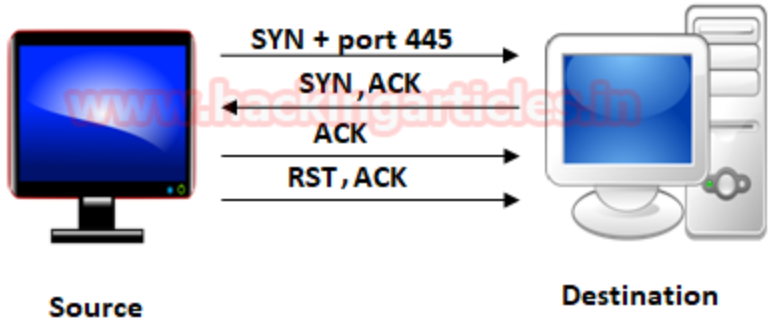
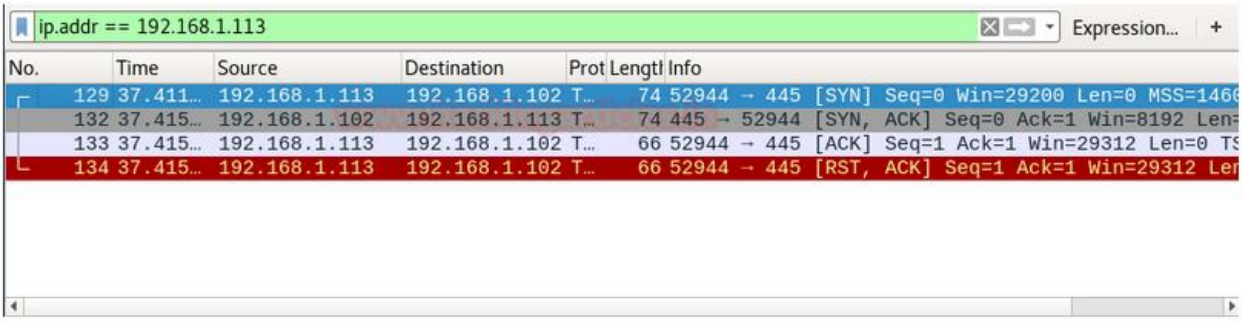
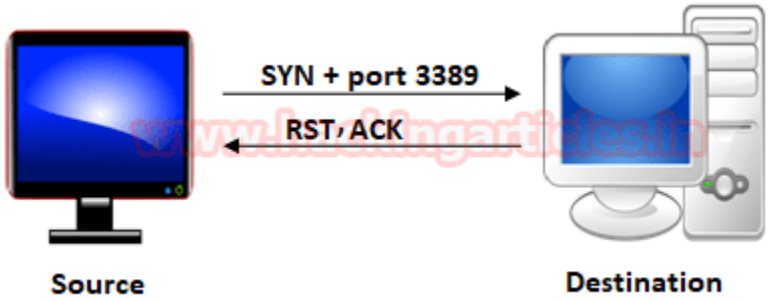
TYPES OF NMAP SCANNING

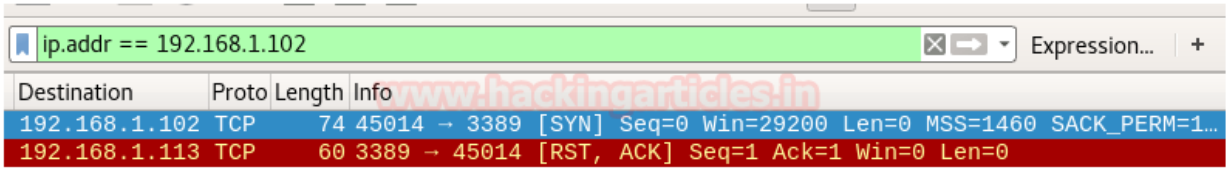
TCP scan for open ports





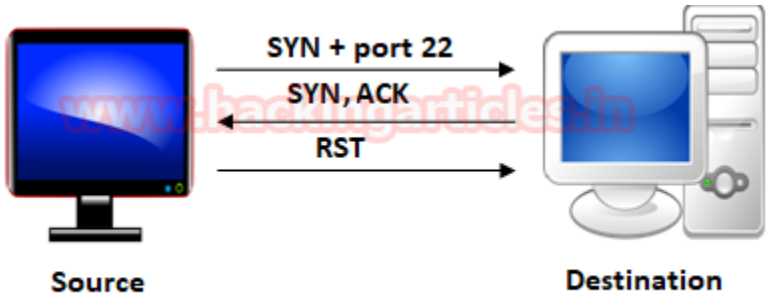
TCP scan for close ports

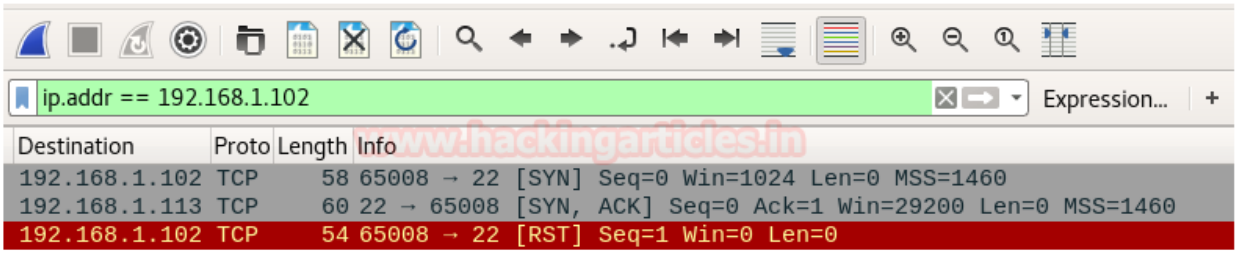




Stealth scan for open ports

- In stealth scan connection establishment is only done halfway.



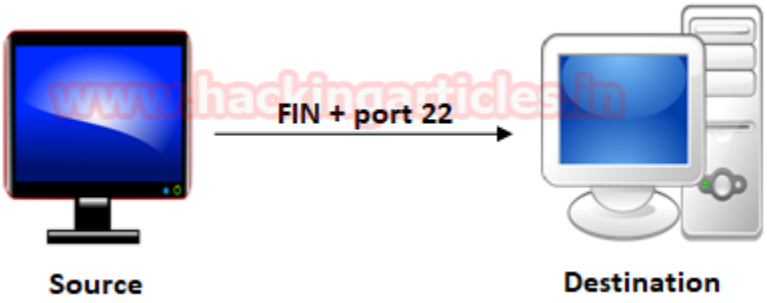


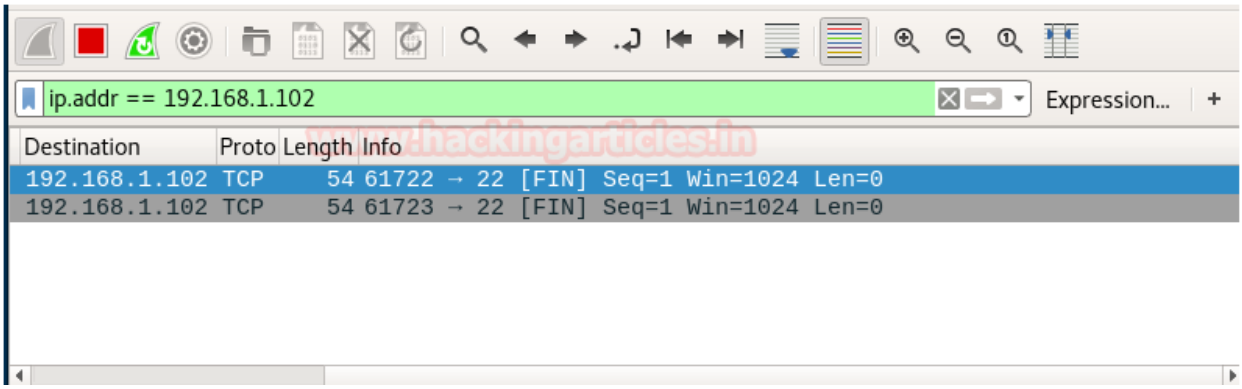
Stealth scan for closed ports

- Same as TCP scan for closed ports

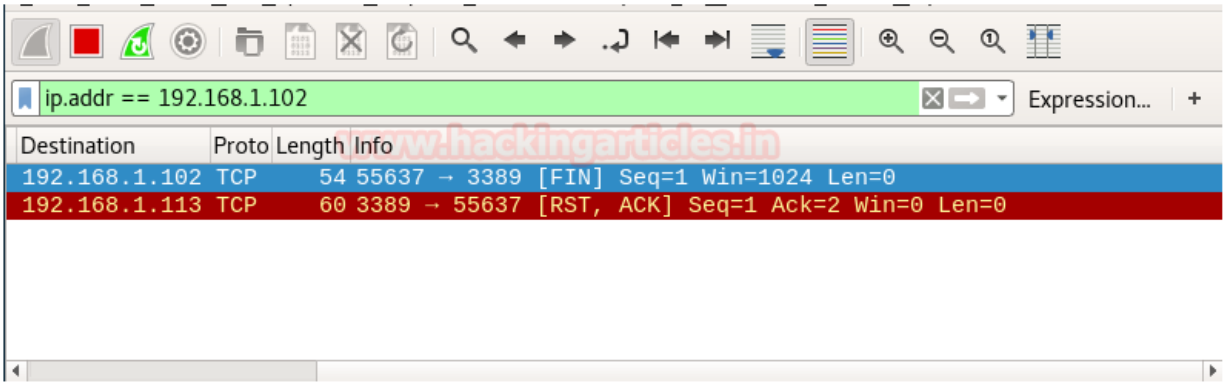
Fin scan for open ports

- If the port is open when the port receives packet with fin flag set without connection establishment destination will never reply back.(Destination not replying back for fin means the port is open)



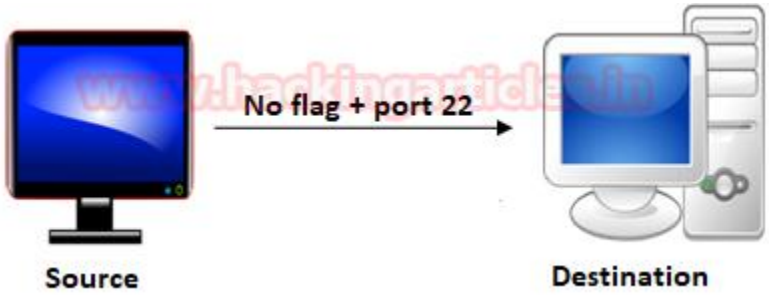


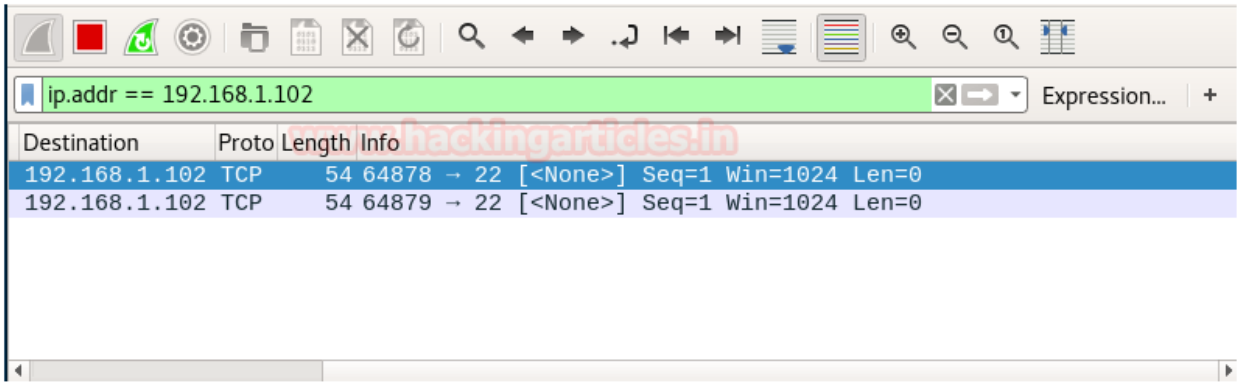
Fin scan for closed ports



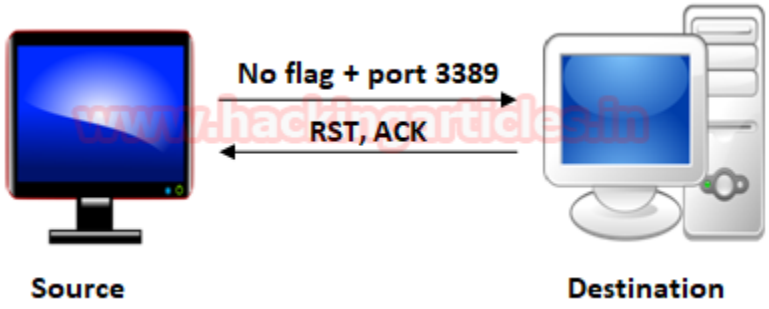
Null scan for open ports

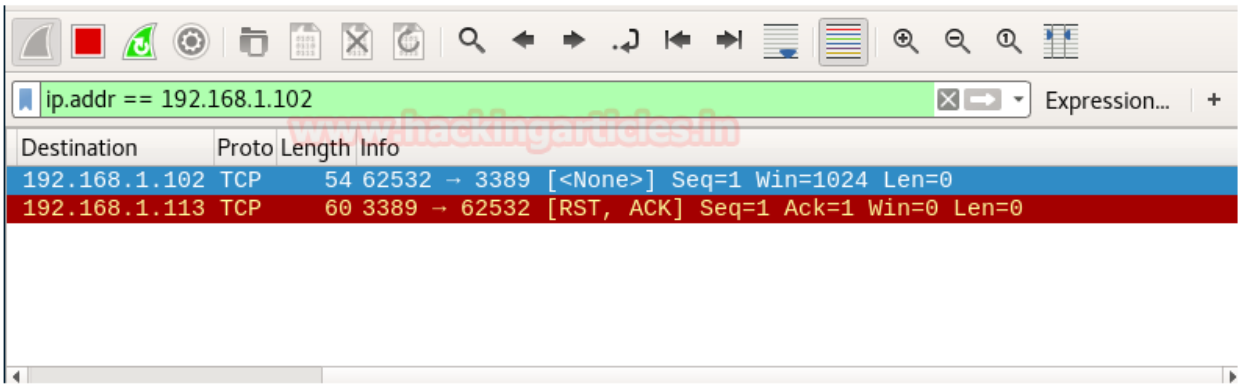
A Null Scan is a series of TCP packets which hold a sequence number of “zeros” (0000000) and since there are none flags set, the destination will not know how to reply the request. It will discard the packet and no reply will be sent, which indicate that port is open.





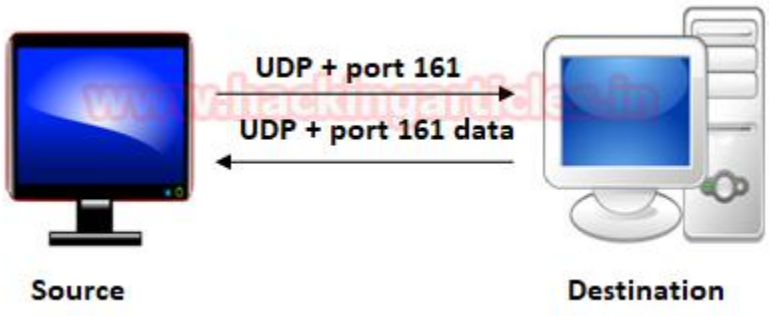
Null scan for closed ports

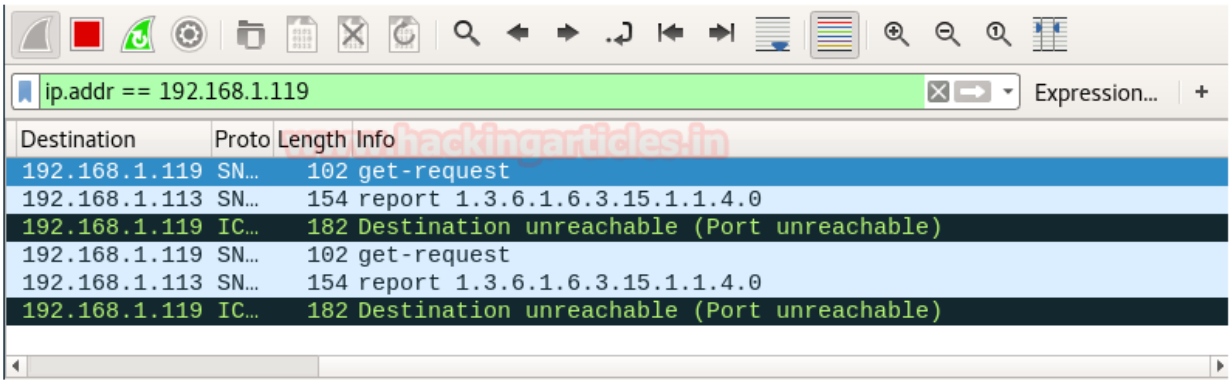




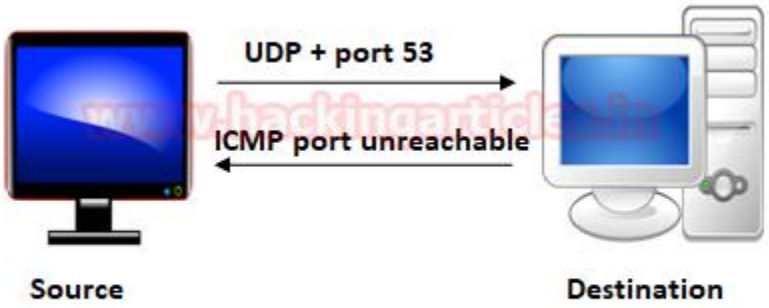
UDP scan for open port

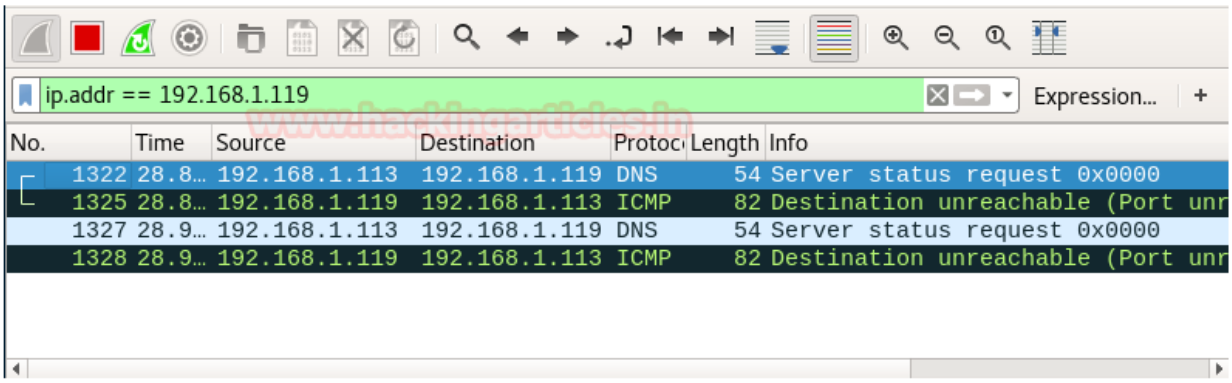
UDP scan works by sending a UDP packet to every destination port; it is a connection less protocol. For some common ports such as 53 and 161, a protocol-specific payload is sent to increase response rate, a service will respond with a UDP packet, proving that it is open. If no response is received after retransmissions, the port is classified as open|filtered. This means that the port could be open, or perhaps packet filters are blocking the communication.





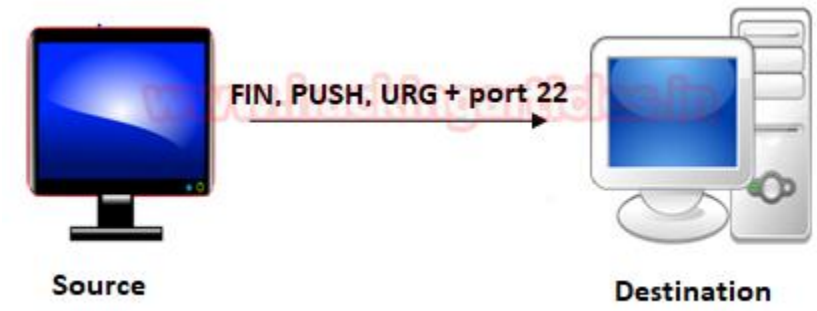
UDP scan for closed port

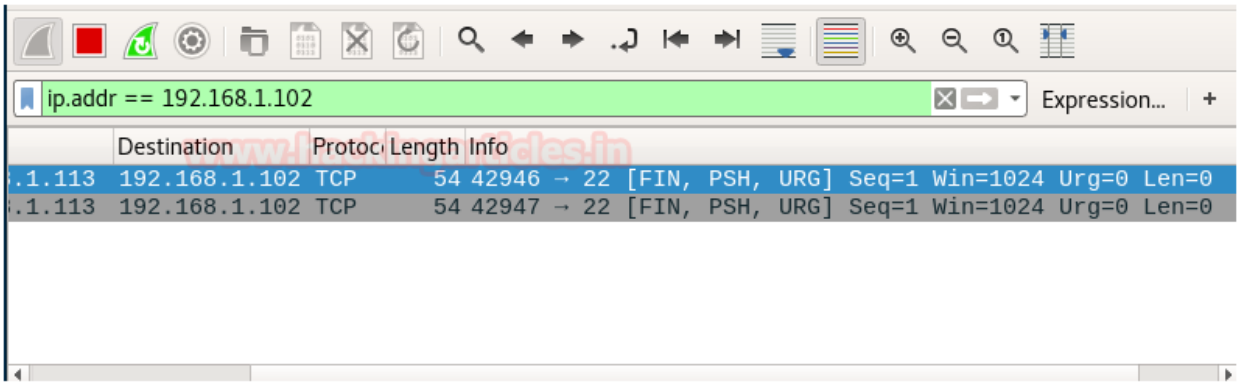




XMAS scan for open ports

These scans are designed to manipulate the PSH, URG and FIN flags of the TCP header, Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree. When source sent FIN, PUSH, and URG packet to specific port and if port is open then destination will discard the packets and will not sent any reply to source.





XMAS scan for closed ports