

Forum:[Hack Forums](#)

Thread: [\[TOOLS\] Useful tools for White-Hat Hacking - Pentesting - Bug Bounty](#)

P??sonl?af - May 30, 2025, 8:42 am

Introduction:

This thoughtfully organized list brings together some of the most powerful tools used by professional ethical hackers, bug bounty hunters, and security researchers. From web vulnerability scanners and packet sniffers to password crackers and reconnaissance frameworks, each tool has been selected for its real-world relevance and efficiency in modern security testing.

Important Disclaimer:

This list is not intended for beginners without a foundational understanding of: Networking fundamentals (TCP/IP, ports, DNS, etc.)

Operating systems (especially Linux & Windows internals)

Cybersecurity principles (threat modeling, privilege escalation, secure coding)

Web application security (HTTP, cookies, sessions, common vulnerabilities)

Without these basics, the tools listed here will be of little use

Burp Suite - Comprehensive web security testing tool

[Source: portswigger.net](#)

Description: Penetration testers widely rely on Burp Suite for analyzing and manipulating web traffic.

Over time, it has become a foundational tool for both manual and automated web app testing.

Intercepting requests through the Burp Proxy lets users inspect and modify every byte of data.

Security professionals value its modularity—Repeater, Intruder, Decoder, and more.

One of its strongest features is the extensibility through BApps and custom Python extensions.

Navigating authentication flows, scanning for vulnerabilities, and even fuzzing inputs are all possible.

Leafing through large volumes of requests is simplified with its powerful logging and filtering.

Even the Community Edition offers solid manual testing functionality.

As you move into more complex scopes, the Professional version's automation becomes indispensable.

For any serious web security practitioner, Burp Suite is hard to replace.

Example Usage:

Intercept and test a login form:

Configure your browser to use Burp as a proxy (127.0.0.1:8080)

Visit the login page, capture the request

Send it to Repeater, modify inputs, and observe responses for weaknesses.

OWASP ZAP- Open-source web application security scanner

[Source: zaproxy.org](#)

Description: ZAP (Zed Attack Proxy) is an open-source web application security scanner developed by OWASP. It's beginner-friendly and includes features for passive and active scanning, spidering, and fuzzing. It's useful for identifying common vulnerabilities and analyzing site structure. It supports scripting and automation via ZAP CLI and APIs.

Example Usage:

Start a passive scan:

Launch ZAP

Enter a target URL

Let the spider and passive scan run to identify headers, cookies, or input fields for further testing.

Nmap - Network mapping and security auditing

[Source: nmap.org](https://nmap.org)

Description: Nmap is a powerful open-source tool for network mapping and security auditing. It's used to discover live hosts, open ports, services, and detect OS and software versions. It can also detect vulnerabilities through NSE scripts.

Example Usage:

Basic port scan:

Code `nmap -sS -Pn 192.168.1.1`

Wireshark - Network protocol analyzer

[Source: wireshark.org](https://wireshark.org)

Description: Wireshark is a network protocol analyzer that captures and inspects packets in real time. It's used for deep traffic analysis and debugging, especially in network pentesting and malware investigation.

Example Usage:

Capture all HTTP traffic:

Start Wireshark

Filter with http to only show HTTP packets

Inspect payloads and headers for sensitive information leaks.

Metasploit Framework - Penetration testing framework

[Source: metasploit.com](https://metasploit.com)

Description: Metasploit is an open-source penetration testing framework that includes exploit code for hundreds of known vulnerabilities. It supports post-exploitation modules and payloads like Meterpreter.

Example Usage:

Exploit a vulnerable service:

Code `msfconsole`

`use exploit/windows/smb/ms17_010_eternalblue`

`set RHOST 192.168.1.5`

`exploit`

Aircrack-ng - WiFi security testing suite

[Source: aircrack-ng.org](https://aircrack-ng.org)

Description: Aircrack-ng is a suite of tools for auditing WiFi networks. It allows capturing packets, cracking WEP/WPA keys, replay attacks, and deauth attacks.

Example Usage:

Crack a WPA handshake:

Code `aircrack-ng handshake.cap -w wordlist.txt`

John the Ripper - Password cracking tool

[Source: openwall.com](https://openwall.com)

Description: A fast password cracking tool supporting multiple hash types. It's ideal for brute-force or dictionary attacks on leaked hashes.

Example Usage:

Code `john hashes.txt --wordlist=rockyou.txt`

SQLmap - Automated SQL injection and database takeover tool

[Source: sqlmap.org](https://sqlmap.org)

Description: Automated tool for detecting and exploiting SQL injection flaws. It supports dumping databases, reading files, and even gaining remote shell access.

Example Usage:

Code `sqlmap -u "http://example.com/page.php?id=1" --dbs`

Nikto - Web server scanner

[Source: cirt.net](https://cirt.net)

Description: Nikto is a basic web server scanner that checks for outdated software, common

misconfigurations, and known vulnerabilities.

Example Usage:

Code `nikto -h http://example.com`

W3af - Web application attack and audit framework

[Source: github.com](https://github.com)

Description: Web Application Attack and Audit Framework; it automates scanning for over 200 types of vulnerabilities.

Example Usage:

Code `./w3af_console`

> target set target http://example.com

> plugins crawl web_spider

> start

Ghidra - Software reverse engineering framework

[Source: github.com](https://github.com)

Description: NSA-developed reverse engineering suite for analyzing binaries. It supports decompilation and scriptable workflows.

Example Usage:

Load a malware binary and decompile to C for analysis.

Python - Programming language useful for scripting custom attacks

[Source: codecademy.com \(Free beginner Python course\)](https://www.codecademy.com/learn/python)

Description: Python is widely used in cybersecurity for writing scripts, automation, and creating custom tooling.

Example Usage:

Code `import requests`

`r = requests.get("http://example.com")`

`print(r.text)`

Kali Linux - Linux distribution for digital forensics and penetration testing

[Source: kali.org](https://kali.org)

Description: Debian-based Linux OS preloaded with hundreds of security tools. Ideal for penetration testing environments.

Example Usage:

Boot into Kali, run:

Code `nmap -A 10.0.0.1`

Maltego - Open-source intelligence and forensics application

[Source: maltego.com](https://maltego.com)

Description: Graph-based open-source intelligence tool used for mapping people, relationships, domains, etc.

Example Usage:

Search a domain to find emails, IPs, and linked domains visually.

Shodan - Search engine for internet-connected devices

[Source: shodan.io](https://shodan.io)

Description: A search engine for internet-connected devices. Can reveal exposed services like RDP, webcams, and industrial systems.

Example Usage:

Code `shodan search "apache country:US"`

ParamSpider - Mines parameters from web archives, JavaScript files, and other sources

[Source: github.com](https://github.com)

Description: Advanced parameter discovery tool for web apps. Extracts parameters from JS, archive.org, and URLs.

Example Usage:

Code `python3 paramspider.py --domain example.com`

Hashcat - Advanced password recovery utility

[Source: hashcat.net](https://hashcat.net)

Description: One of the fastest password recovery tools, supports GPU acceleration.

Example Usage:

Code `hashcat -m 0 -a 0 hashes.txt rockyou.txt`

BeEF - Browser exploitation framework

[Source: github.com](https://github.com)

Description: Browser Exploitation Framework for client-side attacks. Hooks browsers and injects scripts for control.

Example Usage:

Send a malicious link with the BeEF hook to test for vulnerable browser features.

GitHack - Extract contents of a git repository from a website

[Source: github.com](https://github.com)

Description: Tool to download .git folder contents from misconfigured websites.

Example Usage:

Code `python githack.py http://example.com/.git/`

GoBuster - Directory/file & DNS busting tool written in Go

[Source: github.com](https://github.com)

Description: Fast directory and DNS scanner written in Go.

Example Usage:

Code `gobuster dir -u http://example.com -w wordlist.txt`

Postman - Tool for API testing

[Source: postman.com](https://postman.com)

Description: GUI tool for testing APIs. Great for exploring endpoints, headers, and payloads.

Example Usage:

Send a POST request with custom JSON body to `/api/login`.

XSSer- Automated tool for detecting and exploiting XSS

[Source: github.com](https://github.com)

Description: Automated XSS detection and exploitation tool.

Example Usage:

Code `xsser --url "http://example.com/page?q=test"`

Censys - Search engine for analyzing network and system configs

[Source: censys.io](https://censys.io)

Description: Like Shodan, but more focused on SSL/TLS, certificates, and large-scale scans.

Example Usage:

Search by IP or certificate hash via <https://censys.io>.

OpenVAS (Greenbone) - Vulnerability scanning and management

[Source: greenbone.net](https://greenbone.net)

Description: Full vulnerability scanning suite for enterprise-level assessments.

Example Usage:

Launch from GUI, configure scan targets, run full system audit.

Recon-ng - Full-featured reconnaissance framework

[Source: github.com](https://github.com)

Description: Web recon tool with a Metasploit-like interface. Supports APIs, modules, and automated gathering.

Example Usage:

Code `recon-ng`

> `marketplace install all`

> `use recon/domains-hosts/bing_domain_web`

YARA - Helps malware researchers identify and classify malware

[Source: github.com](#)

26. YARA

Description: Malware pattern matching tool. Helps detect and classify files based on rules.

Example Usage:

Code yara myrules.yar suspicious.exe

Sysinternals Suite - Windows troubleshooting and diagnostic tools

[Source: learn.microsoft.com](#)

Description: Collection of Windows tools like Process Explorer, Autoruns, and TCPView. Useful for malware and system analysis.

Example Usage:

Use Autoruns to identify persistent malware on a system.

Fiddler - Web debugging proxy

[Souce: telerik.com](#)

Description: HTTP proxy and traffic debugger, great for inspecting API calls and session tokens.

Example Usage:

Run Fiddler, inspect encrypted traffic using SSL decryption.

Acunetix - Automated web application security scanner

[Source: acunetix.com](#)

Description: Commercial automated scanner for web apps. Detects over 7,000 vulnerabilities.

Example Usage:

Launch a scan against a web target from the GUI, review findings.

Knockpy - Enumerate subdomains on a target domain

[Source: github.com](#)

Description: Subdomain enumeration tool written in Python.

Example Usage:

Code python knockpy.py example.com

padrino - May 30, 2025, 8:59 am

Awesome list, man. Will be saving this to look over! Might be worth adding ParrotOS as an additional choice as well as Kali? Still debian based distro and includes a lot of the same tools but just a more modern UI. I quite like it - and i find it can be less intimidating to new users.

Bastille - June 1, 2025, 3:43 am

Useful list of tools, thanks for the share !

Rose_KALI - June 10, 2025, 3:37 am

thank you for this thread. I finally know where to start for my learning. [warn]