

Tools

BackTrack provided users with easy access to a comprehensive and large collection of security-related tools ranging from port scanners to Security Audit. Support for Live CD and Live USB functionality allowed users to boot BackTrack directly from portable media without requiring installation, though permanent installation to hard disk and network was also an option.

BackTrack included many well known security tools including:

- Metasploit for integration
- Wi-Fi drivers supporting monitor mode (rfmon mode) and packet injection
- Aircrack-ng
- Gerix Wifi Cracker
- Kismet
- Nmap
- Ophcrack
- Ettercap
- Wireshark (formerly known as Ethereal)
- BeEF (Browser Exploitation Framework)
- Hydra
- OWASP Mantra Security Framework, a collection of hacking tools, add-ons and scripts based on Firefox
- Cisco OCS Mass Scanner, a very reliable and fast scanner for Cisco routers with telnet and enabling of a default password.
- A large collection of exploits as well as more commonplace software such as browsers.

BackTrack arranged tools into 12 categories:

- Information gathering
- Vulnerability assessment
- Exploitation tools
- Privilege escalation
- Maintaining access
- Reverse engineering
- RFID tools
- Stress testing
- Forensics
- Reporting tools
- Services
- Miscellaneous