Seminar 3 Preparation Exercise: Evaluation of Pen test tools

	Metasploit	**Nessus**	**Nmap**	**Burp Suite**	**Kali Linux**	**Jawfish**	**OWASP ZAP**	**SQL Map**
Ease of Installation	Available for use on Linux, Mac OS X and Windows Systems	Available for use on Linux, Mac OS X and Windows Systems	Runs on Linux, Mac OS X and windows	Available for use on Linux, Mac OS X and Windows Systems	It is Linux based. Minimal hardware requirements (edureka, 2020)	Linux based. Requires several dependencies such as flask, jinja2 (linuxsecurity. n.d)	Works on most OSes	Runs on Linux, Mac OS X and windows. Python Installation required on Windows system.
Ease of Use	Easy to use. It has both command line and GUI interface	Ease of use is a big selling point	Easy to use, backed by a very active community (esecurityplanet, 2019)	Easy to use	Easy to use, contains a suite of pen testing tools (edureka, 2020)	No active community. Limited instructions on github	Easy to use	Easy to use
Flexibility	It can be used on web applications, networks and servers	Deals with software flaws, operating systems issues, can find vulnerabilities across a network (esecurityplanet, 2019)	Used mainly for network scanning, doesn't probe for vulnerabilities	It can check for the OWASP top 10 web application vulnerabilities, can perform scanning, and used for compliance and security audit purposes (esecurityplanet, 2019)	Used for advanced penetration testing, computer forensics and security auditing. Also contains a suite of tools that can perform a lot of other	Jawfish is commonly used for penetration testing, security assessment, vulnerability scanning, or web application analysis (linuxsecurity. n.d).	An OWASP tool for testing web application security risks (OWASP top 10)	Used for exploiting SQL injection flaws and database takeovers (sqlmap, n.d). Supports a wide range of database applications

					functions (kali, n.d)			
Licensing	Community edition is free while Pro edition costs up to $15,000 per year (esecurityplanet, 2019)	Paid	Free	It has a free version with limitations. Cost-effective professional version and enterprise edition	free	Free, Owned by MIT	Free	Free Software
Privacy	Open source tool	Started as open source but now Proprietary tool	Open source tool	closed	Open source	Open	Open source	Open Source
Reputation	Most widely used penetration testing tool. All in one solution (Metasploit, n.d)	Also widely used. It finds vulnerabilities but cannot penetrate them (esecurityplanet, 2019)	One of the top scanning tools	most widely used for web application security testing (esecurityplanet, 2019)	Very advanced. It is also an operating system (Kali, n.d)	No release found. Not widely used. Still under construction (linuxsecurity. n.d)	Widely used, Developed by OWASP	Appears to be the most popular tool used for testing SQL injection

Popularity Ratings based on facts in table above

Metasploit	5
Nessus	5
Nmap	5
Burp Suite	5
Kali Linux	5
Jawfish	1
OWASP ZAP	4
Sqlmap	3

5 – most popular

1 – least popular

References

Edureka (2020) Everything you need to know about Kali Linux. Available from: https://www.edureka.co/blog/ethical-hacking-using-kali-linux/ [Accessed 14 September 2021]

Esecurityplanet () Best Penetration Testing Tools for 2021 Available from: https://www.esecurityplanet.com/products/best-penetration-testing/ [Accessed 14 September 2021]

Geer, D. (2015) 8 Penetration Testing Tools That Will Do the Job. Available fromhttps://www.networkworld.com/article/2944811/8-penetration-testing-tools-that-will-do-the-job.html [Accessed 13 September 2021]

Kali (n.d) Kali. Available from: https://www.kali.org/#kali-highlights [Accessed 14 September 2021]

Linuxsecurity (n.d) Jawfish Available from: https://linuxsecurity.expert/tools/jawfish/ [Accessed 14 September 2021]

Metasploit (n.d) Metasploit Available from: https://www.metasploit.com/ [Accessed 14 September 2021]

Sqlmap (n.d) sqlmap Available from: https://sqlmap.org/ [Accessed 14 September 2021]