

Stages and Tools

Reconnaissance	Mapping and Fingerprinting e.g NMAP
Vulnerability Assessment	Vulnerability Scanner e.g OpenVAS
Penetration Testing	Exploit Framework e.g Metasploit

Nmap

Network Mapping
and Host Fingerprinting