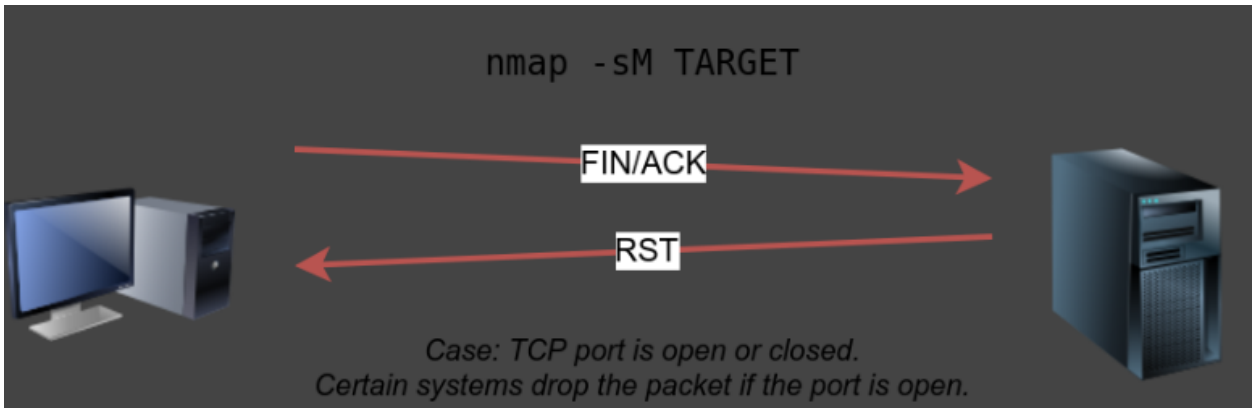
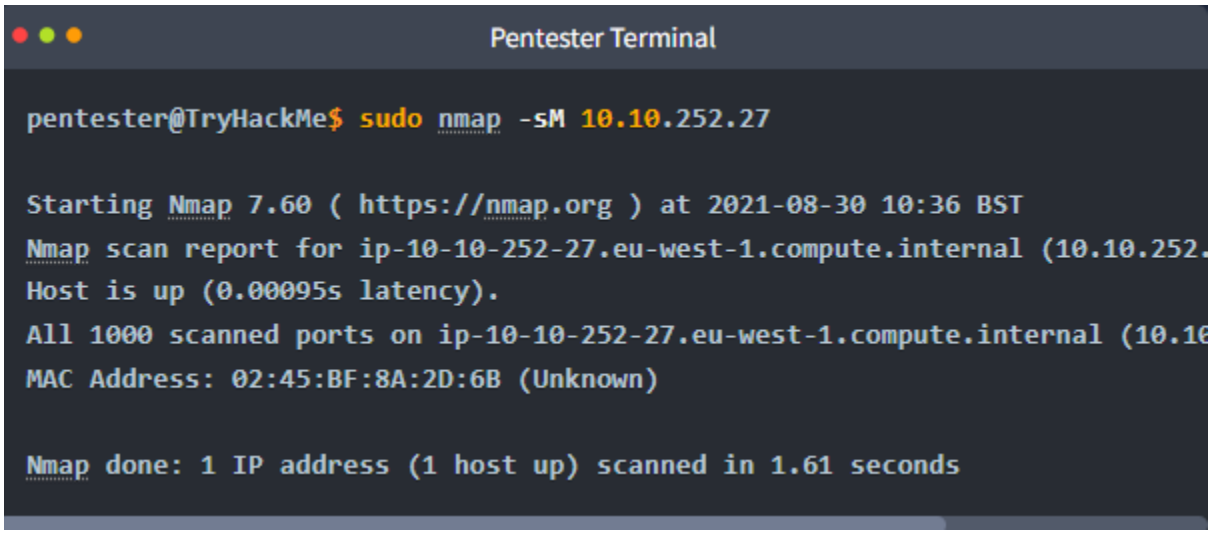
Nmap Maimon Scan

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 opten 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.





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.