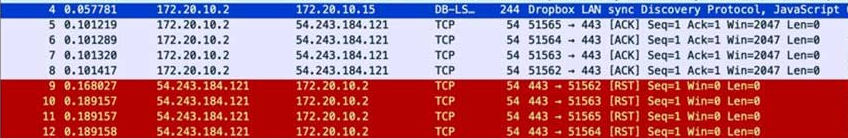
# Scanning - Port scan

How nmap is identifying the open and close ports with packet level ?

Nmap identifies open and closed ports by sending crafted TCP and UDP packets and analyzing the responses. For TCP, it uses the TCP handshake to determine if a port is open, closed, or filtered (firewall). For UDP, it sends packets and looks for responses like ICMP(Internet Control Message Protocol) port unreachable messages to determine if a port is closed or open/filtered.



**TCP Port Scanning:**

**Open Ports:**

When Nmap sends a SYN packet to an open TCP port, the target server responds with a SYN-ACK packet, indicating the port is ready to establish a connection.

**Closed Ports:**

If the port is closed, the target server responds with an RST (reset) packet, signifying the connection attempt is rejected.

**Filtered Ports:**

If no response is received after several retries, Nmap assumes the port is filtered, likely by a firewall, and marks it as such

**UDP Port Scanning:**

**Open/Filtered Ports:**

If Nmap sends a UDP packet to a port and receives no response, it marks the port as open|filtered. This means the port might be open, or it might be blocked by a firewall.

**Closed Ports:**

If Nmap receives an ICMP port unreachable message, it indicates that the UDP port is closed.