Kali Linux – Distribución para pruebas de seguridad

1. ¿Qué es Kali Linux?

- **Distribución GNU/Linux** basada en **Debian**.
- Diseñada específicamente para **auditorías de seguridad informática, pruebas de penetración y análisis forense digital**.
- Desarrollada y mantenida por **Offensive Security** (empresa de formación en ciberseguridad, conocida por la certificación OSCP).
- Es el sistema operativo de referencia para el **hacking ético y la ciberseguridad ofensiva**.

---

2. Características principales

- Kernel de Linux optimizado para **soporte de drivers de tarjetas Wi-Fi** y hardware de red (ideal para auditoría inalámbrica).
- Incluye más de **600 herramientas preinstaladas** para:
    - Análisis de vulnerabilidades.
    - Ataques de red.
    - Criptografía.
    - Forense digital.
    - Ingeniería inversa.
- Totalmente **libre y de código abierto**.
- Soporte en múltiples arquitecturas:
    - **x86/x64**.
    - ARM (Raspberry Pi, etc.).
    - Imágenes listas para máquinas virtuales (VMware, VirtualBox, Hyper-V).
- Permite **ejecutarse en modo live** desde un USB o CD sin necesidad de instalarse.

---

3. Entornos de uso

- **Pentesting (penetration testing)**: pruebas de intrusión controladas.
- **Hacking ético**: evaluación de seguridad con consentimiento.
- **Auditorías de red**: análisis de puertos, servicios, configuraciones inseguras.
- **Análisis forense**: recuperación de datos borrados, análisis de discos y memoria RAM.
- **Formación**: prácticas de Red Team en entornos educativos y de laboratorio.

---

4. Herramientas más utilizadas

Algunas categorías con ejemplos:

- **Recopilación de información (Reconnaissance):**
    - `Nmap` → escaneo de puertos y servicios.
    - `theHarvester` → búsqueda de correos, usuarios y dominios.
    - `Maltego` → análisis OSINT.
- **Análisis de vulnerabilidades:**
    - `Nikto` → análisis de servidores web.
    - `OpenVAS` → escaneo de vulnerabilidades.
- **Explotación:**
    - `Metasploit Framework` → framework para exploits.
    - `sqlmap` → automatiza ataques de inyección SQL.
- **Contraseñas:**
    - `John the Ripper` y `Hashcat` → crackeo de hashes.
    - `Hydra` → fuerza bruta contra servicios.
- **Redes inalámbricas:**
    - `Aircrack-ng` → auditoría de redes Wi-Fi.
    - `Reaver` → ataques a WPS.
- **Sniffing y spoofing:**
    - `Wireshark` → análisis de tráfico de red.
    - `Ettercap` → ataques MITM.
- **Forense digital:**

- `Autopsy` → análisis forense de discos.
- `Volatility` → análisis de memoria RAM.

---

5. Arquitectura y funcionamiento

- Basado en **Debian Testing** → se mantiene actualizado con repositorios propios.
- Sistema **modular**: puedes instalar solo las herramientas que necesites.
- Kernel parcheado con **compatibilidad extendida para hardware de seguridad**.
- Usuario por defecto: `kali` (con privilegios sudo).
- Entorno gráfico ligero: **XFCE** (por defecto), aunque soporta GNOME o KDE.

---

6. Importancia en Red Team y Blue Team

- **Red Team (ataque):**
  Usan Kali Linux para **descubrir vulnerabilidades, explotarlas y simular ataques reales**.

- **Blue Team (defensa):**
  Analizan logs, tráfico y sistemas atacados por Kali → aprenden a **detectar, mitigar y endurecer configuraciones**.