Vulnerability Assessment vs Penetration Testing

Vulnerability assessment

➡ Identify and quantify the vulnerabilities of a system

http://www.sans.org/reading-room/whitepapers/basics/vulnerability-assessment-421

Penetration testing (a.k.a pentest)

➡ Authorized and deliberate attack of a system with the intention
of finding security weaknesses

http://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635

Stages and Tools

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