

# PSP0201

## Week 3

### Writeup

Group Name: ikun no 1

Members

ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

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

Tool used: kali Linux, Firefox, Nmap, Google

Solution/Walkthrough:

Q1

# 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.

Find out the answer through GOOGLE.

Q2

```
(1211101401@kali)-[~]
$ sudo nmap -O 10.10.210.108
[sudo] password for 1211101401:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 01:14 EDT
Nmap scan report for 10.10.210.108
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server
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 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.46 seconds
```

The ports can be found using nmap in the machine. The port number will be shown after the scan is done.

Q3,Q4,Q5,Q6

```
1211101401@kali: ~  
File Actions Edit View Help  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 01:23 EDT  
Nmap scan report for 10.10.210.108  
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-generator: Hugo 0.78.2  
|_ http-title: TBFC&#39;s Internal Blog  
|_ http-server-header: Apache/2.4.29 (Ubuntu)  
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 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
```

Q3. The name can be found in the list.

Q4. The apache version can be found behind the apache/x.x.xx

Q5. The one that runs at port 2222 can be found which is ssh.

Q6. From the title below the port 80 information, it states that it is "Internal Blog". From this we can guess it as a blog.