PSP0201
WEEKLY WRITE UP
WEEK 3
GROUP 7

Group Name : Sang Haekeo (The Hackers)

Sang
- Taken from a Malay word , sang , meaning ‘the’

Haekeo
- Taken from a Korean word , 해커 , meaning ‘hacker’
-

ID	NAME	ROLE	TASK
1211102162	AMILIA NADZEERA BINTI BAHARUDIN	Leader	- Day 6 & 7 write up
1211100930	KU NAJWA SYAUQINA BINTI KU AZRIN	Member	
1211101693	SAVITHA MURUGUMUNISEGARAN	Member	- Day 8 & 9 write up

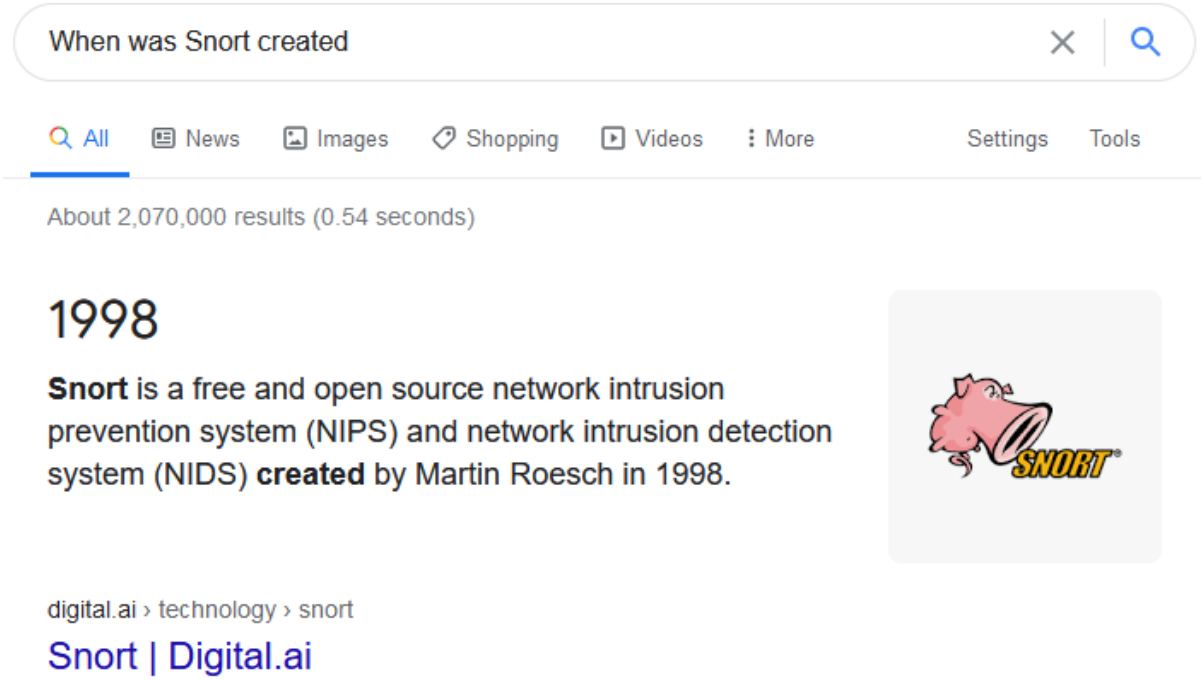
Day 6 ; Web Exploitation : Be careful with what you wish on Christmas Night

Question 1 :

Day 8: What's Under The Christmas Tree!

Question 1
When was Snort created?

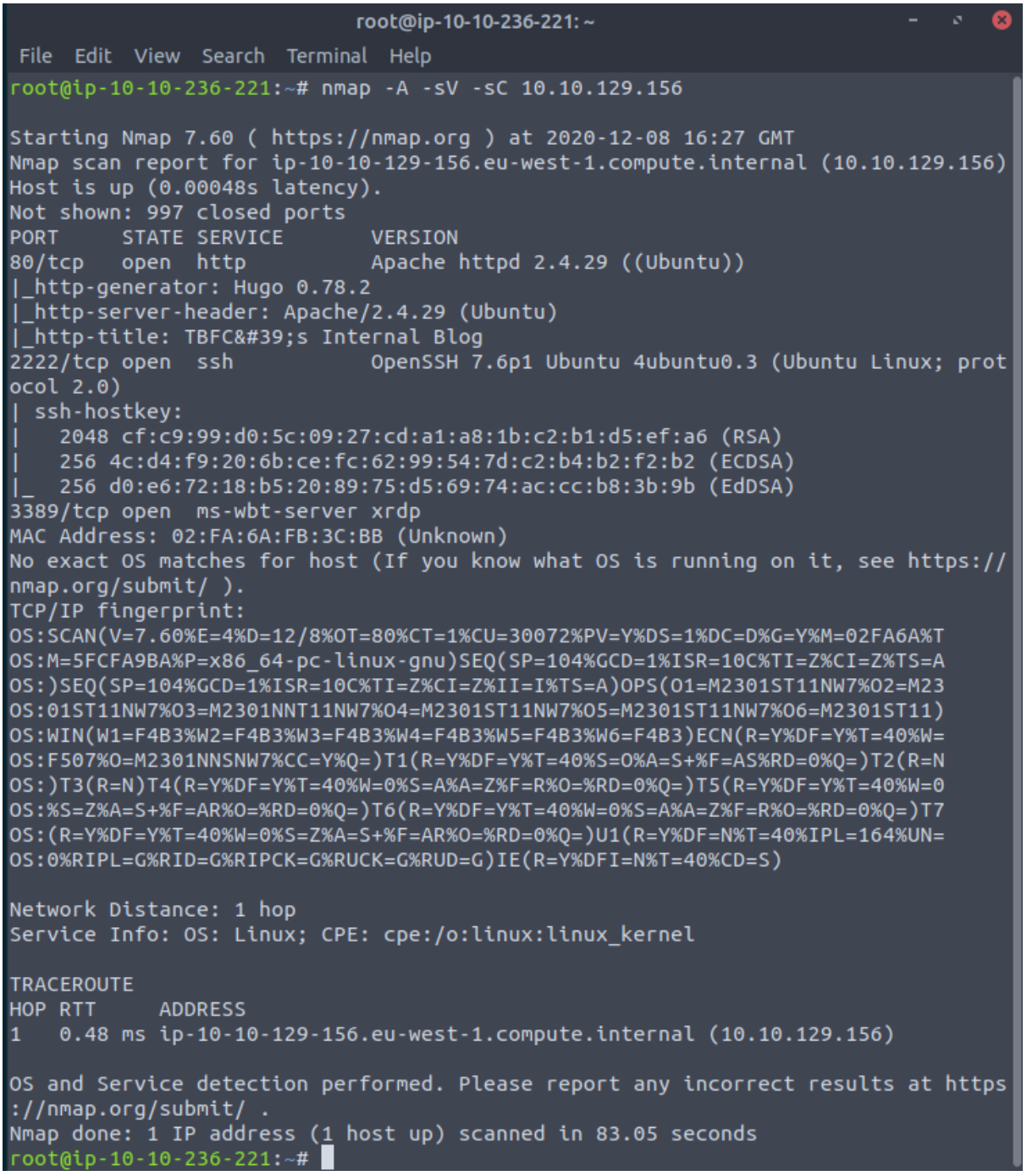
For this one, a short Google search revealed that Snort was developed in 1998:



Question 2

Using Nmap on 10.10.129.156, what are the port numbers of the three services running? (Please provide your answer in ascending order/lowest -> highest, separated by a comma)

We first ran a nmap scan against that IP address:



A HTTP server on port 80, SSH on port 2222, and a remote desktop connection on port 3389 are the three open ports that are displayed here.

Question 5

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

There are multiple references to Ubuntu while looking at the scan results up above.

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-08 16:35 GMT
Nmap scan report for ip-10-10-129-156.eu-west-1.compute.internal (10.10.129.156)
Host is up (0.00050s 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
ocol 2.0)
```

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?

Examine the HTTP-title section carefully, paying great attention to the web server (port 80), using the initial scan as a reference once more. This indicates that it serves as a blog.

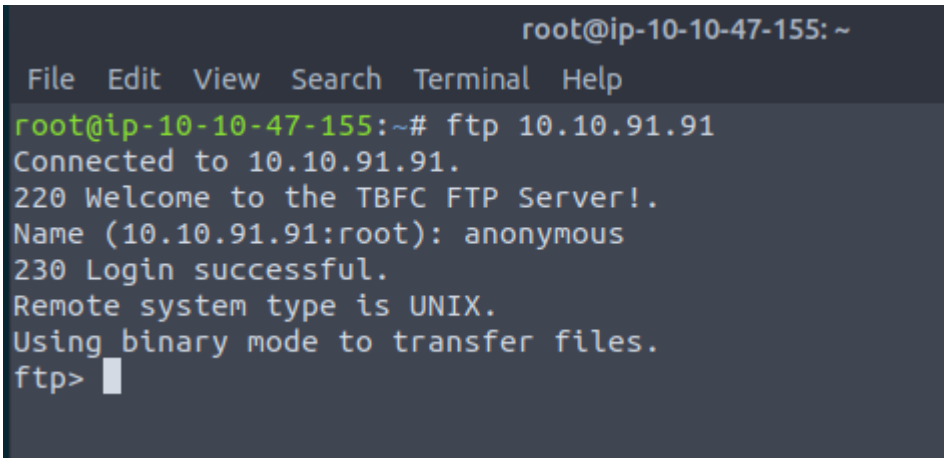
```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-08 16:35 GMT
Nmap scan report for ip-10-10-129-156.eu-west-1.compute.internal (10.10.129.156)
Host is up (0.00050s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_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
ocol 2.0)
| ssh-hostkey:
```

Day 9: Anyone Can Be Santa!

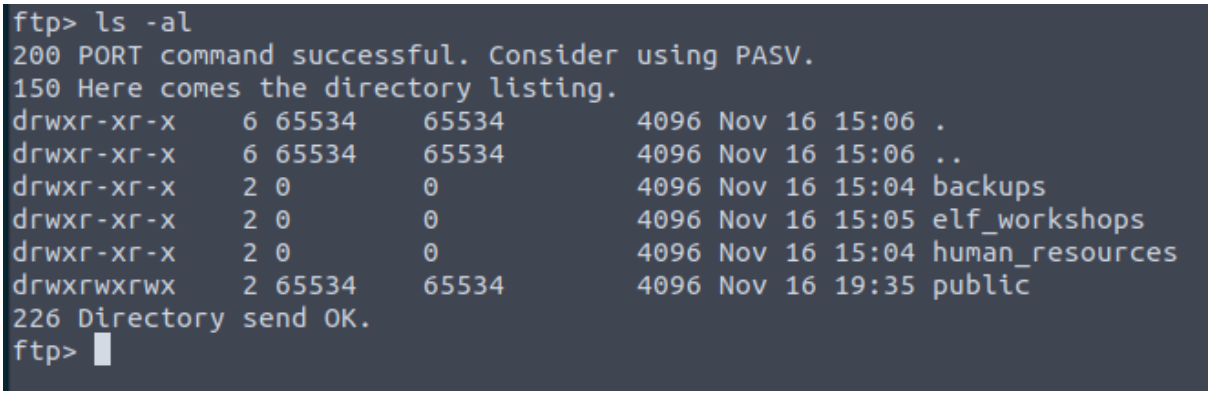
Question 1

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

We first signed in as "anonymous" to the FTP server:



After examining the directories, we can see that there is one that the anonymous user may access and is open to the public:



Question 2

What script gets executed within this directory?

We moved directories into "public" and then searched through the contents to discover the answer to this. Within is a script with the name of backup.sh.

```
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 19:35 .
drwxr-xr-x    6 65534    65534        4096 Nov 16 15:06 ..
-rwxr-xr-x    1 111      113           341 Nov 16 19:34 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16 19:35 shoppinglist.txt
226 Directory send OK.
ftp>
```

Question 3

What movie did Santa have on his Christmas shopping list?

We used the "get" command to acquire the shopping list. We can see it right now since it is on my computer.

```
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 (18.5130 kB/s)
ftp>
```

```
root@ip-10-10-47-155: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-47-155:~# ls
Desktop    Instructions  Postman  shoppinglist.txt
Downloads  Pictures      Scripts  thinclient_drives
root@ip-10-10-47-155:~# cat shoppinglist.txt
The Polar Express Movie
root@ip-10-10-47-155:~#
```

Question 4

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

In the same manner, We first downloaded the file from the ftp site.

```
ftp> get backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.sh (341 bytes).
226 Transfer complete.
341 bytes received in 0.00 secs (6.2539 MB/s)
ftp>
```

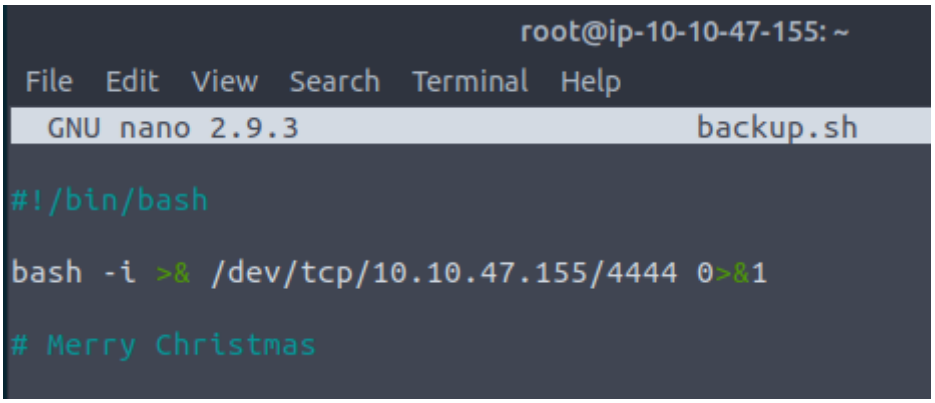
We could then see what was within.

```
root@ip-10-10-47-155: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-47-155:~# ls
backup.sh  Downloads     Pictures  Scripts          thinclient_drives
Desktop    Instructions  Postman   shoppinglist.txt
root@ip-10-10-47-155:~# cat backup.sh
#!/bin/bash

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

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

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

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


root@ip-10-10-47-155:~#
```

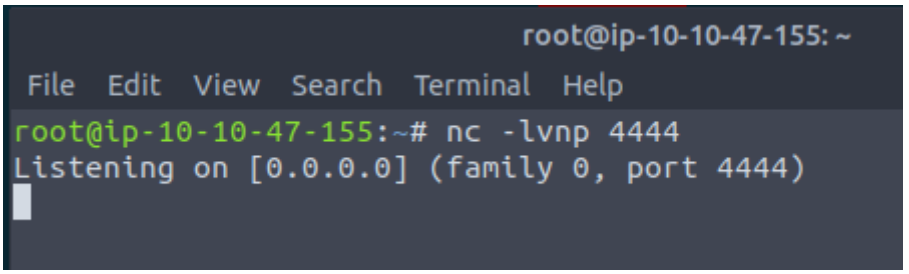
To begin editing, We opened the file in Nano.

```
root@ip-10-10-47-155:~# nano backup.sh
root@ip-10-10-47-155:~#
```

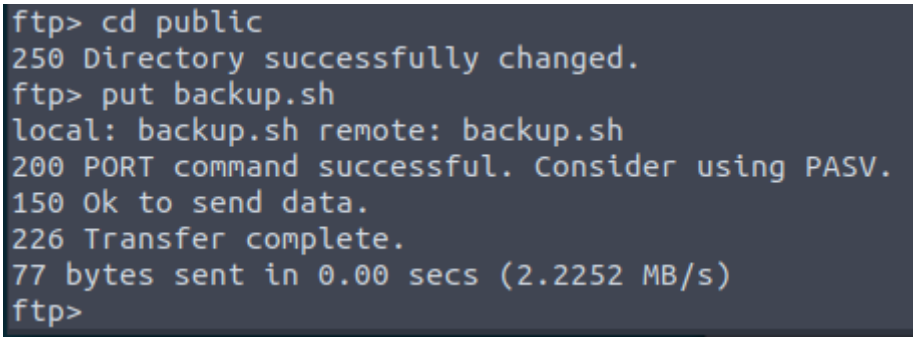
Then removed everything else and replaced it with something that would give me a reverse shell using a Reverse Shell Cheat Sheet.



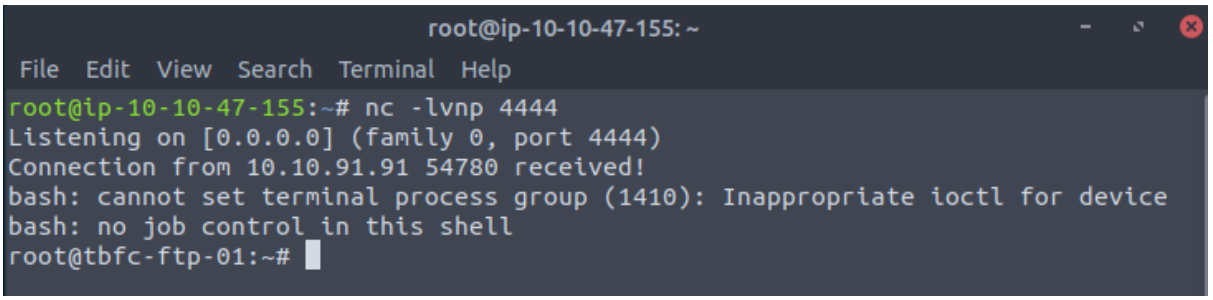
However, before We send it over. We're going to use netcat to create a listener. Use the same port that the script supplied.



Close and save the document using Ctrl + X, then use the "put" command to submit it to the ftp server. It will be added to the same open file that we have access to.



We will obtain a connection at our listener after a little while:



We just need to go to the flag.txt file from here.