Introduction to Kali Linux

What is Kali Linux?

Kali Linux, previously known as BackTrack Linux, is a free, open-source distribution designed for cybersecurity and penetration testing. Developed by Mati Aharoni and Devon Kearns of Offensive Security, it is built on Debian and provides a secure, robust, and customizable environment for professional in information technology.

It comes pre-installed with a wide range of security tools, enabling users to perfrom tasks such as network analysis, reverse engineering, and vulnerability assessments. Whether you're a cybersecurity analyst, student, ethical hacker, or an IT system administrator, its tools must be used for ethical and legal purposes only.

What is Kali Linux used for?

Kali Linux is primarily used to perform the following tasks:

Social engineering attacks: Tests whether users would be tricked into revealing sensitive information, such as passwords or login credentials.

- Social-Engineer Toolkit (SET)

Vulnerability scanning: Finds weaknesses of the system and application.

- Nikto
- OpenVAS

Wireless attacks: Used for performing wireless network assessments, such as cracking poorly secured Wi-Fi passwords to identify vulnerabilities.

- Aircrack-ng
- Bettercap
- Eaphammer

Password cracking: Performing offline and online attacks to audit the strength of stored passwords or authentication systems.

- Hydra
- Hashcat
- John the Ripper

Information Gathering: Gathering information about a target's network, systems, and infrastructure – including servers, domains, IP addresses, and services – to identify potential attack vectors.

- nslookup
- whois
- dig
- dnsrecon

Network packet capturing: Capturing and analyzing network traffic to monitor data flow and detect suspicious activity or vulnerabilities.

- Wireshark
- tcpdump

Virtual Private Network (VPN): Establishing encrypted connections to ensure anonymity, protect data transmission, and securely access remote systems during penetration testing.

- OpenVPN