University of Essex | Online

Penetration Testing Tools

Seminar 3 preparation

Group 3 |

Metasploit

Category	Rating	Comment
Ease of Install	5	Easily available installer provided on their website, or preinstalled in Kali Linux
Ease of Use	4	Comprehensive usage documents and videos provided
Flexibility	4	Includes a wide variety of modules including exploits, payloads, listeners, shellcode etc
Licensing	2	Free and Pro version available for approximately $15,000 with considerably more features
Privacy	N/A	Difficult to obtain without backend analysis
Reputation	5	Very popular penetration testing tool with 26k stars on Github. It is considered by many the "tool of choice" (Maynor, 2011).
Average Score	4.2	

Nessus Vulnerability Scanner

Category	Rating	Comment
Ease of Install	4	Pre-installed with Kali Linux, but requires CMD line knowledge if installed otherwise. Installer available as well.
Ease of Use	4	User friendly GUI with sets of scanning templates that have preconfigured options
Flexibility	4	Wide variety of scan templates available and as it is based on a plug in framework
Licensing	2	Free (16 IP scans) and Pro version available for a cost of £3000 per year (Unlimited IP scans).
Privacy	N/A	Difficult to obtain without backend analysis
Reputation	4	Has been noted as "the world's most popular vulnerability scanner that is used in over 75,000 organizations Worldwide" (Al Shebli & Beheshti, 2018)
Average Score	3.6	

Nmap

Category	Rating	Comment
Ease of Install	4	Self installer available on website, but less comprehensive instructions
Ease of Use	3	Required both CMD line knowledge and an understanding of the used operating system. A separate GUI and web interface is available
Flexibility	3	Useful but limited set of functionality including Host discovery, Port Scanning, Version detection, TCP/IP stack fingerprinting, and scriptable interaction.
Licensing	4	Free, GNU public licenses, but with some conditions
Privacy	N/A	Difficult to obtain without backend analysis
Reputation	3	Well known, but is not an enterprise level tool.
Average Score	3.4	

Burp Suite

Category	Rating	Comment
Ease of Install	5	Easily usable installer on the website, or as part of Kali Linux
Ease of Use	4	Manual and automated testing available. User friendly GUI. Both applicable to new and experienced users. Tutorials and videos available on website.
Flexibility	4	A toolkit that includes a variety of scanning tools, with various functionality
Licensing	3	Three editions Community (free), Professional (£319) and Enterprise (min £5175)
Privacy	N/A	Difficult to obtain without backend analysis
Reputation	4	Well respected software
Average Score	4	

OWASP ZAP

Category	Rating	Comment
Ease of Install	5	Easily usable installer on the website, or as part of Kali Linux
Ease of Use	2	Wide variety of tutorials on website. Ability to provide automated and targeted scans. Slightly dated in use.
Flexibility	2	A very focused tool with a narrow scope of use
Licensing	5	Free, open source software
Privacy	N/A	Difficult to obtain without backend analysis
Reputation	4	Although not the most comprehensive tool, it is created by OWASP which is a well respected organisation
Average Score	3.6	

SQLmap

Category	Rating	Comment
Ease of Install	3	Requires Python installation, and no automated installer. No comprehensive install instructions
Ease of Use	3	Command list provided within Python, and via user manual. Additional research is required outside of official sources to understand usage
Flexibility	2	Used primarily for detecting SQL injection flaws
Licensing	5	Free, Open source
Privacy	N/A	Difficult to obtain without backend analysis
Reputation	3	A good well known tool for its limited purpose
Average Score	3.2	

Kali Linux

Category	Rating	Comment
Ease of Install	4	Knowledge of operating system (Or Virtual Machine) installation is required
Ease of Use	3	Although the Kali Linux is usable in the same method as a standard Linux installation, specific knowledge may be required for pre installed security tools.
Flexibility	5	Contains a variety of preinstalled penetration testing tools such as others mentioned within this analysis (e.g. Metasploit, Nmap, OWASP ZAP etc.)
Licensing	5	Open source operating system
Privacy	N/A	Difficult to obtain without backend analysis
Reputation	5	Widely known and well regarded. Is the recommended platform for a variety of penetration testing tools
Average Score	4.4	

Jawfish

Category	Rating	Comment
Ease of Install	1	Requires a flask installation. Know comprehensive install instructions
Ease of Use	1	Lack of instructions, and information provided by a single GitHub repository
Flexibility	2	Limited set of functionality that is not well explained
Licensing	5	Free
Privacy	N/A	Difficult to obtain without backend analysis
Reputation	1	Not very widely known
Average Score	2	

Summary

- Kali Linux is the best from our score for general implementation (Average : 4.4), as it is an amalgamation of most aforementioned tools, with a good reputation. It should be noted Kali Linux is an OS not a single program.
- For a specific single enterprise tool we would recommend Metasploit (Average : 4.2) as it is a comprehensive tool with a good reputation.

Tool	Score
Kali Linux	4.4
Metasploit	4.2
Burp Suite	4
Nessus Vulnerability Scanner	3.6
OWASP ZAP	3.6
Nmap	3.4
SQLMap	3.2
Jawfish	2

References

Geer, D. (2015) 8 Penetration Testing Tools That Will Do The Job. Network World

Maynor, D., 2011. *Metasploit toolkit for penetration testing, exploit development, and vulnerability research*. Elsevier.

Al Shebli, H.M.Z. and Beheshti, B.D., 2018, May. A study on penetration testing process and tools. In *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1-7). IEEE.