```
==============================
Kali Linux Command Cheatsheet
==============================

--- SYSTEM INFORMATION ---
whoami                          # Show current user
id                              # UID, GID, groups
hostname                        # System hostname
uname -a                        # System and kernel version
uptime                          # System uptime
date                            # Current date and time
arch                            # CPU architecture
lscpu                           # Detailed CPU info
lsblk                           # Block device info
free -h                         # Memory usage
df -h                           # Disk usage
du -sh *                        # Size of directories/files

--- USER MANAGEMENT ---
adduser newuser                 # Add a new user
usermod -aG sudo newuser        # Add user to sudo group
deluser username                # Delete a user
passwd username                 # Change user's password
groups                          # Show group memberships
who                             # List users logged in
last                            # Login history

--- FILE & DIRECTORY COMMANDS ---
ls -la                          # List all files with details
cd /path                        # Change directory
mkdir folder                    # Make a new directory
rm -rf folder/                  # Delete directory and contents
cp file1 /dest/                 # Copy file
mv file1 /dest/                 # Move or rename file
touch file.txt                  # Create a blank file
cat file.txt                    # View contents
less file.txt                   # View with navigation
find / -name file.txt           # Search for a file

--- PACKAGE MANAGEMENT ---
apt update                      # Refresh repo list
apt upgrade                     # Upgrade installed packages
apt install toolname            # Install a package
apt remove toolname             # Remove a package
dpkg -i package.deb             # Install local .deb file
```

```
--- NETWORKING & SCANNING ---
ip a                            # Show IP addresses
ifconfig                        # Show interfaces
netdiscover                     # Find hosts on LAN
ping -c 4 target.com            # Test connectivity
nmap -sS -T4 192.168.1.0/24     # Fast stealth scan
nmap -A -p- target              # Aggressive scan all ports
whois target.com                # WHOIS info
dig target.com                  # DNS lookup
nslookup target.com             # DNS lookup
traceroute target.com           # Trace path to host
tcpdump -i eth0                 # Capture traffic

--- WIRELESS HACKING ---
airmon-ng                       # Show wireless interfaces
airmon-ng start wlan0           # Enable monitor mode
airodump-ng wlan0mon            # View networks
airodump-ng -c 6 -w capture wlan0mon
                                 # Capture handshake
aireplay-ng -0 10 -a <BSSID> wlan0mon
                                 # Deauth attack
aircrack-ng capture.cap -w wordlist.txt
                                 # Crack WPA/WEP

--- PASSWORD ATTACKS ---
hydra -l admin -P pass.txt ssh://192.168.1.10
                                 # Brute-force SSH
john --wordlist=rockyou.txt hash.txt
                                 # Crack password hashes
hashcat -m 0 hash.txt wordlist.txt
                                 # GPU-based cracking

--- PRIVILEGE ESCALATION ---
sudo -l                         # Show sudo rights
sudo su                         # Become root
find / -perm -4000 -type f 2>/dev/null
                                 # SUID files
getcap -r / 2>/dev/null         # Files with capabilities
pspy                            # Watch unprivileged processes

--- EXPLOITATION TOOLS ---
msfconsole                      # Start Metasploit
searchsploit exploit_name       # Search ExploitDB
exploitdb                       # Exploit database
```

```
setoolkit                       # Launch SET toolkit
sqlmap -u URL --dbs             # SQL injection automation

--- WEB APPLICATION TESTING ---
burpsuite                       # Web proxy and testing
nikto -h http://target          # Web server scan
gobuster dir -u URL -w wordlist # Directory brute-force
wpscan --url http://site        # WordPress scanner

--- SYSTEM MONITORING ---
top                             # Live process viewer
htop                            # Enhanced top
ps aux                          # Show all processes
kill -9 PID                     # Force kill
lsof -i                         # List open ports and processes

--- MISC / AUTOMATION ---
cronjob                         # Edit scheduled tasks: crontab -e
echo "Hello" > file.txt         # Write to a file
chmod +x script.sh              # Make script executable
bash script.sh                  # Run shell script
python3 exploit.py              # Run Python 3 script

--- SHORTCUTS ---
Ctrl+C                          # Cancel command
Ctrl+Z                          # Pause command
Ctrl+D                          # Logout/EOF
!!                              # Repeat last command
!n                              # Run nth command in history
history                         # View command history
clear                           # Clear terminal
```