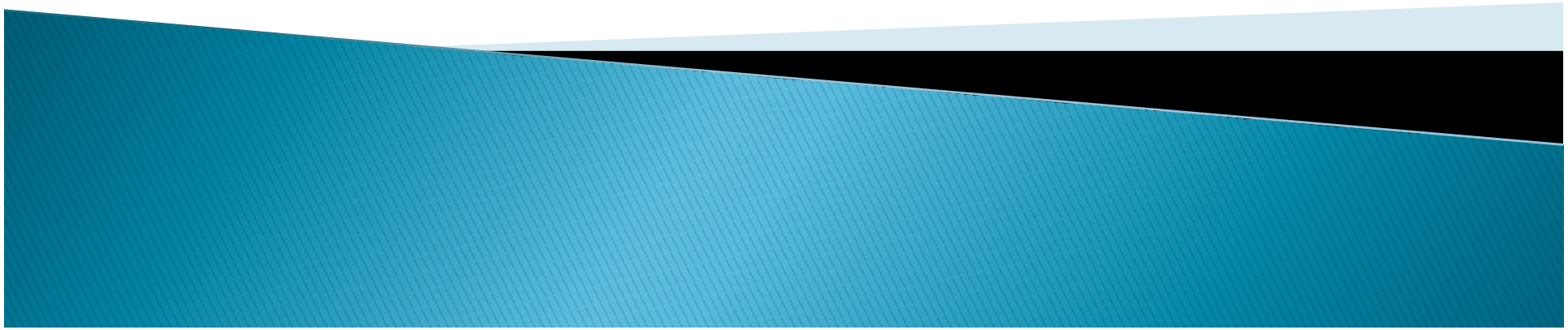
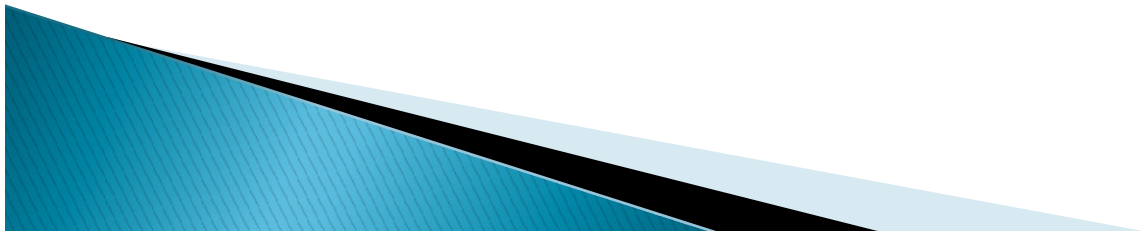
Rating of 8 penetation testing tools

Group 1



Rated tools:

- Metasploit
- Nessus Vulnerability Scanner
- Nmap
- Burp Suite
- OWASP – ZAP
- SQLmap
- Kali Linux
- Jawfish

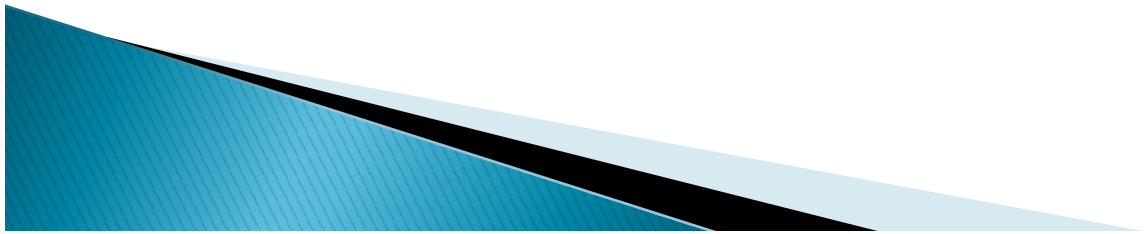


	Ease of install	Ease of use	Flexibility	Licensing	Privacy	Reputation
Metasploit	Easy to download and install	Detailed explanation of how to use but complex; User-friendly interface	Huge variarity of penetration testing; Enables easy testing of large networks with Ruby interface	Open Source & Commercial version	Higher Collects device and network data, user behavior; share it with third-partys	(metasploit & Rapid7) Developed with help from open source community
Nessus Vulnerability Scanner	Easy to download and install	Good support; User-friendly interface	Checks computers and firewalls for open ports and potential vulnerable software; Scans only known vulnerability signatures	Commercial tool (chargeable)	Higher Collects “any Personal Data you provide to us” Device and network data	(tenable) High reputation based on external rewards
Nmap	More difficult to install on Windows OS	Rudimentary interface; More complex to use	Identify open ports, software versions as wells as types of computers, servers and hardware of a network	Open Source	Lower Use of cookies – no more detailed information	(Insecure.org, Gordon Lyon) Good reputation based on his work
Burp Suite	Easy to download and install	Good support; User-friendly interface	Analyzing web applications functionality and security holes; Enables custom attacks	Commercial tool (chargeable)	Higher Collects personal, financial and usage data	(PortSwigger) Used by major Campanies like: Amazon, Google, Microsoft, FedEx

	Ease of install	Ease of use	Flexibility	Licensing	Privacy	Reputation
OWASP ZAP	Easy to download and install	User-friendly interface	Automated and manual web application scanning; Port scanning, brute force scanning	Open Source	Lower “Any content you add or any change that you make to a OWASP Site will be publicly and permanently available in addition to being associated with your GitHub username.”	(nonprofit OWASP Foundation) High repudation based on known corporate supporters like Adobe, GitLab, Fortify & BlackBelt Security
SQLmap	Easy to download and install	Rudimentary interface; More complex to use	Discovers SQL Injection holes	Open Source	Lower No privacy informations found	(sqlmap.org) Disclaimer: “This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY.”
Kali Linux	Easy to download and install; Possibility of mobile penetration testing for Android	Huge packet of testing tools; Rudimentary interface; Both aspects together could lead to overwhelming for beginners	Huge variarity of penetration testing; Combines many tools in one (e.g. Metasploit, Nmap , Burp Suit and SQLmap)	Open Source	Lower Collects personal information and uses cookies. Share information with governmental agencies or third-partys	(kali.org) Corporate supporters: GitLab, CLOUDFLARE, Ampere
Jawfisch	Difficult to find (Website not available);https://github.com/war-and-code/jawfish	Cannot be used intuitively; few explanations of use	Usability without signature database	Open Source	Lower No privacy information found	(Randy Gingeleski)

Rating:

	Ease of install	Ease of use	Flexibility	Licensing	Privacy	Reputation	total	average
Metasploit	4	4	4	4	3	4	23	3,8
Nessus Vulnerability Scanner	5	5	2	3	4	5	24	4
Nmap	3	3	3	5	2	4	20	3,3
Burp Suite	5	4	3	3	4	5	24	4
OWASP ZAP	4	3	3	5	1	4	20	3,3
SQLmap	4	3	2	5	1	3	18	3
Kali Linux	5	4	5	5	2	4	25	4,2
Jawfisch	2	2	3	5	1	2	15	2,5



Websites:

- Metasploit by RAPID 7: https://www.metasploit.com/
- Nessus Vulnerability Scanner by tenable: https://www.tenable.com/products/nessus/nessus-professional
- Nmap: https://nmap.org/
- Burp Suite by PortSwigger: https://portswigger.net/burp
- OWASP ZAP: https://owasp.org/www-project-zap/
- Sqlmap: https://sqlmap.org/
- Kali Linux: https://www.kali.org/
- Jawfish: https://github.com/war-and-code/jawfish