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)

➡ 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

Security tools

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