

# PSP0201

## Week 3

## Writeup

Group Name: ikun no 1

Members

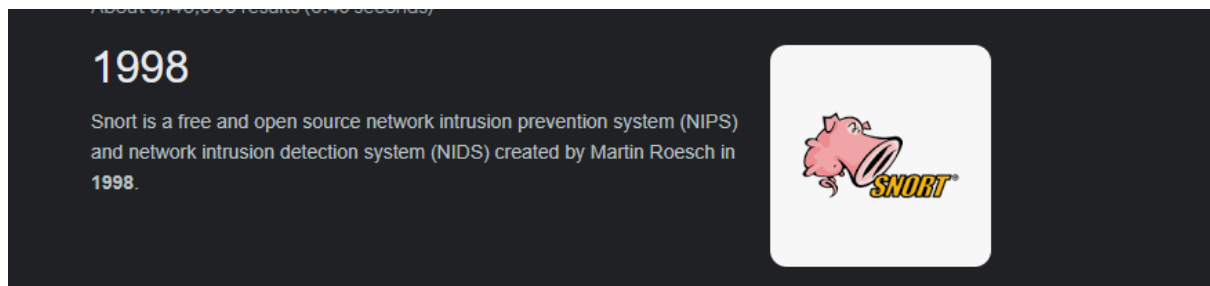
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

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

**Tool used:** Kali-Linux, Nmap's Scripting Machine

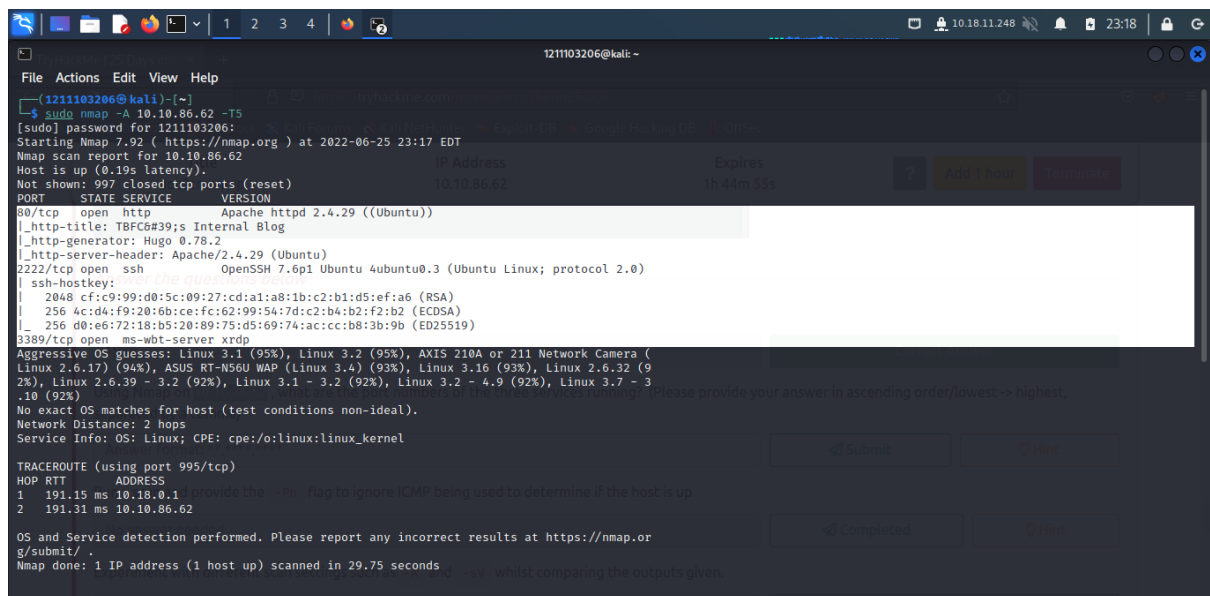
**Solution/walkthrough:**

### Question 1



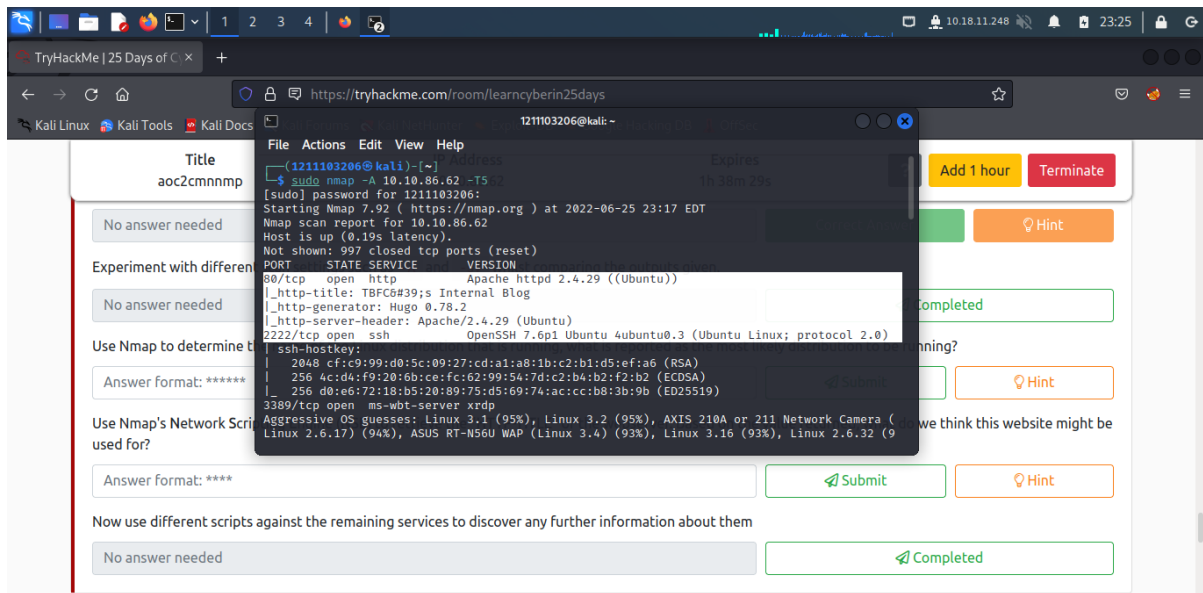
Search the answer in Google.

### Question 2



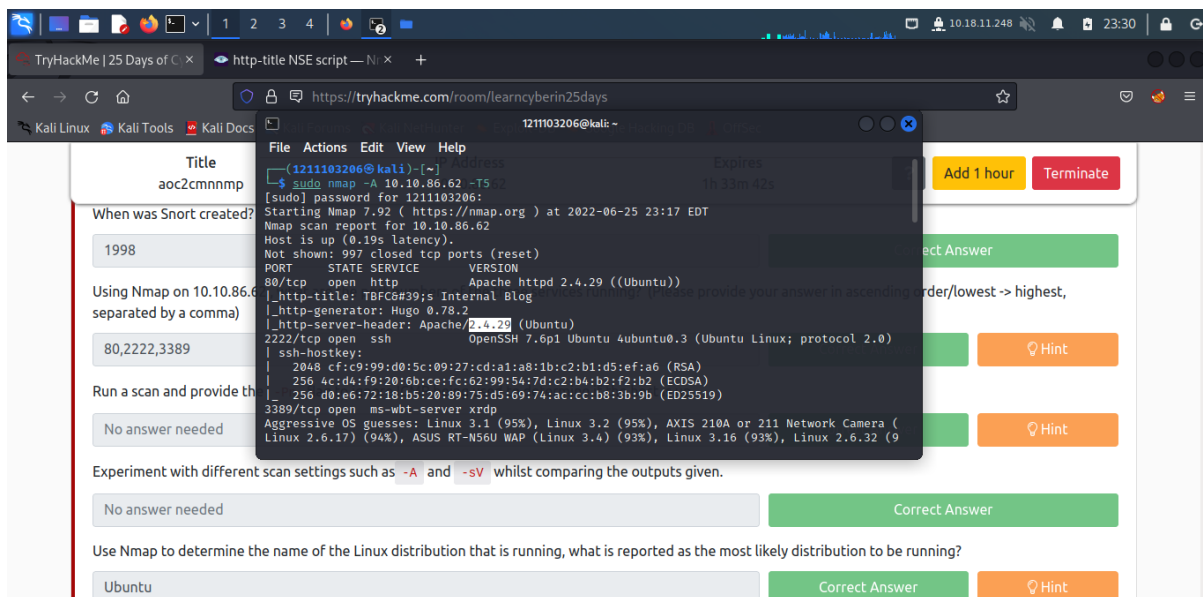
Using nmap machine ip to find the port and port shown.

### Question 3



Look to the nmap again, Ubuntu is processing.

#### Question 4



Still can find the answer in the nmap again.

#### Question 5

TryHackMe | 25 Days of CTF

https://tryhackme.com/room/learnycyberin25days

1211103206@kali -

File Actions Edit View Help

```

(1211103206@kali)~$ sudo nmap -A 10.10.86.62 -T5
[sudo] password for 1211103206:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 23:17 EDT
Nmap scan report for 10.10.86.62
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  ssh
3389/tcp  open  ms-wbt-server

OS: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (93%)
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (93%)

```

When was Snort created?

1998

Using Nmap on 10.10.86.62 separated by a comma

80,2222,3389

Run a scan and provide the results

No answer needed

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

The port 2222 that running is SSH.

## Question 6

TryHackMe | 25 Days of CTF

https://tryhackme.com/room/learnycyberin25days

1211103206@kali -

File Actions Edit View Help

```

(1211103206@kali)~$ nmap -script http-title 10.10.86.62 -T5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 23:33 EDT
Nmap scan report for 10.10.86.62
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNet/IP-1
3389/tcp  open  ms-wbt-server

OS: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (93%)
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (93%)

```

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

Use Nmap's Network Scripting Engine used for?

blog

Now use different scripts against the host

No answer needed

Task 11 [Day 9] Networking Anyone can be Santa!

Task 12 [Day 10] Networking Don't be sELfish!

Using the scripting machine and type with format `--script http-title <ip address> -T5`. Then the answer shown.