100 Offensive Linux Security Tools

Boni Yeamin

Cyber Security Engineer
Akij group ,Bangladesh.
https://www.linkedin.com/in/boniyeamin/

In the realm of cybersecurity, having a robust arsenal of tools is crucial for both defending and attacking systems. Offensive security tools help penetration testers and security professionals identify vulnerabilities before malicious actors can exploit them. Here, we present an extensive list of 100 offensive Linux security tools, detailing their functionalities and applications.

S.L.	Tool Name	Description
1	Metasploit	Penetration testing framework that allows for the discovery and exploitation of vulnerabilities.
2	Nmap	Network scanning tool used to discover hosts and services on a computer network.
3	Wireshark	Network protocol analyzer used for network troubleshooting and analysis.
4	Aircrack-ng	Suite of tools for assessing Wi-Fi network security.
5	John the Ripper	Password cracking tool that detects weak passwords.
6	Hydra	Network logon cracker supporting many protocols.
7	Burp Suite	Integrated platform for performing security testing of web applications.
8	sqlmap	Automated tool for SQL injection and database takeover.
9	Nikto	Web server scanner that detects vulnerabilities and misconfigurations.
10	OpenVAS	Full-featured vulnerability scanner.
11	Nessus	Comprehensive vulnerability scanner.
12	Snort	Network intrusion detection system (NIDS).
13	Ettercap	Comprehensive suite for man-in-the-middle attacks on LAN.
14	Mimikatz	Tool to extract Windows credentials from memory.
15	Yersinia	Framework for performing Layer 2 attacks.
16	Cain & Abel	Password recovery tool for Microsoft Operating Systems.
17	Social-Engineer Toolkit (SET)	Framework for automating social engineering attacks.
18	Armitage	GUI for Metasploit that makes penetration testing easier.
19	Hashcat	Advanced password recovery tool.
20	Maltego	Tool for link analysis and data mining.
21	BeEF	Browser Exploitation Framework, focusing on client-side attacks.
22	THC-Hydra	Fast network logon cracker supporting many different services.
23	Recon-ng	Full-featured web reconnaissance framework written in Python.
24	Wifite	Automated wireless attack tool.
25	Responder	Tool for LLMNR, NBT-NS and MDNS poisoning.
26	Sqlninja	Tool for exploiting SQL injection vulnerabilities on Microsoft SQL Server.

27	Reaver	Tool for breaking into Wi-Fi Protected Setup (WPS) enabled networks.
28	Slowloris	DoS tool that allows one machine to take down a web server.
29	SEToolkit	Python-driven suite for social engineering attacks.
30	Sqlsus	MySQL injection and takeover tool.
31	Wapiti	Web application vulnerability scanner.
32	Fimap	Tool for finding, exploiting and managing file inclusion bugs in web applications.
33	Arachni	High-performance web application security scanner framework.
34	Skipfish	Fully automated, active web application security reconnaissance tool.
35	W3af	Web application attack and audit framework.
36	Veil-Evasion	Tool designed to generate payloads that bypass antivirus solutions.
37	PowerSploit	Collection of Microsoft PowerShell modules for exploiting and auditing Windows machines.
38	WPScan	WordPress vulnerability scanner.
39	Immunity Debugger	Powerful way to write exploits, analyze malware, and reverse engineer binary files.
40	Volatility	Advanced memory forensics framework.
41	Binwalk	Firmware analysis tool.
42	Apktool	A tool for reverse engineering Android APK files.
43	Clang	A compiler front end for the C, C++, and Objective-C programming languages.
44	Flawfinder	Scans C/C++ source code for security vulnerabilities.
45	GDB	The GNU Project debugger, a standard debugger for the GNU operating system.
46	Radare2	Open-source software for reverse engineering and analyzing binaries.
47	Cuckoo Sandbox	Malware analysis system.
48	OllyDbg	32-bit assembler level analyzing debugger for Microsoft Windows.
49	ZAP Proxy	Integrated penetration testing tool for finding vulnerabilities in web applications.
50	MobSF	Mobile Security Framework for automated mobile app analysis.
51	RIPS	Static code analysis tool to find vulnerabilities in PHP applications.
52	Lynis	Security auditing tool for Unix-based systems.
53	Tiger	Security audit and intrusion detection tool for Linux.
54	Bastille	Hardening program for Unix and Linux systems.
55	Lynx	Text-based web browser used for examining web vulnerabilities.
56	Xplico	Network forensic analysis tool.
57	DFF (Digital Forensics Framework)	Open-source tool for digital forensics investigation.
58	Foremost	Console program to recover files based on their headers, footers, and internal data structures.
59	Scalpel	File carving and indexing application.
60	Sleuth Kit	Collection of command-line tools for investigating disk images.
61	Autopsy	Graphical interface to The Sleuth Kit and other digital forensics tools.
62	CAINE	Computer Aided INvestigative Environment, a Linux live distribution for digital forensics.
63	DEFT	Digital Evidence and Forensics Toolkit, another Linux distribution for forensics.
64	REMnux	Linux distribution for reverse-engineering and analyzing malicious software.
65	Tsurugi Linux	Linux distribution for digital forensics, OSINT, and incident response.

66	Paladin Forensics	Live operating system based on Ubuntu that provides a range of forensic tools.
67	SIFT Workstation	Forensics and incident response toolkit.
68	Plaso	Tool for automatic creation of a super timeline from various digital artifacts.
69	Bulk Extractor	Forensic tool to scan a disk image, directory, or file for features of interest.
70	Rekall	Memory forensic framework.
71	Kismet	Wireless network and device detector, sniffer, and intrusion detection system.
72	dsniff	Collection of tools for network auditing and penetration testing.
73	Tcpdump	Command-line packet analyzer.
74	Yara	Tool for identifying and classifying malware samples.
75	UPX	Ultimate Packer for Executables, a free and portable executable packer for several file formats.
76	Valgrind	Programming tool for memory debugging, memory leak detection, and profiling.
77	QEMU	Generic and open-source machine emulator and virtualizer.
78	VirtualBox	Free and open-source hosted hypervisor for x86 virtualization.
79	Docker	Platform to develop, ship, and run applications inside containers.
80	Vagrant	Tool for building and maintaining portable virtual software development environments.
81	Ansible	Open-source software provisioning, configuration management, and application-deployment tool.
82	Puppet	Configuration management tool for automating the management of server infrastructure.
83	Chef	Configuration management tool for streamlining the task of configuring and maintaining servers.
84	SaltStack	Configuration management software for managing server infrastructure.
85	Terraform	Infrastructure as code tool for building, changing, and versioning infrastructure safely.
86	Kubernetes	Open-source container orchestration system for automating software deployment, scaling, and management.
87	Apache JMeter	Open-source software designed to load test functional behavior and measure performance.
88	OWASP ZAP	Open-source web application security scanner.
89	Sublist3r	Fast subdomains enumeration tool for penetration testers.
90	Dirbuster	Multi-threaded application designed to brute-force directories and files names on web servers.
91	Medusa	Speedy, massively parallel, modular, login brute-forcer.
92	Gobuster	Tool used to brute-force URIs (directories and files) and DNS subdomains.
93	DMitry	Deepmagic Information Gathering Tool, a UNIX/(GNU)Linux CLI program coded in C.
94	WhatWeb	Next generation web scanner.
95	theHarvester	E-mail, subdomain, and people names harvester.
96	Amass	In-depth DNS enumeration and network mapping.
97	Masscan	TCP port scanner, potentially faster than Nmap.
98	ExploitDB	Database of exploits and vulnerable software.
99	SearchSploit	Command line search tool for ExploitDB.

100	**Commix**	**Automated command injection and exploitation tool.**

This extensive list of tools offers a comprehensive set of resources for any security professional involved in offensive security, penetration testing, or ethical hacking. Mastery of these tools can significantly enhance one's ability to identify and mitigate potential security threats effectively.