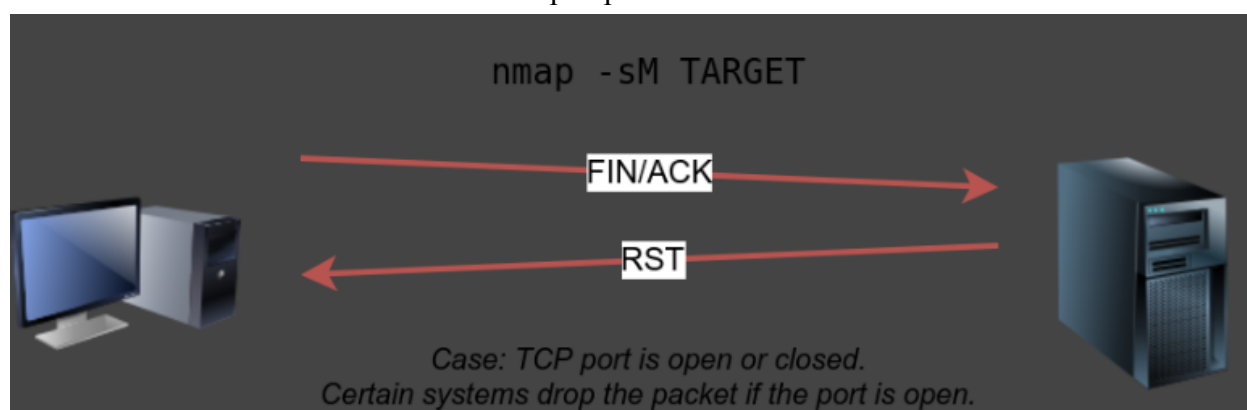


Nmap Maimon Scan

What is a Maimon scan? **Uriel Maimon first described it in 1996** - in this scan the FIN and ACK bits are set. The target should send an RST packet in response.

However, certain BSD-Derived systems drop the packet if it is an open port exposing the open ports. The scan won't work on most targets encountered in modern networks. However, it helps generate a picture of the different methods used in hacking. This can be done by **-sM** to achieve this.

Most target systems respond with an RST packet regardless of whether the TCP port is open. In such a case we won't be able to discover open ports.



```
Pentester Terminal

pentester@TryHackMe$ sudo nmap -sM 10.10.252.27

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:36 BST
Nmap scan report for ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.27)
Host is up (0.00095s latency).
All 1000 scanned ports on ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.27)
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.61 seconds
```

This type of scan is not the first one would pick to discover a system however, there may come a time where it could come in handy.