**Herramientas de Kali-Linux**

Podemos enumerar una serie de herramientas de hacking para satisfacer cada una de tus necesidades.

**1. AIRCRACK-NG**

Aircrack-ng es una de las mejores herramientas inalámbricas para hackear contraseñas para el craqueo WEP/WAP/WPA2 utilizado en todo el mundo.

Funciona al tomar paquetes de la red, lo analiza a través de contraseñas recuperadas. También posee una interfaz de consola. Además de esto, Aircrack-ng también utiliza el ataque estándar de FMS (Fluhrer, Mantin y Shamir) junto con algunas optimizaciones como los ataques KoreK y el ataque PTW para acelerar el ataque, que es más rápido que el WEP.

Si encuentras que Aircrack-ng es difícil de usar, simplemente consulta los tutoriales disponibles en línea.

**2. THC HYDRA**

THC Hydra utiliza el ataque de fuerza bruta para crackear prácticamente cualquier servicio de autenticación remota. Admite ataques rápidos de diccionario para más de 50 protocolos, incluidos ftp, https, telnet, etc.

Puedes usarlo para entrar en escáneres web, redes inalámbricas, crafters de paquetes, gmail, etc.

**3. JOHN THE RIPPER**

John the Ripper es otra herramienta popular de cracking utilizada en la comunidad de pruebas de penetración (y hacking).

Inicialmente fue desarrollado para sistemas Unix, pero ha crecido para estar disponible en más de 10 distros.

Cuenta con un cracker personalizable, detección de hash de contraseña automática, ataque de fuerza bruta y ataque de diccionario (entre otros modos de cracking).

**4. METASPLOIT FRAMEWORK**

Metasploit Framework es un marco de código abierto con el cual los expertos y equipos de seguridad verifican las vulnerabilidades, así como también realizan evaluaciones de seguridad para mejorar la conciencia de la seguridad.

Cuenta con una gran cantidad de herramientas con las que puedes crear entornos de seguridad para las pruebas de vulnerabilidad y funciona como un sistema de prueba de penetración.

**5. NETCAT**

Netcat, usualmente abreviado como nc, es una utilidad de red con la cual puedes usar protocolos TCP / IP para leer y escribir datos a través de conexiones de red.

Puedes usarlo para crear cualquier tipo de conexión, así como para explorar y depurar redes utilizando el modo túnel, escaneo de puertos, etc.

**6. NMAP (“NETWORK MAPPER”)**

Network Mapper es una herramienta gratuita y de código abierto utilizada por los administradores del sistema para descubrir redes y auditar tu seguridad.

Es rápido en su funcionamiento, está bien documentado, cuenta con una interfaz gráfica, admite transferencia de datos, inventario de red, etc.

**7. NESSUS**

Nessus es una herramienta de escaneo remoto que puedes usar para verificar las vulnerabilidades de seguridad de los ordenadores. No bloquea activamente las vulnerabilidades que tienen, pero podrás detectarlas ejecutando más de 1200 comprobaciones de vulnerabilidad y lanzando alertas cuando sea necesario realizar parches de seguridad.

**9. SNORT**

Snort es un NIDS gratuito y de código abierto con el que puedes detectar vulnerabilidades de seguridad en tu sistema.

Con él puedes ejecutar análisis de tráfico, búsqueda/coincidencia de contenido, registro de paquetes en redes IP y detectar una variedad de ataques de red, entre otras características, todo en tiempo real.

**10. KISMET WIRELESS**

Kismet Wireless es un sistema de detección de intrusos, detector de red y detector de contraseñas. Funciona predominantemente con redes Wi-Fi (IEEE 802.11) y puede tener su funcionalidad extendida usando complementos.

**11. NIKTO**

Nikto2 es un escáner web gratuito y de código abierto para realizar pruebas rápidas y completas contra elementos en la web. Lo hace buscando más de 6500 archivos potencialmente peligrosos, versiones de programas desactualizados, configuraciones de servidores vulnerables y problemas específicos del servidor.