**KALI-LINUX**

**1.- Kali-Linux: Descripción de Kali-Linux.**

**Kali Linux** es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informatica en general. Se fundó por Offensive Security Ltd. Mati Aharoni y Devon Kearns, ambos pertenecientes al equipo de Offensive Security.

**Kali** es desarrollado en un entorno seguro; el equipo de **Kali** está compuesto por un grupo pequeño de personas de confianza quienes son los que tienen permitido modificar paquetes e interactuar con los repositorios oficiales. Todos los paquetes de **Kali** están firmados por cada desarrollador que lo compiló y publicó. A su vez, los encargados de mantener los repositorios también firman posteriormente los paquetes utilizando GNU Privacy Guard.

**2.- Sistema Operativo: Sistema Operativo en el que está basado Kali-Linux.**

Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general.

Debian GNU/Linux es un sistema operativo libre, desarrollado por miles de voluntarios de todo el mundo, que colaboran a través de Internet.

Nació en el año 1993, de la mano del proyecto Debian, con la idea de crear un sistema GNU usando Linux como núcleo ya que el proyecto Debian, organización responsable de su mantenimiento en la actualidad, también desarrolla sistemas GNU basados en otros núcleos

Debian GNU/Linux puede instalarse utilizando distintos mecanismos de instalación, como DVD, CD, USB, e incluso directamente desde la red.

**3.-** **Herramientas: Herramientas de Kali-Linux.**

Este sistema operativo viene con un montón de herramientas de seguridad informática, penetración y hacking ético(sin fines maliciosos). Sin embargo, también hay mucha gente que lo usa para “hacer el mal” y realizar delitos informáticos.

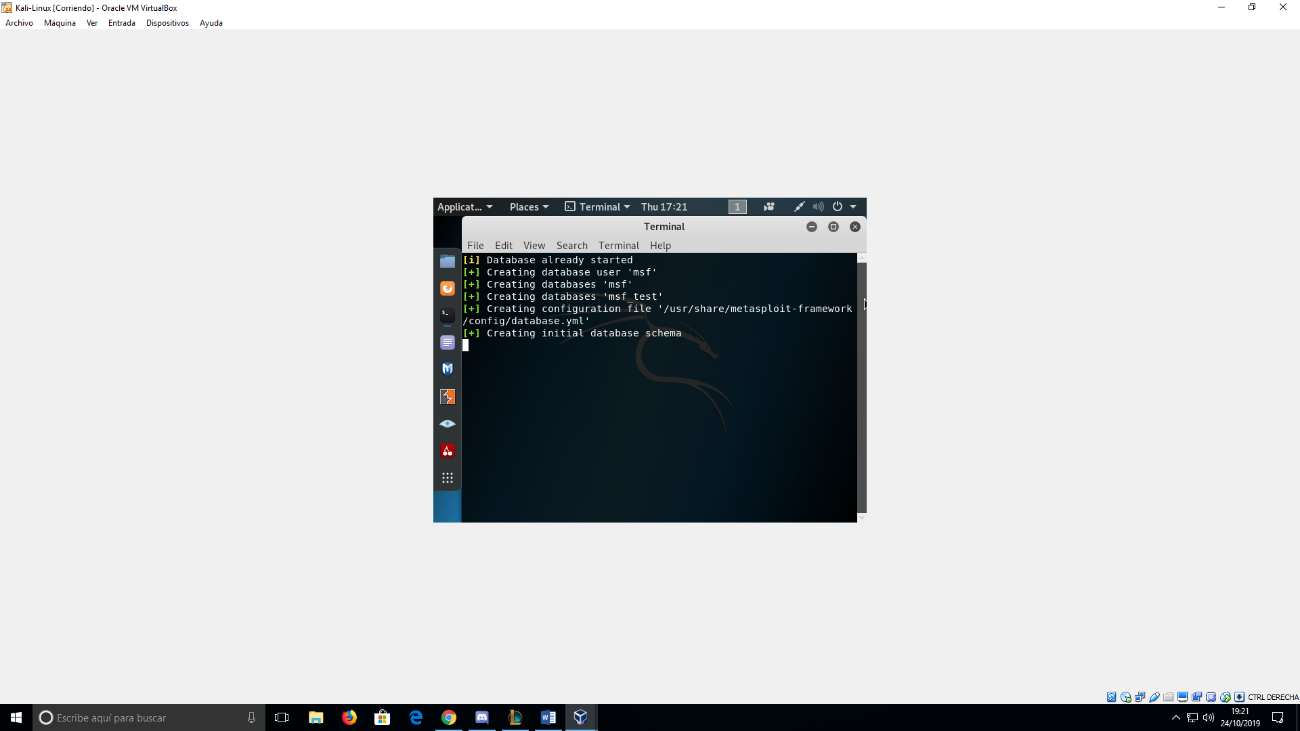
Aquí he recopilado 5 herramientas que son muy utilizadas en kali-linux.

* **Wireshark:** Este programa es todo un clásico en el mundo de la seguridad informática y no podía faltar en Kali Linux. Este programa **se encarga de analizar paquetes de tu red**, los cuales luego puedes abrir y ver de manera detallada lo que significa.
* **Zenmap(Nmap):** Zenmap es la versión “modo fácil” de Nmap, es decir, una interfaz gráfica que te permite utilizar Nmap sin meter comandos. Nmap **te puede ayudar para ver los host que tiene una red**, para comprobar quien está conectado y cuantos equipos hay en esa red.
* **Oswap:** Esta aplicación nos sirve para encontrar contenido malintencionado en páginas web, como por ejemplo algún código java script que realice alguna acción maliciosa(por ejemplo modificar el etc/hosts para hacer pharming). Este programa permite un escáner manual de la red o un escáner en segundo plano que actuará cada vez que visites páginas web.
* **Armitage:** Este programa es una GUI de ataques Metasploit, la cual te permitirá hacer estos ataques de una forma visual e intuitiva. Con esta aplicación, podremos comprobar si nuestros equipos son vulnerables o no a sploits. Además de poder ejecutar ataques metasploit sin saber comandos, también podremos hacer análisis de Nmap e incluso hacer ataques de fuerza bruta.
* **Suite Aircrack-ng:** La suite aircrack-ng te permite comprobar la robustez de tu clave Wi-Fi, ya que permite autoatacarte tanto por fuerza bruta como por ataque de diccionario(para las wpa). En esta suite, vienen programas como el airmon-ng, el aireplay, airodump o aircrack, los cuales están relacionados entre si y trabajan juntos por romper la contraseña. Lo malo es que no ataca al protocolo WPS(para eso tendrás que usar reaver).

Esperamos que tras leer el post, ya tengas más claro qué es Kali Linux y el potencial que tienen todas sus herramientas.

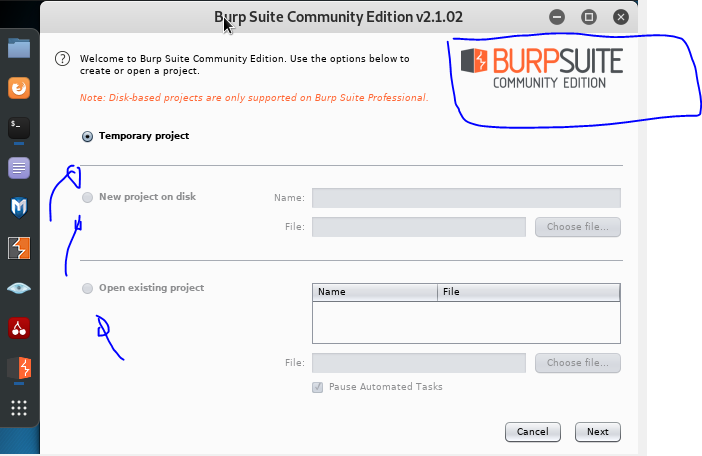
**4.- Ejemplos De Herramientas: Metasploit Framework**

Metasploit Framework es una infraestructura que puede ser personalizada y utilizada para necesidades específicas. también hay que mencionar que Metasploit Framework está respaldada por una comunidad de más de 200.000 usuarios, sin contar que esta herramienta también está respaldad por una empresa, Rapid7.

****

**5.- Ejemplos De Herramientas: Burpsuite**

Burp Suite es una herramienta fundamental dentro de la seguridad informática, creada por la empresa PortSwigger y escrita en Java que permite realizar pruebas de seguridad de aplicaciones web, Burp Suite cuenta con una versión gratuita (Burp Free) y una versión de pago (Burp Professional).

****