50 MOST USED KALI LINUX COMMANDS IN 2025

CREATED BY BLACKPANDA999 TEAM

50 Most Used Kali Linux Commands in 2025

Introduction

Welcome to the 2025 Edition of "50 Top Kali Linux Commands," a meticulously curated guide designed for cybersecurity enthusiasts, penetration testers, and IT professionals. Kali Linux, a Debian-based distribution tailored for security research and ethical hacking, offers a robust set of tools accessible via the command line. This eBook provides a detailed overview of 50 essential commands, categorized into Basic System Commands, Network Scanning & Reconnaissance, Exploitation & Vulnerability Analysis, Wireless Attacks, Packet Analysis & Sniffing, Password & Hash Tools, and Post-Exploitation & Forensics. Each command includes a one-line explanation, a detailed description, and practical use cases to enhance your skill set. Whether you're preparing for a certification, conducting a security audit, or exploring ethical hacking, this guide is your go-to resource. Dive in and master these commands to elevate your cybersecurity expertise.

ifconfig

Displays network interfaces and IP addresses.

Example: ifconfig eth0

iwconfig

Displays or configures wireless network interfaces.

Example: iwconfig wlan0

ip a

Shows all IP addresses assigned to all network interfaces.

Example: ip a

ping

Sends ICMP echo request to test network connectivity.

Example: ping google.com

netstat

Displays network connections, routing tables, and stats.

> ***Example: netstat -tulnp***

nmap

Scans networks to discover hosts and services.

> ***Example: nmap -sV 192.168.1.1***

traceroute

Traces the path packets take to a network host.

> ***Example: traceroute google.com***

whois

Provides domain ownership and registration info.

> ***Example: whois example.com***

dig

Performs DNS queries and displays detailed results.

> ***Example: dig google.com***

dnsenum

Performs DNS enumeration for a domain.

> ***Example: dnsenum example.com***

tcpdump

Captures network packets for analysis.

> ***Example: tcpdump -i eth0***

wireshark

Graphical tool for deep network protocol analysis.

> ***Example: wireshark***

airmon-ng

Enables monitor mode on wireless interfaces.

Example: airmon-ng start wlan0

airodump-ng

Captures packets and displays wireless network info.

Example: airodump-ng wlan0mon

aireplay-ng

Injects frames into a wireless network to test security.

Example: aireplay-ng --deauth 10 -a [AP_MAC] wlan0mon

aircrack-ng

Cracks WEP and WPA/WPA2-PSK keys.

Example: aircrack-ng capture.cap

hydra

Brute-force attack tool for login cracking.

Example: hydra -l admin -P passlist.txt ftp://192.168.1.1

john

Password cracking tool supporting multiple formats.

Example: john --wordlist=rockyou.txt hashes.txt

hashcat

Advanced password recovery and cracking tool.

Example: hashcat -m 0 hashes.txt rockyou.txt

metasploit

Framework for developing and executing exploit code.

Example: msfconsole

msfvenom

Generates custom payloads for Metasploit.

Example: msfvenom -p windows/meterpreter/reverse_tcp LHOST=...

burpsuite

Web vulnerability scanner and proxy tool.

Example: Launch via GUI

sqlmap

Automates detection and exploitation of SQL injection.

Example: sqlmap -u http://example.com?id=1 --dbs

nikto

Web server vulnerability scanner.

Example: nikto -h http://example.com

dirb

Brute force tool for web content discovery.

Example: dirb http://example.com

gobuster

Tool for directory and file brute-forcing on web servers.

Example: gobuster dir -u http://example.com -w /path/to/wordlist

wpscan

Scans WordPress for vulnerabilities.

Example: wpscan --url http://example.com

enum4linux

Enumerates information from Windows machines.

Example: enum4linux 192.168.1.10

smbclient

Accesses shared folders on Windows using SMB protocol.

Example: smbclient //192.168.1.10/share

ncat

Reads and writes data across networks using TCP/UDP.

Example: ncat -lvp 4444

netcat

Tool for network diagnostics and backdoors.

Example: nc -lvp 1234

openssl

Toolkit for SSL/TLS and cryptographic operations.

Example: openssl s_client -connect google.com:443

sslyze

Analyzes SSL configuration of a server.

Example: sslyze --regular example.com

fcrackzip

Cracks password-protected .zip archives.

Example: fcrackzip -v -u -D -p wordlist.txt file.zip

dnsrecon

Performs DNS enumeration and reconnaissance.

Example: dnsrecon -d example.com

theharvester

Collects emails, domains, and subdomains from public sources.

Example: theharvester -d example.com -b google

xsser

Automates testing for XSS vulnerabilities in web apps.

Example: xsser -u http://example.com

yersinia

Attacks Layer 2 network protocols.

Example: yersinia -G

zmap

Performs fast single-packet network scans.

Example: zmap -p 80 192.168.0.0/16

ettercap

Performs man-in-the-middle attacks on LAN.

Example: ettercap -G

setoolkit

Social engineering attacks framework.

Example: setoolkit

msfconsole

Command-line interface for Metasploit Framework.

Example: msfconsole

autopsy

GUI digital forensics platform.

Example: autopsy

binwalk

Analyzes binary files for embedded files and code.

Example: binwalk firmware.bin

strings

Extracts readable text from binary files.

Example: strings binaryfile

volatility

Memory forensics framework.

Example: volatility -f memdump.img --profile=Win7SP1x64 pslist

chkrootkit

Scans system for signs of rootkits.

Example: chkrootkit

rkhunter

Scans for rootkits and local exploits.

Example: rkhunter --check

searchsploit

Searches Exploit-DB database for vulnerabilities.

Example: searchsploit apache

exploitdb

Local copy of Exploit-DB exploits and tools.

Example: search through /usr/share/exploitdb

Created by Blackpanda999 Team

Follow us for more cybersecurity, ethical hacking, and tech content.