|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Metasploit** | **Nessus** | **Nmap** | **BurpSuite** | **ZAP** | **SQLMap** | **Kali Linux** | **Jawfish** |
| **Ease of Install** | 4 | 4 | 5 | 5 | 5 | 4 | 4 | 4 |
| **Ease of Use** | 5 | 4 | 5 | 4 | 5 | 4 | 4 | 3 |
| **Flexibility** | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 3 |
| **Licensing** | 3 | 3 | 5 | 3 | 5 | 5 | 5 | 5 |
| **Privacy** | 4 | 4 | 4 | 4 | 5 | 3 | 4 | 3 |
| **Reputation** | 5 | 5 | 5 | 4 | 4 | 4 | 5 | 3 |
|  | 4.33 | 4.17 | 4.83 | 4.17 | 4.67 | 4 | 4.33 | 3.5 |

**Unit 6 - Penetration Testing Tools Assessment**

1. Nmap – 4.83
2. ZAP – 4.67
3. Kali Linux – 4.33
4. Metasploit – 4.33
5. BurpSuite – 4.17
6. Nessus – 4.17
7. SQLmap – 4
8. Jawfish – 3.5

The factors that influenced the scores for each factor are as follows:

**Ease of install** – Based on complexity of the steps to install.

**Ease of use** – Based on GUI availability, quality of documentation, etc.

**Flexibility** – Based on compatibility with different OS/DBs, customisation available, number of features, etc.

**Licensing** – Open Source (5), Open Source Basic but Paid Add Ons (3) and Commercial (1)

**Privacy** – Based on compatibility with proxy/VPN, ease of compromise, likelihood of targeted attacks, etc.

**Reputation** – Based on the size of the current user base, level of commercial uptake, etc.

Some observations based on the results of the scoring:

These tools were raised in an article about recommended penetration testing tools by a professional penetration tester so I am not surprised by the scores all falling between 3.5 and 4.83. They were also scored relative to the market, as opposed to each other, to make the scoring extendable to other tools that might not be as advanced.

Bibliography

<https://www.metasploit.com/>

<https://www.tenable.com/products/nessus>

<https://nmap.org/>

<https://www.kali.org/>

<https://owasp.org/www-project-zap/>

<https://sqlmap.org/>

<https://portswigger.net/burp>

<https://github.com/war-and-code/jawfish>

<https://www.varonis.com/blog/penetration-testing-tools/>

<https://www.csoonline.com/article/2943524/11-penetration-testing-tools-the-pros-use.html>