Penetration Testing Tools

1. **Kali Linux**

Function: There are many different tools and utilities available on the Kali Linux penetration testing platform. Kali Linux gives IT and security experts the ability to evaluate the security of their systems from data collection to comprehensive reporting.

Use Case: They give testers the ability to thoroughly examine a target system's overall security posture, exploit vulnerabilities, and look for weaknesses.

Open Source/ Paid: Open Source

Pros	Cons
● Free of charge ● Comprehensive ● Provides community support ● Regularly updated ● Open source for customization	● Steep learning curve ● Potential for misuse ● Resource-Intensive

2. **Metasploit**

Function: Network security experts use this tool to perform penetration tests; system administrators use it to test patch installations; product vendors use it to conduct regression testing; and security engineers from various industries use it.

Use Case: Vulnerability Assessment, Exploitation Testing, Penetration Testing, Privilege Escalation, Payload Delivery, Client-Side Attacks, Password Cracking

Open Source/ Paid: Open Source

Pros	Cons
● Easy to use ● Integration with other tools ● Automation capabilities	● Manual intervention for certain exploits ● Lack of robust menus and plugin inter-operation ● Dashboard improvements for better understanding

3. Wireshark

Function: It is helpful for evaluating traffic vulnerabilities in real time because of its packet sniffing, network analysis, and protocol analysis features. It is capable of closely examining both the different components that make up a data packet and connection-level information.

Use Case: An ethical hacker can use this tool to expose system security vulnerabilities related to user authentication. This method of finding vulnerabilities is judged appropriate since the testing strategy is quick and successful in finding vulnerabilities.

Open Source/ Paid: Open Source

Pros	Cons
● Affordable ● Packet Analysis capabilities ● Real-time network capabilities	● Confusing User Interface ● Steep Learning Curve ● Lack of user-friendliness

4. Burp Suite

Function: It is a graphical tool/integrated platform for web application security testing. From the first mapping and analysis of an application's attack surface to the identification and exploitation of security vulnerabilities, all of its tools function in unison to support the entire testing process.

Use Case: Its primary attribute is the Proxy. Burp can function as a go-between for the client (web browser) and the server that hosts the web application thanks to the Proxy. Burp can intercept all requests and conversations between the web browser and the server by putting itself in the way of these two elements.

Open Source/ Paid: Closed Source

Pros	Cons
● Automated scans ● Detailed reporting of bugs ● Less costly or cost effective	● User interface can be improved ● Automated scan report can be further improved to reduce false positive ● Tool crashes when open large number of threads

5. SQL Map

Function: SQL injection vulnerabilities are exploited automatically with the help of this tool. With SQLMap, we can check websites and databases for security holes and use those holes to gain control of the database.

Use Case: It enables you to automate the process of finding SQL injection vulnerabilities, using them, and then taking over database servers. It also includes a detection engine with sophisticated features to facilitate penetration testing.

Open Source/ Paid: Open Source

Pros	Cons
● Streamlined penetration testing process ● Automates repetitive tasks involved in detecting and exploiting SQL injection vulnerabilities	● Confusing table relationships

6. Nmap

Function: It quickly scans large networks for available hosts and services by identifying them from raw IP packets. In order to hide their tracks, hackers and pen testers often add custom options and scripts that carry out numerous tasks automatically.

Use Case: It is a versatile tool that is frequently used for penetration testing to provide you with a detailed understanding of the security of your network. Its capabilities encompass information gathering, enumeration, and vulnerability and security loophole detection.

Open Source/ Paid: Open Source

Pros	Cons
● Extensiveness and Advanced Networking features ● Lightweight and easy to use ● Speedy network mapping	● Steep learning curve on Windows ● Limited functions on Windows ● Noisy scans and system appearance of being attacked

7. OWASP ZAP

Function: Web application vulnerabilities that it can detect include insecure deserialization, SQL injection, cross-site scripting (XSS), exposed sensitive data, compromised authentication, and components with known vulnerabilities.

Use Case: Vulnerability Scanning, Automated Testing, Manual Testing, Spidering and Crawling, Fuzz Testing, Session Management Testing, Authentication Testing, API Security Testing, Web Services Testing, Reporting and Integration

Open Source/ Paid: Open Source

Pros	Cons

• Wide range of application security testing methods that can help identify potential vulnerabilities. • Reporting features are comprehensive and customizable.	• Outdated UI that can sometimes be clunky and may require some customization before it is comfortable. • Automated scanning capabilities are limited compared to other tools • Complicated to use for novice users. • There is no web version. You have to download it into your system to use it. • Documentation is rough and difficult to understand.

8. John The Ripper

Function: The software is typically used in a UNIV/Linux and Mac OS X environment where it can detect weak passwords. John the Ripper jumbo supports many cipher and hash types.

Use Case: Using various encryption technologies and useful wordlists, brute-force attacks can be carried out with the help of this password cracking tool. It's frequently used by ethical hackers and pen testers to decipher the actual passwords hidden behind hashes.

Open Source/ Paid: Open Source

Pros	Cons
● Easily finds plantect passwords. ● Simply detects password hashes. ● Has a fully bespoke cracker that can be modified to users requirements. ● Excellent for UNIX and Windows usage.	● It needs to be modified to be able to break SHA 256, 512 and the lastest hashes. ● Can be slow and wildly against the lastest hashes. ● Require admin access to set up an account. ● Old and is being superseded by

	better applications.

9. OpenVAS

Function: It offers a strong capacity for gathering and turning vulnerability data into actionable insights. Setting priorities for the data is another crucial step in the risk assessment process. Prioritizing risks based on how easily attackers can exploit vulnerabilities is the main focus.

Use Case: Using a network scan, OpenVAS looks for software, configuration, and system vulnerabilities that are known to exist. You can prevent cybercriminals from taking advantage of these vulnerabilities by identifying them and taking proactive steps to fix them.

Open Source/ Paid: Open Source

Pros	Cons
● Comprehensive coverage for a free solution ● A dedicated community of developers ● Open-source and free of charge ● Support for multiple OS	● Overwhelming for non-tech-savvy users ● Outdated user interface

10. Hashcat

Function: It is a tool for cracking passwords that can be used both legally and illegally. Hashat is a hacking tool that is especially quick, effective, and adaptable. It helps with brute-force attacks by using hash values of passwords that the tool is guessing or applying

Use Case: It finds a quick and easy way to crack passwords by using brute-force techniques, rainbow tables, and precomputed dictionaries.

Open Source/ Paid: Open Source

Pros	Cons
● GPU accelerated password cracking ● Rule based attacks ● Supports all the hash formats	● When drivers for your GPU aren't working it can be very frustrating to get started ● Does not have its own GUI