

Forum:[Hack Forums](#)

Thread: [Essential Penetration Testing Tools Guide What They Do & When to Use Them](#)

mohamad123d7 - July 13, 2026, 7:48 pm

When you start in penetration testing, you're overwhelmed by hundreds of tools. Understanding what each tool does and when to reach for it is what separates a professional tester from someone just pushing buttons.

This guide breaks down the most important tools by category, explains exactly what they do, and tells you when to use them.

1. Reconnaissance Tools (Information Gathering)

This is always step one. Before you attack, you must understand your target.

Nmap — The godfather of scanning tools. Discovers live hosts on a network, open ports, running services, and often their versions. It gives you a complete map of what's exposed.

Maltego — A graphical tool that connects the dots. Enter a name, company, or domain, and it maps out relationships: email addresses, social media accounts, websites, phone numbers. Excellent for OSINT (Open Source Intelligence).

theHarvester — Collects emails, subdomains, and hosts associated with a target by scraping Google, LinkedIn, and other public sources.

Shodan — A search engine for internet-connected devices. Search for "security camera" or "web server" or "medical device" in a specific country, and it shows every exposed device.

2. Vulnerability Scanning Tools

These tools automatically search for known weaknesses.

Nessus — Industry-standard commercial scanner. Run a full scan on your network and it produces a report with every vulnerability found, severity ratings, and remediation steps.

OpenVAS — The powerful open-source alternative. Less polished than Nessus but completely free and actively maintained.

Nikto — Specialized for web servers. Checks server configuration, dangerous files, outdated software, and default insecure settings.

3. Exploitation Tools

After finding a vulnerability, these tools help you exploit it.

Metasploit Framework — The most famous exploitation framework. Contains thousands of ready-to-use exploits. Search by CVE number or name, configure, and launch. Also lets you generate payloads to run on compromised machines.

Searchsploit — Offline command-line interface for the Exploit-DB database. Check if a public exploit exists without needing internet access.

BeEF (Browser Exploitation Framework) — Targets web browsers. If you can trick a victim into opening a link, you gain control over their browser entirely.

4. Web Application Testing Tools

Since you run an online store, this category matters most.

Burp Suite — The #1 web testing tool. See every request your browser sends, modify it on the fly, and resend it. Detects SQL Injection, XSS, and every web vulnerability class.

OWASP ZAP — The free alternative to Burp. Easy to use, has an automated scanner, and is great for beginners.

Dirb / Gobuster / Dirsearch — Tools that brute-force hidden files and directories on a website. If there's an admin panel or a backup ZIP file, these tools find it.

WPScan — For WordPress sites. Scans plugins, themes, and weak passwords.

SQLMap — Fully automated SQL Injection detection and exploitation. Feed it a URL, and it handles the rest.

5. Password Cracking & Brute-Force Tools

Hydra — Online password brute-forcer for services (SSH, FTP, login pages). Tries passwords from a wordlist against the target service.

John the Ripper — Offline hash cracker. If you have a file of encrypted passwords, this tries to crack them.

Hashcat — The fastest hash cracker. Uses your GPU for dramatically faster cracking than CPU-based tools.

6. Post-Exploitation Tools

After compromising a machine, what do you do?

Cobalt Strike — The most powerful commercial C2 (Command & Control) framework. Expensive but extremely capable.

Empire — Open-source C2 framework. Free alternative to Cobalt Strike with similar post-exploitation capabilities.

Netcat / Ncat — Simple but powerful. Creates reverse shells, listens for incoming connections, transfers files.

BloodHound — Active Directory analysis tool. Maps the path from a regular user to Domain Admin. Invaluable for internal network penetration testing.

7. Wireless Network Tools

Aircrack-ng — The most famous Wi-Fi testing suite. Captures packets, cracks WEP encryption, brute-forces WPA/WPA2 handshakes.

Reaver — Specialized for WPS attacks. Targets the WPS PIN feature on older routers.

Quick Reference — When to Use What

Vincent62666 - July 14, 2026, 12:34 am

These guides are really helpful fr