

Report PSP0201 T2130 - Tutorial Week 3

Group: **Marceline**

ID	Name	Role
1211100899	Muhammad Shahril Aiman	Leader
1211101533	Muhammad Aniq Fahmi	member
1211101303	Aiman Faris	member
1211102759	Muhammad Zaquan	member

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

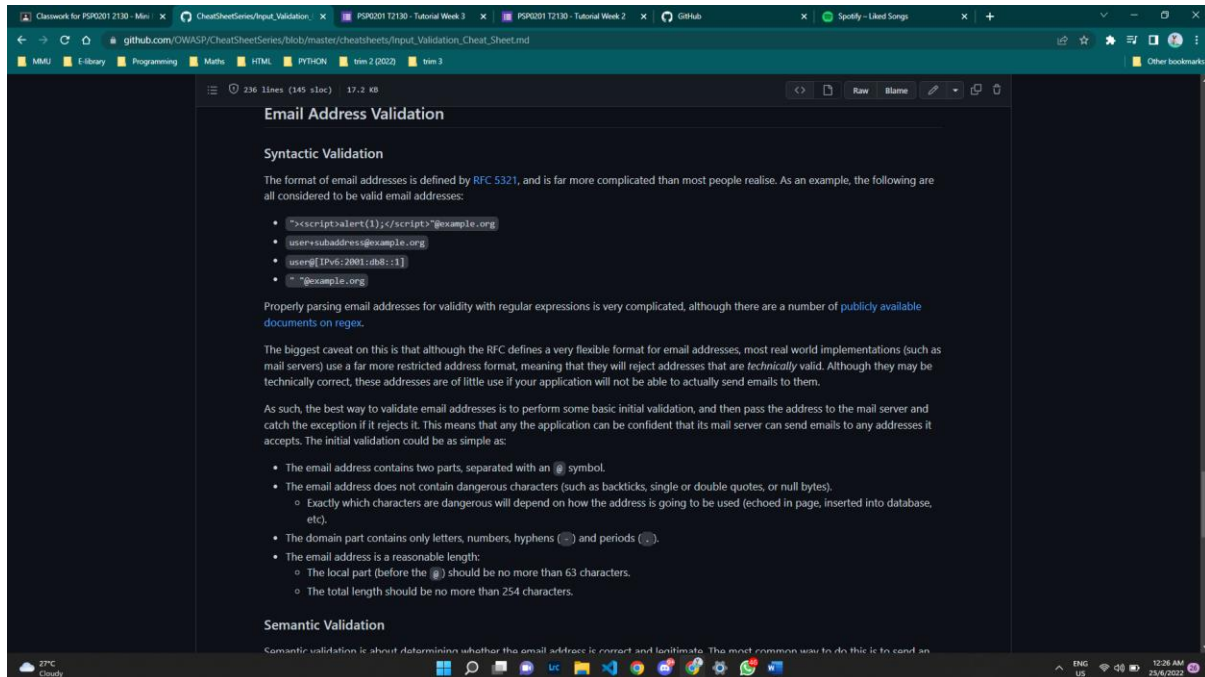
Tools used: Kali Linux, Firefox, OWASP

Solution/walkthrough:

Question 1: Examine the OWASP Cheat Sheet. Match the input validation level with the correct description.

-enforce correct syntax of structured fields (SYNTHETIC)

-enforce correctness of their values in the specific business context (SEMANTIC)



QUESTION 2: Examine the OWASP Cheat Sheet. What is the regular expression used to validate a US Zip code?

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

The screenshot shows the OWASP Cheat Sheet Series page for Input Validation. The page is titled "Input Validation" and features a search bar and a navigation menu on the left. The main content area includes an introduction to input validation, a list of resources, and a section titled "Allow List Regular Expression Examples". This section provides examples of regular expressions for validating a U.S. Zip Code and a U.S. State Selection. The regular expression for a U.S. Zip Code is `^\d{5}(-\d{4})?$`. The page also includes a "Table of contents" on the right side.

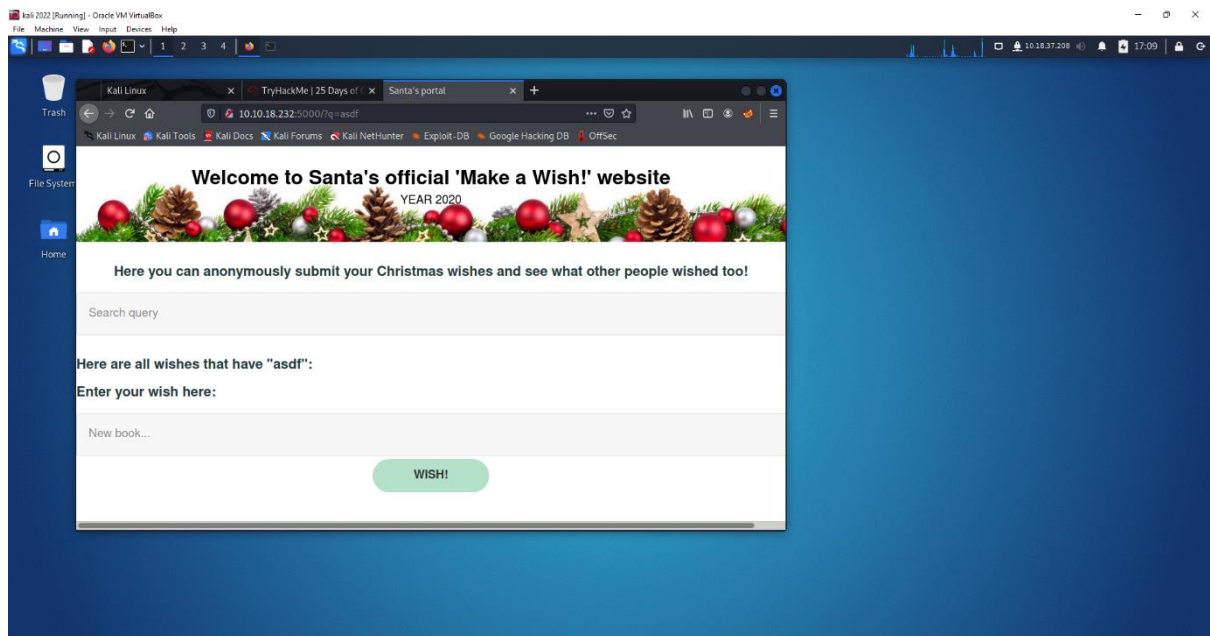
Question 3: What vulnerability type was used to exploit the application?

ANSWER: Stored

The screenshot shows a web application interface for Santa's official "Make a Wish!" website. The page has a festive theme with a header featuring pine cones and red berries. The main content area includes a search bar, a section titled "Here are all wishes that have 'asdf':", and a form for submitting a wish. The form has a "WISH!" button. The page is displayed in a browser window with the address bar showing `10.10.18.232:5000/?q=asdf`.

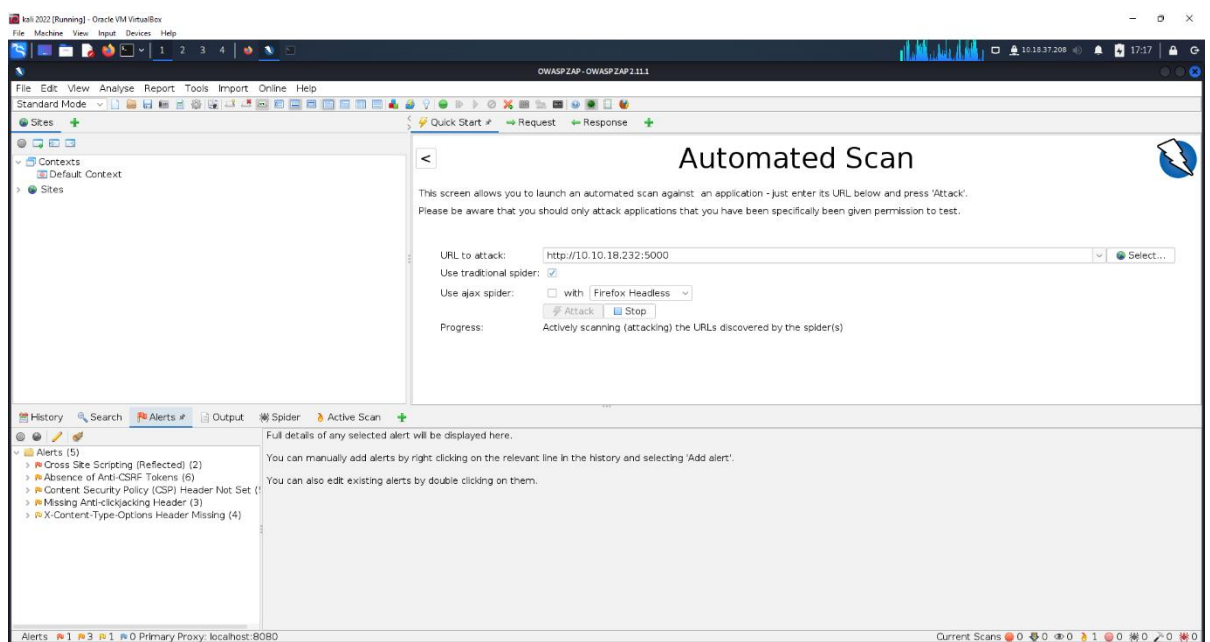
QUESTION 4: What query string can be abused to craft a reflected XSS?

ANSWER: q



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

ANSWER: 2



QUESTION 6: What JavaScript code should you put in the wish text box if you want to show an alert saying "PSP0201"?

ANSWER: <script>alert('PSP2021')</script>

#jaVasCript:/*-*/'/'/*/**/(/ /*oNcliCk=alert(5397) %/%0D%0A%0d%0a//x3csVg/

#javascript:alert(5397)

Enter your wish here:

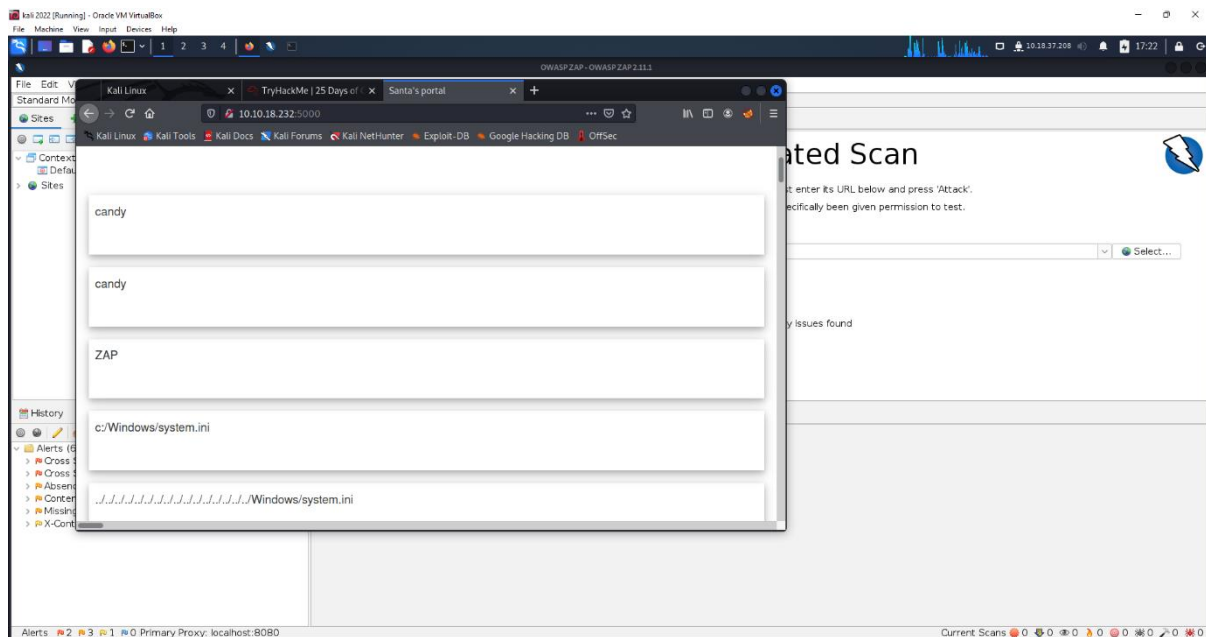
<script>alert("PSP0201")</script>

WISH!



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

ANSWER: YES



METHODOLOGY:

Firstly, I open the try hack and read the question. So, the first question, I read at the OWASP Cheat Sheet to answer the Q1. For Q2 I use the OWASP Cheat Sheet to check the regular expression used to validate a US Zip code. We check and get the answer for Q2. Then for Q3, I start the machine, got the Ip address and paste it to the Firefox. It will lead us to "welcome to Santa official make a wish website". I put the wish that I wanted and enter it. Then, the data store and it means Stored vulnerability. So, for the Q4, I already entered my wish and its show the URL show "q" at first of the URL. So, the query string is "q" can be abused to craft a reflected XSS. For the Q5, I open the OWASP and put the ip address to scan the website at there and the OWASP will check there have error or not. They show 2 error at Alert Section. For the Q6, I open the Santa's wish website to put the command at the wish, so the code that I put is "<script>alert('PSP2021')</script>". After that, the website shows error. Lastly for the Q7, I re check the website and put a new wish at the Santa's wish website, our XSS attack persist still can attack the website.

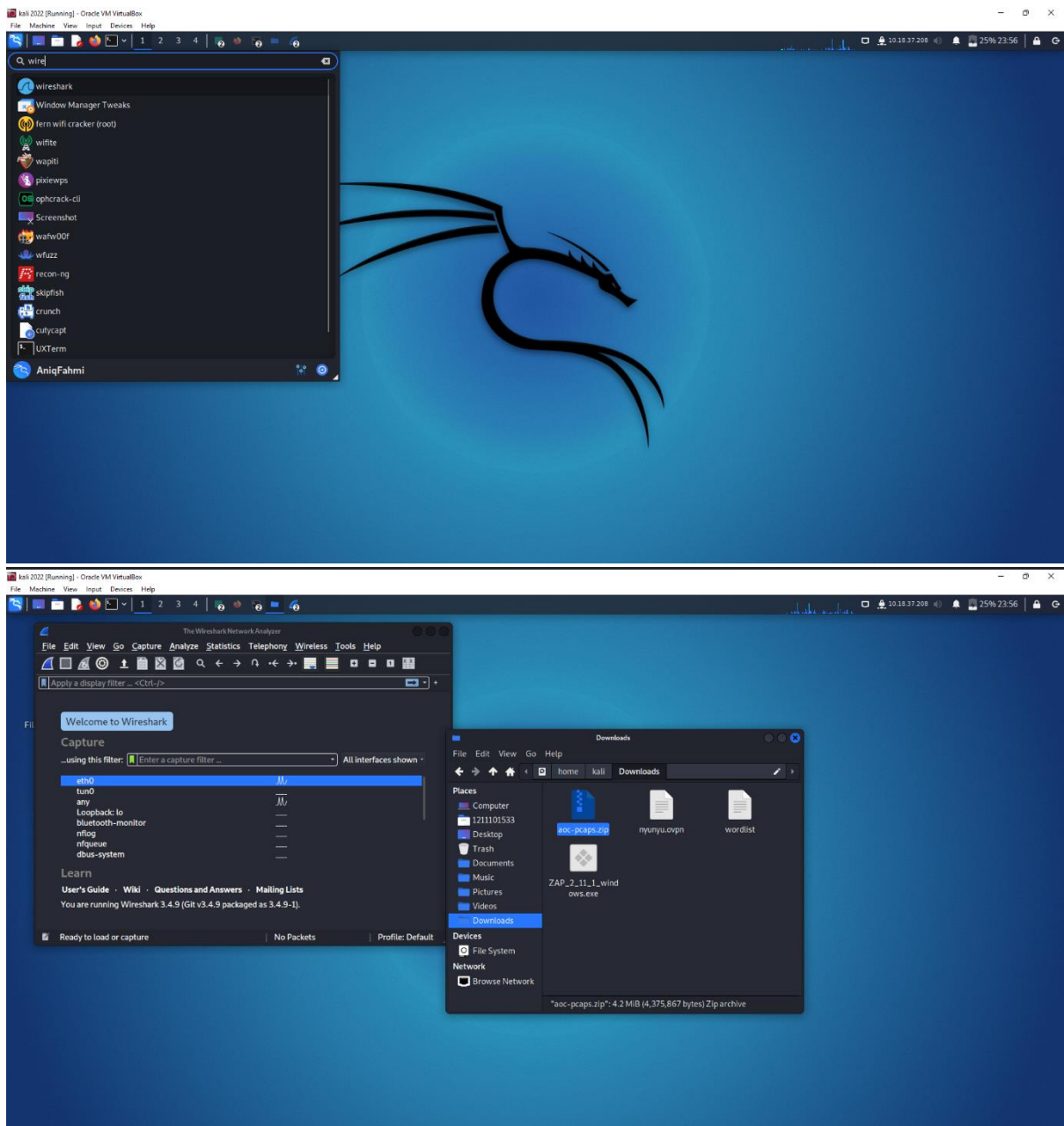
Day 7: Web Exploitation -- The Grinch Really Did Steal Christmas

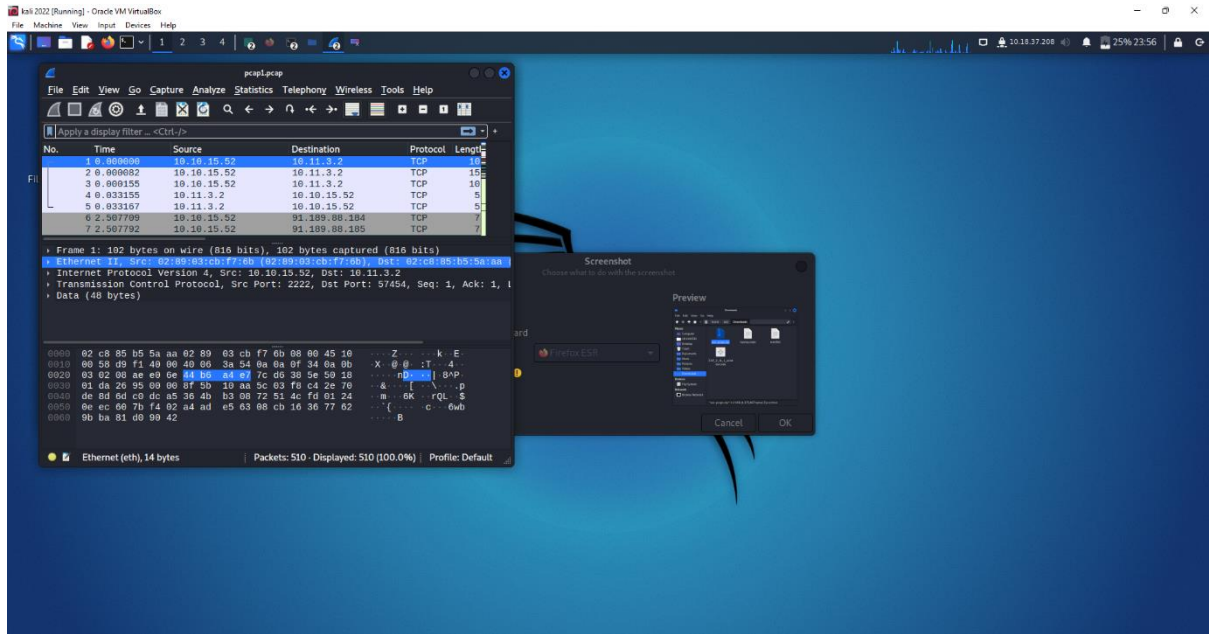
Tools used: Kali Linux, Firefox, Wireshark

Solution/walkthrough:

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

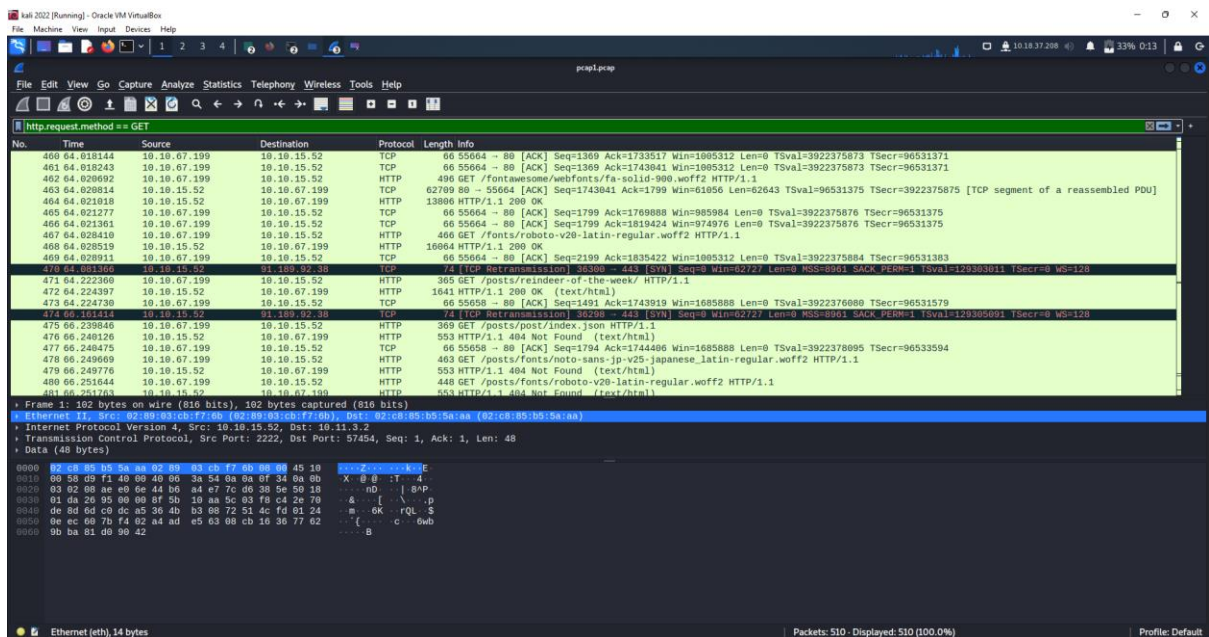
ANSWER: 10.11.3.2





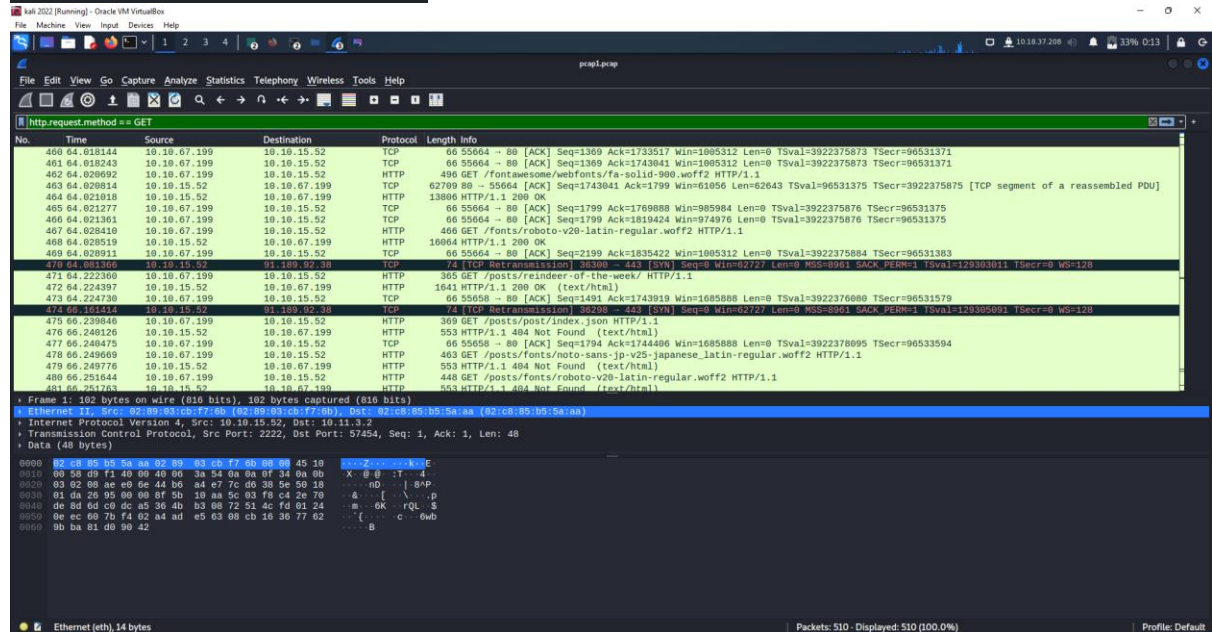
QUESTION 2: If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

ANSWER: http.request.method == GET



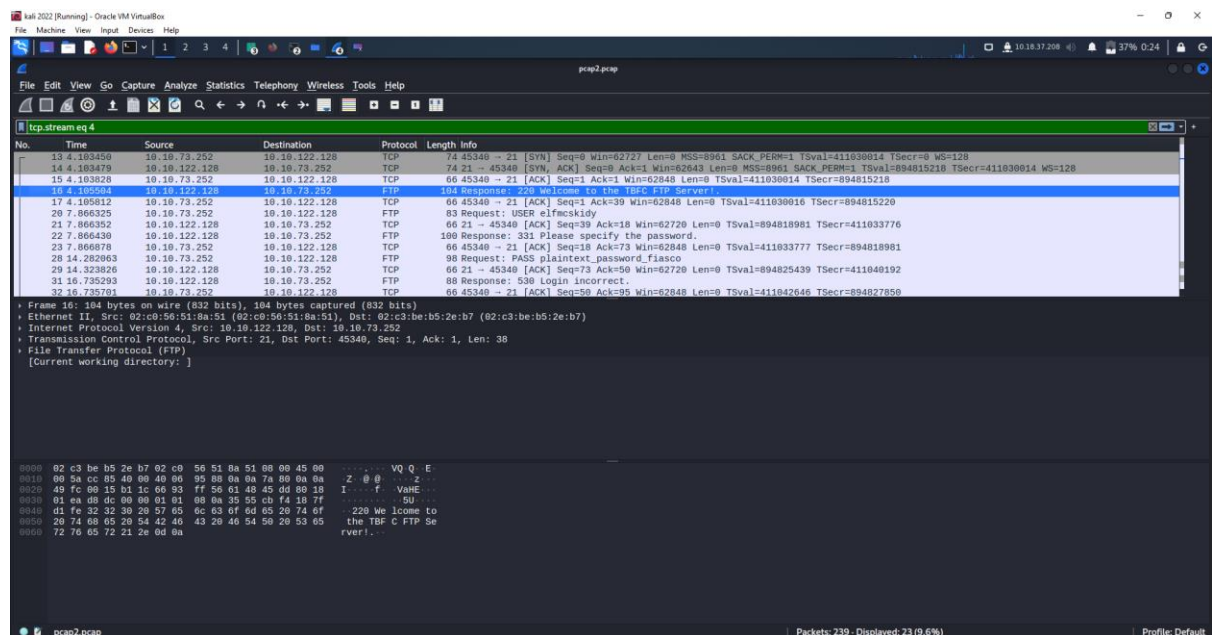
QUESTION 3: Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "10.10.67.199" visited

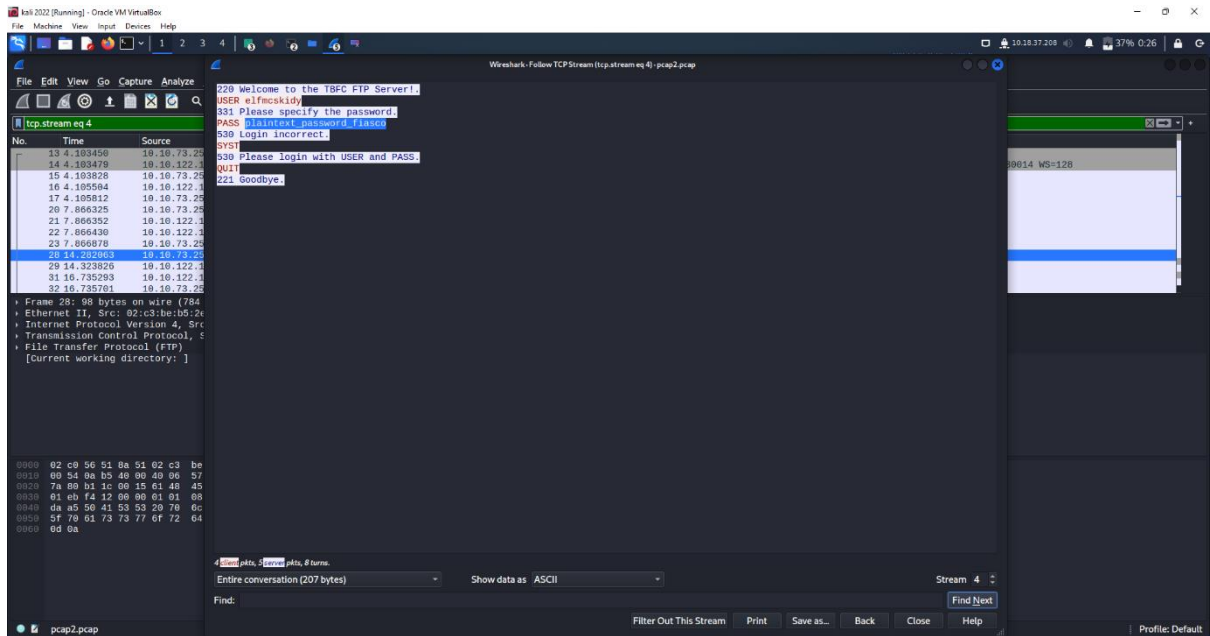
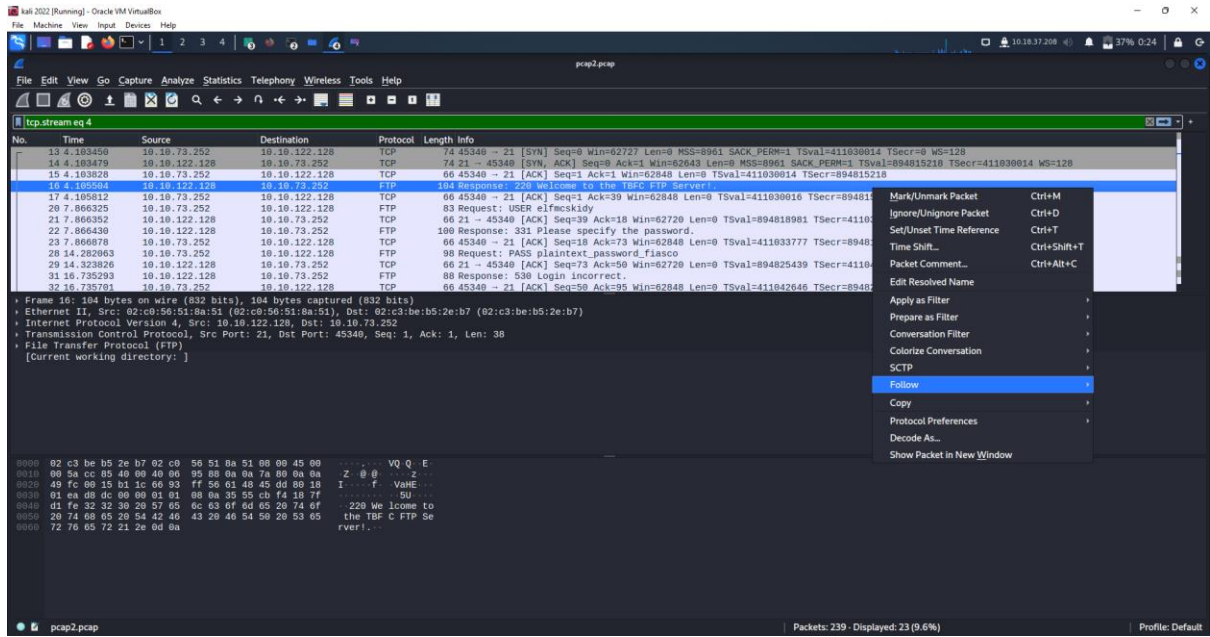
ANSWER: reindeer-of-the-week



QUESTION 4: Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process?

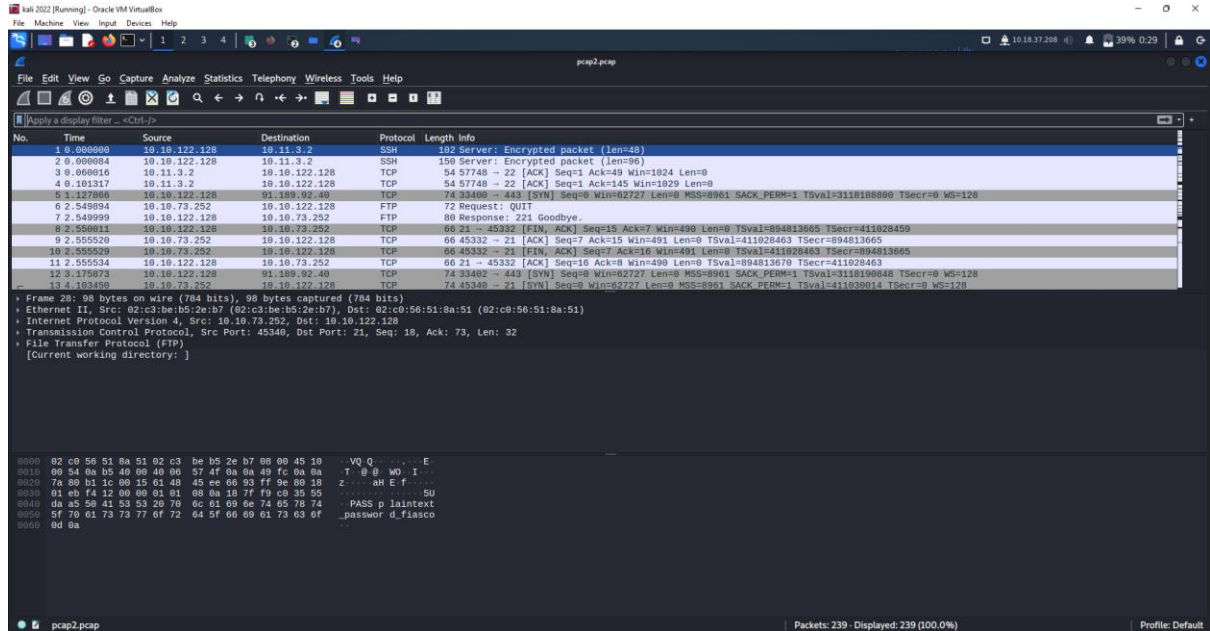
ANSWER: plaintext password fiasco





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

ANSWER: SSH



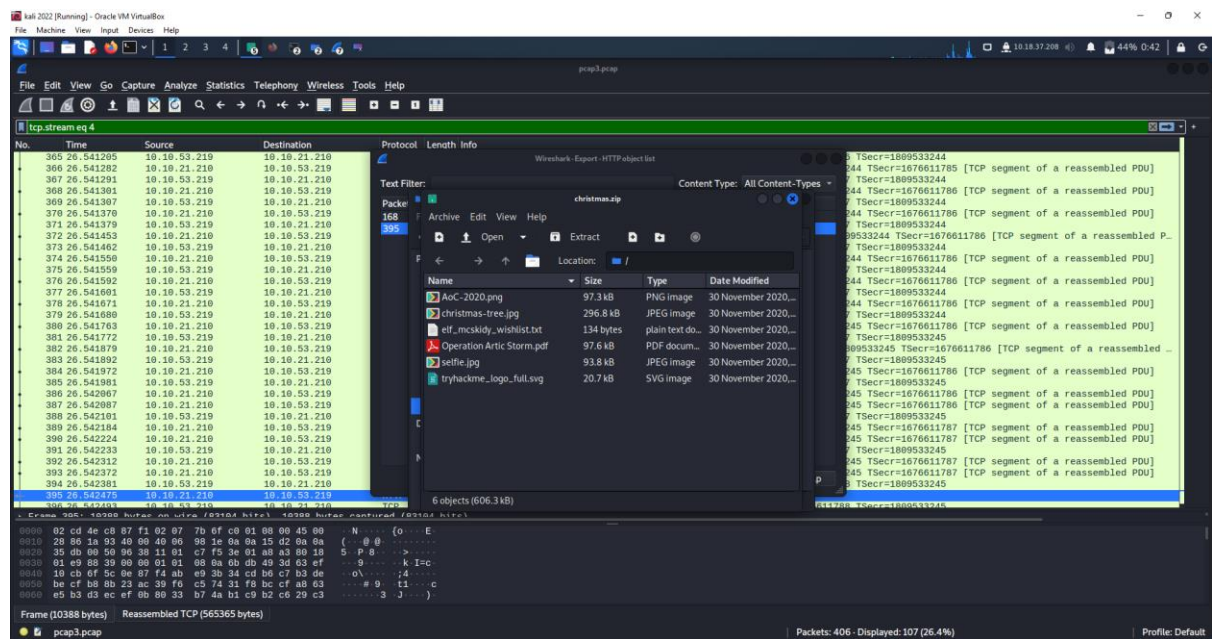
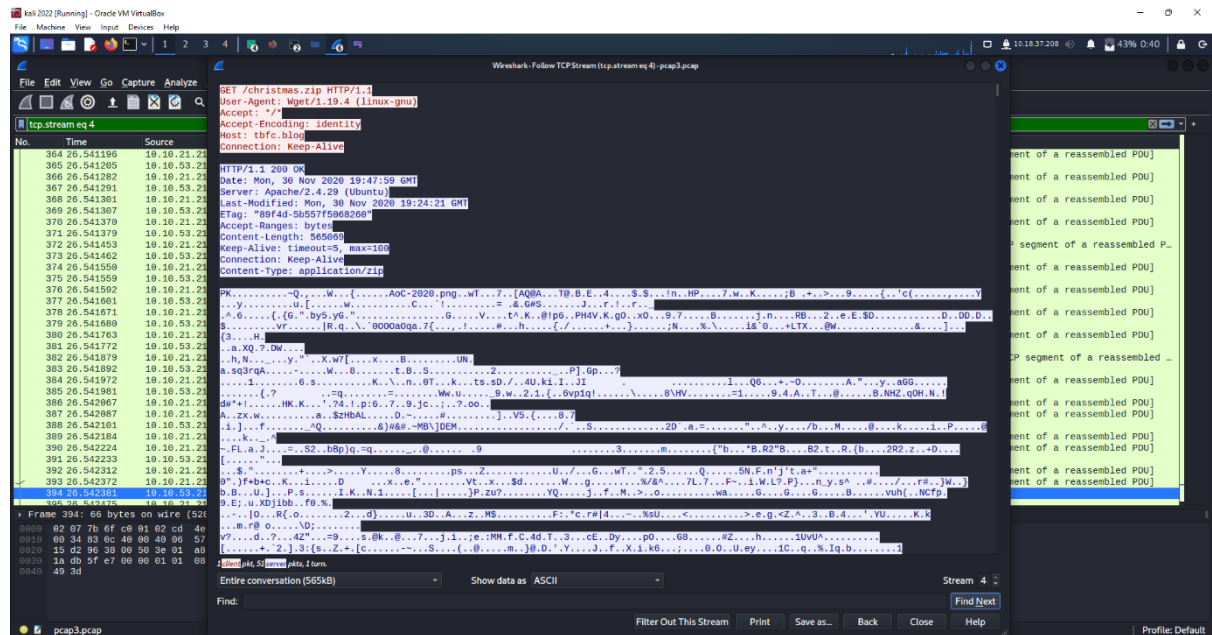
QUESTION 6: Examine the ARP communications. Who has 10.10.122.128? Tell 10.10.10.1.
Answer: 10.10.122.128 is at

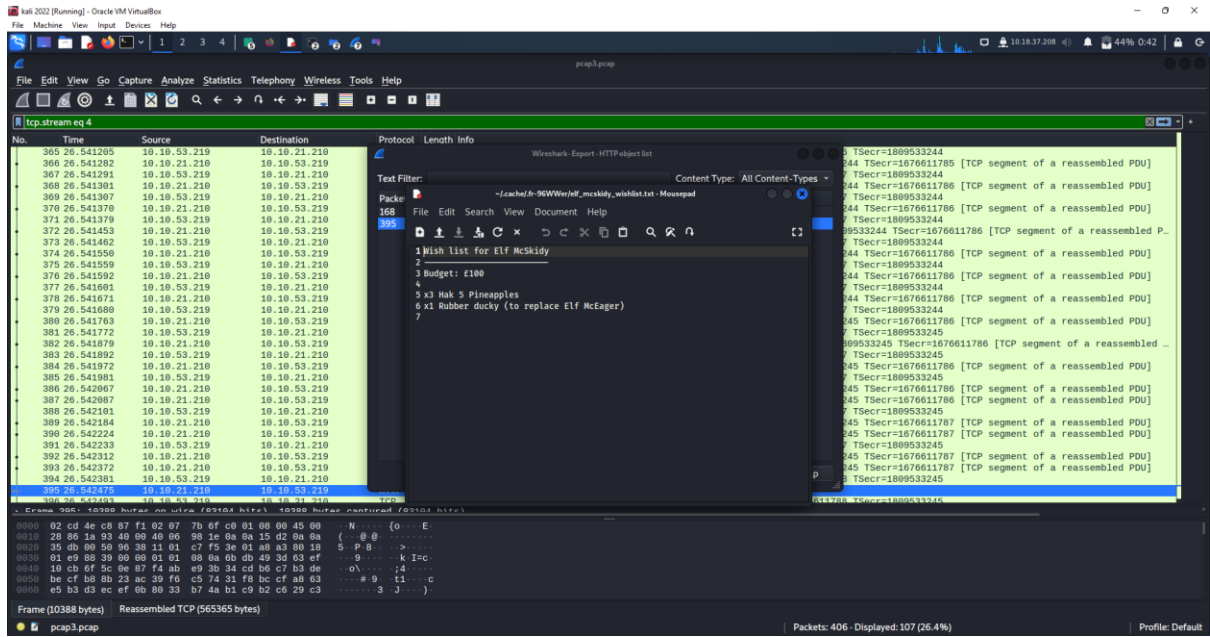
ANSWER: 02:c0:56:51:8a:51



QUESTION 7: Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

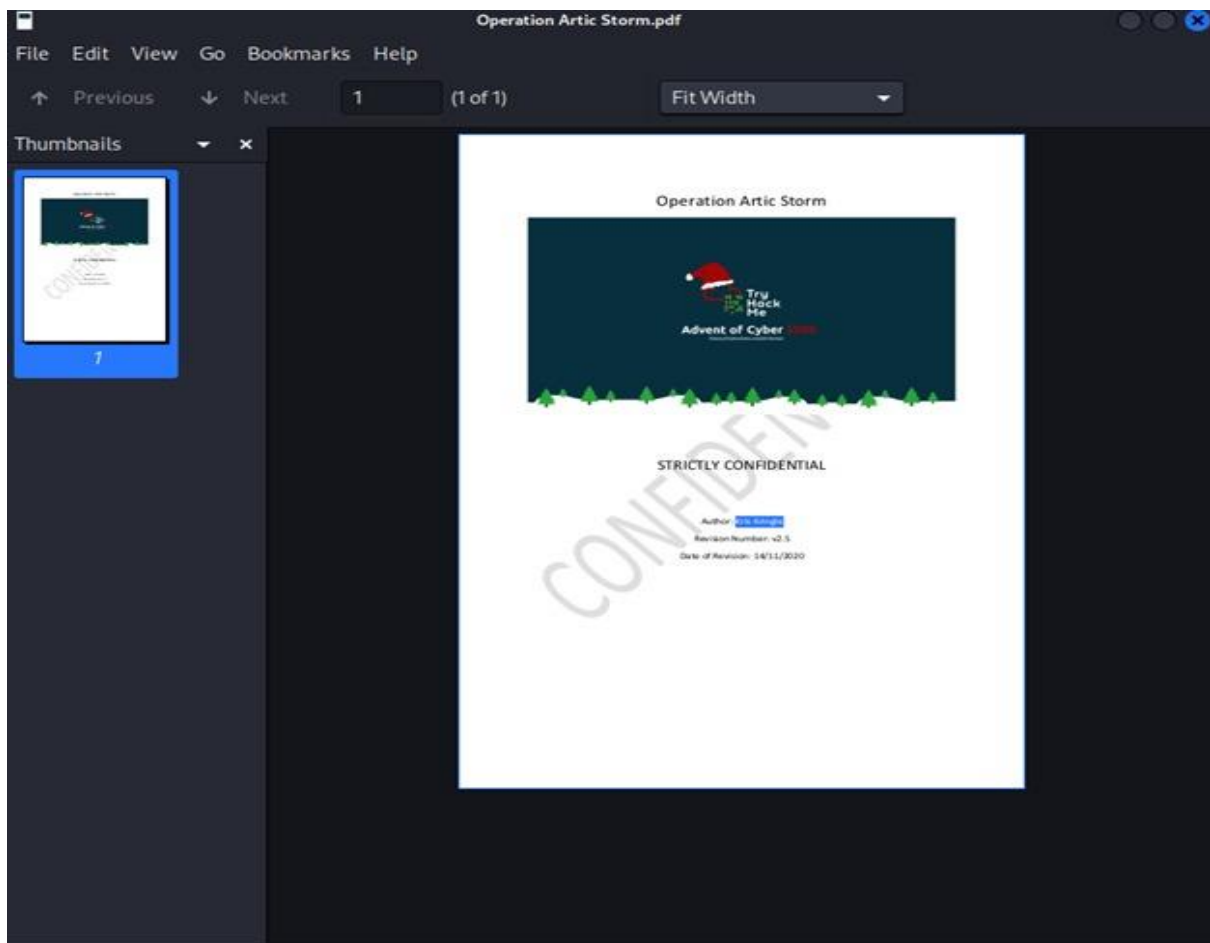
ANSWER: RUBBER DUCKY





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

ANSWER: Kris Kringle



METHODOLOGY:

Firstly, I open the try hack and read the question. I download the file that shows at the tryhackme.

After that, I open Wireshark at my application on my kali Linux. Then I open the pcap1.pcap at Wireshark and that's for the Q1. For the Q2, I use filter "http.request.method == GET" at the url section. This thing will show HTTP GET requests in our "pcap1.pcap" file. After that, the Q3 asked me to find the the name of the article that the IP address "10.10.67.199" visited. The name of the article is "reindeer-of-the-week". So, for the Q4, I open the pcap2.pcap. I find where the login was successful. Then, I follow the Ip address and lead us to the leaked password. For Q5, I checked the name of the protocol that is encrypted is SSH. After that Q6, I examine the ARP communication, and it says 02:c0:56:51:8a:51 at the Answer: 10.10.122.128. Then, for Q7, I open the code that leads us to Elf McEager, and we download it and shows the Wishlist of Elf McEager, at that text. For the last question, I open the file that I downloaded it at pcap3.pcap and open it. The author of Operation Artic Storm is Kris Kringle.

Day 8 - What's Under the Christmas Tree?

Tools used: AttackBox

Solution/Walkthrough:

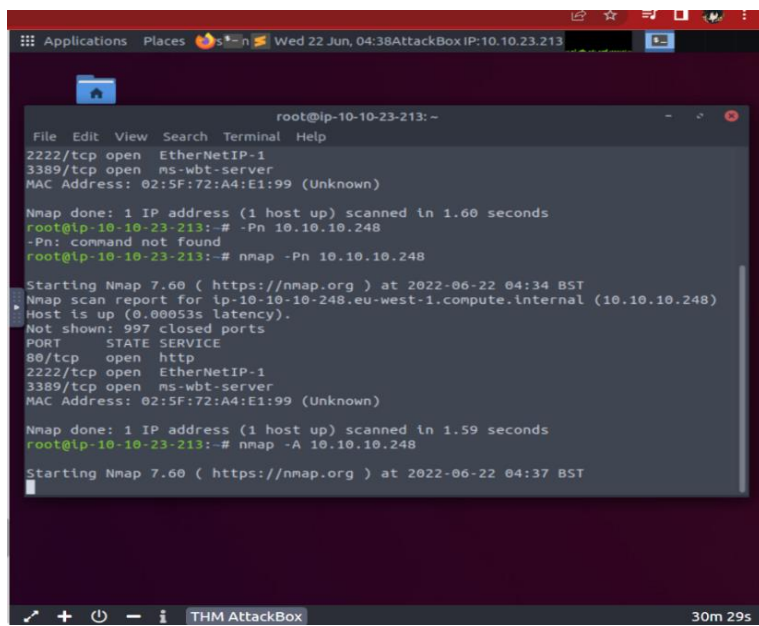
Question 1:

When was Snort created?

=1998

Question 2:

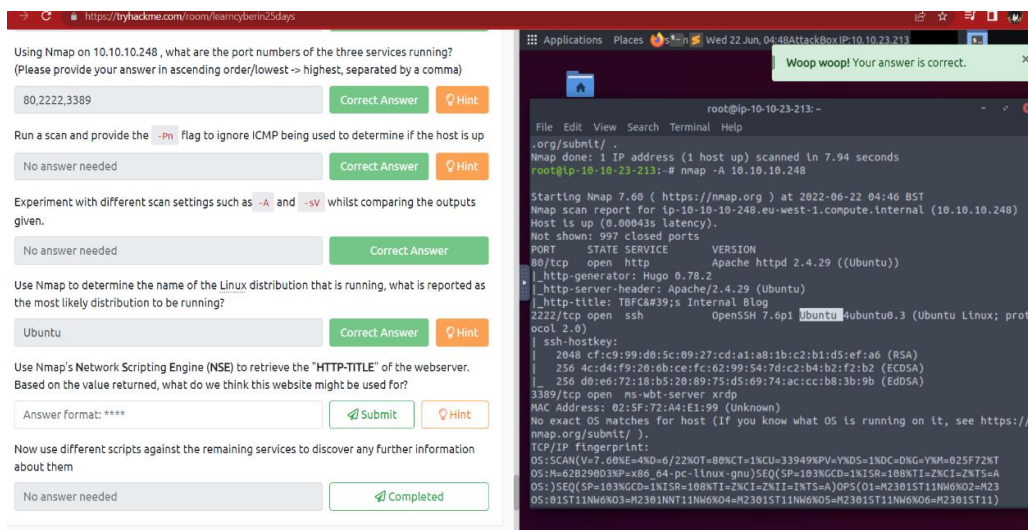
Using Nmap on MACHINE IP, what are the port numbers of the three services running?



```
root@ip-10-10-23-213: ~  
File Edit View Search Terminal Help  
2222/tcp open  EtherNetIP-1  
3389/tcp open  ms-wbt-server  
MAC Address: 02:5F:72:A4:E1:99 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds  
root@ip-10-10-23-213:~# -Pn 10.10.10.248  
-Pn: command not found  
root@ip-10-10-23-213:~# nmap -Pn 10.10.10.248  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-22 04:34 BST  
Nmap scan report for ip-10-10-10-248.eu-west-1.compute.internal (10.10.10.248)  
Host is up (0.00053s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
80/tcp    open  http  
2222/tcp  open  EtherNetIP-1  
3389/tcp  open  ms-wbt-server  
MAC Address: 02:5F:72:A4:E1:99 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds  
root@ip-10-10-23-213:~# nmap -A 10.10.10.248  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-22 04:37 BST
```

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?



Using Nmap on 10.10.10.248, what are the port numbers of the three services running?
(Please provide your answer in ascending order/lowest -> highest, separated by a comma)

80,2222,3389 Correct Answer Hint

Run a scan and provide the `-Pn` flag to ignore ICMP being used to determine if the host is up

No answer needed Correct Answer Hint

Experiment with different scan settings such as `-A` and `-sv` whilst comparing the outputs given.

No answer needed Correct Answer

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 Correct Answer Hint

Use Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. Based on the value returned, what do we think this website might be used for?

Answer format: **** Submit Hint

Now use different scripts against the remaining services to discover any further information about them

No answer needed Completed

What is the version of Apache?

Question 5:

What is running on port 2222?

A screenshot of a Kali Linux terminal window. The window title is "THM AttackBox". The terminal shows a netmap scan of the IP address 10.10.23.213. The output includes:
- Host is up (0.00043s latency).
- Not shown: 997 closed ports
- Open ports: 80/tcp (http), 22/tcp (ssh)
- Service versions: Apache httpd 2.4.29, OpenSSH 7.6p1
- OS detection: Linux (Ubuntu 4ubuntu0.3)
- TCP/IP fingerprint: A long string of scan results including V=7.60E=4D=6, 22OT=80CT=1, CU=33949PV=YDS=1DC=D%G=Y%M=025F72%T, OS=M=62B29D03P=x86_64-pc-linux-gnu, SEQ(SP=103%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A), OPS(O1=M2301ST11NW6%O2=M2301ST11NW6%O3=M2301NNT11NW6%O4=M2301ST11NW6%O5=M2301ST11NW6%O6=M2301ST11), WTN(W1=F4B3W2=F4B3W3=F4B3W4=F4B3W5=F4B3W6=F4B3)ECN(R=Y%DF=Y%T=40%W=0S=F507%O=M2301NNSNW6CC=Y%Q=)T1(R=Y%DF=Y%T=40%W=0S=A+S+%F=AS%RD=0%Q=)T2(R=N OS=)T3(R=N)T4(R=Y%DF=Y%T=40%W=0S=A+Z%F=R%O=0%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0 S=%S=Z%A+S+%F=AR%O=0%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0S=A+Z%F=R%O=0%RD=0%Q=)T7 OS=(R=Y%DF=Y%T=40%W=0S=Z%A+S+%F=AR%O=0%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN= OS=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
The terminal window has a dark background with a terminal menu (File, Edit, View, Search, Terminal, Help) at the top. The bottom status bar shows "THM AttackBox" and "07m 54s".

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?

The screenshot shows a TryHackMe challenge interface on the left and a terminal window on the right. The challenge interface has several questions and answers:

- Question: Using Nmap on 10.10.10.248, what are the port numbers of the three services running? (Please provide your answer in ascending order/lowest -> highest, separated by a comma)
- Answer: 80,2222,3389
- Question: Run a scan and provide the `-Pn` flag to ignore ICMP being used to determine if the host is up
- Answer: No answer needed
- Question: Experiment with different scan settings such as `-A` and `-sV` whilst comparing the outputs given.
- Answer: No answer needed
- Question: Use Nmap to determine the name of the Linux distribution that is running, what is reported as the most likely distribution to be running?
- Answer: Ubuntu
- Question: Use Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. Based on the value returned, what do we think this website might be used for?
- Answer: blog
- Question: Now use different scripts against the remaining services to discover any further information about them
- Answer: No answer needed

The terminal window shows the output of an Nmap scan on 10.10.10.248:

```
root@ip-10-10-23-213: ~
File Edit View Search Terminal Help
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.94 seconds
root@ip-10-10-23-213: ~# nmap -A 10.10.10.248

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-22 04:46 BST
Nmap scan report for ip-10-10-10-248.eu-west-1.compute.internal (10.10.10.248)
Host is up (0.00043s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Apache httpd 2.4.29 ((Ubuntu))
|_ http-generator: Hugo 0.78.2
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: TBFC&#39;s Internal Blog
2222/tcp  open  ssh            OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; prot
occol 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 (EdDSA)
3389/tcp  open  ms-wbt-server  xrdp
MAC Address: 02:5F:72:A4:E1:99 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.68%E=4ND=6/22%OT=80%CT=1%CU=33949%PV=Y%DS=1%DC=D%G=Y%M=025F72%T
OS:M=62B29003%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=108%TI=Z%CI=Z%TS=A
OS:SEQ(SP=103%GCD=1%ISR=108%TI=Z%CI=Z%II=INTS=A)OPS(O1=M2301ST11NW6%O2=M23
OS:01ST11NW6%O3=M2301NNT11NW6%O4=M2301ST11NW6%O5=M2301ST11NW6%O6=M2301ST11)
```

=Blog

METHODOLOGY

First of all, we started the Machine and the AttackBox waiting to obtain Ip address. Then, we open the terminal and run the scan using Nmap with the Ip provided to get the port numbers of the three services running it. Lastly, we scan again the Nmap with different scan settings using `-A` to retrieve the outputs to solve the name of the Linux distribution that is running, the version of Apache, type running of the port numbers and the value of the webserver.

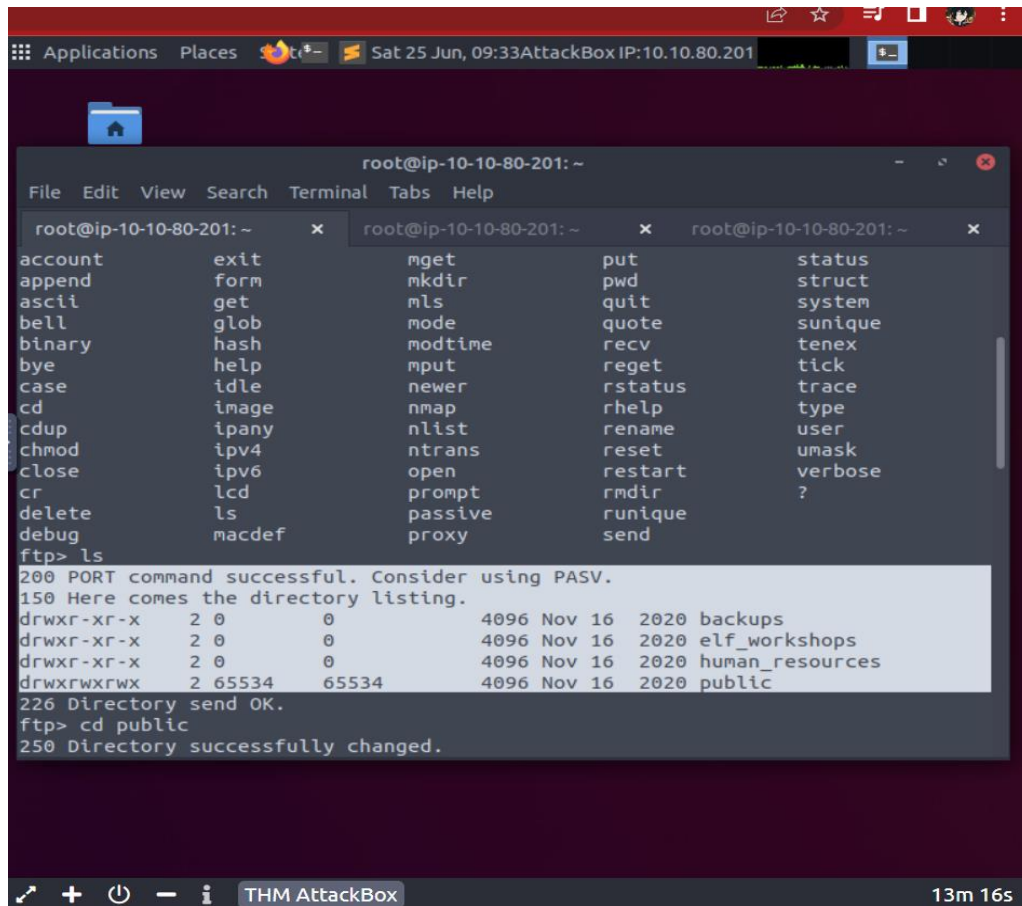
Day 9 – Anyone can be Santa!

Tools used: AttackBox

Solution/ Walkthrough:

Question 1:

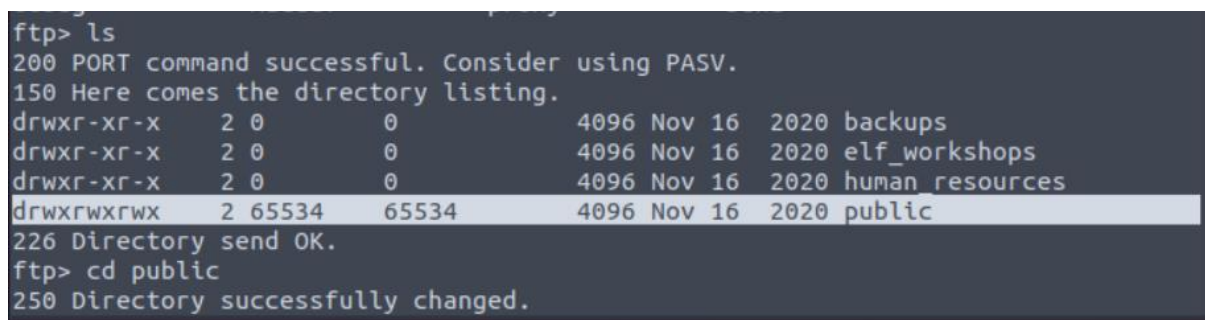
What are the directories you found on the FTP site?



```
root@ip-10-10-80-201: ~  
File Edit View Search Terminal Tabs Help  
root@ip-10-10-80-201: ~ x root@ip-10-10-80-201: ~ x root@ip-10-10-80-201: ~ x  
account      exit          mget          put           status  
append       form          mkdir          pwd           struct  
ascii        get           mls           quit          system  
bell         glob          mode          quote         sunique  
binary       hash          modtime       recv          tenex  
bye          help          mput          reget         tick  
case         idle          newer         rstatus       trace  
cd           image         nmap          rhelp         type  
cdup         ipany         nlist         rename        user  
chmod        ipv4          ntrans        reset         umask  
close        ipv6          open          restart        verbose  
cr           lcd           prompt         rmdir         ?  
delete       ls            passive       runique  
debug        macdef        proxy          send  
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.
```

Question 2:

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

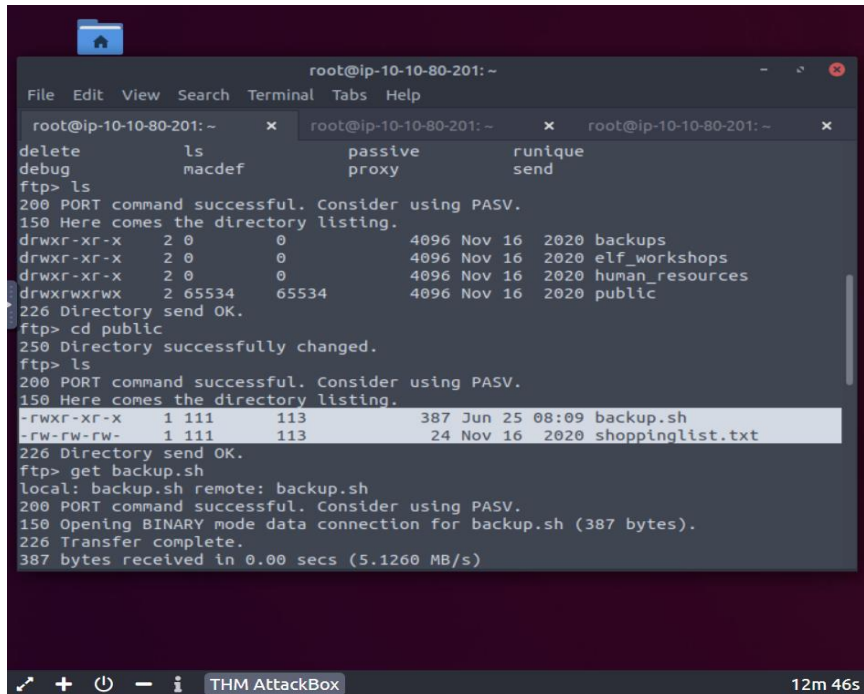


```
ftp> ls  
200 PORT command successful. Consider using PASV.  
150 Here comes the directory listing.  
drwxr-xr-x  2 0      0          4096 Nov 16  2020 backups  
drwxr-xr-x  2 0      0          4096 Nov 16  2020 elf_workshops  
drwxr-xr-x  2 0      0          4096 Nov 16  2020 human_resources  
drwxrwxrwx  2 65534 65534       4096 Nov 16  2020 public  
226 Directory send OK.  
ftp> cd public  
250 Directory successfully changed.
```

Question 3:

What script gets executed within this directory?

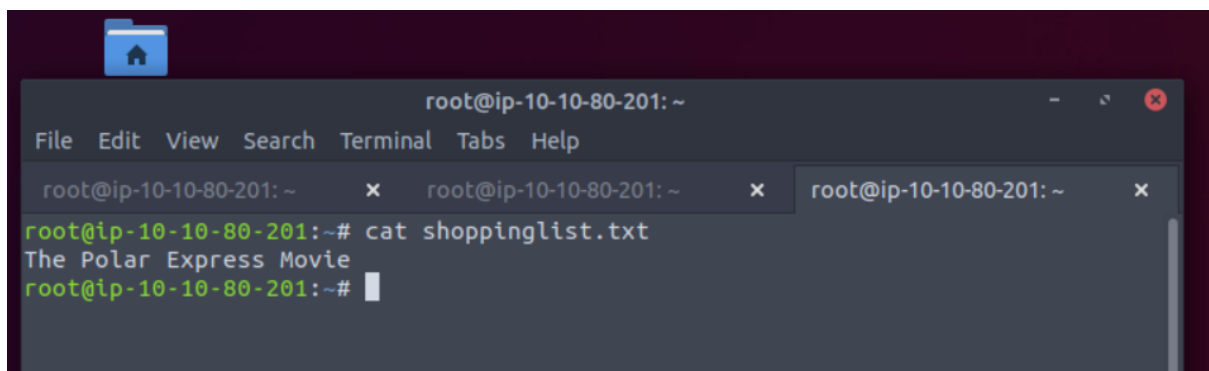
=backup.sh



```
root@ip-10-10-80-201: ~  
File Edit View Search Terminal Tabs Help  
root@ip-10-10-80-201: ~ x root@ip-10-10-80-201: ~ x root@ip-10-10-80-201: ~ x  
delete ls passive runique  
debug macdef proxy send  
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.  
-rwxr-xr-x 1 111 113 387 Jun 25 08:09 backup.sh  
-rw-rw-rw- 1 111 113 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 (387 bytes).  
226 Transfer complete.  
387 bytes received in 0.00 secs (5.1260 MB/s)
```

Question 4:

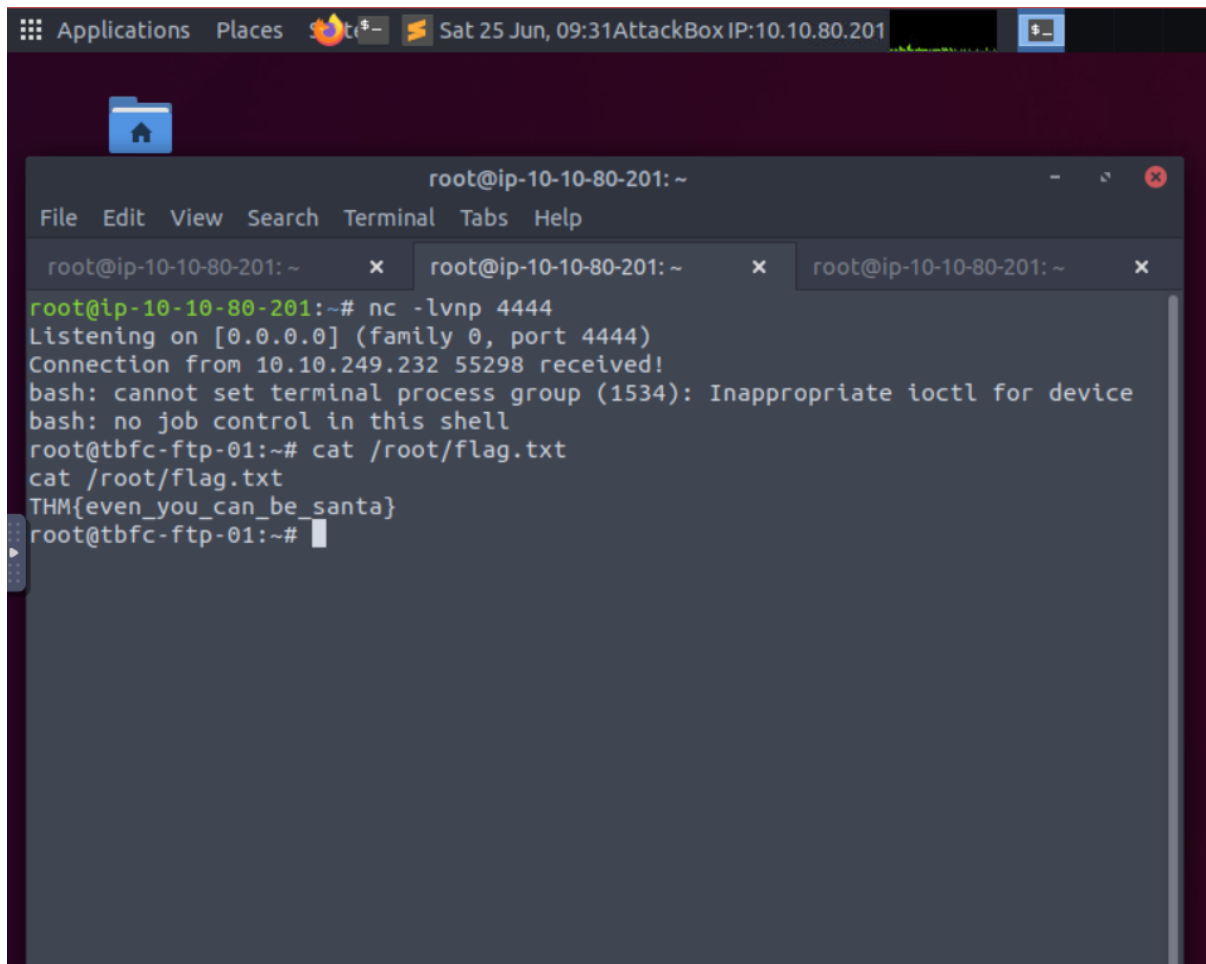
What movie did Santa have on his Christmas shopping list?



```
root@ip-10-10-80-201: ~  
File Edit View Search Terminal Tabs Help  
root@ip-10-10-80-201: ~ x root@ip-10-10-80-201: ~ x root@ip-10-10-80-201: ~ x  
root@ip-10-10-80-201: ~# cat shoppinglist.txt  
The Polar Express Movie  
root@ip-10-10-80-201: ~#
```

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!



```
root@ip-10-10-80-201: ~  
File Edit View Search Terminal Tabs Help  
root@ip-10-10-80-201: ~ x root@ip-10-10-80-201: ~ x root@ip-10-10-80-201: ~ x  
root@ip-10-10-80-201:~# nc -lvnp 4444  
Listening on [0.0.0.0] (family 0, port 4444)  
Connection from 10.10.249.232 55298 received!  
bash: cannot set terminal process group (1534): Inappropriate ioctl for device  
bash: no job control in this shell  
root@tbfc-ftp-01:~# cat /root/flag.txt  
cat /root/flag.txt  
THM{even_you_can_be_santa}  
root@tbfc-ftp-01:~#
```

METHODOLOGY:

We run the Machine and the AttackBox. To connect, we simply use ftp and provide the IP address of the Instance. When prompted for our "Name", we enter "anonymous". If successful, we have confirmed that the FTP Server has "anonymous" mode enabled - successful login. We apply command "ls" to look at the directories available in the FTP server and find out which directory that has data accessible by the anonymous user. Then we use nano to see the scripts. By that we work pentesters cheatsheet to get a good command that will be executed by the server to generate a shell to our AttackBox, replacing the IP_ADDRESS with the TryHackMe IP. We set up a netcat listener to catch the connection on our AttackBox and return to our FTP prompt and employ put to put the file into that directory. Lastly, we go back to our netcat listener, wait for about one minute to succeed. Now we have a reverse system shell on the FTP Server as the most powerful user that we can re-upload the script by putting the output contents of /root/flag.txt!

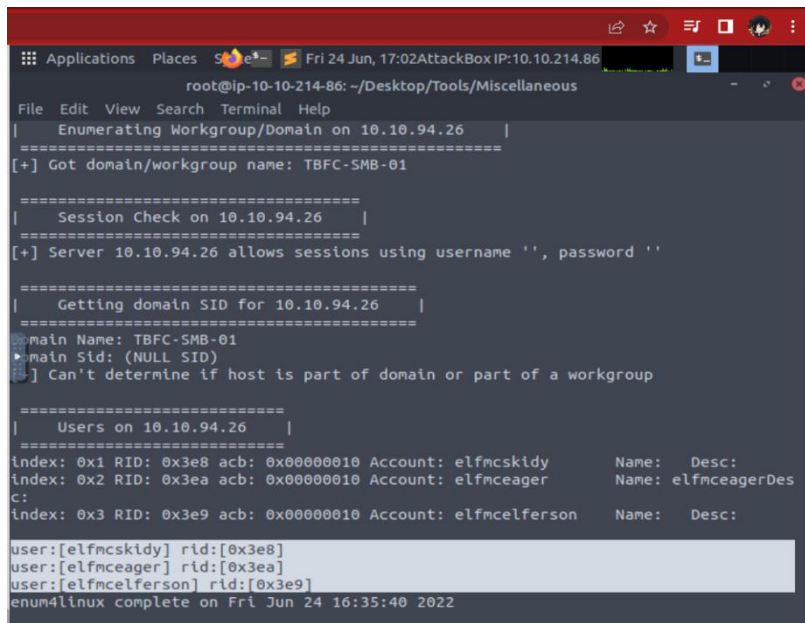
Day 10 - Don't be sElfish!

Tools used: AttackBox

Solution/ Walkthrough:

Question 2:

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



```
root@ip-10-10-214-86: ~/Desktop/Tools/Miscellaneous
File Edit View Search Terminal Help
| Enumerating Workgroup/Domain on 10.10.94.26 |
=====
[+] Got domain/workgroup name: TBFC-SMB-01

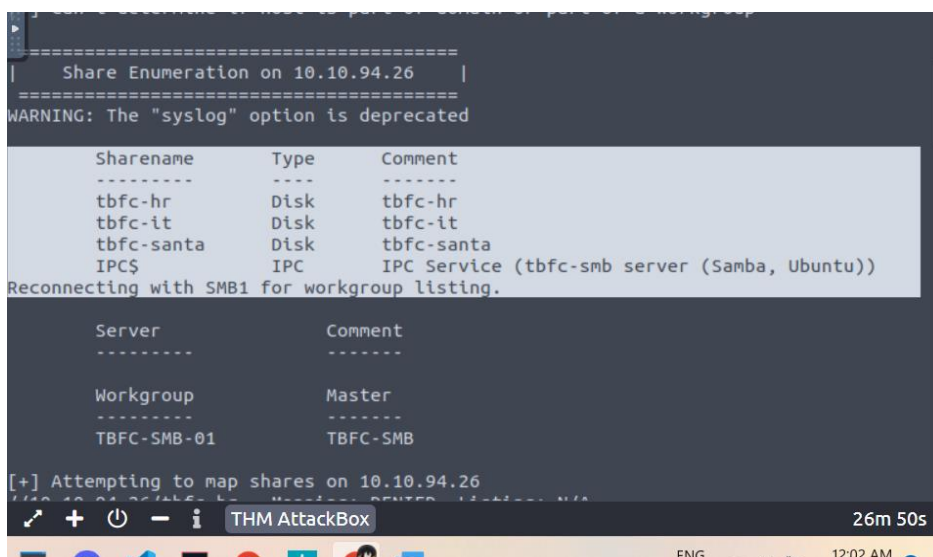
=====
| Session Check on 10.10.94.26 |
=====
[+] Server 10.10.94.26 allows sessions using username '', password ''

=====
| Getting domain SID for 10.10.94.26 |
=====
Domain Name: TBFC-SMB-01
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

=====
| Users on 10.10.94.26 |
=====
Index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy Name: Desc:
Index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager Name: elfmceagerDes
c:
Index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelerson Name: Desc:
user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelerson] rid:[0x3e9]
enum4linux complete on Fri Jun 24 16:35:40 2022
```

Question 3:

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



```
=====
| Share Enumeration on 10.10.94.26 |
=====
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
-----
TBFC-SMB-01     TBFC-SMB

[+] Attempting to map shares on 10.10.94.26
THM AttackBox 26m 50s
```

Question 4:

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

we will demonstrate below:

1. Remember that the IP address of the Samba server is that of the Instance you deployed (10.10.94.26)
2. Use the `smbclient` tool to begin accessing the Samba server and its shares, replacing "sharename" with the name of the share you wish to access:
`smbclient //REPLACE_INSTANCE_IP_ADDRESS/**sharename**`
3. You will be asked for a password, the easiest password is no password! We can just press "Enter" to test this theory. If successful, this means that the share requires no authentication and we are now logged in.

For example, accessing "share1" on another device:

```
root@kali:~# smbclient //192.168.1.200/share1
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \>
```

You can use the `help` command to list some of the commands you can run whilst connected to the Samba share. Here's a quick rundown of the fundamentals:

Command	Description
<code>ls</code>	List files and directories in the current location
<code>cd <directory></code>	Change our working directory
<code>pwd</code>	Output the full path to our working directory
<code>more</code>	Find out more about the contents of a file. To close the open file, you press <code>:q</code>
<code><filename></code>	
<code>get <filename></code>	Download a file from a share
<code>put <filename></code>	Upload a file from a share

```
root@ip-10-10-214-86: ~/Desktop/Tools/Miscellaneous
root@ip-10-10-214-86:~/Desktop/Tools/Miscellaneous# smbclient //10.10.94.26/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> help
?
blocksize      allinfo        altname        archive        backup
chown          cancel         case_sensitive cd              chmod
du             close         del            deltree       dir
geteas         echo          exit           get           getfacl
lcd            hardlink      help           history        iosize
ls             link          lock           lowercase     ls
mask          md            mget          mkdir          mkdir
mput          newer        notify        open           open
posix          posix_encrypt posix_open     posix_mkdir   posix_rmdir
posix_unlink  posix_whoami  print         prompt         put
pwd           q            queue         quit          readlink
rd            recurse      reget         rename        reput
rm            rmdir        showacl       setea         setmode
scopy         stat         symlink       tar           tarnode
timeout       translate    unlock        volume        vuid
wdel          logon        listconnect   showconnect   tcon
tdis         tid          logoff        ..            !
smb: \>
```

Question 5:

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

Answer the questions below

Question #1 Using `enum4linux`, how many users are there on the Samba server (10.10.94.26)?

3 Correct Answer

Question #2 Now how many "shares" are there on the Samba server?

4 Correct Answer

Question #3 Use `smbclient` to try to login to the shares on the Samba server (10.10.94.26). What share doesn't require a password?

tbfc-santa Correct Answer

Question #4 Log in to this share, what directory did ElfMcSkidy leave for Santa?

jingle-tunes Correct Answer Hint

Task 13 [Day 11] Networking The Rogue Gnome

Task 14 [Day 12] Networking Ready, set, elf.

Task 15 [Day 13] Networking Coal for Christmas

Task 16 [Day 14] OSINT Where's Rudolph?

```
root@ip-10-10-214-86: ~/Desktop/Tools/Miscellaneous
root@ip-10-10-214-86:~/Desktop/Tools/Miscellaneous# smbclient //10.10.94.26/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> help
?
blocksize      allinfo        altname        archive        backup
chown          cancel         case_sensitive cd              chmod
du             close         del            deltree       dir
geteas         echo          exit           get           getfacl
lcd            hardlink      help           history        iosize
ls             link          lock           lowercase     ls
mask          md            mget          mkdir          mkdir
mput          newer        notify        open           open
posix          posix_encrypt posix_open     posix_mkdir   posix_rmdir
posix_unlink  posix_whoami  print         prompt         put
pwd           q            queue         quit          readlink
rd            recurse      reget         rename        reput
rm            rmdir        showacl       setea         setmode
scopy         stat         symlink       tar           tarnode
timeout       translate    unlock        volume        vuid
wdel          logon        listconnect   showconnect   tcon
tdis         tid          logoff        ..            !
smb: \> ls
.                D          0   Thu Nov 12 02:12:07 2020
..               D          0   Thu Nov 12 01:32:21 2020
jingle-tunes     D          0   Thu Nov 12 02:10:41 2020
note_from_mcskidy.txt N         143 Thu Nov 12 02:12:07 2020

10252564 blocks of size 1024. 5369400 blocks available
smb: \>
```


METHODOLOGY:

As usual we started the Machine and the AttackBox, then we open a terminal prompt and navigate to enum4linux: `cd /root/Desktop/Tools/Miscellaneous`. We continue running enum4linux using `(./enum4linux.pl -h)` to study all the list possible options we can use. Next, we want to find out who can be used to access the server through Samba: `(./enum4linux.pl -U [the Ip address])` then enum4linux showed four users in the Samba server. Now we want to know how many “shares” in the Samba server so we use `(./enum4linux.pl -S [Ip address])` to obtain the share list. Moving on we use the smbclient tool to accessing the share that doesn’t require a password. Lastly, we use command “ls” in the smbclient tools to receive the directory.