PSP0201

Week 3

Writeup

Group Name: DNA

Members

ID	Name	Role
1211102532	DHARVIN SHAH KUMAR BIN MOHAMAD SHAH RAVIN	Leader
1211101179	ALIPH RAIHAN BIN ANUAR	Member
1211102427	NUR NATHIFA BINTI MOHD IZHAR	Member

Day 6: Web Exploitation - Be careful with what you wish for

Tools used : Firefox, OWASP Zap

Solution/Walkthrough:

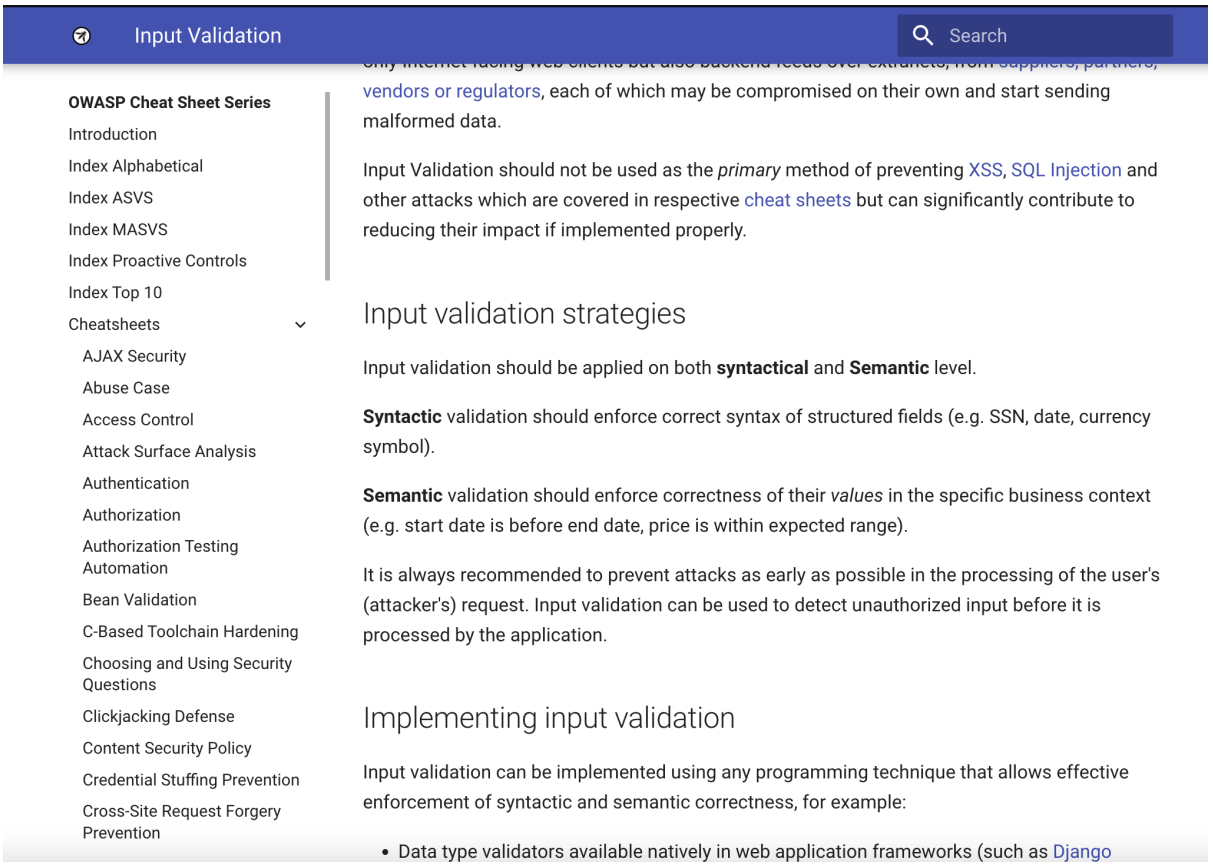
Question 1

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

Examining the OWASP Cheat Sheet the input validation are described as followed:

Syntactic - enforce correct syntax of structured fields

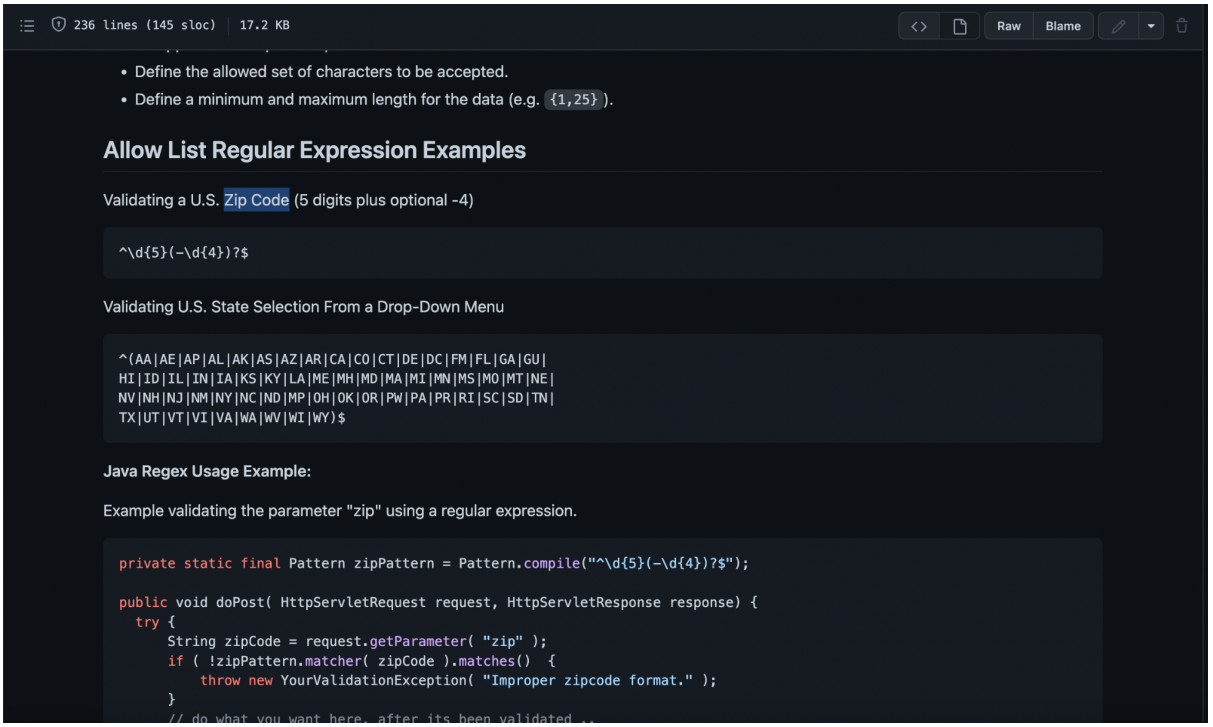
Semantic - enforce correctness of their values in the specific business context



Question 2

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

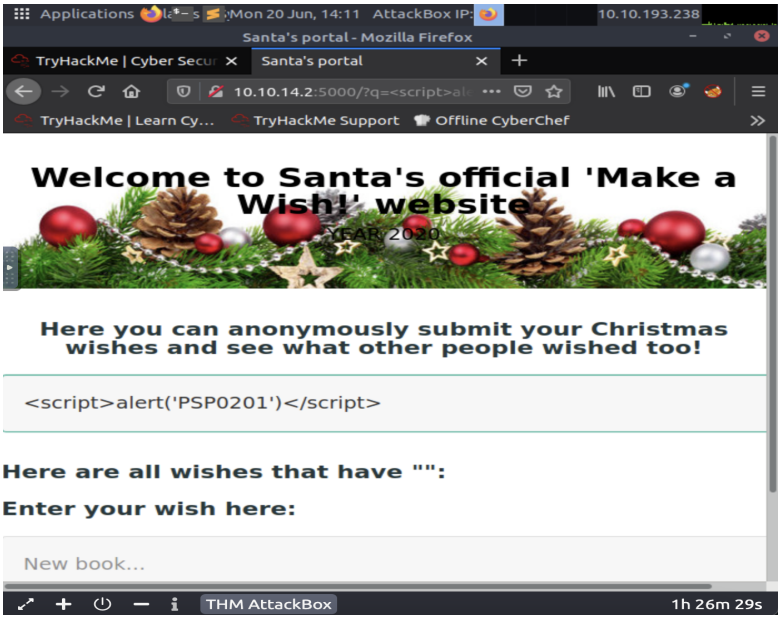
^\d{5}(-\d{4})?$ is the *regex*.

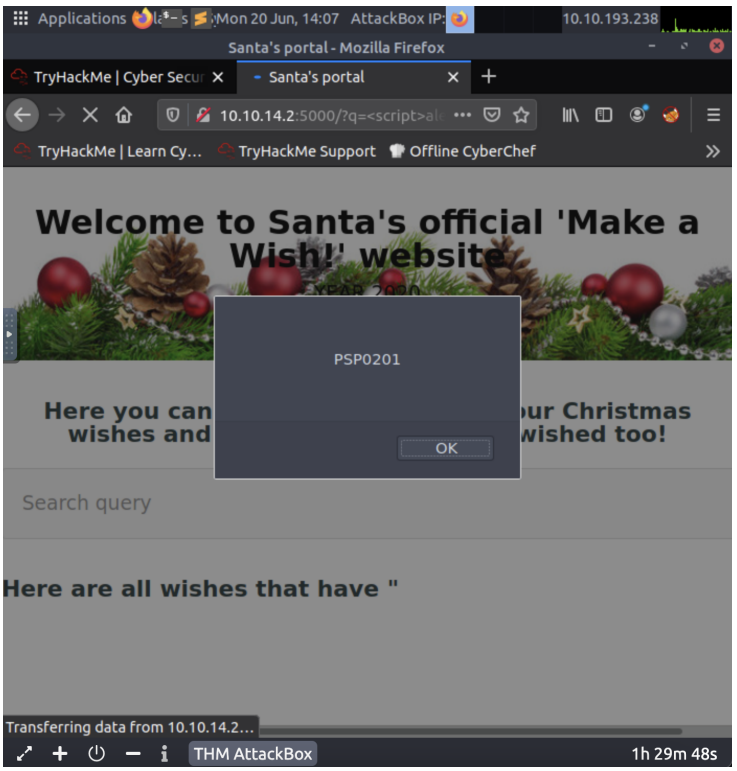


Question 3

What vulnerability type was used to exploit the application?

When we entered <script>alert(“PSP0201”)</script> for an example, in the the query box a pop-up will show that says PSP0201. This means the site is susceptible to **stored cross-site** vulnerability.



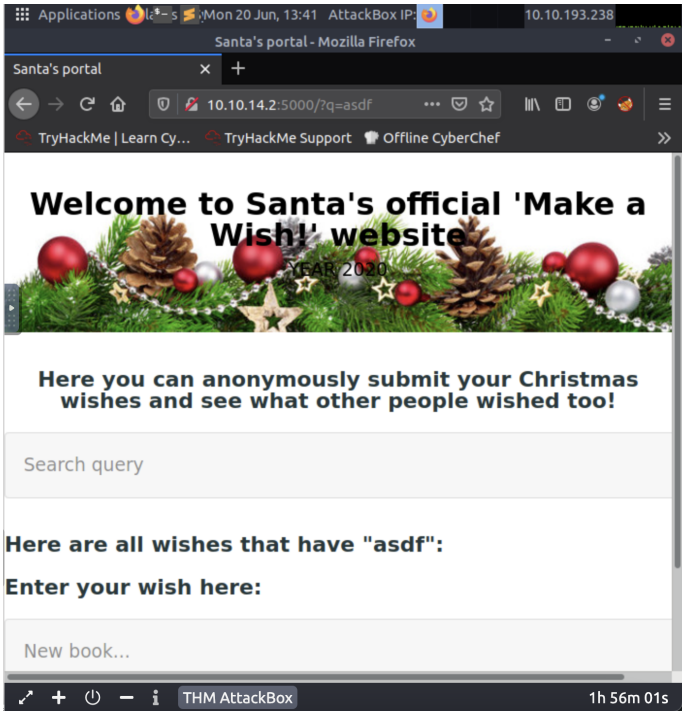


Question 4

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

When we enter a random query the **q** parameter is shown on the search bar.

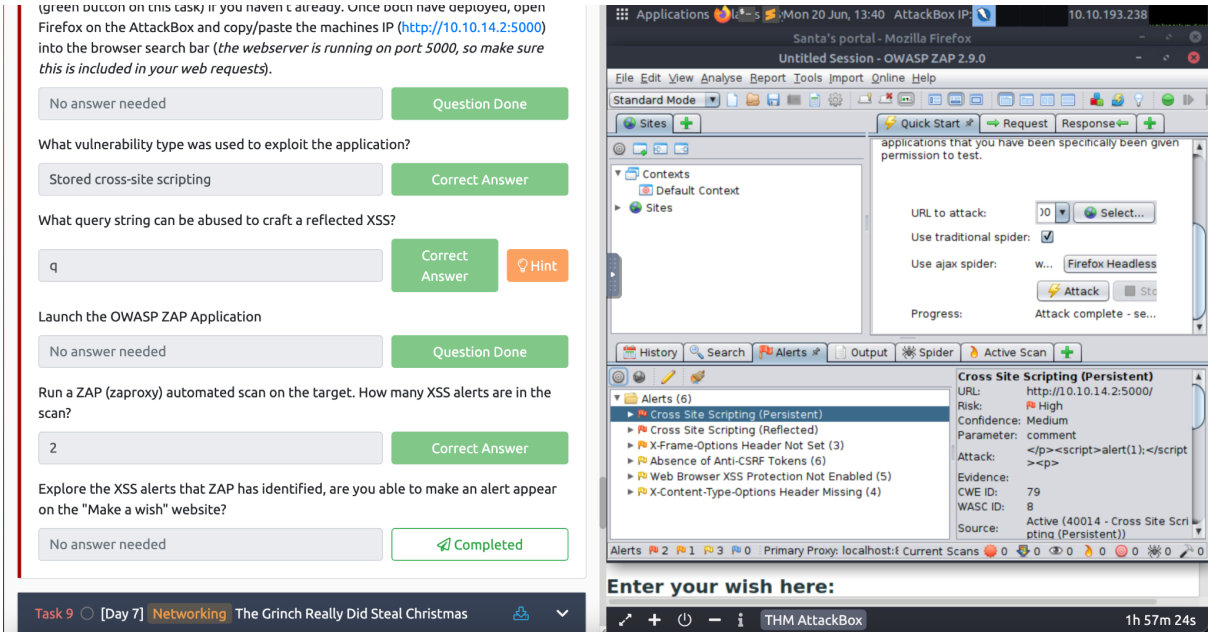
10.10.14.2:5000??**q**=asdf



Question 5

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

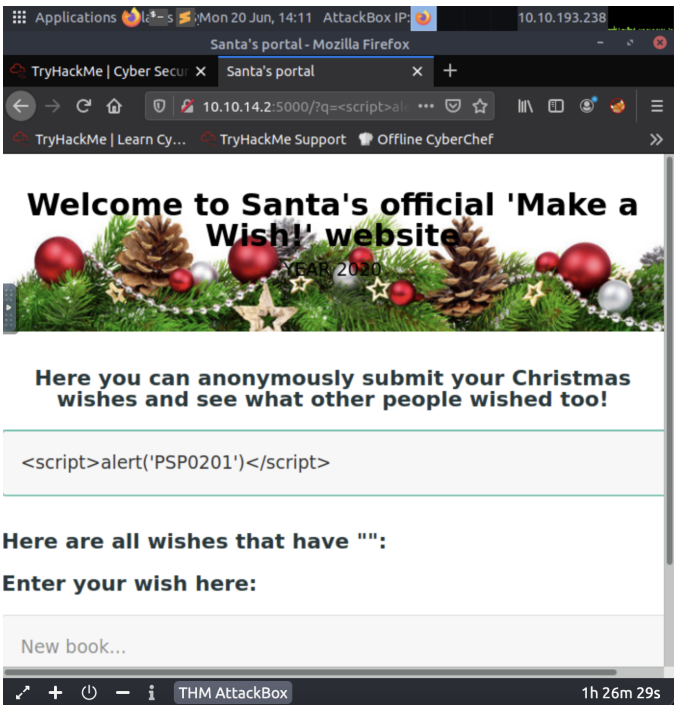
On OWASP zap the automated scan option was selected. The URL 10.10.14.2:5000 was entered in the URL to attack entry. After scanning we went to the alert tab, and we can see **two** XSS alerts of high priority.

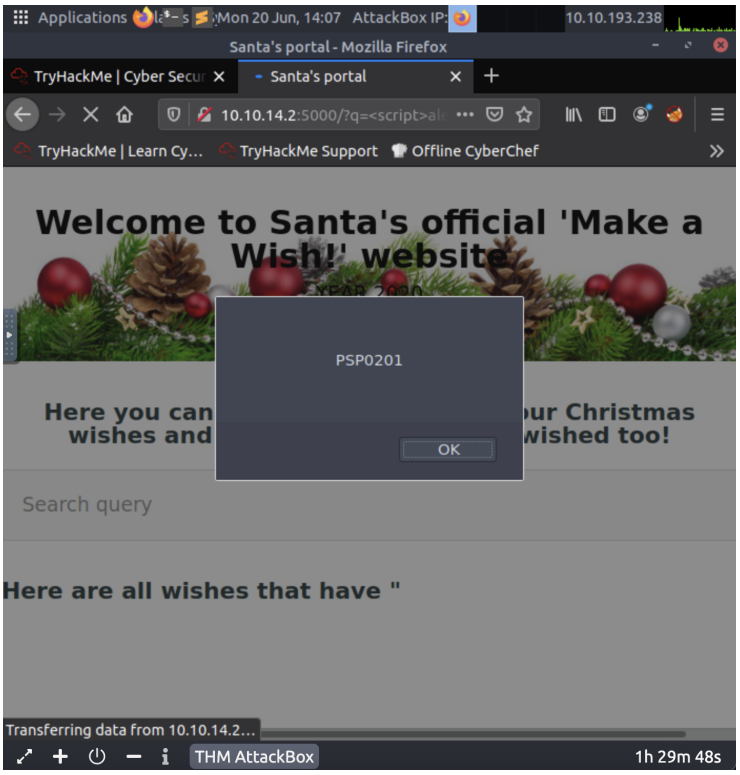


Question 6

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

The proper script format is <script>alert(“PSP0201”)</script> if we follow <script>alert(1)</script> by substituting 1 with the string “PSP0201”.

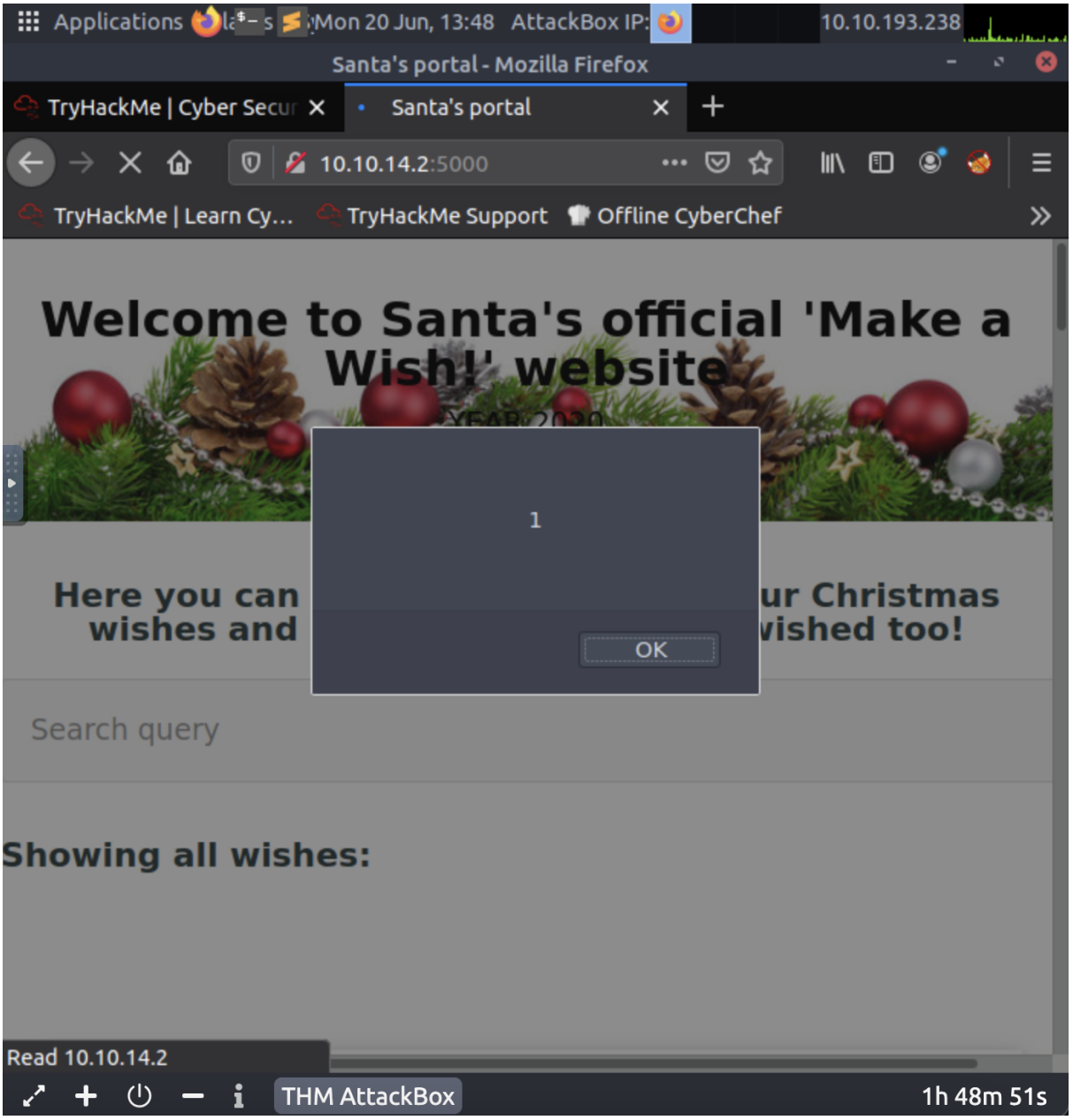




Question 7

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

The pop-up message 1 still appeared when revisiting the site. So **yes** the XSS attack still persists.



Thought process/Methodology:

On the attackbox we opened firefox and entered the site <MACHINE-IP>:5000. There we were welcomed to Santa's official make a wish website. When entering a random query of the site the link of the site displayed the q parameter followed by the search query we entered. We assume at first that this website has a vulnerability which was XSS. By using OWASP zap we can know more about the website and its vulnerabilities. Santa's official make a wish website was scanned and the website was found to have two XSS risks of high priority. To test we entered `<script>alert("PSP0201")</script>` in the query bar and the message "PSP0201" popped up. We further identified that this website is susceptible to stored cross-site scripting.

Day 7: Networking - The Grinch Really Did Steal Christmas

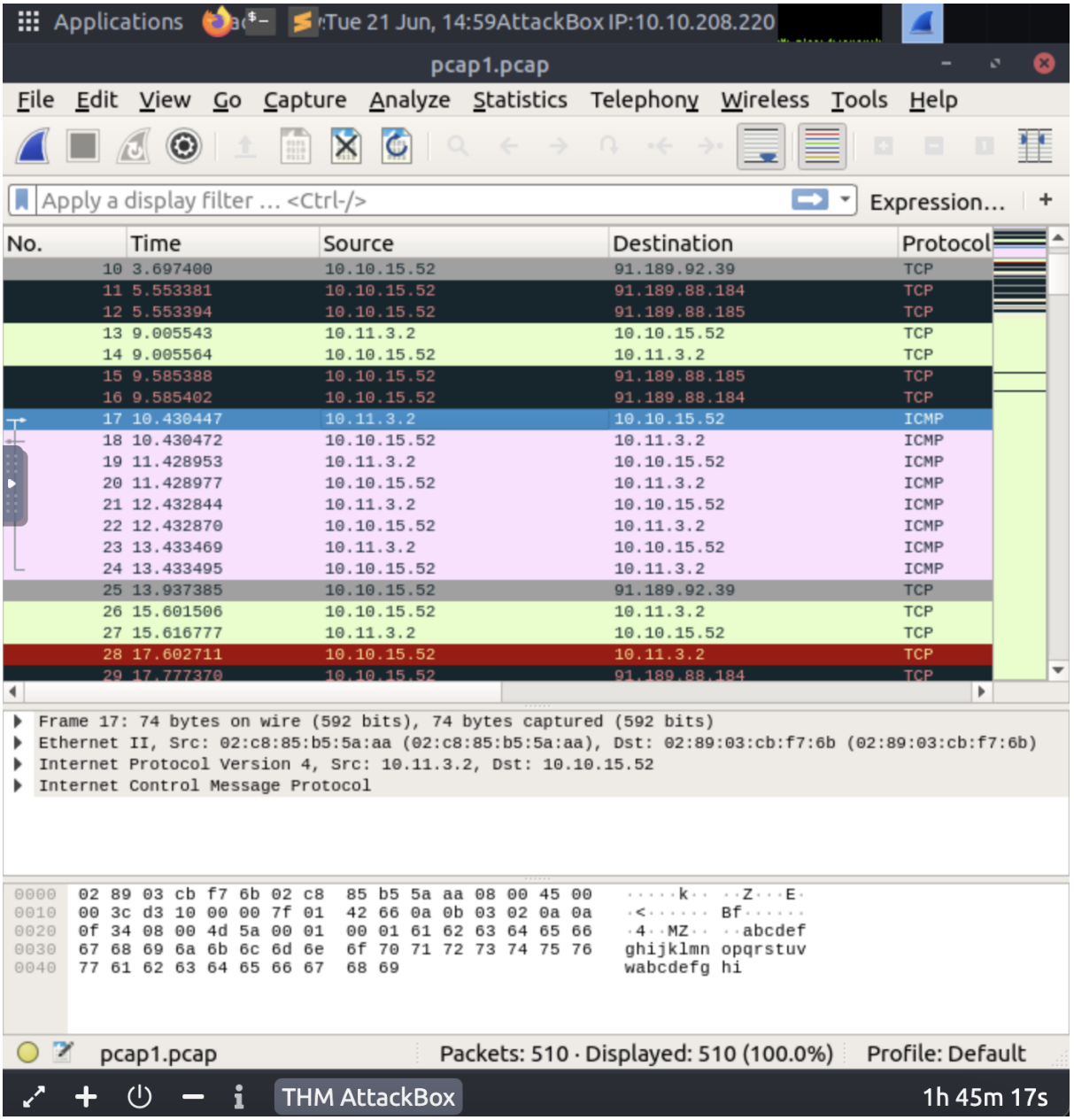
Tools used: Wireshark, Attackbox

Solution/Walkthrough:

Question 1

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

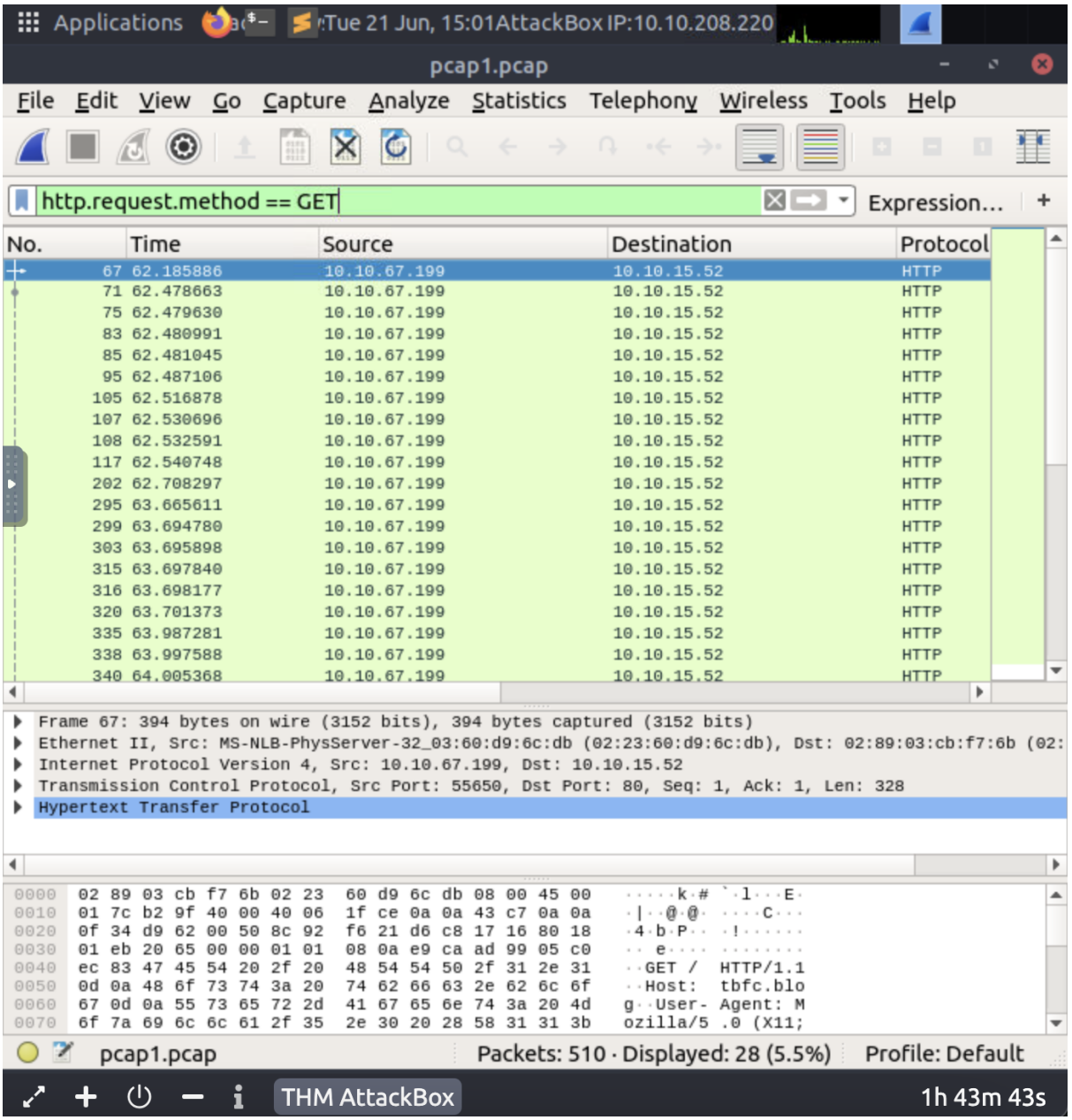
Wireshark has identified that **10.11.3.2** is the IP address that initiated a ping when we looked at the info section.



Question 2

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

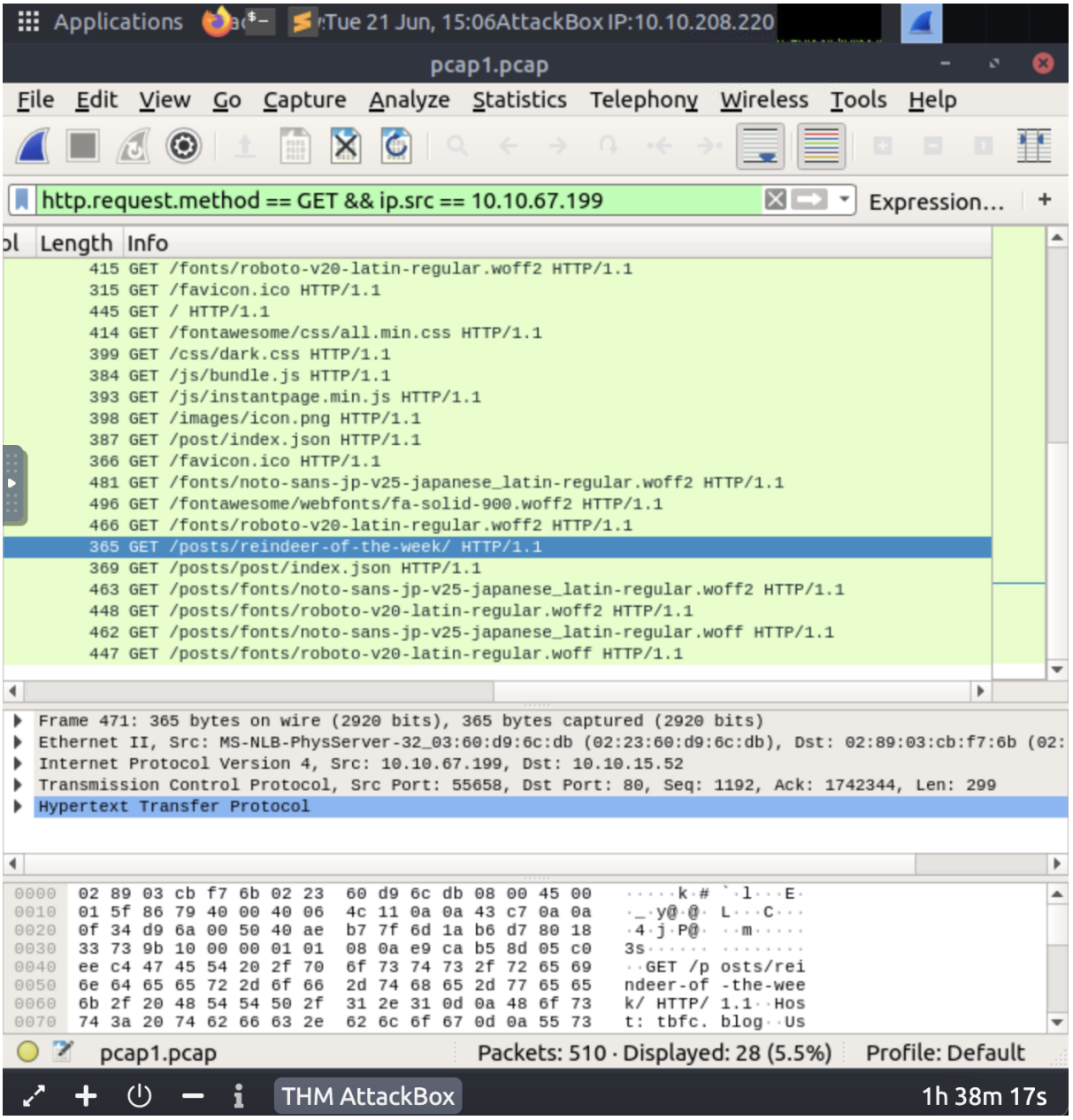
We used the **http.request.method == GET** as the filter.



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?

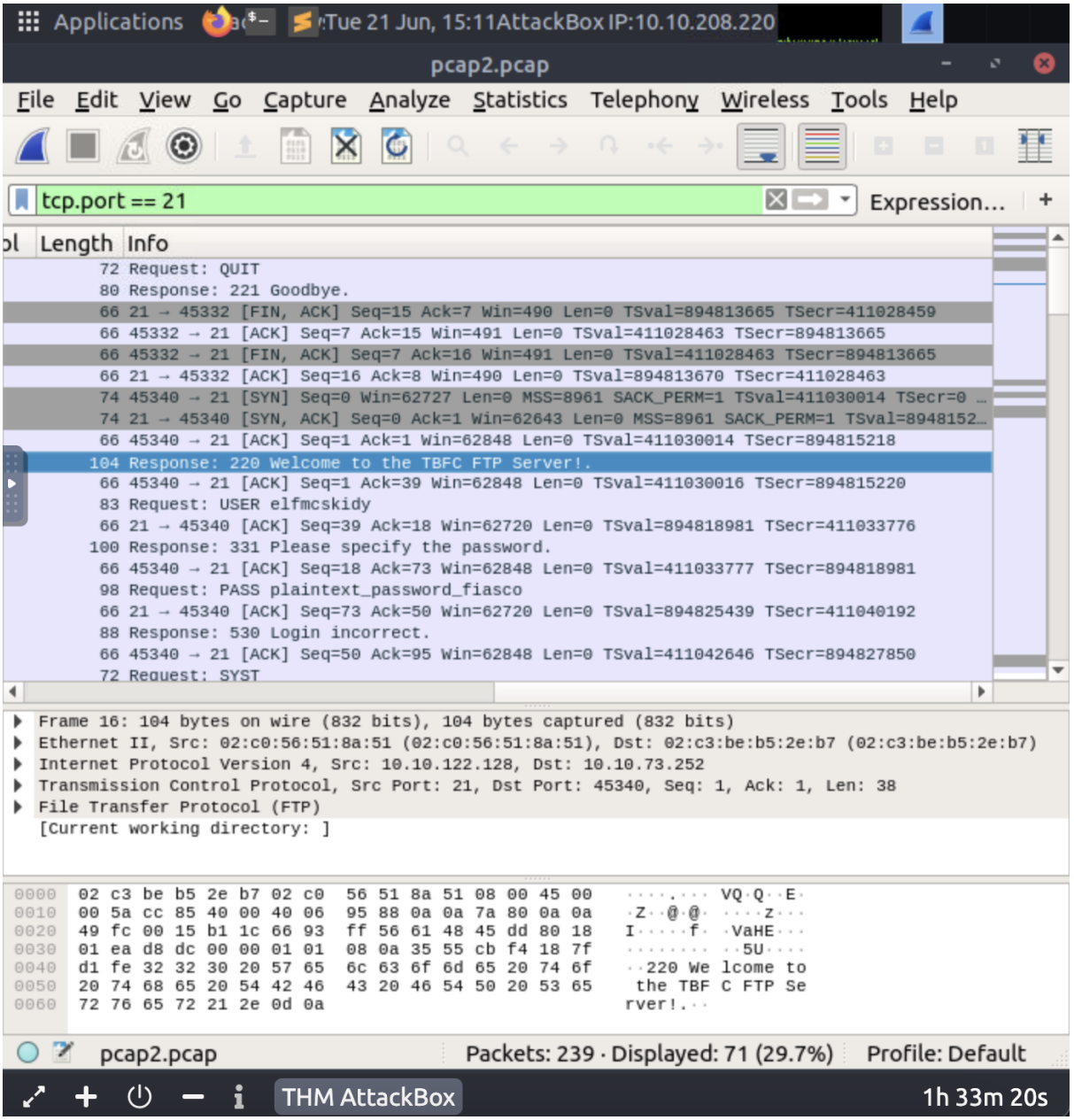
By using the filter **ip.src == 10.10.67.199** and skimming through info we can view the name of the article and sites where IP adress 10.10.67.199 visited.

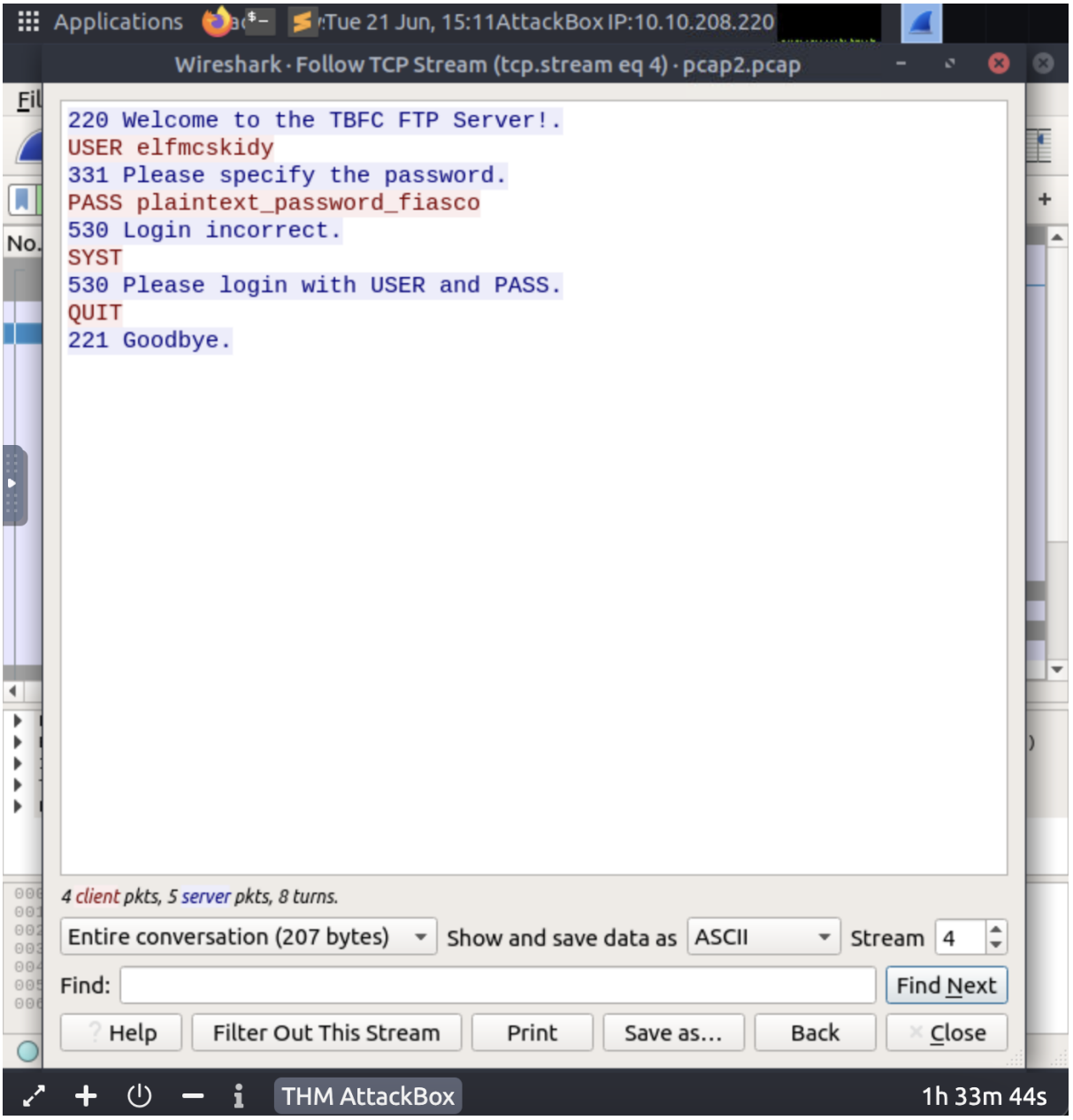


Question 4

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

The password was plaintext_password_fiasco

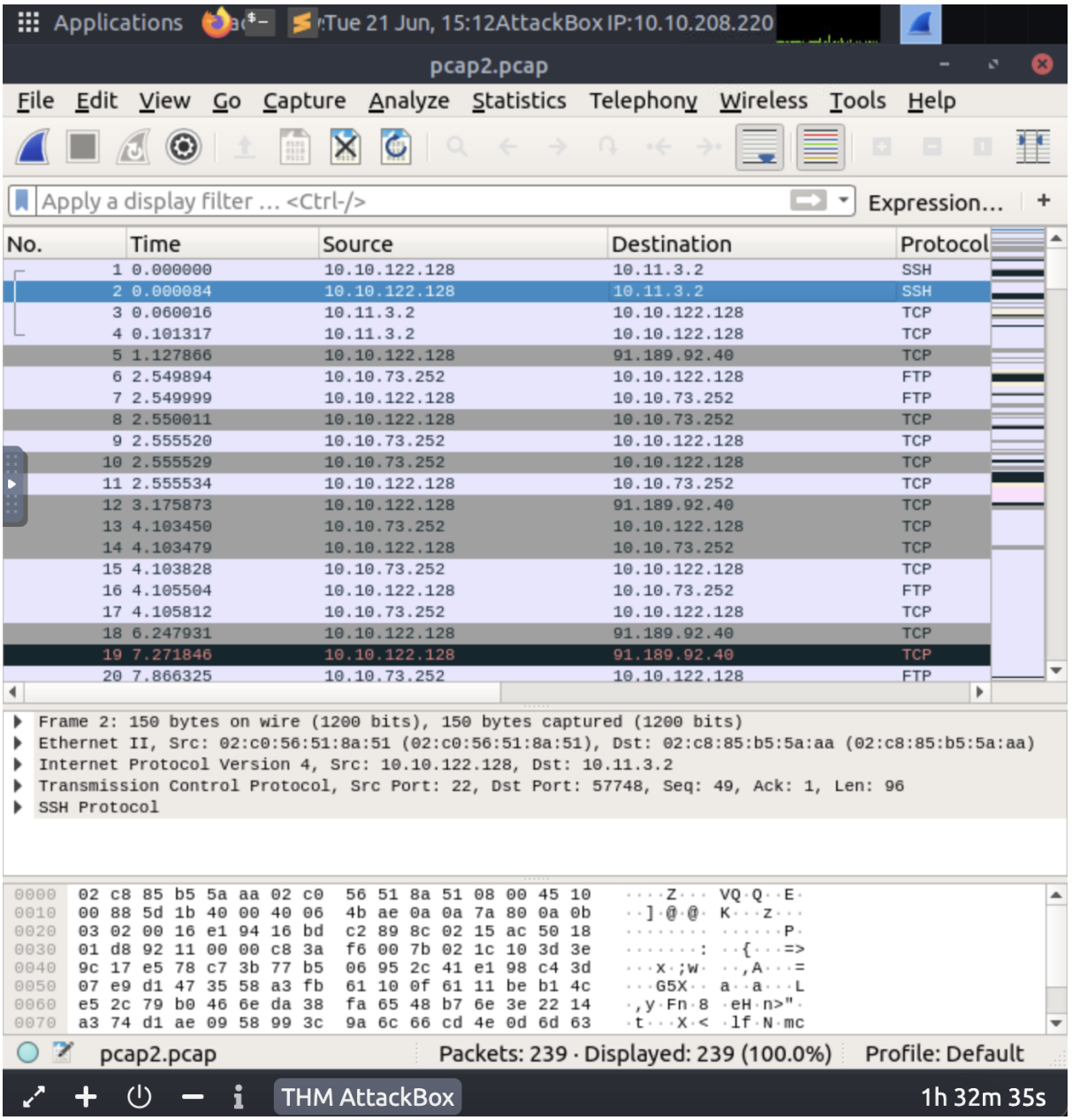

Applications
Tue 21 Jun, 15:11
AttackBox IP:10.10.208.220
pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 21
Expression...
Length Info
72 Request: QUIT
80 Response: 221 Goodbye.
66 21 → 45332 [FIN, ACK] Seq=15 Ack=7 Win=490 Len=0 TSval=894813665 TSecr=411028459
66 45332 → 21 [ACK] Seq=7 Ack=15 Win=491 Len=0 TSval=411028463 TSecr=894813665
66 45332 → 21 [FIN, ACK] Seq=7 Ack=16 Win=491 Len=0 TSval=411028463 TSecr=894813665
66 21 → 45332 [ACK] Seq=16 Ack=8 Win=490 Len=0 TSval=894813670 TSecr=411028463
74 45340 → 21 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=411030014 TSecr=0
74 21 → 45340 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM=1 TSval=8948152
66 45340 → 21 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=411030014 TSecr=894815218
104 Response: 220 Welcome to the TBFC FTP Server!.
66 45340 → 21 [ACK] Seq=1 Ack=39 Win=62848 Len=0 TSval=411030016 TSecr=894815220
83 Request: USER elfmcskidy
66 21 → 45340 [ACK] Seq=39 Ack=18 Win=62720 Len=0 TSval=894818981 TSecr=411033776
100 Response: 331 Please specify the password.
66 45340 → 21 [ACK] Seq=18 Ack=73 Win=62848 Len=0 TSval=411033777 TSecr=894818981
98 Request: PASS plaintext_password_fiasco
66 21 → 45340 [ACK] Seq=73 Ack=50 Win=62720 Len=0 TSval=894825439 TSecr=411040192
88 Response: 530 Login incorrect.
66 45340 → 21 [ACK] Seq=50 Ack=95 Win=62848 Len=0 TSval=411042646 TSecr=894827850
72 Request: SYST
Frame 16: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c3:be:b5:2e:b7 (02:c3:be:b5:2e:b7)
Internet Protocol Version 4, Src: 10.10.122.128, Dst: 10.10.73.252
Transmission Control Protocol, Src Port: 21, Dst Port: 45340, Seq: 1, Ack: 1, Len: 38
File Transfer Protocol (FTP)
[Current working directory:]
0000 02 c3 be b5 2e b7 02 c0 56 51 8a 51 08 00 45 00
0010 00 5a cc 85 40 00 40 06 95 88 0a 0a 7a 80 0a 0a
0020 49 fc 00 15 b1 1c 66 93 ff 56 61 48 45 dd 80 18
0030 01 ea d8 dc 00 00 01 01 08 0a 35 55 cb f4 18 7f
0040 d1 fe 32 32 30 20 57 65 6c 63 6f 6d 65 20 74 6f
0050 20 74 68 65 20 54 42 46 43 20 46 54 50 20 53 65
0060 72 76 65 72 21 2e 0d 0a
pcap2.pcap
Packets: 239 · Displayed: 71 (29.7%)
Profile: Default
THM AttackBox
1h 33m 20s


Applications
Tue 21 Jun, 15:11
AttackBox IP:10.10.208.220
Wireshark · Follow TCP Stream (tcp.stream eq 4) · pcap2.pcap
220 Welcome to the TBFC FTP Server!.
USER elfmcskidy
331 Please specify the password.
PASS plaintext_password_fiasco
530 Login incorrect.
SYST
530 Please login with USER and PASS.
QUIT
221 Goodbye.
4 client pkts, 5 server pkts, 8 turns.
Entire conversation (207 bytes)
Show and save data as
ASCII
Stream
4
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close
THM AttackBox
1h 33m 44s

Question 5

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

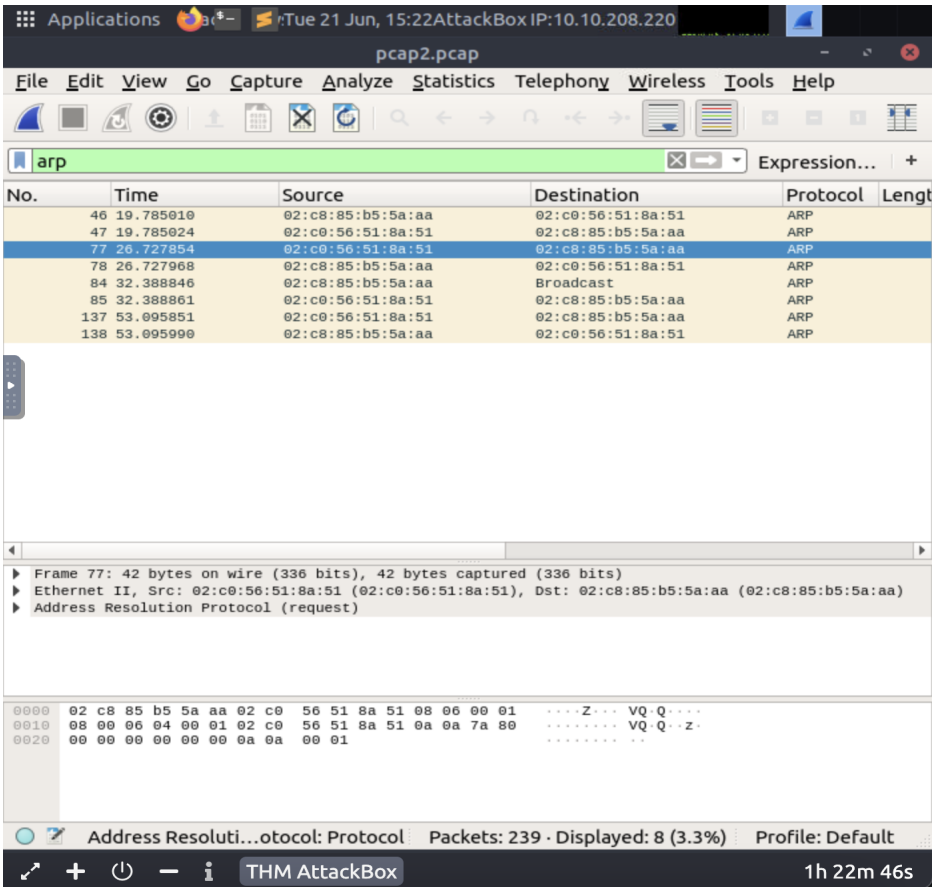
SSH

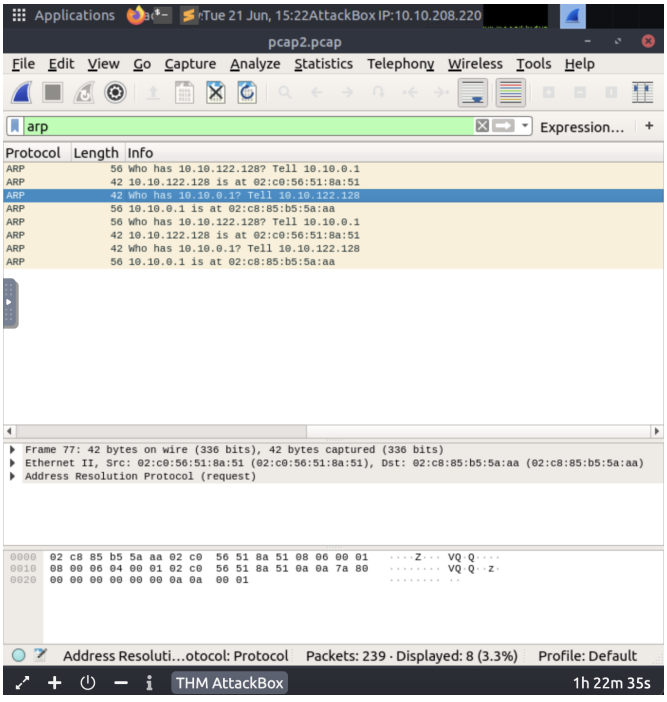


Question 6

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

02:c:56:51:8a:51

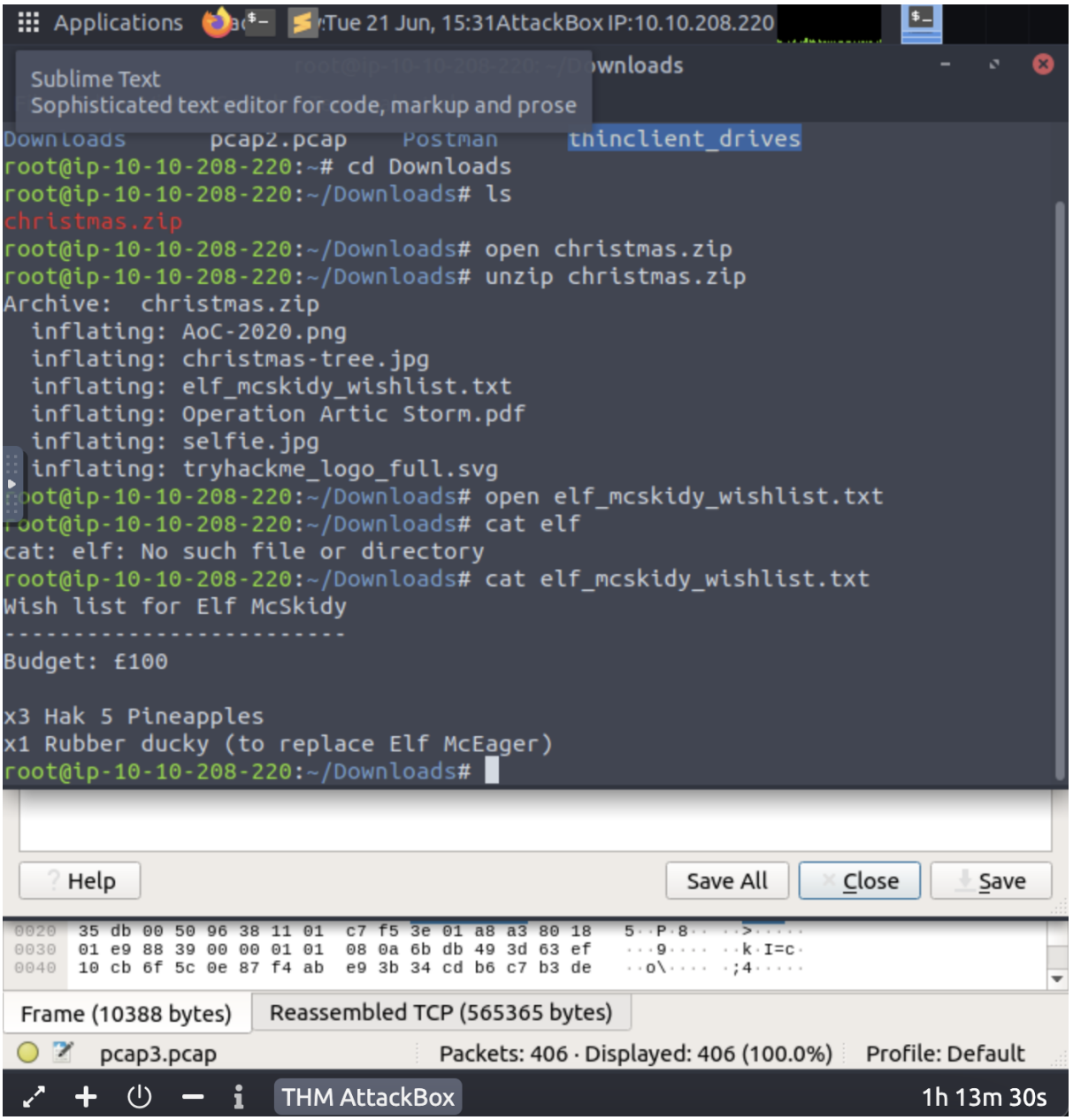




Question 7

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

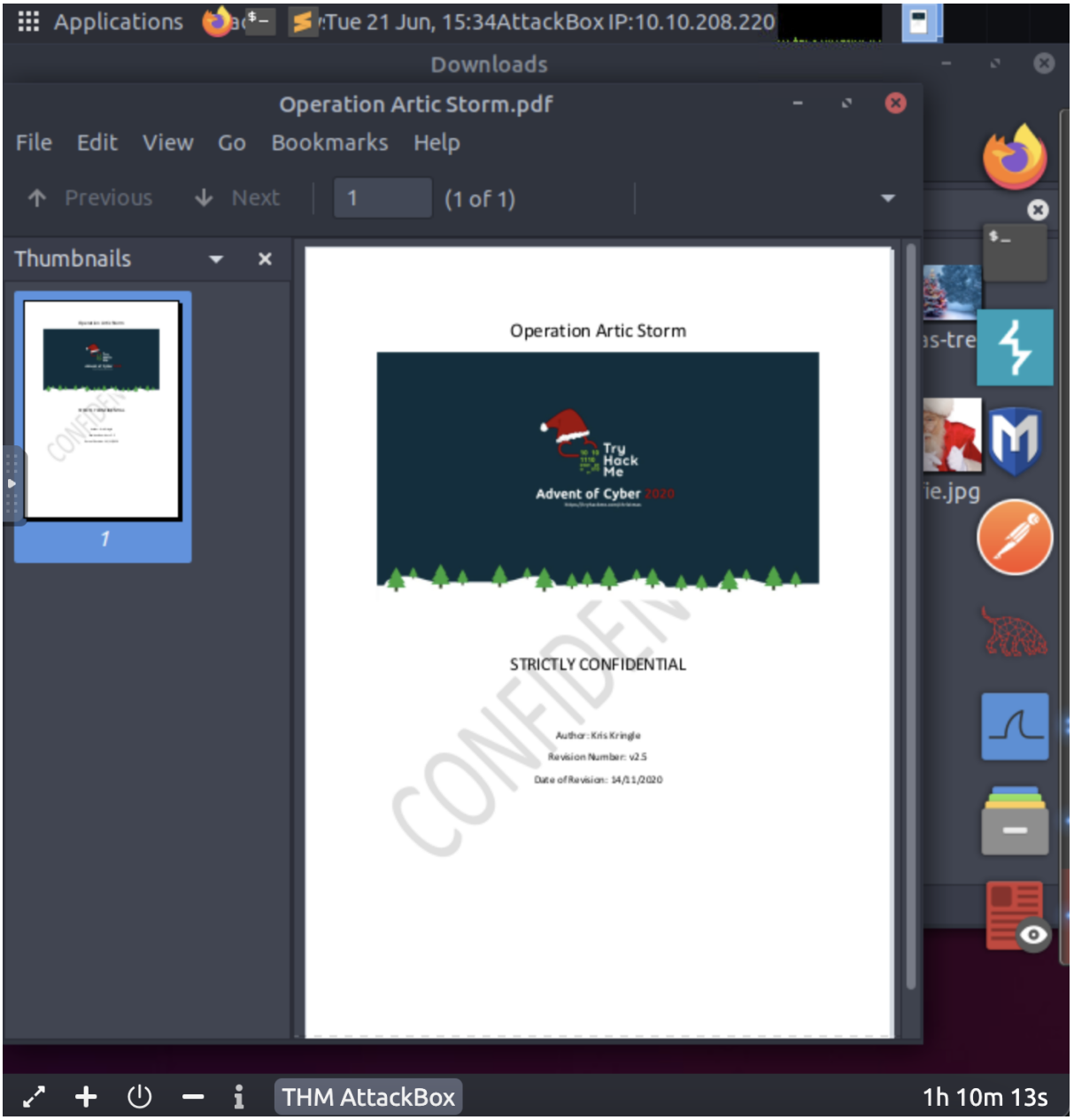
The pdf file states that a rubber ducky was to replace Elf McEager.



Question 8

Who is the author of Operation Artic Storm?

Kris Kringle.



Methodology/Thought process:

We are using wireshark to find IP addresses and what they were assigned to. We analysed the files in aocpcaps.zip.To help analyse FTP traffic in wireshark we can use filters and various tools to help identify users' activities and find information from their IP addresses. First, we open pcap1.pac on wireshark. On the file, pcap1.pac to find the IP that initiated a ping we used wireshark which identified the

IP address. We surveyed the info section and found that IP 10.11.3.2 was the one that initiated the ping. We only wanted to see HTTP GET requests thus the correct filter to use is “http.request.method == GET” which helps filter all the irrelevant requests and display only HTTP GET requests. To find the article that the IP address 10.10.67.199 visited we can add the filter “ip.src == 10.10.67.199” to easily locate the IP address. Skimming through the info section we can view the sites that they have visited. We found that the article they visited was reindeer-of-the-week. In pcap2.cap we wanted to know what password was leaked during the login process. The file contains a lot of irrelevant data. So to help sort it we can use a filter. The FTP uses the TCP protocol and runs on port 21. So we’d use the “tcp.port == 21” filter to find the leaked password in the FTP traffic. We found a successful login access thus we followed its TCP stream. The password as well as other info are displayed. The password that was leaked was plaintext_password_fiasco. On the FTP traffic we can view that the protocol that was encrypted was SSH. Now on pcap3.cap we want to GET the christmas.zip among the FTP traffic. We extract the request by exporting objects HTTP and saved the file. We extracted the christmas.zip file and view its content. One of the files named elf_mcskidy_wishlist.txt says that a rubber ducky will be used to replace Elf McEager and another file stated that Kris Kringle was the author of the Operation Arctic Storm.

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

Solution/walkthrough:

Question 1

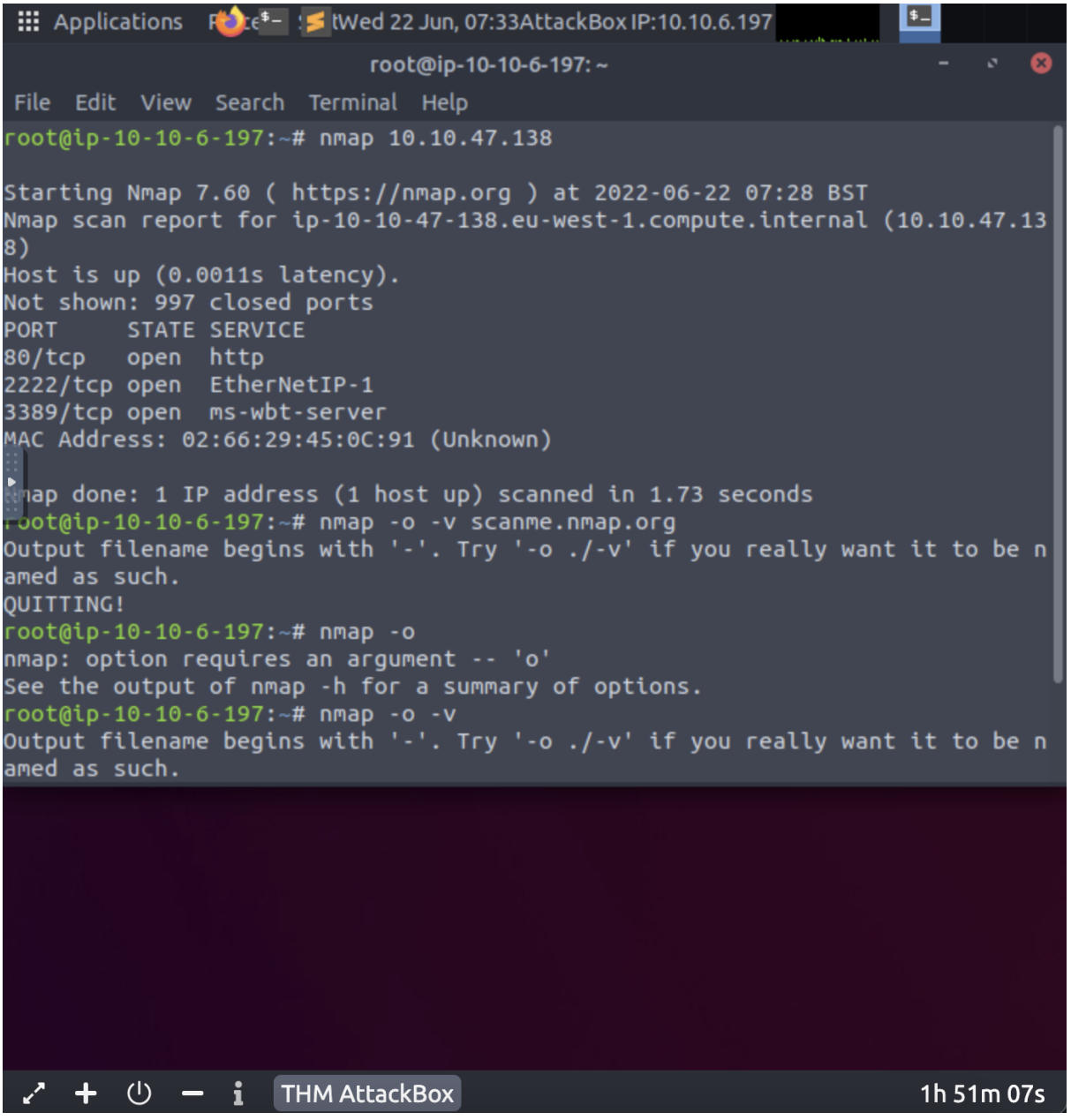
When was Snort created?

In 1998

Question 2

Using Nmap on MACHINE_IP, what are the port numbers of the three services running?

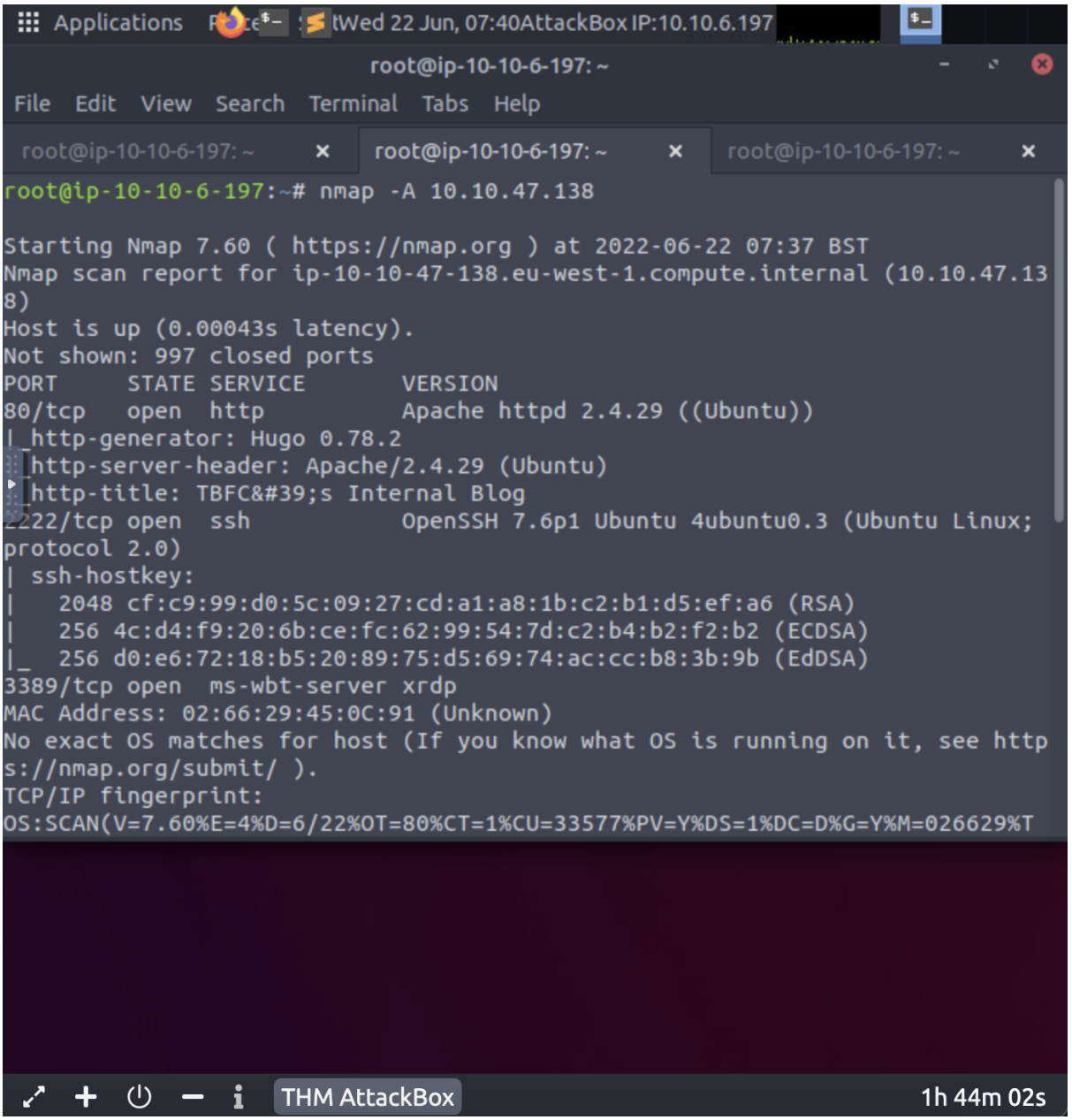
We entered Nmap <machine_IP> to find the port numbers which were **80, 2222 and 3389.**



Question 3

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

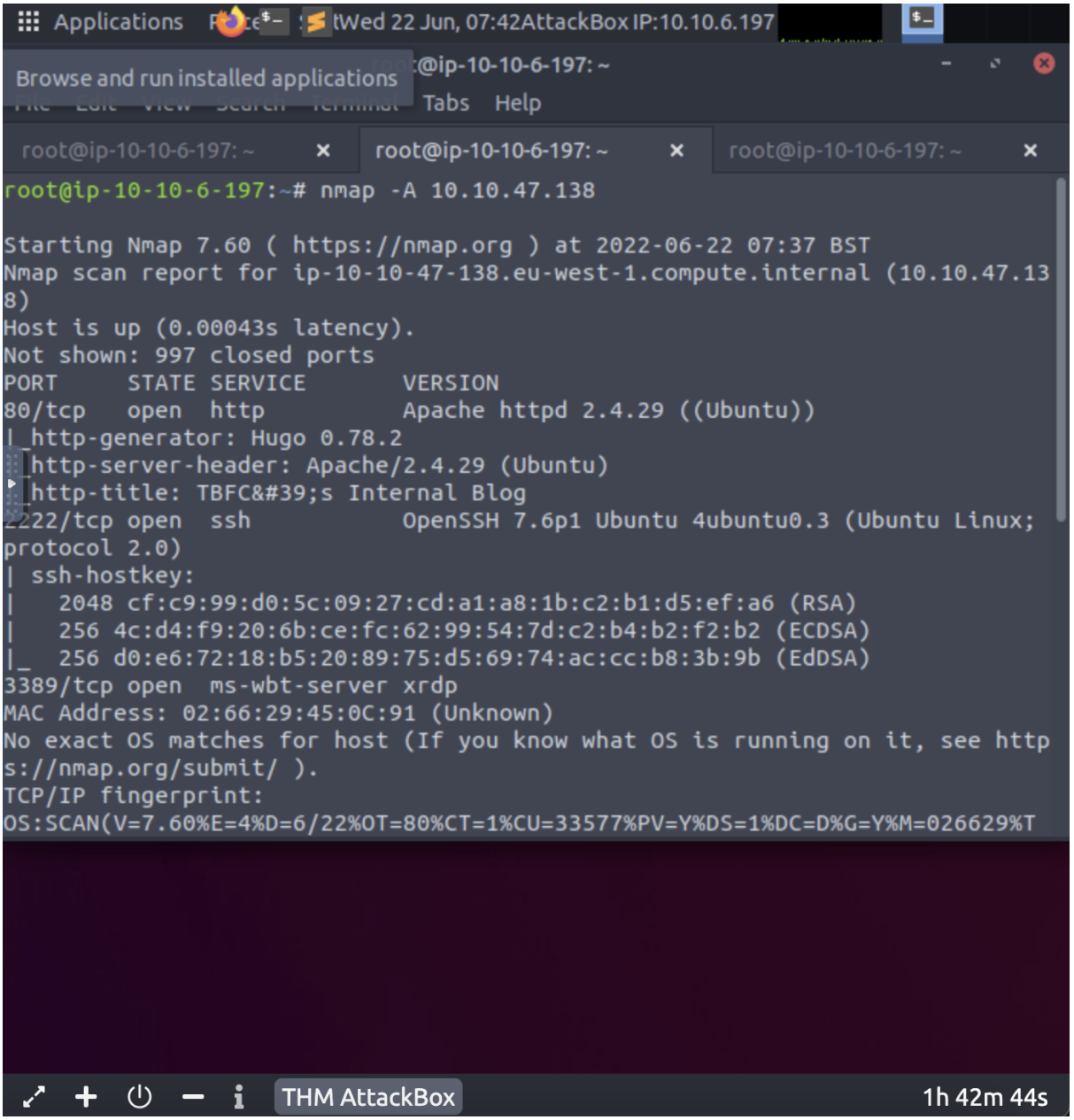
Ubuntu was the most likely Linux distribution that was running.



Question 4

What is the version of Apache?

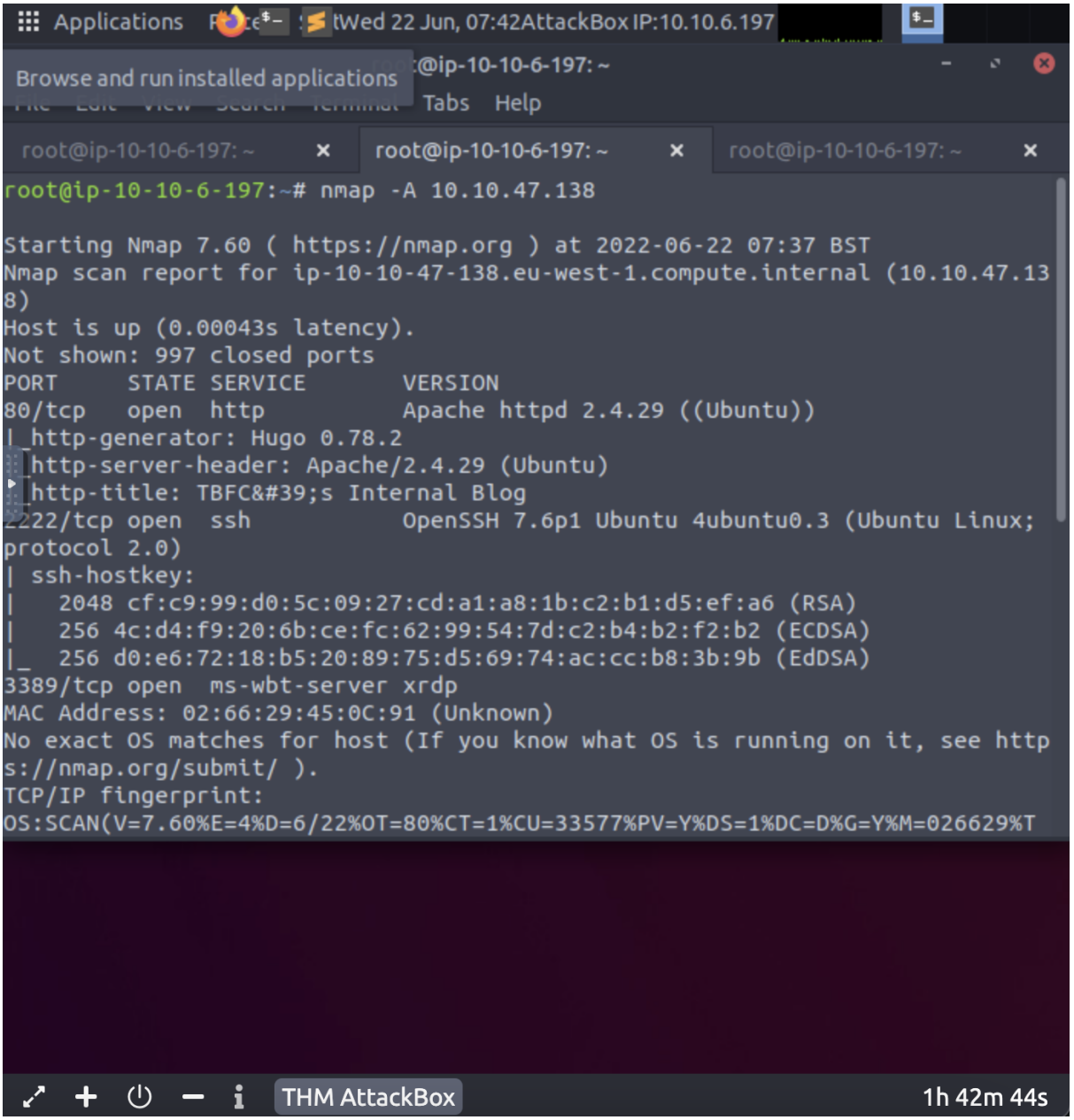
The apache version is **2.4.29**.



Question 5

What is running on port 2222?

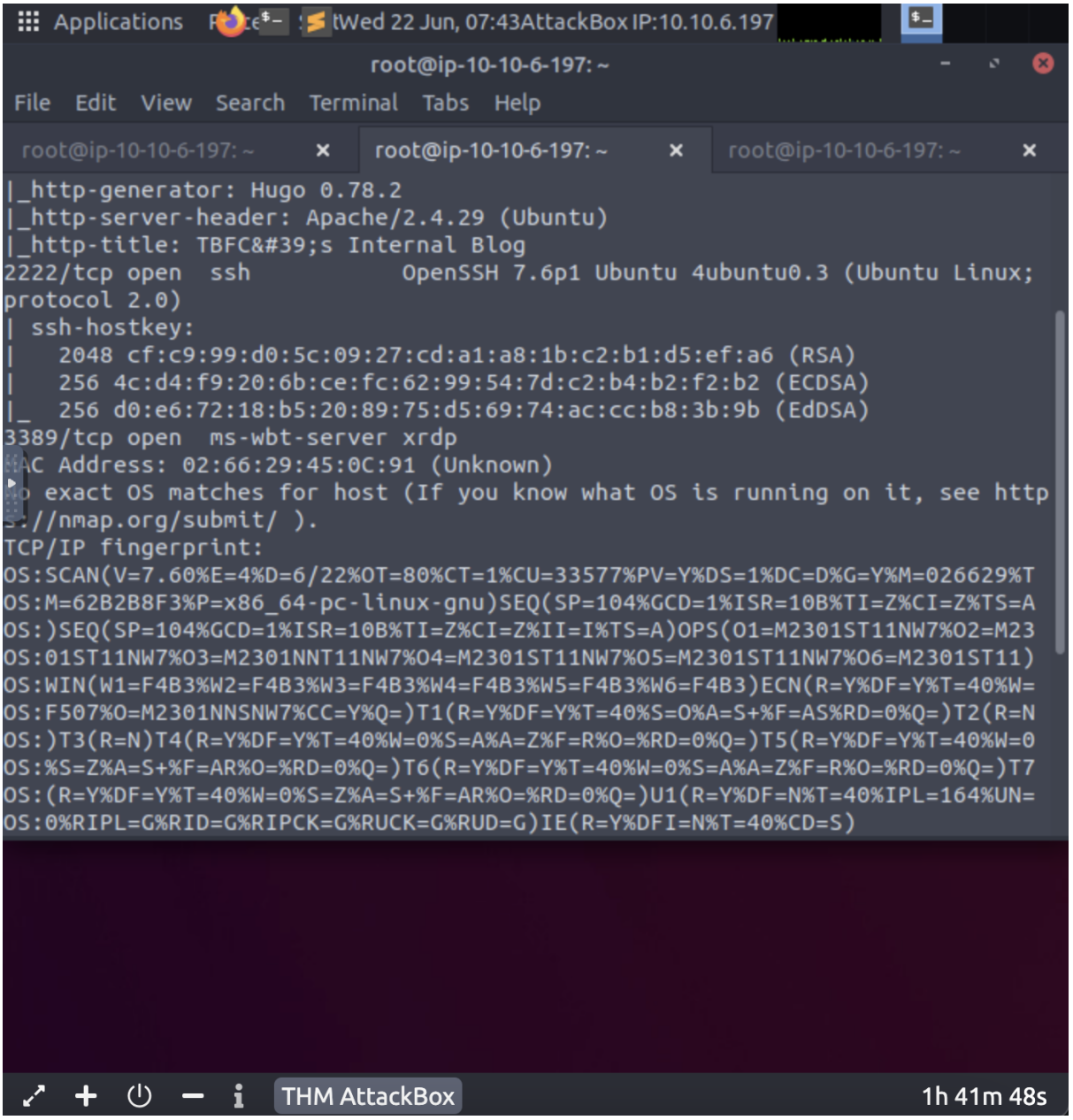
SSH was the service that was running on port 2222.



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?

It is a **blog**.



Methodology/Though process:

We use the Nmap scanner to gather information during the gathering information stage of penetration testing. We also use various scan types that are useful for certain information we want to gather. Nmap scans can find port connection services, and devices connected to a network and give information about the operating systems they are running. We use the aggressive or -A scan type which is just a combination of the -O, -sV and -sC scan types to help find the information we need. We entered Nmap then the flag -A scan type followed by the host's IP address in the terminal to find information such as the name of the Linux distribution which was Ubuntu, port connections where for example port 2222 was running SSH and apache version which was 2.4.29.

Day 9 : Anyone can be Santa!

Tool used : Attackbox

Solution/walkthrough:

Question 1

What are the directories you found on the FTP site?

backups, elf_workshops, human resources, public

```
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    6 65534    65534        4096 Nov 16  2020 .
drwxr-xr-x    6 65534    65534        4096 Nov 16  2020 ..
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

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

Public

First, log into FTP server as “anonymous”

```
root@ip-10-10-135-5: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-135-5:~# ftp 10.10.123.129
Connected to 10.10.123.129.
220 Welcome to the TBFC FTP Server!.
Name (10.10.123.129:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    6 65534    65534        4096 Nov 16  2020 .
drwxr-xr-x    6 65534    65534        4096 Nov 16  2020 ..
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.
```

At the directory, one that is available for anonymous users to access is public

Question 3

What script gets executed within this directory?

Backup.sh

```
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 .
drwxr-xr-x    6 65534    65534        4096 Nov 16  2020 ..
-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>
```

We changed the directories to public and looked at the content and we can see backup.sh

Question 4

What movie did Santa have on his Christmas shopping list?

The Polar Express

We used get command

```
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 (12.4074 kB/s)
ftp>
```

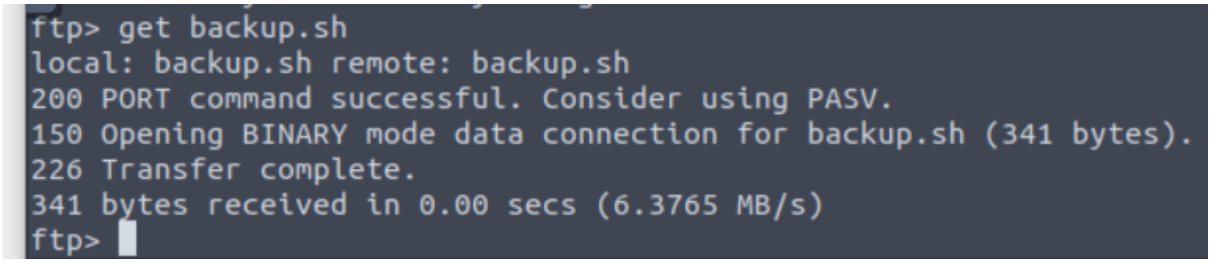
```
root@ip-10-10-135-5: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-135-5:~# ls
Desktop    Instructions  Postman  Scripts          thinclient_drives
Downloads  Pictures      Rooms    shoppinglist.txt  Tools
root@ip-10-10-135-5:~# cat shoppinglist.txt
The Polar Express Movie
root@ip-10-10-135-5:~#
```

Question 5

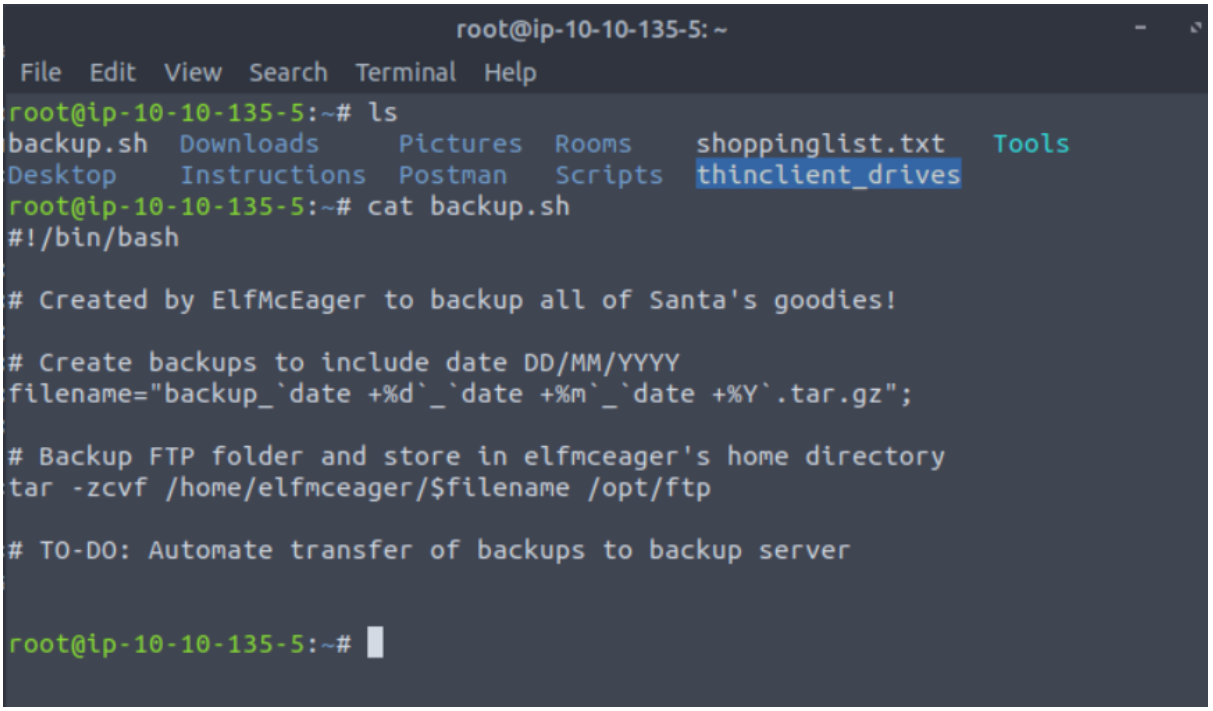
re-upload this script to contain malicious data (just like we did in section 9.6. Output the contents of /root/flag.txt!

THM{even_you_can_be_santa}

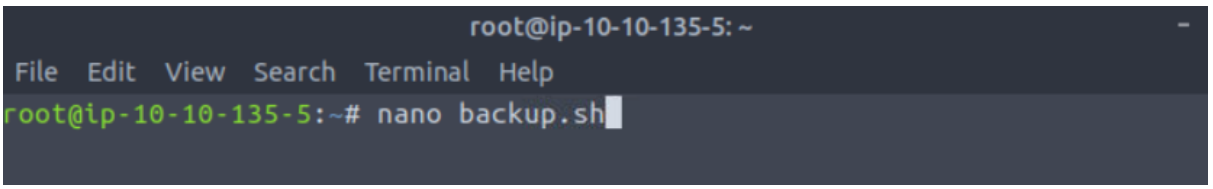
We grab file from FTP server



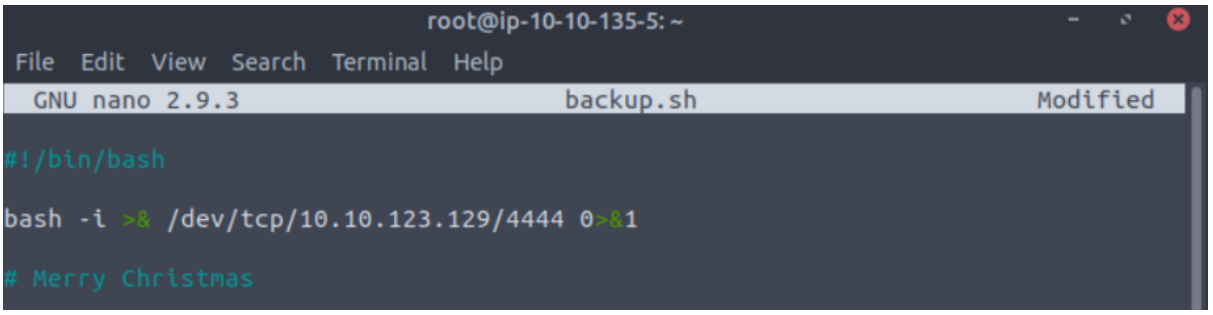
We can see the contents



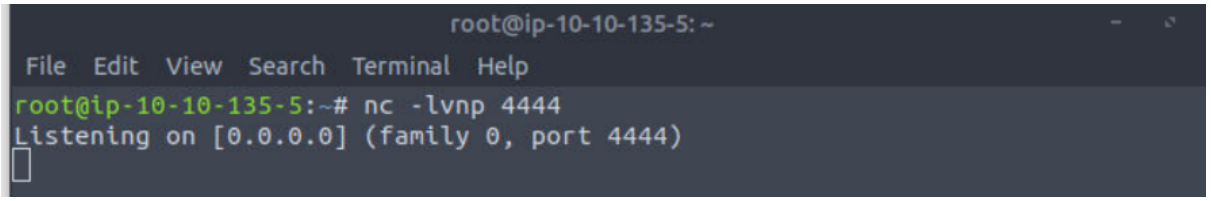
Open up nano



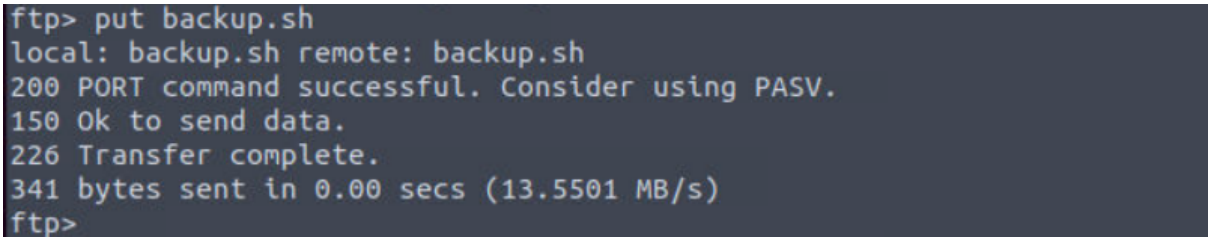
We use the reverse shell cheat sheet



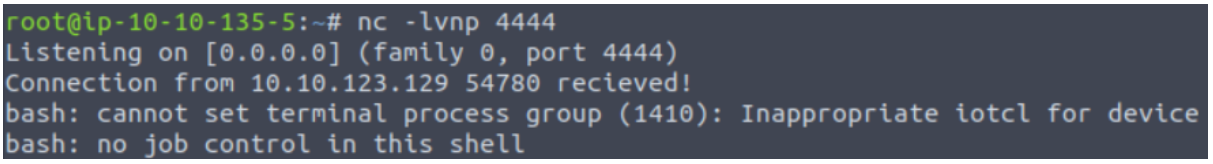
Set up listener with netcat



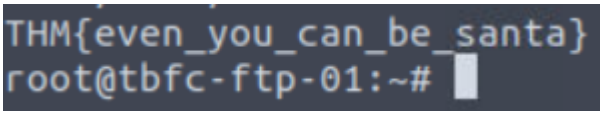
Upload to ftp server using put command



In a little while, listener will receive connection



navigate the flag.txt.file and the flag will show up



Methodology/Though process: As we logged in the ftp with a given ip address using 'anonymous' to have anonymous access. At the directory, one that is available for anonymous users to access is public.we changed the directory into public with 'dc public'. We use ls in order to be able to list the contents and backup.sh and shoppinglist.txt will come out. We use the get command; get shoppinglist.txt, type is ls to see the list and use cat shopping.txt to see the name of the movie. First is to

take a file from ftp server and use ls to see the contents. We open them up using nano and use reverse shell cheat sheet. But before that, we need to set up listener with netcat. After that we use put command and after a while, listener will receive a connection and lastly, we navigate to flag.txt.file and the flag will show up.

Day 10 : Don't be SElfish !

Tool used : enum4linux

Solution/walkthrough:

Question 1

We used the following command to see all users.

```
root@ip-10-10-120-212:~# enum4linux -U 10.10.221.211
WARNING: polenum.py is not in your path.  Check that package is installed and your PATH is sane.
WARNING: ldapsearch is not in your path.  Check that package is installed and your PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Dec 1
1 00:02:30 2020

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.221.211
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

Question 2

Three users are present.

```
 ==============================
|    Users on 10.10.221.211    |
 ==============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy       Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager       Name: elfmceagerDesc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson    Name:   Desc:

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

Question 3

Four shares are present.

```
root@ip-10-10-120-212:~# enum4linux -S 10.10.221.211
WARNING: polenum.py is not in your path.  Check that package is installed and your PATH is sane.
WARNING: ldapsearch is not in your path.  Check that package is installed and your PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Dec 1
```

```
 ========================================
|    Share Enumeration on 10.10.221.211    |
 ========================================
WARNING: The "syslog" option is deprecated

        Sharename       Type      Comment
        ---------       ----      -------
        tbfc-hr         Disk      tbfc-hr
        tbfc-it         Disk      tbfc-it
        tbfc-santa      Disk      tbfc-santa
        IPC$            IPC       IPC Service (tbfc-smb server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        TBFC-SMB-01          TBFC-SMB
```

Question 4

Without a password, we were unable to access the IT or HR files, but it appears that the tbfc-Santa share is not password-protected.

```
root@ip-10-10-120-212:~# smbclient //10.10.221.211/tbfc-hr
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-120-212:~# smbclient //10.10.221.211/tbfc-it
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-120-212:~# smbclient //10.10.221.211/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \>
```

Question 5

The right response turned out to be "jingle-tunes." Even though that directory was empty, we did read the note that was on the sharing.

```
root@ip-10-10-120-212:~# cat note_from_mcskidy.txt
Hi Santa, I decided to put all of your favourite jingles onto this share - allowing you acces
s it from anywhere you like! Regards ~ ElfMcSkidy
root@ip-10-10-120-212:~#
```