Top 25 Penetration Testing Tools (2023)

Tools	Features
1. Wireshark	1. It analyzes network traffic. 2. Inspect network protocol. 3. Troubleshoot network performance problems. 4. Decrypt protocols. 5. Collect real-time data from Ethernet, LAN, USB, etc.
2. Metasploit	1. Bunch of many tools. 2. Quickly execute tasks. 3. Automatic reporting.
3. NMAP/ZenMap	1. OS Detection 2. Target specification 3. Port Scanning 4. Firewall/IDS Evasion and Spoofing 5. Host discovery 6. Scan techniques 7. Script scan 8. Service or version detection 9. Evasion and spoofing
4. BurpSuite	1. Intercepting browser traffic 2. Break HTTPS 3. Manage recon data 4. Expose hidden attack surface 5. Speed up granular work flows 6. Test for clickjacking attacks 7. Work with WebSockets 8. Assess token strength 9. Manually test for out-of-band vulnerabilities
5. sqlmap	1. Powerful testing engine. 2. capable of carrying out multiple injection attacks. 3. Supports MySQL, Microsoft Access, IBM DB2, and SQLite servers.
6. Intruder	1. Security testing tool for businesses. 2. There are security features that only banks and the government can use.
7. Nessus	1. Nessus can check the system for over 65,000 vulnerabilities. 2. Facilitate efficient vulnerability assessment. 3. Nessus is constantly updated with new features to mitigate emerging potential risks. 4. It is compatible with all other tenable products.

8. Zed Attack Proxy	1. Compatible with Mac OS X, Linux, and Windows. 2. Capable of identifying a wide range of vulnerabilities in web applications. 3. An interface that is easy to use. 4. Pentesting platform for beginners. 5. Many pentesting activities are supported.
9. Nikto	1. Identifies 1250 servers running out-of-date software. 2. Fully compatible with the HTTP protocol. 3. Templates can be used to make custom reports. 4. Several server ports scan simultaneously.
10. BeEF	1. Solid command-line tool. 2. Fantastic for checking up on any suspicious activation the network through the browser. 3. Comprehensive threat searches. 4. Good for mobile devices.
11. Invicti	1. Fully automated. 2. Bunch of many tools. 3. System intelligence. 4. Fast scanning. 5. Automatic assessment report.
12. PowerShell-Suite	1. PowerShell-Suite works with macOS, Linux, and Windows. 2. pipeline for command chaining and an in-console help system. 3. Post-exploitation, infrastructure scanning and information gathering, and attacks.
13. w3af	1. Assembled tools available. 2. Covers everything about known network vulnerabilities. 3. Enables reusing test parameters.
14. Wapiti	1. Proxy support for HTTP, HTTPS, and SOCKS5. 2. Variations in Verbosity. 3. Modular attack systems that can be activated and deactivated quickly and easily. 4. A Customizable number of concurrent HTTPrequest processing tasks. 5. A payload can be added as easily as a line. 6. Can provide terminal colors to highlight vulnerabilities. 7. It is a command-line application.
15. Radare	1. Multi-architecture and multi-platform. 2. Highly scriptable. 3. Hexadecimal editor. 4. IO is wrapped. 5. Filesystems and debugger support. 6. Examine the source code at the basic block and function levels.

16. MobSF	1. Information gathering. 2. Analyze security headers. 3. Find vulnerabilities in mobile APIs like XXE, SSRF, Path Traversal, and IDOR. 4. Monitor additional logical issues associated with Session and API.
17. FuzzDB	1. For fault injection testing, FuzzDB provides exhaustive lists of attack payload primitives. 2. By providing a comprehensive dictionary structured by framework, language, and application, FuzzDB reduces the impact of brute force testing. 3. FuzzDB stores dictionaries of regular coding sequences that can be used to explore and investigate server feedback. 4. FuzzDB has regular expressions for various data types, including credit cards, social security numbers, and common server error messages.
18. Aircrack-ng	1. Password cracking 2. Packet sniffing 3. Attacking 4. OS Compatibility
19. Social Engineering Toolkit	1. open-source penetration testing framework 2. Phishing Attacks 3. Pretexting 4. Tailgating and CEO fraud analysis 5. Web jacking attack 6. Credential Harvester Attack
20. Hexway	1. Custom branded docx reports 2. All security data in one place 3. Issues knowledge base 4. Integrations with tools (Nessus, Nmap, Burp, etc.) 5. Checklists & pentest methodologies 6. API (for custom tools) 7. Team collaboration 8. Project dashboards 9. Scan comparisons 10. LDAP & Jira integration 11. Continuous scanning 12. PPTX reports 13. Customer support

21. Shodan	1. Cyber security Search engine 2. Network Monitoring 3. Shodan crawls the entire Internet 4. Looking up IP Information 5. Internet routers. 6. Enterprise Security 7. Academic Research 8. Market Research
22. Intruder	1. Ongoing attack surface monitoring 2. Intelligent results 3. Cloud Security. 4. System Security. 5. Application Security. 6. Confidentiality. 7. Data Security. 8. Email Security. 9. Endpoint Protection. 10. Identity Management.
23. Dnsdumpster	1. Actions. Automate any work ow. 2. Security. Find and x vulnerabilities. 3. Copilot. Write better code with AI. 4. Manage code changes. 5. Issues. Plan and track work. 6. Discussions. Collaborate outside of code.
24. Hunter	1. Email searches & verifications 2. Link tracking 3. Find emails while web surfing 4. Searching or verifying lists of email addresses 5. Domain Tracking
25. URL Fuzzer	1. Fuzz URL set from an input file. 2. Concurrent relative path search. 3. A configurable number of fuzzing workers. 4. Configurable time wait periods between fuzz tests per worker. 5. Custom HTTP headers support. 6. Various HTTP methods support.