Nmap

Nmap: used to perform many different kinds of port scan. Determines if port is open, closed, or filtered.

Port: networking construct that is used to direct traffic to the right application on a server.

Scan Types:

-TCP Connect Scans (-sT):

TCP three-way handshake-

Diagram

Description automatically generated

Stage 1: connecting terminal sends a TCP request to target server with SYN flag set.

Stage 2: Server acknowledges this packet with a TCP response containing the SYN flag and ACK flag.

Stage 3: Terminal completes the handshake by sending a TCP request with the ACK flag set.

Diagram

Description automatically generated

If port is closed, target sever with RST (Reset) flag.

If nothing is sent back after a SYN request, then the port is considered to be filtered, which means it’s being hidden.

-SYN Scans:

Diagram

Description automatically generated

Used to scan TCP port-range of target(s).

-Often referred to as a “half-open” or “stealth” scans.

-Doesn’t fully complete 3-way handshake, and returns RST to keep it from continuing request repeatedly.

-It scans for open port, but is considered to be stealthy because it doesn’t complete the 3-way handshake, it’s not logged by applications listening on open ports, and are significantly faster than TCP connect scan. So it’s just scanning for open port w/o actually connecting.

Disadvantages: -require sudo permissions and unstable services can sometimes be brought down by SYN scans.

-UDP Scans:

UDP connections are stateless—meaning that rather than initiating a connection with a back and forth handshake, they rely on sending packets to a target port and hoping they make it. It prioritizes speed over quality. Lack of acknowledgement makes it more difficult/slower to scan.

No response usually means the port is open|filtered.

A closed UDP port responds with an ICMP (ping) packet saying port is unreachable.

It’s hard to tell if UDP port is actually open, making it much slower than TCP scans.

-NULL, FIN and Xmas Scans:

Less commonly used. All three are interlinked and then to be even stealthier than a SYN “stealth” scan.