penetration testing tools

Name	description	Advantage	Ease of use	flexibility	reputation	licensing	Ease to install	Average score
Metasploit	“Metasploit is the most popular pen test tool,”	complex	5	5	5	5	5	5
Nessus Vulnerability Scanner	Nessus’ can only compare scans to a database of known vulnerability signatures,”	very noisy	5	5	4	3	5	4.4
Nmap	Nmap network scanner enables pen testers to determine the types of computers, servers, and hardware the enterprise has on its network.	useful for enumerating user access	4	5	5	4	4	4.4
Burp Suite	It maps and analyzes web applications, finding and exploiting vulnerabilities	rich tool & allows transparency	5	5	5	2	4	4.2
OWASP ZAP	ZAP offers automated and manual web application scanning,	not as feature rich, but is free and open-source & people who are just entering web application pen testing,	5	3	5	5	4	4.4
SQLmap	SQLmap automates the discovery of SQL Injection holes. It then	script-friendly tool	5	3	5	5	5	4.6

	exploits those vulnerabilities and takes complete control of databases and underlying servers							
Kali Linux	Kali Linux is an all-in-one tool comprising a suite of dedicated, pre-installed penetration testing (and security and forensics) tools. “It has tools for people who have no knowledge of security,”	Can open more than a dozen pen testing / exploit tools	2	1	5	5	3	3.2
Jawfish	Jawfish is a pen test tool that uses genetic algorithms. “Genetic algorithms look for things in the context of search,” says Saez. Based on search criteria, as Jawfish gets closer to what it is looking for, in this case a vulnerability, it can find a result. Jawfish does not require a signature database.	This tool is entirely new and not vetted for enterprise adoption. (Simply input an IP address for the server, a vulnerable web address at that IP address)	2	1	1	5	1	2