# Top Penetration Testing Software & Tools

## 1. Netsparker

Netsparker Security Scanner is a popular automatic web application for penetration testing. The software can identify everything from cross-site scripting to SQL injection. Developers can use this tool on websites, web services, and web applications.

The system is powerful enough to scan anything between 500 and 1000 web applications at the same time. You will be able to customize your security scan with attack options, authentication, and URL rewrite rules. Netsparker automatically takes advantage of weak spots in a read-only way. Proof of exploitation is produced. The impact of vulnerabilities is instantly viewable.

**Benefits:**

- Scan 1000+ web applications in less than a day!
- Add multiple team members for collaboration and easy shareability of findings.
- Automatic scanning ensures a limited setup is necessary.
- Searches for exploitable SQL and XSS vulnerabilities in web applications.
- Legal web application and regulatory compliance reports.
- Proof-based scanning Technology guarantees accurate detection.

## 2. Wireshark

Once known as Ethereal 0.2.0, Wireshark is an award-winning network analyzer with 600 authors. With this software, you can quickly capture and interpret network packets. The tool is open-source and available for various systems, including Windows, Solaris, FreeBSD, and Linux.

Benefits:

- Provides both offline analysis and live-capture options.
- Capturing data packets allows you to explore various traits, including source and destination protocols.
- It offers the ability to investigate the smallest details for activities throughout a network.
- Optional adding of coloring rules to the pack for rapid, intuitive analysis

## 3. Metasploit

Metasploit is the most used penetration testing automation framework in the world. Metasploit helps professional teams verify and manage security assessments, improves awareness, and arms, and empowers defenders to stay a step ahead in the game.

It is useful for checking security and pinpointing flaws, setting up a defense. An Open source software, this tool will allow a network administrator to break in and identify fatal weak points. Beginner hackers use this tool to build their skills. The tool provides a way to replicate websites for social engineers.

Benefits:

- Easy to use with GUI clickable interface and command line.
- Manual brute-forcing, payloads to evade leading solutions, spear phishing, and awareness, an app for testing OWASP vulnerabilities.
- Collects testing data for over 1,500 exploits.
- MetaModules for network segmentation tests.
- You can use this to explore older vulnerabilities within your infrastructure.
- Available on Mac OS X, Windows, and Linux.
- Can be used on servers, networks, and applications.

## 4. BeEF

This is a pen-testing tool and is best suited for checking a web browser. Adapted for combating web-borne attacks and could benefit mobile clients. BeEF stands for Browser Exploitation Framework and uses GitHub to locate issues. BeEF is designed to explore weaknesses beyond the client system and network perimeter. Instead, the framework will look at exploitability within the context of just one source, the web browser.

Benefits:

- You can use client-side attack vectors to check security posture.
- Connects with more than one web browser and then launches directed command modules.

## 5. John The Ripper Password Cracker

Passwords are one of the most prominent vulnerabilities. Attackers may use passwords to steal credentials and enter sensitive systems. John the Ripper is an essential tool for password cracking and provides a range of systems for this purpose. The pen testing tool is free open-source software.

Benefits:

- Automatically identifies different password hashes.
- Discovers password weaknesses within databases.
- The pro version is available for Linux, Mac OS X, Hash Suite, and Hash Suite Droid.
- Includes a customizable cracker.
- Allows users to explore documentation online. This includes a summary of changes between separate versions.

## 6. Aircrack

Aircrack NG is designed for cracking flaws within wireless connections by capturing data packets for an effective protocol in exporting through text files for analysis. While the software seemed abandoned in 2010, Aircrack was updated again in 2019.

This tool is supported on various OS and platforms with support for WEP dictionary attacks. It offers an improved tracking speed compared to most other penetration tools and supports multiple cards and drivers. After capturing the WPA handshake, the suite is capable of using a password dictionary and statistical techniques to break into WEP.

Benefits:

- Works with Linux, Windows, OS X, FreeBSD, NetBSD, OpenBSD, and Solaris.
- You can use this tool to capture packets and export data.
- It is designed for testing wifi devices as well as driver capabilities.
- Focuses on different areas of security, such as attacking, monitoring, testing, and cracking.
- In terms of attacking, you can perform de-authentication, establish fake access points, and perform replay attacks.

## 7. Burp Suite Pen Tester

There are two different versions of the Burp Suite for developers. The free version provides the necessary and essential tools needed for scanning activities. Or, you can opt for the second version if you need advanced penetration testing. This tool is ideal for checking web-based applications. There are tools to map the tack surface and analyze requests between a browser and destination servers. The framework uses Web Penetration Testing on the Java platform and is an industry-standard tool used by the majority of information security professionals.

Benefits:

- Capable of automatically crawling web-based applications.
- Available on Windows, OS X, Linux, and Windows.

## 8. Ettercap

The Ettercap suite is designed to prevent man-in-the-middle attacks. Using this application, you will be able to build the packets you want and perform specific tasks. The software can send invalid frames and complete techniques which are more difficult through other options.

Benefits:

- This tool is ideal for deep packet sniffing as well as monitoring and testing LAN.
- Ettercap supports active and passive dissection of protections.
- You can complete content filtering on the fly.
- The tool also provides settings for both network and host analysis.

## 9. Kali Linux

Kali Linux advanced penetration testing software is a Linux distribution used for penetration testing. Many experts believe this is the best tool for both injecting and password snipping. However, you will need skills in both TCP/IP protocols to gain the most benefit. An open-source project, Kali Linux, provides tool listings, version tracking, and meta-packages.

Benefits:

- With 64-bit support, you can use this tool for brute-force password cracking.
- Kali uses a live image loaded into the RAM to test the security skills of ethical hackers.
- Kali has over 600 ethical hacking tools.
- Various security tools for vulnerability analysis, web applications, information gathering, wireless attacks, reverse engineering, password cracking, forensic tools, web applications, spoofing, sniffing, exploitation tools, and hardware hacking are available.
- Easy integration with other penetration testing tools, including Wireshark and Metasploit.
- The BackTrack provides tools for WLAN and LAN vulnerability assessment scanning, digital forensics, and sniffing.