Seminar 3: Penetration Testing Tools

This seminar looked at the following tools as highlighted by the article by Greer (2015): Metasploit, the Nessus Vulnerability Scanner, Nmap, Burp Suite, OWASP ZAP, SQLmap, Kali Linux, and Jawfish.

Product Ratings

The listed products are rated on a scale of 1 to 5 where 5 represents the best/highest score possible.

> *Privacy was a difficult metric to evaluate because it is not clear what is meant by "privacy": does it refer to how the product handles, stores or transmits data, or does it relate to the target tool's data.*

Table 1 Penetration testing tools

Product\Criteria	Ease of install	Ease of use	Flexibility	Licensing	Privacy	Reputation	Average Score
Metasploit	5	4	4	5	N/A	4	4.4
Nessus Vulnerability Scanner	4	5	4	2	N/A	4	3.8
Nmap	3	3	3	4	N/A	3	3.2
Burp Suite	5	4	3	4	N/A	4	3.8
OWASP ZAP	5	3	2	5	N/A	4	4
SQLMap	3	3	2	5	N/A	3	3.2
Kali Linux	3	4	5	5	N/A	5	4.4
Jawfish	1	2	2	5	N/A	2	2.4

Product Notes

- **Metasploit.** (https://www.metasploit.com/).

  Description. A Ruby-based open-source framework that allows testing via command line or GUI. Boston-based company, Rapid7 owns Metasploit as part of IDS tools.

  Extensible. Yes.

  Exploits supported: 1677 exploits and supports over 25 platforms (Petters, 2020).

  Licensing. Open source.

- **Nessus Vulnerability Scanner.** (https://www.tenable.com/products/nessus)

  Description. Vulnerability assessment tool.

  Extensible. Yes. (166K plugins)

  Exploits supported. 100 zero-day vulnerabilities, 67000 CVEs.

  Customer base. 30000 organisations.

  Licensing. Free and Paid-for Pro-version costing upwards of £2894 per annum.

- **Nmap.** (https://nmap.org/)

  Description. Nmap ("Network Mapper") is a free and open-source utility for network discovery and security auditing.

  Extensible. No, but supports complex scripting through the Nmap scripting engine.

  Exploits supported.

  Customer base.

  Licensing. Free.

  Other: Not listed on Gartner's reviews (Gartner, 2021) but well-known in academic circles. Command-line driven. Featured in movies like The Matrix and the series Mr. Robot.

- **Burp Suite.** (https://portswigger.net/burp)

  Description. A web application attack took that intercepts HTTP requests.

  Extensible. Yes.

  Exploits supported. 153 web-based issues.

  Customer base. 53K organisations.

  Licensing. Free but has a paid-for professional version upward of £319.

  Other: In existence for over 17 years. Focuses on ***Out of band application security testing***.

- **OWASP ZAP.** (https://www.zaproxy.org/)

  Description. Zed Attack Proxy (ZAP) is a man-in-the-middle free, open-source proxy used for penetration testing of web applications.

  Extensible. Yes.

Exploits supported.

Customer base.

Licensing. Free.

Other.

- **SQLMap.** (https://sqlmap.org/)

  Description. An open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.

  Extensible.

  Exploits supported.

  Customer base.

  Licensing. Open source.

  Other. Supports the following databases: MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, MariaDB, MemSQL, TiDB, CockroachDB, HSQLDB, H2, MonetDB, Apache Derby, Amazon Redshift, Vertica, Mckoi, Presto, Altibase, MimerSQL, CrateDB, Greenplum, Drizzle, Apache Ignite, Cubrid, InterSystems Cache, IRIS, eXtremeDB, FrontBase, Raima Database Manager, YugabyteDB and Virtuoso.

- **Kali Linux.** (https://www.kali.org/)

  Description. Kali Linux (formerly known as BackTrack Linux) is a multi-platform, open-source, Debian-based Linux distribution that contains several tools targeted towards information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

  Extensible. Yes.

  Exploits supported.

  Customer base.

  Licensing. Open source.

  Other.

- **Jawfish.**

  Description.

  Extensible.

  Exploits supported.

  Customer base.

  Licensing.

  Other.

Summary

Table 2 Penetration Testing Tool Rankings

Product	Score	Reason
Kali Linux	4.4	Well-known, and has over 600 built-in tools which include Burp Suite, Nmap, Metasploit framework, sqlmap.
Metasploit	4.4	Decent framework with excellent support and plugins available.
OWASP ZAP	4	Well-known and backed by the OWASP foundation.
Nessus	3.8	Expensive when opting for the Professional version, otherwise the Community edition is limited in features.
Burp Suite	3.8	Focused on intercepting HTTP requests.
Nmap	3.2	Not a comprehensive network scanner.
SQLMap	3.2	Focused purely on SQL injection attacks.
JawFish	2.4	Next to no documentation or source code available.

References

Gartner (2021). Vulnerability Assessment solutions Reviews and Ratings. Available from https://www.gartner.com/reviews/market/vulnerability-assessment [Accessed 16 Dec. 2021]

Greer, D. (2015). 8 penetration testing tools that will do the job. Available from https://www.networkworld.com/article/2944811/8-penetration-testing-tools-that-will-do-the-job.html [Accessed 17 Dec. 2021]

Nessus, (ND). Nessus Professional. Available from https://static.tenable.com/marketing/datasheets/DataSheet-Nessus_Professional.pdf. [Accessed 16 Dec. 2021]

Petters, J. (2020). What is Metasploit? The Beginner's Guide. Available from https://www.varonis.com/blog/what-is-metasploit/ [Accessed 16 Dec. 2021]

Bibliography

Green, A. (2020). Penetration Testing Explained, Part II: RATs! Available from https://blogvaronis2.wpengine.com/penetration-testing-explained-part-ii-rats/ [Accessed 16 Dec. 2021]