Host Discovery:

It is the initial phase in network reconnaissance and vulnerability assessment, aimed at identifying which devices or hosts within a specified IP address range are currently active and reachable on the network. This step is crucial because it narrows down the list of potential targets, making subsequent scans more efficient and focused.

Launch this scan to see what hosts are on your network and associated information such as IP address, FQDN, operating systems, and open ports, if available. After you have a list of hosts, you can choose what hosts you want to target in a specific vulnerability scan.

This saves time and avoids false positives from scanning offline systems. Nessus uses multiple methods to determine if a host is alive. If any of these checks succeed, Nessus marks the host or target as alive:

- ICMP Echo (Ping Scan)
- TCP ACK to port 443 or 80
- TCP SYN to port 22, 53, 443, 445, 3389
- ARP ping (for local subnets only)