

# PSP0201

## Week 3

## Writeup

Group Name: Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha binti Muhd Firdaus	Member

## Day 8 : Networking – What's under the Christmas tree?

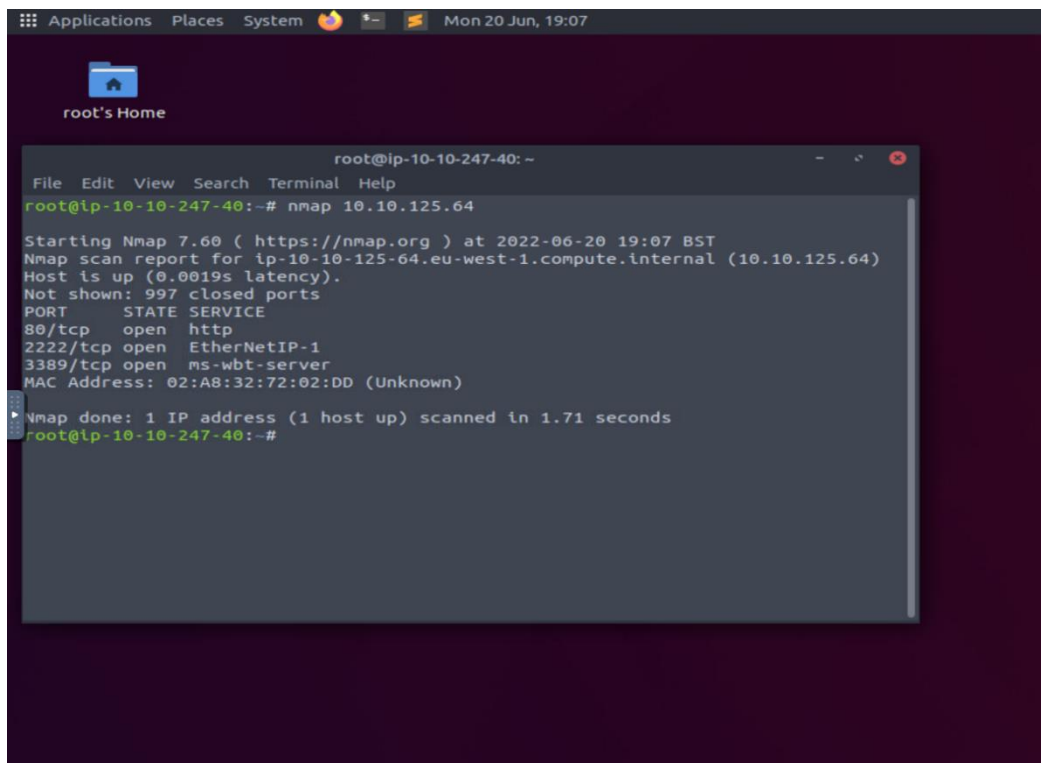
**Tools used:** Kali Linux

### Question 1

After some research, we gather that Snort was created in 1998.

### Question 2

With the nmap command, we found three port numbers which are 80, 2222, and 3389.

A screenshot of a Kali Linux desktop environment. The background is a dark purple wallpaper with a folder icon labeled 'root's Home'. A terminal window is open, displaying the output of an nmap scan. The terminal title is 'root@ip-10-10-247-40: ~'. The command 'nmap 10.10.125.64' has been executed. The output shows the scan starting at 2022-06-20 19:07 BST, reporting the host is up with 0.0019s latency, and listing three open ports: 80/tcp (http), 2222/tcp (EthernetIP-1), and 3389/tcp (ms-wbt-server). The scan was completed in 1.71 seconds.

```
root@ip-10-10-247-40: ~  
File Edit View Search Terminal Help  
root@ip-10-10-247-40:~# nmap 10.10.125.64  
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-20 19:07 BST  
Nmap scan report for ip-10-10-125-64.eu-west-1.compute.internal (10.10.125.64)  
Host is up (0.0019s 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:A8:32:72:02:DD (Unknown)  
Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds  
root@ip-10-10-247-40:~#
```

**-Pn scan:**

```
root's Home
root@ip-10-10-247-40: ~
File Edit View Search Terminal Help
Nmap scan report for ip-10-10-125-64.eu-west-1.compute.internal (10.10.125.64)
Host is up (0.0019s 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:AB:32:72:02:DD (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds
root@ip-10-10-247-40:~# nmap -Pn 10.10.125.64

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-20 19:14 BST
Nmap scan report for ip-10-10-125-64.eu-west-1.compute.internal (10.10.125.64)
Host is up (0.0012s 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:AB:32:72:02:DD (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
root@ip-10-10-247-40:~# a
```

### Question 3,4 ,5 & 6

With the port numbers that we obtained, we run 'nmap -pn and -V -sC' scan command. Here we found the name of the linux distribution, the version of Apache and the what's running on port 2222. From the http-title, we also concluded that the website might be used for a blog.

```
root's Home
root@ip-10-10-85-47: ~
File Edit View Search Terminal Help
Nmap scan report for ip-10-10-18-103.eu-west-1.compute.internal (10.10.18.103)
Host is up (0.0013s 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: 02:49:CA:8A:8C:F1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds
root@ip-10-10-85-47:~# nmap -Pn 10.10.18.103

Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-06 23:12 GMT
Nmap scan report for ip-10-10-18-103.eu-west-1.compute.internal (10.10.18.103)
Host is up (0.0011s 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: 02:49:CA:8A:8C:F1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
root@ip-10-10-85-47:~# nmap -A -O -sV -iC 10.10.18.103
```

```
root@ip-10-10-85-47: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-85-47: ~ x root@ip-10-10-85-47: ~ x
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:
|   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)
```

### Thought Process/Methodology:

First, we did a little research and found that the Snort was created back in 1998. Then, we start running the nmap command to find the ports. Using nmap \*IP address\*, we manage to obtain the port numbers. With the port numbers that we obtained, we run 'nmap -pn and -V -sC' scan command. Here we found the name of the linux distribution, the version of Apache and the what's running on port 2222. From the http-title, we also concluded that the website might be used for a blog.