

Forum:[Hack Forums](#)

Thread: [The Best 100 Hacking Tools: Your Guide to Ethical Hacking](#)

leste - November 15, 2025, 6:14 pm

If you are interested in ethical hacking, the good news is that there are many tools available to learn this field. In this article, we will present a compilation that will allow you to discover the best hacking and ethical hacking tools to start your ethical hacking journey.

Network Scanning Tools

Nmap: A free and open-source network scanning tool. Nmap supports various scanning types and protocols, including TCP, UDP, SYN, and more.

Angry IP Scanner: A free and open-source IP address scanner. Users can scan IP addresses and ports and receive basic information about each host.

Zenmap: A free and open-source Nmap GUI interface. Zenmap offers a visual interpretation of Nmap results, allowing you to organize and interpret Nmap scans more easily.

Advanced IP Scanner: A free IP scanner tool. Advanced IP Scanner offers features like remote shutdown and wake-on-LAN.

Fping: A free and open-source ping tool for network diagnostics. Fping sends ICMP pings to multiple hosts simultaneously to help diagnose network issues.

SuperScan: A free multi-functional port scanner. SuperScan offers features like host discovery and trace routing.

Unicornsscan: A free and open-source TCP and UDP port scanner. Unicornsscan uses asynchronous scanning techniques that allow users to scan large networks faster and more efficiently.

Netcat: A free and open-source network utility tool. Netcat can be used for a wide range of tasks, including port scanning, file transfer, and remote command execution.

NetScanTools: A network diagnostics toolkit with free and paid versions. NetScanTools includes utilities for pings, traceroutes, DNS lookups, and more.

Nessus: A paid vulnerability scanner for network analysis. Nessus helps identify vulnerabilities through comprehensive network scans and provides detailed reports to users.

Vulnerability Scanning Tools

OpenVAS: A free and open-source vulnerability scanner. OpenVAS can perform comprehensive security assessments and performance tuning.

Acunetix: A paid web application vulnerability scanner. Acunetix offers advanced scanning techniques and comprehensive reporting to detect over 7,000 vulnerabilities in web applications.

Qualys Cloud Platform: A paid cloud-based vulnerability management platform with a 30-day trial. Qualys provides continuous monitoring and visibility across networks, web applications, and

endpoints in an IT ecosystem.

Nexpose: A paid comprehensive on-premise vulnerability scanner with a 30-day trial. Nexpose scans and identifies vulnerabilities in network assets, databases, web applications, and even virtualization and cloud infrastructure.

SAINT Security Suite: A paid security scanner and penetration testing tool with a free trial. SAINT includes features for vulnerability management, configuration assessment, penetration testing, incident response, and reporting.

Nikto: A free and open-source web server scanner and testing tool. Nikto can check for over 6,000 potentially dangerous files and programs on web servers, as well as outdated servers and other issues.

GFI LanGuard: A paid network security scanner and tool for endpoint protection and patch management with a demo available. GFI LanGuard can scan networks to identify vulnerabilities, manage patches, and ensure compliance with security standards.

Password Cracking Tools

John the Ripper: A free and open-source password cracking tool for auditing and recovery. John the Ripper supports hundreds of hash and password types, including Unix, Windows, macOS, WordPress, database servers, file systems, archives, and more.

Hashcat: A free and open-source advanced password recovery tool. Hashcat calls itself the "world's fastest password cracker" and provides advanced features like distributed cracking networks.

Cain and Abel: A free password recovery tool for Windows computers. Cain and Abel uses techniques such as brute-force, dictionary, and cryptanalysis password attacks.

RainbowCrack: A free and open-source hash cracker tool that uses Rainbow tables. RainbowCrack is available for Windows and Linux and supports GPU acceleration using NVIDIA and AMD GPUs.

Aircrack-ng: A free and open-source suite of Wi-Fi network security tools. Aircrack-ng includes utilities for monitoring, packet capturing, attacking, testing, and cracking Wi-Fi passwords.

Hydra: A free and open-source parallel network login cracking tool. Hydra can crack dozens of protocols, including Cisco, HTTP(S), ICQ, IMAP, MySQL, Oracle, SMTP, and more.

THC Hydra: A free and open-source "proof of concept" password cracking tool. THC Hydra is available for Windows, macOS, and Linux and supports protocols like FTP, SMTP, and HTTP-GET.

Medusa: A free and open-source, fast, massive parallel password cracking tool. Medusa can perform brute-force password testing against multiple hosts or users simultaneously.

L0phtCrack: A free and open-source password auditing and recovery tool. L0phtCrack supports attack techniques including dictionary and brute-force attacks and rainbow tables.

Exploitation Tools

Metasploit: A penetration testing framework with free and paid versions. Metasploit is a Ruby-based, modular tool that comes pre-installed on the Kali Linux distribution.

Burp Suite: A paid web application security testing tool, Burp Suite comes with features for both automated dynamic web scanning and tools to enhance manual vulnerability testing.

Canvas: A paid penetration testing and vulnerability assessment tool. Canvas is available for Windows and Linux and supports over 800 exploits.

Core Impact: A paid penetration testing and vulnerability assessment tool with a free trial. Core Impact can run automated rapid penetration tests and provides an exploit library for testers.

Social-Engineer Toolkit (SET): A free and open-source penetration testing framework for social engineering attacks. Users can execute attacks via Java applications, credential harvesting, SMS spoofing, and much more.

BeEF: A free and open-source browser exploitation penetration testing tool. BeEF can integrate with Metasploit and uses attack vectors to target different web browsers and contexts.

PowerSploit: A free and open-source penetration testing framework containing PowerShell scripts and modules. The PowerSploit toolkit includes exploits for code execution, script modification, data exfiltration, and more.

SQLMap: A free and open-source SQL injection vulnerability testing tool. SQLMap allows users to retrieve data from a SQL database, access the underlying file system, and execute operating system commands.

Armitage: A free and open-source graphical cyber attack management tool. Armitage helps red team members visualize their targets and offers recommendations for exploits and attacks.

Zed Attack Proxy (ZAP): A free and open-source web application security scanner and testing tool. ZAP provides features to automate web security and offers an extensive library of community add-ons.

Packet Sniffing and Spoofing Tools

Wireshark: A free and open-source network protocol analyzer and packet capture tool. Wireshark allows users to examine hundreds of protocols and dozens of file formats.

tcpdump: A free and open-source command-line network packet analyzer. Users can specify a specific filter to search for packets matching that description.

Ettercap: A free and open-source comprehensive suite for man-in-the-middle attacks. Ettercap offers both command-line and GUI interfaces and includes features like live packet sniffing and content filtering.

Bettercap: A free and open-source fork of the Ettercap project and a so-called "Swiss Army Knife" for network attacks. Bettercap can be used on Wi-Fi networks, Bluetooth connections, and 2.4 GHz wireless devices.

Snort: A free and open-source intrusion detection and prevention system. Users can define rules in Snort that indicate malicious network activity and search for packets matching these rules.

Ngrep: A free and open-source network packet analyzer using grep-like patterns. The Ngrep tool supports many different protocols across a wide range of interface types.

NetworkMiner: A free and open-source network forensic analysis tool. NetworkMiner can extract files, images, emails, passwords, and more from network traffic in PCAP files.

Hping3: A free and open-source command-line packet crafting and analysis tool. The Hping3 tool can send custom ICMP/UDP/TCP packets for use cases such as testing firewalls or network performance.

Nemesis: A free and open-source packet crafting and injection tool, Nemesis supports many different protocols and can be used for Layer 2 injection on both Windows and Linux systems.

Wireless Hacking Tools

Wifite: A free and open-source automated wireless network audit tool. Wifite uses tools like Aircrack-ng and Reaver to test WEP and WPA encrypted wireless networks.

Kismet: A free and open-source wireless network detector, sniffer, and IDS. Kismet can run on Windows, macOS, and Linux and tests connections like Wi-Fi, Bluetooth, Zigbee, and RF.

Reaver: A free and open-source brute-force attack tool for WPS. Reaver takes an average of 4 to 10 hours to recover the plaintext WPA/WPA2 password.

Fern Wi-Fi Cracker: A free and open-source wireless security audit and attack tool for Linux. Fern can help crack and recover WEP/WPA/WPS keys and supports other network-based attacks.

Bully: A free and open-source WPS brute-force attack tool. Bully is written in C and offers improved memory and CPU performance compared to Reaver.

CoWPAtty: A free and open-source brute-force WPA2-PSK password cracking tool. CoWPAtty can help users identify weak passphrases that generate the pair-wise master key (PMK).

InSSIDer: A free Wi-Fi network scanning and troubleshooting tool. InSSIDer provides information about Wi-Fi network configuration and the impact of nearby Wi-Fi networks on performance.

Web Application Hacking Tools

Skipfish: A free and open-source web application security reconnaissance tool for Kali Linux. Skipfish crawls a website to create an interactive sitemap and then performs a series of security checks.

Grendel-Scan: A free and open-source automated web application scanning tool. Grendel-Scan also supports features for manual security testing.

Vega: A free and open-source web vulnerability scanner and testing platform. Vega can look for vulnerabilities such as SQL injection, cross-site scripting, and disclosure of sensitive data.

WebScarab: A free and open-source web application vulnerability testing tool. WebScarab is written in Java and offers a set of modular interface components that users can plug and unplug.

IronWASP: A free and open-source web application security testing platform. IronWASP provides a set of pre-built plugins and also allows users to build their own plugins.

Forensic Tools

EnCase: Paid software for digital forensics and incident response. EnCase processes files quickly and efficiently and supports a wide range of computers and mobile devices.

Autopsy: A free and open-source digital forensics platform. Autopsy supports computer hard drives and smartphones and is extensible with various add-on modules.

SIFT: A free and open-source toolkit for forensic analysis and triage. SIFT includes support for dozens of file systems and images and offers tools for incident response.

FTK: Paid forensic investigation software with a demo available. FTK allows users to create full disk forensic images and handles various data types.

X-Ways Forensics: Paid forensic software with advanced file carving features. X-Ways Forensics is a fully portable, high-performance, resource-efficient tool on a USB drive.

Helix3 Pro: A paid incident response and forensic live CD. Helix3 Pro can create forensic images of all internal devices and physical memory on Windows, macOS, and Linux.

Foremost: A free and open-source Linux-based file recovery tool for forensic analysis. Foremost is designed for law enforcement purposes but also supports other use cases.

Scalpel: A free and open-source fast file carving tool based on Foremost for digital forensics. Scalpel is more efficient than Foremost and supports Windows, macOS, and Linux devices.

Sleuth Kit: A free and open-source library of digital investigation software. The Sleuth Kit allows users to investigate disk images and analyze volume and system data.

CAINE: A free and open-source Linux-based digital forensics environment. CAINE offers a user-friendly graphical interface and integration with dozens of tools and other software.

Social Engineering Tools

King Phisher: A free and open-source phishing campaign toolkit. King Phisher helps users simulate real-world phishing attacks and includes features like embedded email images, credential harvesting, and website cloning.

Maltego: A powerful OSINT and link analysis tool with free and paid versions. Maltego features integration with dozens of data sources, including Mandiant, Censys, PolySwarm, Splunk, and more.

Wifiphisher: A free and open-source rogue access point framework for Wi-Fi security testing. Wifiphisher allows users to execute man-in-the-middle and web phishing attacks to capture user credentials and spread malware.

ReelPhish: A free and open-source automated tool for two-factor authentication phishing. ReelPhish was developed by Mandiant and supports multi-page authentication techniques.

Evilginx: A free and open-source man-in-the-middle attack framework. Evilginx can be used to steal user login credentials and session cookies, allowing the tool to bypass two-factor authentication.

Ghost Phisher: A free and open-source wireless and ethernet phishing tool. Ghost Phisher supports features like webpage hosting, credential logging, Wi-Fi access point emulation, session hijacking, and more.

GoPhish: A free and open-source phishing toolkit for organizations. GoPhish runs on Windows, macOS, and Linux and allows users to launch phishing attacks quickly and easily.

Credential Harvester Attack: A free and open-source tool for credential theft within the Social-Engineer Toolkit (SET). The Credential Harvester tool clones a legitimate website and steals users' login information and passwords.

Miscellaneous Tools

OpenSSL: A free and open-source security toolkit for SSL and TLS encryption. OpenSSL is widely used by Internet servers for secure network communications.

Pcredz: A free and open-source tool to extract different types of credentials from packet capture files. Pcredz includes support for a wide range of protocols and saves all credentials to a single file for easy access.

Mimikatz: A free and open-source tool to extract passwords and other credentials from Windows memory. Mimikatz can also perform credential theft attacks such as pass-the-hash and pass-the-ticket.

Sysinternals Suite: A free collection of Windows system utilities for debugging and security analysis from Microsoft. Sysinternals Suite contains over 80 tools for working with Windows systems.