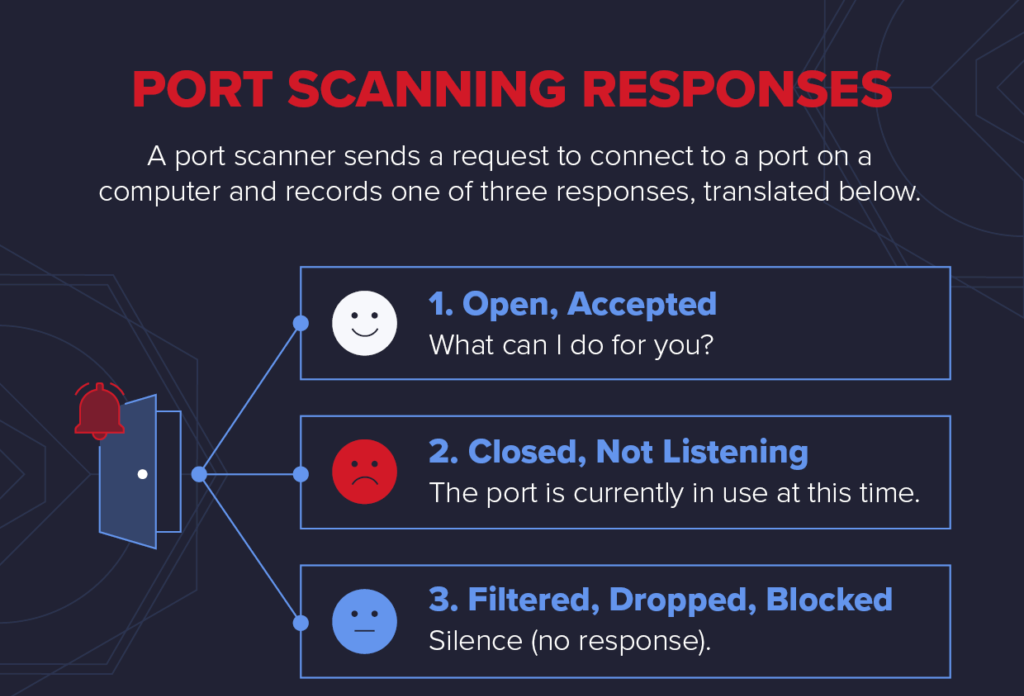
**PORT SCANNER**

A port scanner is a computer program that checks network ports for one of three possible statuses – open, closed, or filtered.

Port scanners are valuable tools in diagnosing network and connectivity issues. However, attackers use port scanners to detect possible access points for infiltration and to identify what kinds of devices you are running on the network, like firewalls, proxy serversor VPN servers.



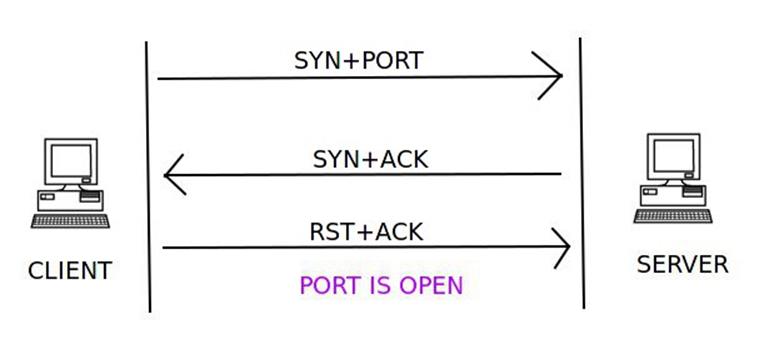
**SCAPY**

Scapy is a powerful python library that allows us to manipulate as to work with network packets. I is able to forge or decode packets of a wide number of protocols, send them on the wire, capture them, match requests and replies, and much more. It can easily handle most classical tasks like scanning, tracerouting, probing, unit test, attacks or network discovery. It also performs a lot of other specific tasks that most other tools cant handle, like sending invalid frames.

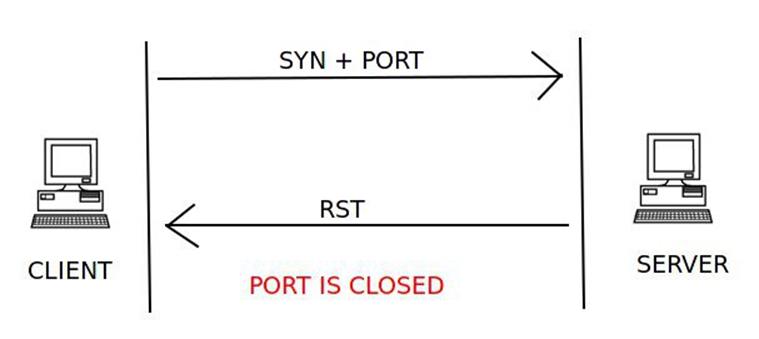
**PORT SCANNING USING SCAPY**

**TCP CONNECT SCAN:**

TCP connect is a three-way handshake between the client and the server. If the three-way handshake takes place, then communication has been established.

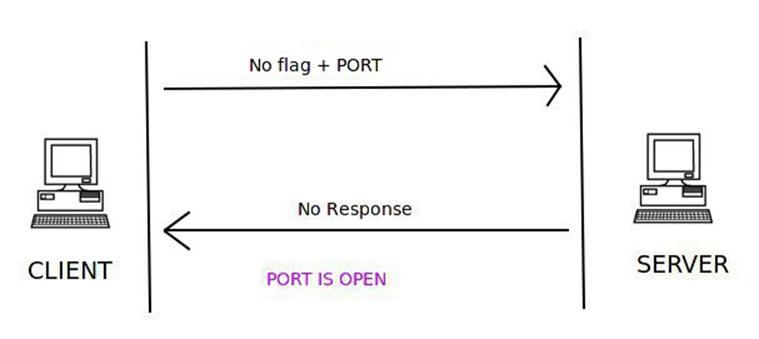


A client trying to connect to a server on port 80 initializes the connection by sending a TCP packet with the SYN flag set and the port to which it wants to connect (in this case port 80). If the port is open on the server and is accepting connections, it responds with a TCP packet with the SYN and ACK flags set. The connection is established by the client sending an acknowledgement ACK and RST flag in the final handshake. If this three-way handshake is completed, then the port on the server is open.

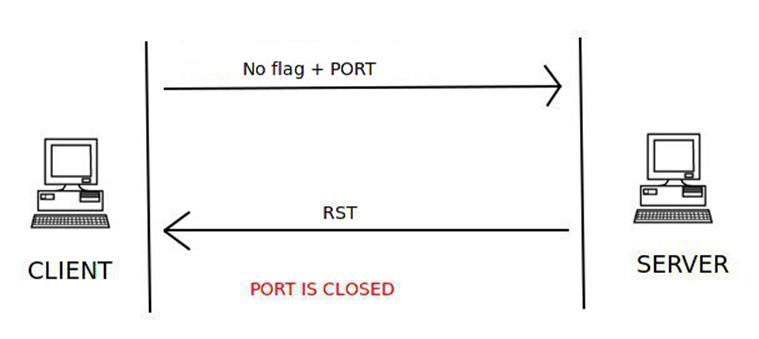


The client sends the first handshake using the SYN flag and port to connect to the server in a TCP packet. If the server responds with a RST instead of a SYN-ACK, then that particular port is closed on the server.

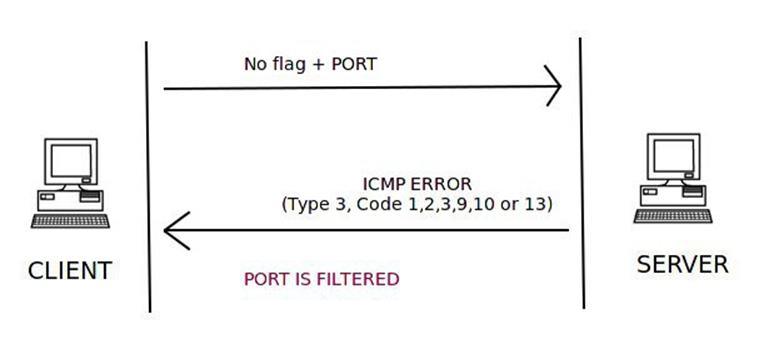
**NULL PORT SCANNER:**



In a NULL scan, no flag is set inside the TCP packet. The TCP packet is sent along with the port number only to the server. If the server sends no response to the NULL scan packet, then that particular port is open.



If the server responds with the RST flag set in a TCP packet, then the port is closed on the server.



An ICMP error of type 3 and code 1, 2, 3, 9, 10, or 13 means the port is filtered on the server.