◆ What is This Step About?

Kali Linux is a special operating system **built for cybersecurity and ethical hacking**. It comes with hundreds of tools **pre-installed**—meaning you don't have to download or install them manually.

These tools are **grouped by purpose** (e.g., information gathering, password cracking, etc.). This step is about exploring and learning how to find and launch them.

◆ How to Access the Tools

You can access all these tools using:

📁 **Graphical Menu:**

1. Click on the **Kali Dragon Icon** (top-left corner).

2. Go to **"Applications" → "Kali Linux"**.

3. You'll see folders like:

    o **Information Gathering**

    o **Vulnerability Analysis**

    o **Exploitation Tools**

    o etc.

Each folder contains relevant tools for a specific task.

🖥️ **Terminal Commands:**

You can also run these tools directly using the terminal.
For example:

nmap

or

msfconsole

◆ **Categories Explained with Tools**

Here's a breakdown of what each category does and examples of tools inside:

Category	Purpose	Example Tools	What They Do
🕵️ **Information Gathering**	Collect info about targets	nmap, whois	Scan IPs/ports, get domain details
🔍 **Vulnerability Analysis**	Find weak spots in systems	nikto, wpscan	Scan for known vulnerabilities
💣 **Exploitation Tools**	Use exploits to test vulnerabilities	Metasploit	Try exploiting a target with payloads
🔒 **Password Attacks**	Crack or guess passwords	John the Ripper, Hydra	Brute force passwords for services
📊 **Wireless Attacks**	Attack or audit Wi-Fi networks	aircrack-ng	Capture and crack Wi-Fi handshakes
📡 **Sniffing & Spoofing**	Monitor or manipulate traffic	Wireshark	Capture and analyze network packets
🌐 **Web App Testing**	Test websites for bugs	Burp Suite	Intercept and modify web requests
🧪 **Forensics**	Analyze evidence after an attack	Autopsy	Recover deleted files, analyze logs

◆ **How to Launch a Tool**

There are **two ways**:

1. From GUI Menu

- Click: **Applications → Kali Linux → Information Gathering → Nmap**

2. From Terminal

- Just type the name of the tool, like:

nmap -v scanme.nmap.org

Why Is This Important?

As a cybersecurity student or professional, you'll use these tools **daily** to:

- Test systems for vulnerabilities

- Investigate breaches

- Learn offensive and defensive techniques

By exploring them, you get familiar with their **interface**, **options**, and **use cases**.

*Here Explaining each one's purpose, usage, and basic command with examples. This will give you a strong practical understanding of the most essential **Kali Linux tools**.*

Essential Kali Linux Tools – Usage Guide

1. Information Gathering

Tool: nmap

- **Use**: Scans networks for open ports, services, and operating systems.

- **Command**:

<mark>nmap -sV 192.168.1.1</mark>

- **Example**: Checks which services (like SSH, FTP) are running on a system.

Tool: whois

- **Use**: Looks up domain registration information.

- **Command**:

<mark>whois example.com</mark>

- **Example**: Tells you who owns a website and their contact details.

2. Vulnerability Analysis

Tool: nikto

- **Use**: Scans websites for known vulnerabilities.

- **Command**:

nikto -h http://testphp.vulnweb.com

 Tool: wpscan

- **Use**: Scans WordPress websites for vulnerabilities.

- **Command**:

wpscan --url http://example.com --enumerate vp

(Make sure to use --api-token if needed.)

3. Exploitation Tools

Tool: Metasploit

- **Use**: Framework for launching and testing exploits.

- **Command**:

msfconsole

- **Steps**:

    1. Launch msfconsole

    2. Search for an exploit:

search vsftpd

    3. Use the exploit and run:

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOST 192.168.1.5

run

4. Password Attacks

Tool: John the Ripper

- **Use**: Cracks password hashes.

- **Command**:

john /etc/shadow

Tool: Hydra

- **Use**: Performs brute force login attacks on services (like SSH).

- **Command**:

hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.5

5. Wireless Attacks

Tool: aircrack-ng

- **Use**: Cracks Wi-Fi passwords from captured handshake files.

- **Command**:

aircrack-ng capture-01.cap -w rockyou.txt

6. Sniffing and Spoofing

Tool: Wireshark

- **Use**: Captures and analyzes network packets.

- **Launch**: From GUI or:

wireshark

- **Example**: Analyze HTTP, FTP, or DNS traffic in real-time.

7. Web Application Testing

Tool: Burp Suite

- **Use**: Intercepts and modifies HTTP/HTTPS requests.
- **Steps**:

    1. Launch Burp Suite
    2. Set browser proxy to 127.0.0.1:8080
    3. Intercept login forms or URLs

8. Forensics

Tool: Autopsy

- **Use**: Digital forensics GUI for analyzing disk images and deleted files.
- **Launch**:

autopsy

Open in browser: Usually at http://localhost:9999/autopsy