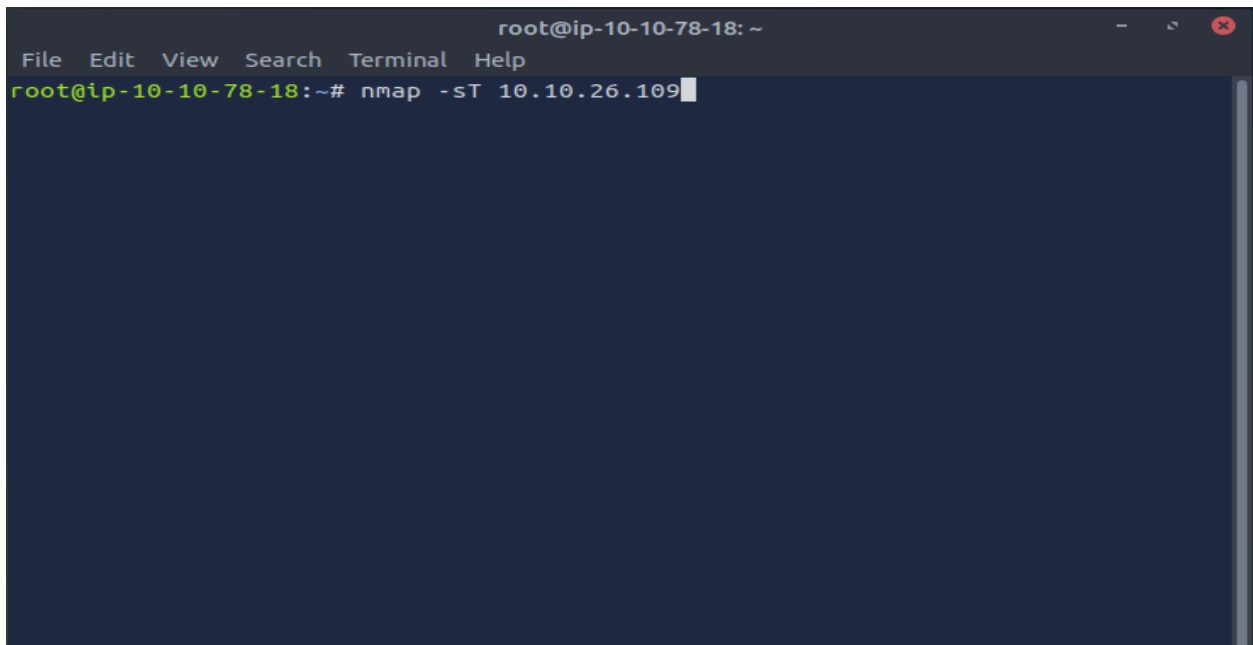


# Nmap Port Scan

What is a port scan? A port scan is the ability to discover the identity of open ports on a network device or system. Port scanning can reveal **6** types of port configuration types that can either allow us to establish a connection, or identify an insight as to why the connection was not established.

## 6 types of port configurations:

1. **OPEN:** Some services listening on port
2. **CLOSED:** No services listening on port
3. **FILTERED:** Nmap cannot determine if port is open/closed due to eg. firewall
4. **UNFILTERED:** Cannot determine if port open/closed but is accessible eg. ACK -sA
5. **OPEN/FILTERED:** Cannot determine if port is open or filtered
6. **CLOSED/FILTERED:** Cannot determine if port is closed or filtered

A screenshot of a terminal window with a dark blue background. The title bar at the top reads 'root@ip-10-10-78-18: ~'. Below the title bar is a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The main area of the terminal shows a prompt 'root@ip-10-10-78-18:~#' followed by the command 'nmap -sT 10.10.26.109' entered in green text. A white cursor is positioned at the end of the command.

Here we have our console, and we are going to demonstrate a port scan. Let's break it up though. "nmap" is us essentially telling the console we wish to use nmap, we must specify this at the beginning.

"-sT" is the TCP connect scan and is used to establish a TCP connection to each port it finds.

But! **It is noisy.**

"10.10.26.109" is the IP (**Internet Protocol**) we wish to use, which essentially identifies a host on the network.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-26 10:29 BST
Nmap scan report for ip-10-10-26-109.eu-west-1.compute.internal (10.10.26.109)
Host is up (0.00099s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
993/tcp   open  imaps
995/tcp   open  pop3s
MAC Address: 02:FA:1F:3D:A0:F3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

So here we can see once we send the data into the command prompt, it received ports and tells us what they are, and that they are open!

**SSH = Secure Shell**

**SMTP = Simple Mail Transfer Protocol**

**HTTP = Hyper Text Transfer Protocol**

**POP3 = Post Office Protocol 3**

**RPCBIND = Port Map / Remote Procedure Call**

**IMAP = Internet Message Access Protocol**

**IMAPS = Internet Message Access Protocol Secure**

**POP3S = Post Office Protocol Secure**

```
Pentester Terminal

pentester@TryHackMe$ nmap -sT 10.10.26.109

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 09:53 BST
Nmap scan report for 10.10.26.109
Host is up (0.0024s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
111/tcp    open  rpcbind
143/tcp    open  imap
993/tcp    open  imaps
995/tcp    open  pop3s
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

We are also asked 2 questions:

Which port number was closed in the scan above but is now open on this virtual machine?

**110 - POP3** Was closed as shown above, when we ran the scan port 110 was open! But during the exercise example, it was closed.

What is Nmap's guess about the newly installed service?

**POP3** - This was the example missing on the above port, but we know on our scan POP3 is associated with port 110.

Conclusion: Nmap is a very simple tool, allowing us to establish open ports! However, using -sT generates us with very useful information, but also generates network traffic, this is vital in offensive tests, when we are trying to keep a low profile whilst reeling in as much information as possible.