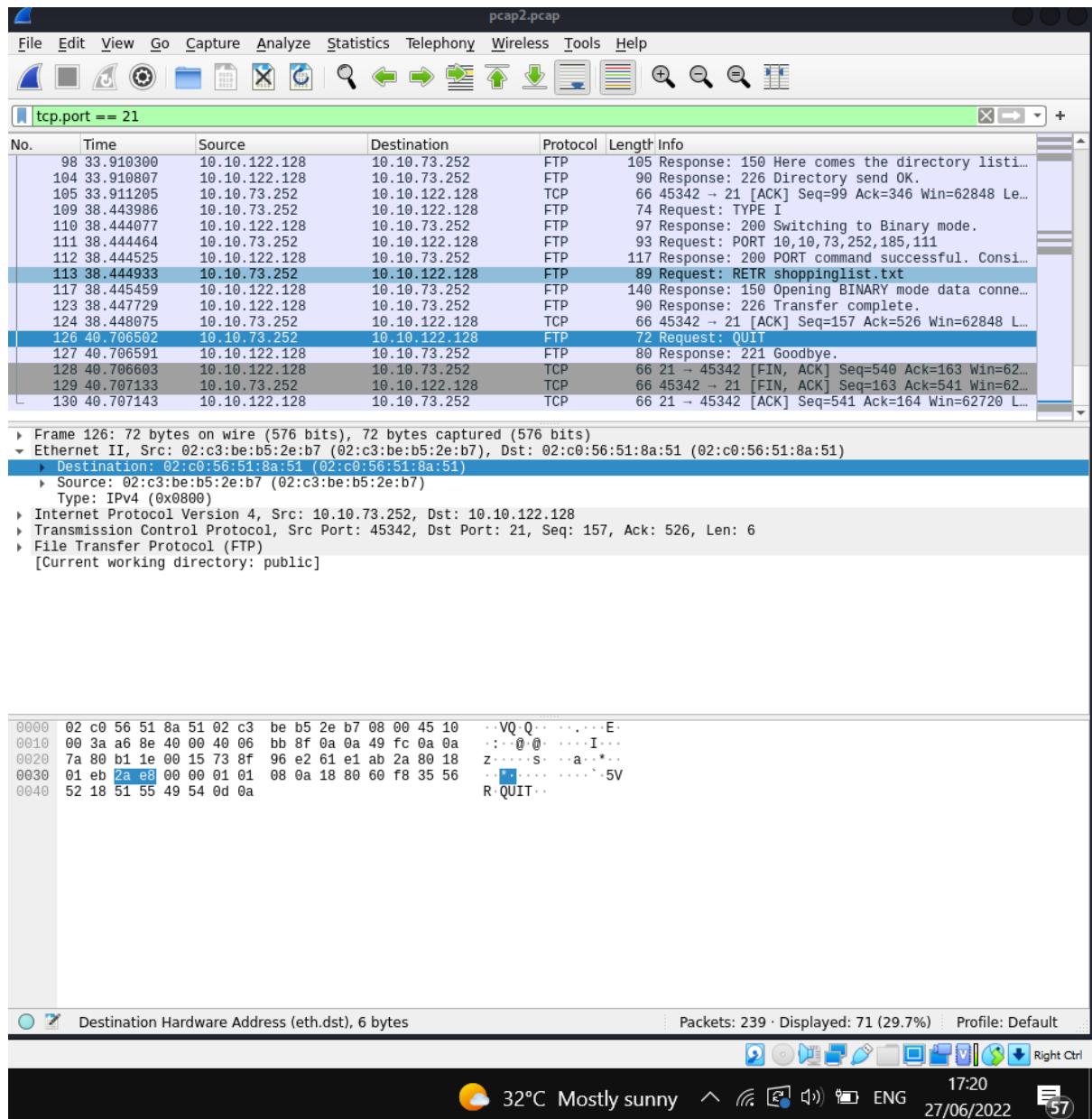
## Question 5

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



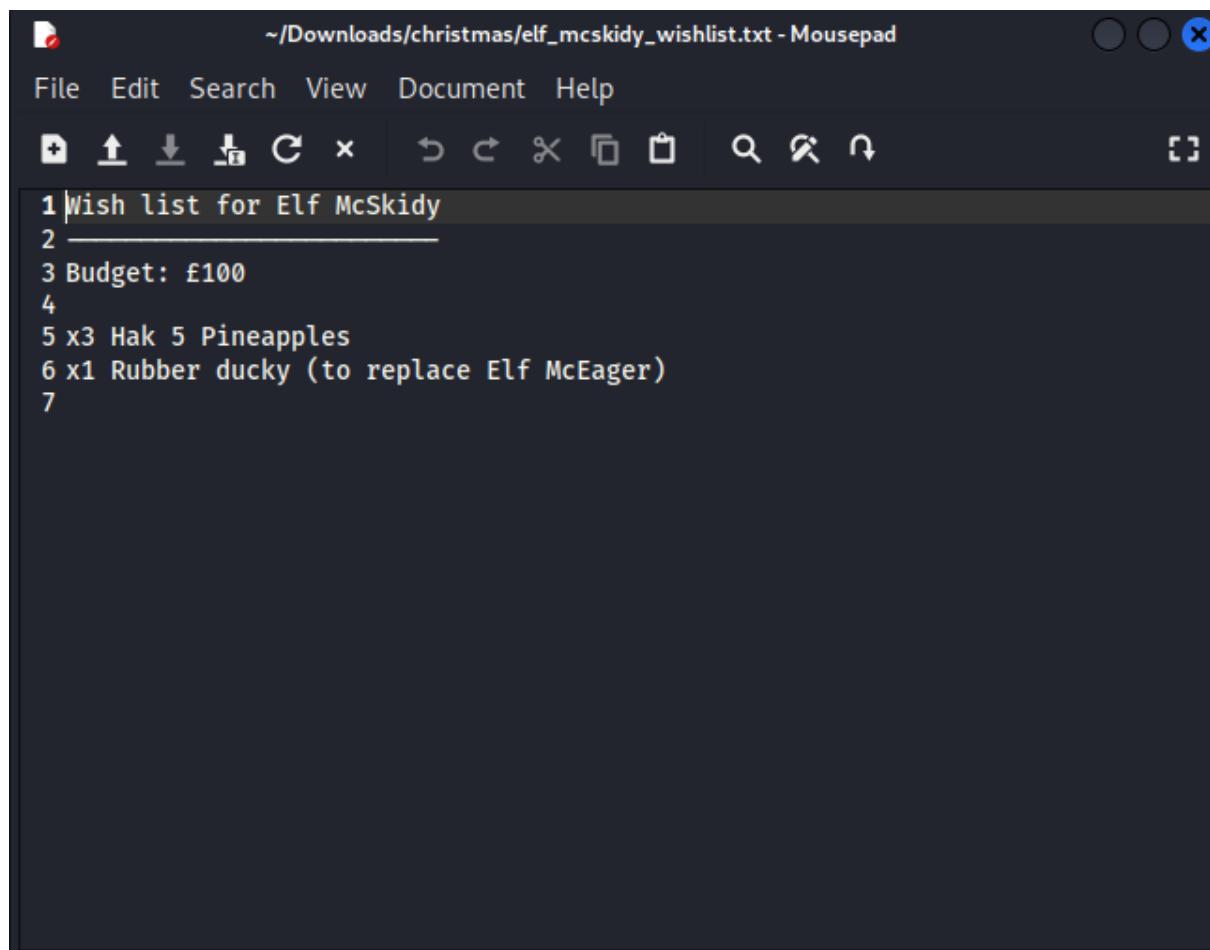
## Question 6

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



## Question 7

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



~/Downloads/christmas/elf\_mcskidy\_wishlist.txt - Mousepad

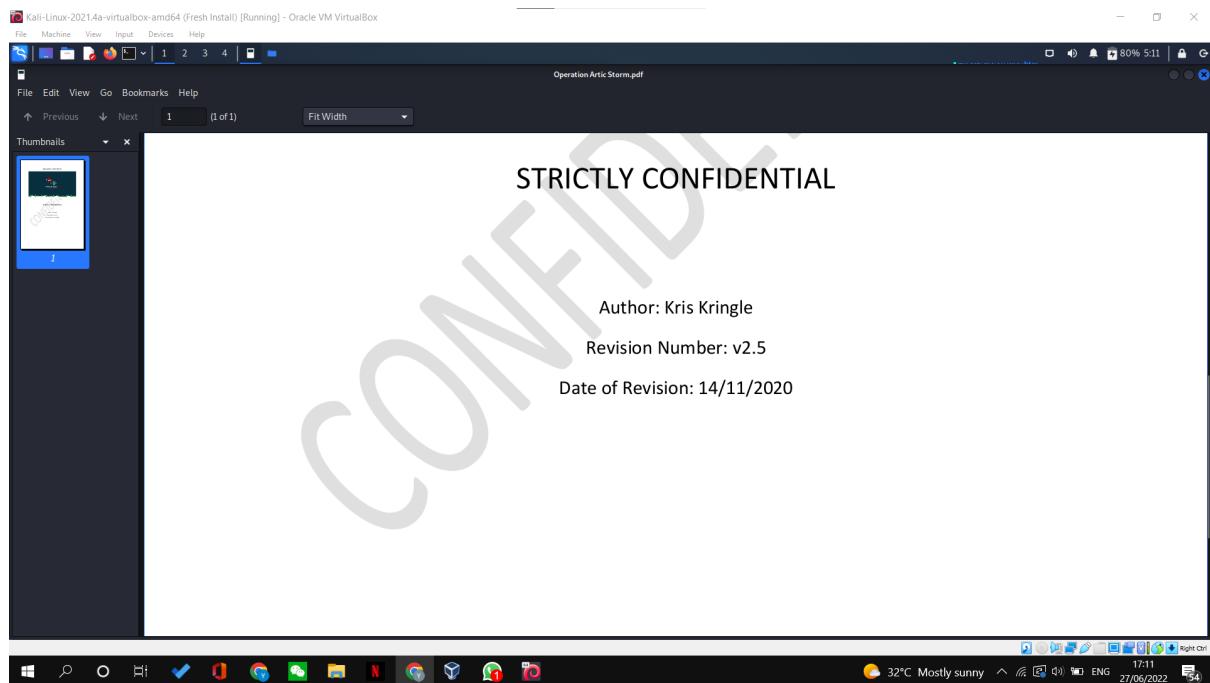
File Edit Search View Document Help

D

```
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

Who is the author of Operation Artic Storm?



## **Thought Process/Methodology:**

I downloaded the zipped file and extracted it. Then, I used wireshark to open pcap1.pcap. I filtered in icmp to see the IP address. Next, I filtered in the IP address provided by TryHackMe and http.request.method == GET to see the name of the article that IP address "10.10.67.199" visited. Next, I opened the pcap2.pcap and filtered in tcp.port == 21. Then, I viewed the information needed and followed a successful login. Then, it shows the leaked password. Next, I opened pcap3.pcap to export christmas.zip and viewed the files.

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

**Tools used:** Kali Linux, Chrome

**Solution/walkthrough:** DarkSec

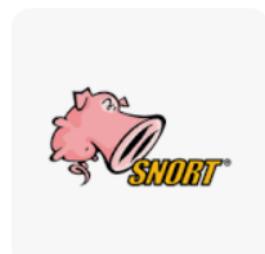
### **Question 1**

When was Snort created?

About 1,670,000 results (0.51 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.



### **Question 2**

Using Nmap on MACHINE\_IP , what are the port numbers of the three services running?

```
kali@kali:~
```

```
File Actions Edit View Help
PORT STATE SERVICE VERSION
80/tcp open  http  Apache httpd 2.4.29 ((Ubuntu))
|_http-title: TBFC&#39;s Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_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:d0:05:c0:27: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 3.1 - 3.2 (92%), Linux 3.11 (92%), Linu x 3.2 - 4.9 (92%), Linux 3.7 - 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
GATEWAY: 10.0.2.2/255.255.255.0  IFACE=eth0  HWADDR=00:00:27:50:4c:14
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 143/tcp)
HOP RTT ADDRESS
1  193.64 ms 10.8.0.1  route_v4.add: 10.10.0.0/16 via 10.8.0.1 dev [NULL] table 0 metric 1000
2  193.83 ms 10.10.233.172: this configuration may cache passwords in memory -- use the auth-nocache option to pre
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.50 seconds
```

### 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?

```
kali@kali:~$ sudo nmap -A 10.10.233.172 -T5
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 07:49 EDT
Nmap scan report for 10.10.233.172
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-title: TBFC's Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_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%), Linux 2.6.32 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%), Linux 3.7 - 3.10 (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
```

### Question 4

What is the version of Apache?

```
kali@kali:~$ sudo nmap -A 10.10.233.172 -T5
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 07:49 EDT
Nmap scan report for 10.10.233.172
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-title: TBFC's Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_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%), Linux 2.6.32 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%), Linux 3.7 - 3.10 (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
```

### Question 5

What is running on port 2222?

```

kali@kali:~ 
File Actions Edit View Help topology subnet,ping 5,ping-restart 120,ifconfig 10.8.93.138 255.255.0.0,peer-id 111
└$ sudo nmap -A 10.10.233.172 -T5
[+] Nmap scan report for 10.10.233.172
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
80/tcp    open  http           Apache httpd 2.4.29 ((Ubuntu))
|_http-title: TBFC's Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_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%), Linux 2.6.32 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linu x 3.2 - 4.9 (92%), Linux 3.7 - 3.10 (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

```

## 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?

```

kali@kali:~ 
File Actions Edit View Help topology subnet,ping 5,ping-restart 120,ifconfig 10.8.93.138 255.255.0.0,peer-id 111
PORT      STATE SERVICE          VERSION
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server
Nmap done: 1 IP address (1 host up) scanned in 2.83 seconds
[kali㉿kali] [-]
└$ sudo nmap --script http-title 10.10.134.169 -T5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 08:43 EDT
Warning: 10.10.134.169 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.134.169
Host is up (0.22s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
80/tcp    open  http           Apache httpd 2.4.29 ((Ubuntu))
|_http-title: TBFC's Internal Blog
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server
Nmap done: 1 IP address (1 host up) scanned in 11.20 seconds
[kali㉿kali] [-]
└$ 

```

## **Thought Process/Methodology:**

I opened the terminal and typed in 'man nmap' to view the commands. After I know which commands to use, I started nmap with my IP address and viewed the information I needed like the port numbers, the linux distribution ,the version of Apache and others. Next, I used Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver.

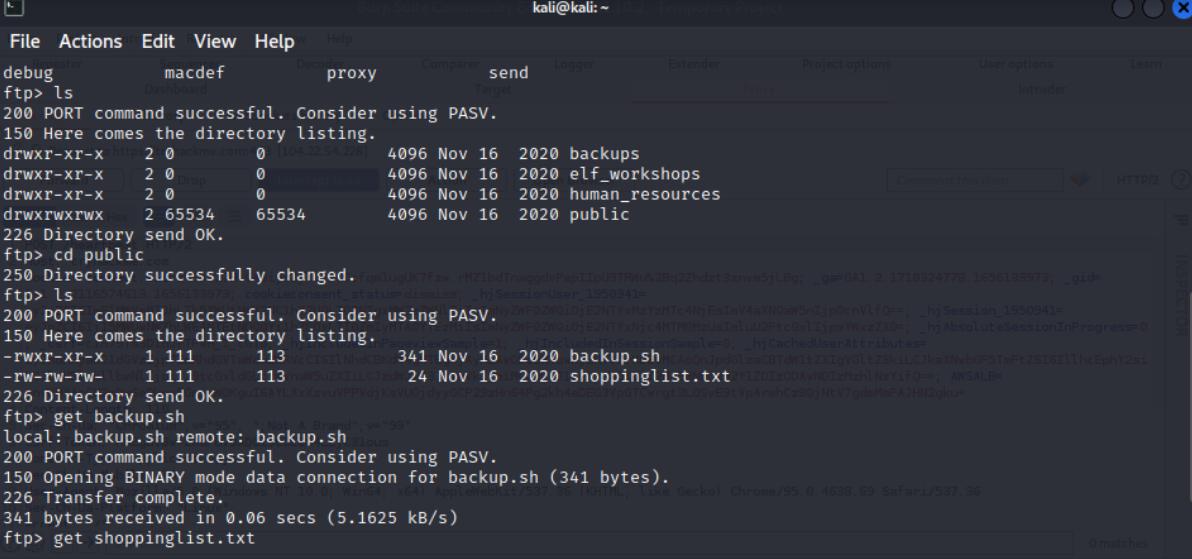
## **Day 9: Networking – Anyone can be Santa!**

**Tools used:** Kali Linux, Chrome

**Solution/walkthrough:** DarkSec

### Question 1

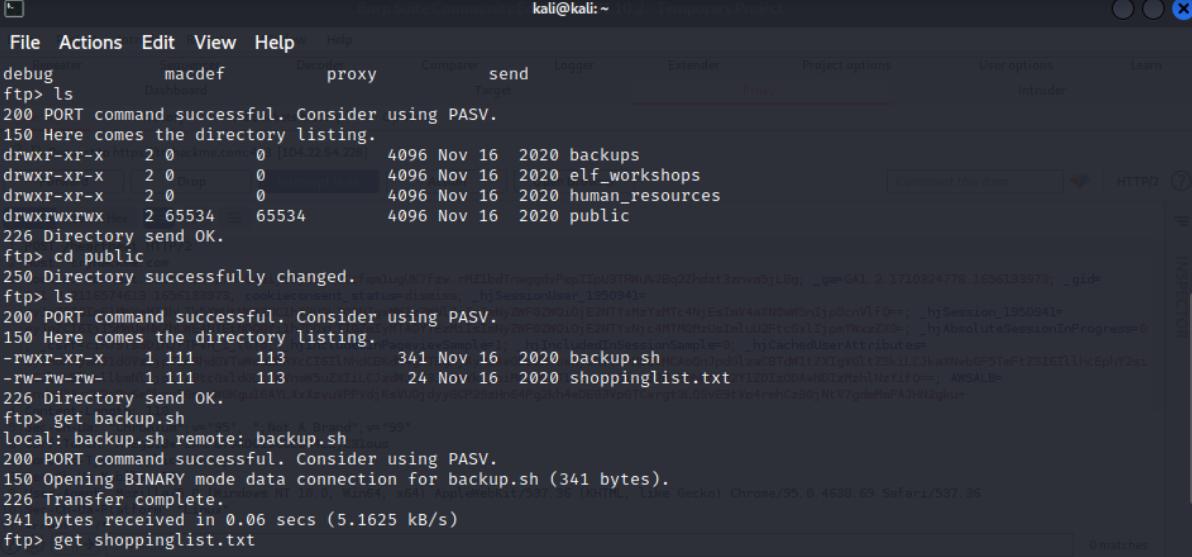
What are the directories you found on the FTP site?



```
kali@kali: ~
File Actions Edit View Help
debug macdef Dec proxy Compara send Logger Extender Project options User options Learn
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x http 2 0 ackme.com 0 [104.22.54.228] 4096 Nov 16 2020 backups
drwxr-xr-x 2 0 Drop 0 [104.22.54.228] 4096 Nov 16 2020 elf_workshops
drwxr-xr-x 2 0 0 0 [104.22.54.228] 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-- www 1 113 www 341 Nov 16 2020 backup.sh
-rw-rw-rw- www 1 113 www 24 Nov 16 2020 shoppinglist.txt
226 Directory send OK.
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 0.06 secs (5.1625 kB/s)
ftp> get shoppinglist.txt
```

### Question 2

Name the directory on the FTP server that has data accessible by the "anonymous" user



```
kali@kali: ~
File Actions Edit View Help
debug macdef Dec proxy Compara send Logger Extender Project options User options Learn
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x http 2 0 ackme.com 0 [104.22.54.228] 4096 Nov 16 2020 backups
drwxr-xr-x 2 0 Drop 0 [104.22.54.228] 4096 Nov 16 2020 elf_workshops
drwxr-xr-x 2 0 0 0 [104.22.54.228] 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-- www 1 113 www 341 Nov 16 2020 backup.sh
-rw-rw-rw- www 1 113 www 24 Nov 16 2020 shoppinglist.txt
226 Directory send OK.
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 0.06 secs (5.1625 kB/s)
ftp> get shoppinglist.txt
```

### Question 3

What script gets executed within this directory?

```
Burp Suite Community   kali@kali: ~  [12] Temporary Project

File Actions Edit View Help
File   Actions   Edit   View   Help
debug   macdef   Decoding   Comparer   send   Logger   Extender   Project options   User options   Learn
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x 2 0 hackme.com 0 [104.23.54.228] 4096 Nov 16 2020 backups
drwxr-xr-x 2 0 Drop 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
150 Here comes the directory listing.
drwxr-xr-x 1 113 www-data 341 Nov 16 2020 backup.sh
-rw-rw-rw- 1 113 root 113 24 Nov 16 2020 shoppinglist.txt
226 Directory send OK.
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 0.06 secs (5.1625 kB/s)
ftp> get shoppinglist.txt
0 matches
```

## Question 4

What movie did Santa have on his Christmas shopping list?

\*~/shoppinglist.txt - Mousepad

File Edit Search View Document Help

File Open Save Copy Paste Cut Find Replace Search

1 |The Polar Express Movie

2

### 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!

```

File Actions Edit View Help
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 stackme.com 0 [77.67.77.10] 4096 Nov 16 2020 backups
drwxr-xr-x 2 0 Drop 0 [77.67.77.10] 4096 Nov 16 2020 elf_workshops
drwxr-xr-x 2 0 stackme.com 0 [77.67.77.10] 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
10567413 1656133973 cookiecomment_statusdismiss _hjSessionUser_1950941=
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xr-x 1 113 ncovar 341 Nov 16 2020 backup.sh
-rw-rw-rw- 1 113 cokd 113 novW5uZT1L1C1zde 24 Nov 16 2020 shoppinglist.txt
226 Directory send OK.
ftp> put backup.sh -s: "/", "Not A Brand", "v=99"
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
58 bytes sent in 0.00 secs (1.7285 MB/s)
ftp> 

```

```

File Actions Edit View Help
2022-06-25 10:35:09 H Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
—(kali㉿kali)-[~]
$ nano backup.sh
VERIFY EKU OK
2022-06-25 10:35:09 VERIFY OK: depth=0, CN=server
—(kali㉿kali)-[~] Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bit RSA
$ nc -lvpn 4444 [server] Peer Connection Initiated with [AF_INET]18.202.129.195:1194
invalid local port n
ENT CONTROL [server]: 'PUSH_REQUEST' (status1)
2022-06-25 10:35:10 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route-metric 1000,comp-
—(kali㉿kali)-[~] 10.8.0.1,topology subnet,ping 5,ping-restart 120,ifconfig 10.8.93.138 255.255.0.0,peer-id 12
$ nc -lvpn 4444 OPTIONS IMPORT: timers and/or timeouts modified
2022-06-25 10:35:10 OPTIONS IMPORT: compression parms modified
listening on [any] 4444 ...
OPTIONS IMPORT: —ifconfig/up options modified
2022-06-25 10:35:10 OPTIONS IMPORT: route options modified
connect to [10.8.93.138] from [UNKNOWN] [10.10.164.207] 60456
bash: cannot set terminal process group (1532): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~# adjusting link_mtu to 1625
root@tbfc-ftp-01:~# Using peer cipher 'AES-256-CBC'
root@tbfc-ftp-01:~# ls
going Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
ls: going Data Channel: Using 512 bit message hash 'SHA512' for HMAC authentication
flag.txt: Using 256 bit message hash 'SHA512' for HMAC authentication
root@tbfc-ftp-01:~# cat flag.txt
Channel: Using 512 bit message hash 'SHA512' for HMAC authentication
cat flag.txt: Preserving previous TUN/TAP instance: tun0
THM{even_you_can_be_santa}
root@tbfc-ftp-01:~# 

```

### Thought Process/Methodology:

I opened the terminal and the ftp server with my ip address. When it is connected, I used the ls command to view the directories. After that, I changed to public and viewed the public directories. Then, I downloaded said directories with the get command. After it was done, I opened the script and viewed what was inside the shoppinglist.txt. Next, I altered the script with nano and put in the pentesters cheatsheet provided. Then, set up a netcat listener to catch the connection. After that, I put in in the backup.sh. When the listener is connected, I opened the flag.txt with the command (cat).

### Day 10: Networking – Don't be sElfish!

**Tools used:** Kali Linux, Chrome

## Solution/walkthrough: DarkSec

## Question 1

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

```
kali㉿kali: ~
```

```
File Actions Edit View Help
-p pass specify password to use (default "") timeouts modified
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) For HMAC authentication
-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"
Get OS information
Get printer information
Specify workgroup manually (usually found automatically)
Do an nmblookup (similar to nbtstat)
Verbose. Shows full commands being run (net, rpcclient, etc.)
```

## Question 2

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

```
kali@kali: ~
File Actions Edit View Help
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.10.15.64 from smbclient: parsed modified
[+] Got OS info for 10.10.15.64 from srvinfo: /up options modified
[2012-06-25 14:24:13] Wk Sv PrQ Unx NT SNT tbfc-smb server (Samba, Ubuntu)
[2012-06-25 14:24:13] platform_id    OPTIONS IMPOSSIBLE route-related options modified
[2012-06-25 14:24:13] os version    OPTIONS IMPOSSIBLE peerid set
[2012-06-25 14:24:13] server type   OPTIONS IMPOSSIBLE setting link_mtu to 1625
[2012-06-25 14:24:13] Using peer cipher 'AES-256-CBC'
=====
| Users on 10.10.15.64 | Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
|                         | Data Channel: Using 512 bit message hash 'SHA512' for HMAC authentication
|                         | Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy messageName: Desc: for HMAC authentication
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager.0     Name: elfmceager      Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson2 deName: Desc:
=====
[2012-06-25 14:24:13] ROUTE GATEWAY 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:50:4c:14
user:[elfmcskidy] rid:[0x3e8] device tun0 opened
user:[elfmceager] rid:[0x3ea] tu_set: mtu 1500 for tun0
user:[elfmcelferson] rid:[0x3e9]: set tun0 UP
=====
[2012-06-25 14:24:13] net add br0: add: 10.8.93.138/16 dev tun0
=====
| Share Enumeration on 10.10.15.64 | 0.0.0/16 via 10.8.0.1 dev [NULL] table 0 metric 1000
|                                         | igration may cache passwords in memory -- use the auth-nocache option to prev
=====
[2012-06-25 14:24:13] Initialization Sequence Completed

Sharename          Type        Comment

```

### Question 3

Now how many "shares" are there on the Samba server?

```

kali@kali: ~
File Actions Edit View Help
=====
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy fied Name: Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager modif Name: elfmceager Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson Name: Desc:
[22-06-25 14:24:13] OPTIONS IMPORT: route-related options modified
user:[elfmcskidy] rid:[0x3e8] IMPORT: peer-id set
user:[elfmceager] rid:[0x3ea] IMPORT: adjusting link_mtu to 1625
user:[elfmcelferson] rid:[0x3e9] cipher 'AES-256-CBC'
[22-06-25 14:24:13] Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
[22-06-25 14:24:13] Using 512 bit message hash 'SHA512' for HMAC authentication
[22-06-25 14:24:13] Share Enumeration on 10.10.15.64 | Cipher 'AES-256-CBC' initialized with 256 bit key
[22-06-25 14:24:13] Using 512 bit message hash 'SHA512' for HMAC authentication
[22-06-25 14:24:13] net_route_v4_best_sw query: dst 0.0.0.0
[22-06-25 14:24:13] Sharename: net Type: v4 Comment: via 10.0.2.2 dev eth0
[22-06-25 14:24:13] ROUTE_GATEWAY: 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:50:4c:14
[22-06-25 14:24:13] TUN_Disk device tbfc-hr opened
[22-06-25 14:24:13] Disk _mtu tbfc-it 1500 for tun0
[22-06-25 14:24:13] Disk _up: tbfc-santa
[22-06-25 14:24:13] net IPC$ IPC Service (tbfc-smb server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing. 0/19 via 10.8.0.1 dev [NULL] table 0 metric 1000
[22-06-25 14:24:13] WARNING: This configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Server Comment
[22-06-25 14:24:13] Initialize sequence Completed

```

#### Question 4

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

```

kali@kali: ~
File Actions Edit View Help
=====
(kali㉿kali)-[~] OPTIONS IMPORT: timers and/or timeouts modified
$ sudo smbclient //10.10.15.64/tbfc-it Enter WORKGROUP\root's password: 1 x
tree connect failed: NT_STATUS_ACCESS_DENIED
[22-06-25 14:24:13] OPTIONS IMPORT: route-related options modified
-(kali㉿kali)-[~] OPTIONS IMPORT: peer-id set
$ sudo smbclient //10.10.15.64/tbfc-santa Enter WORKGROUP\root's password: 1 x
Try "help" to get a list of possible commands. 1 AES-256-CBC
smb: > ls 14:24:13 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
. 22-06-25 14:24:13 Del: Cip 0 Wed Nov 11 21:12:07 2020 with 256 bit Key
.. 22-06-25 14:24:13 Incoming Data Channel: Del: Usi 0 Wed Nov 11 20:32:21 2020 12" for HMAC authentication
jingle-tunes 24:13 net_route_v4_best_Dw query 0 Wed Nov 11 21:10:41 2020
note_from_mcskidy.txt route v4_best_Nw resu 143 Wed Nov 11 21:12:07 2020
[22-06-25 14:24:13] ROUTE_GATEWAY 10.0.2.2/255.255.155.155 IFACE=eth0 HWADDR=08:00:27:50:4c:14
[22-06-25 14:24:13] 10252564 blocks of size 1024.0 5369080 blocks available
smb: > dir 14:24:13 net_iface_mtu_set: mtu 1500 for tun0
. 22-06-25 14:24:13 net_iface_up: set Dmdu up 0 Wed Nov 11 21:12:07 2020
.. 22-06-25 14:24:13 net_addr_v4_add: D.8.93.1.0 0 Wed Nov 11 20:32:21 2020
jingle-tunes 24:13 net_route_v4_add: D.0.10.0.0 Wed Nov 11 21:10:41 2020 table 0 metric 1000
note_from_mcskidy.txt ING: this configuration may -- use the auth-nocache option to prevent this
[22-06-25 14:24:13] 10252564 blocks of size 1024.0 5369080 blocks available
smb: > 

```

#### Question 5

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

```
(kali㉿kali)-[~] OPTIONS IMPORT: timers and/or timeouts modified
$ sudo smbclient //10.10.15.64/tbfc-snata
Enter WORKGROUP\root's password: 1 x
tree connect failed: NT_STATUS_ACCESS_DENIED
2022-06-25 14:24:13 OPTIONS IMPORT: route-related options modified
(kali㉿kali)-[~] OPTIONS IMPORT: peer-id set
$ sudo smbclient //10.10.15.64/tbfc-snata
Enter WORKGROUP\root's password: 1 x
Try "help" to get a list of possible commands.
her 'AES-256-CBC' initialized with 256 bit key
smb: \> ls
2022-06-25 14:24:13 Outgoing Data Channel: Using 512 bit message hash '5H4512' for HMAC authentication
. 2022-06-25 14:24:13 Incoming Data Channel: Delt: Ciph 0 Wed Nov 11 21:12:07 2020 with 256 bit key
.. 2022-06-25 14:24:13 Incoming Data Channel: Usr1 0 Wed Nov 11 20:32:21 2020 12" for HMAC authentication
jingle-tunes 2022-06-25 14:24:13 net_route_v4_best_Dw query 0 Wed Nov 11 21:10:41 2020
note_from_mcskidy.txt 2022-06-25 14:24:13 net_route_v4_best_Nw resu143 Wed Nov 11 21:12:07 2020
2022-06-25 14:24:13 ROUTE_GATEWAY 10.0.2.2/255.255.255.0/255.255.255.0/110 HWADDR=00:00:27:50:4c:14
2022-06-25 14:24:13 10252564 blocks of size 1024. 5369080 blocks available
smb: \> dir
2022-06-25 14:24:13 net_iface_mtu_set.mtu 1500 For tuning
. 2022-06-25 14:24:13 net_iface_up: set Dmdu up 0 Wed Nov 11 21:12:07 2020
.. 2022-06-25 14:24:13 net_addr_v4_add: D.8.93.1 0 Wed Nov 11 20:32:21 2020
jingle-tunes 2022-06-25 14:24:13 net_route_v4_add: D.0.10.0. 0 Wed Nov 11 21:10:41 2020 table 0 metric 1000
note_from_mcskidy.txt 2022-06-25 14:24:13 10252564 blocks of size 1024. 5369080 blocks available
smb: \>
```

### Thought Process/Methodology:

I opened the terminal and examined the help options for enum4linux. Then, I ran enum4linux with my IP address. After that, I used smbclient to try to login to the shares on the Samba server and see what share doesn't require a password. After I found out that tbfc-snata doesn't require a password, I logged into it.