Nmap: - Scans networks to discover devices and services; used for network mapping and security auditing.

Recon-ng: - A web reconnaissance tool with a modular framework for gathering open-source intelligence (OSINT).

Zenmap: - A graphical front-end for Nmap, making it easier to use for beginners.

Maltego :- A tool for gathering and visualizing relationships between people, domains, IPs, etc. (OSINT).

Gobuster: - A tool for brute-forcing URIs, DNS subdomains, and virtual hosts. Fast and command-line based.

