# **Es sorprendente cuánta gente está interesada en aprender a piratear, ¿Posiblemente porque las personas tienen una visión más salvaje del hacking de lo que realmente es?**

# **De todos modos, gracias a la comunidad de código abierto, existen incontables herramientas de piratería que se adaptan a todo tipo de necesidades.**

# **Solamente recuerda centrarte en el hacking ético y no en otros menesteres.**

# **En algunas publicaciones anteriores, hemos visto algunos de** [**los mejores sistemas operativos para comenzar a piratear**](https://ciberninjas.com/mejores-sistemas-operativos-para-hackear/)**, vimos** [**los mejores sitios web en los que aprender a hackear**](https://ciberninjas.com/14-mejores-sitios-aprender-hackear/)**.**

# **Además, repasamos todas** [**las herramientas que aparecen en Mr. Robot**](https://ciberninjas.com/software-mister-robot/)**, la famosa serie basada en el hacker Elliot Allerson y representado excepcionalmente por Rami Malek.**

# **Hoy, vamos a echar el ojo a algunas de las mejores herramientas que se pueden utilizar desde uno de los mejores sistemas centrados en el hacking y la ciberseguridad, como por ejemplo:** [**Kali Linux**](https://ciberninjas.com/mejores-sistemas-operativos-para-hackear/#1_Kali_Linux)**.**

# 

# **20 Mejores herramientas de Hacking y Pentesting para la distro Kali Linux**

Contenidos

* [1. Aircrack-ng](https://ciberninjas.com/kali-herramientas-20/#1_Aircrack-ng)
* [2. THC Hydra](https://ciberninjas.com/kali-herramientas-20/#2_THC_Hydra)
* [5. Netcat](https://ciberninjas.com/kali-herramientas-20/#5_Netcat)
* [6. Nmap](https://ciberninjas.com/kali-herramientas-20/#6_Nmap)
* [7. Nessus](https://ciberninjas.com/kali-herramientas-20/#7_Nessus)
* [8. WireShark](https://ciberninjas.com/kali-herramientas-20/#8_WireShark)
* [9. Snort](https://ciberninjas.com/kali-herramientas-20/#9_Snort)
* [10. Kismet Wireless](https://ciberninjas.com/kali-herramientas-20/#10_Kismet_Wireless)
* [11. Nikto](https://ciberninjas.com/kali-herramientas-20/#11_Nikto)
* [12. Yersinia](https://ciberninjas.com/kali-herramientas-20/#12_Yersinia)
* [13. Escáner Burp Suite](https://ciberninjas.com/kali-herramientas-20/#13_Escaner_Burp_Suite)
* [14. Hashcat](https://ciberninjas.com/kali-herramientas-20/#14_Hashcat)
* [15. Maltego](https://ciberninjas.com/kali-herramientas-20/#15_Maltego)
* [16. BeEF (el framework de explotación del navegador)](https://ciberninjas.com/kali-herramientas-20/#16_BeEF_el_framework_de_explotacion_del_navegador)
* [17. Fern Wifi Cracker](https://ciberninjas.com/kali-herramientas-20/#17_Fern_Wifi_Cracker)
* [18. GNU MAC Changer](https://ciberninjas.com/kali-herramientas-20/#18_GNU_MAC_Changer)
* [19. Wifite2](https://ciberninjas.com/kali-herramientas-20/#19_Wifite2)
* [20 .Pixiewps](https://ciberninjas.com/kali-herramientas-20/#20_Pixiewps)
* [Conclusión](https://ciberninjas.com/kali-herramientas-20/#Conclusion)

## **1. Aircrack-ng**

[Aircrack-ng](https://www.aircrack-ng.org/) es una de las herramientas para descifrar contraseñas inalámbricas WEP/WAP/ WPA2.

El funcionamiento de Aircrack se basa en tomar los paquetes de la red, y analizarlos mediante contraseñas recuperadas.

Además de esto, Aircrack-ng también hace uso de ataques FMS estándar (Fluhrer, Mantin y Shamir) junto con algunas optimizaciones como los ataques KoreK o el ataque PTW para acelerar los ataques.

Si encuentras que Aircrack-ng es difícil de usar, te tocara buscar los tutoriales más adecuados para ello. ?

## **2. THC Hydra**

[THC Hydra](http://sectools.org/tool/hydra/) utiliza un ataque de fuerza bruta para descifrar prácticamente cualquier servicio de autenticación remota.

Admite ataques de diccionario rápidos para **más de 50 protocolos distintos**, como por ejemplo: FTP, HTTPS, telnet, etc.

Se utiliza para acceder a redes inalámbricas, creadores de paquetes, servidores de correos, etc.

## **5. Netcat**

[Netcat](http://netcat.sourceforge.net/) más comocido por **nc**, es una utilidad de red con la que se pueden utilizar protocolos TCP/IP para leer y escribir datos a través de conexiones de red.

Se puede utilizar para crear cualquier tipo de conexión, así como para explorar y depurar redes usando un modo de túnel, escaneo de puertos, etc.

## **6. Nmap**

Nmap o [Network Mapper](https://nmap.org/) es una herramienta de utilidad gratuita y de código abierto que utilizan los administradores de sistemas para descubrir redes y auditar su seguridad.

Su funcionamiento es rápido, está bien documentado, cuenta con una GUI, admite transferencia de datos, inventario de red, etc.

## **7. Nessus**

[Nessus](https://www.cs.cmu.edu/~dwendlan/personal/nessus.html) es una herramienta de escaneo remoto que puedes utilizar para verificar las computadoras en busca de vulnerabilidades de seguridad.

No sirve para bloquear activamente ninguna de las vulnerabilidades que tengan los equipos, pero puede **detectarlas** ejecutando rápidamente más de **12.00 comprobaciones de vulnerabilidad** y activando alertas para cuando sea necesario realizar parcheados de seguridad.

## **8. WireShark**

[WireShark](https://www.tecmint.com/wireshark-network-traffic-analyzer-for-linux/) es un analizador de paquetes de código abierto que puedes utilizar de forma gratuita.

Con Wireshark, correctamente configurado, se puede ver la actividad dentro de una red desde el nivel más bajo, junto con el acceso a archivos pcap, informes personalizables, disparadores avanzados, alertas, etc.

Probablemente, Wirreshark es el analizador de protocolos de red más utilizado en todo el mundo de Linux.

## **9. Snort**

[Snort](https://www.snort.org/) es un NIDS gratuito y de código abierto con el que puedes detectar vulnerabilidades de seguridad en las computadoras.

Con Snorte se puede ejecutar análisis de tráfico, búsqueda/coincidencia de contenidos, registro de paquetes en redes IP y hasta detectar ciertas variedades de ataques a una red, entre otras muchas funciones más; y todo ello a tiempo real.

## **10. Kismet Wireless**

[Kismet Wireless](https://www.kismetwireless.net/) es un sistema de detección de intrusos, detector de redes y rastreador de contraseñas.

Funciona principalmente con redes Wi-Fi (IEEE 802.11) y se le pueden ampliar sus funcionalidades mediante numerosos complementos.

## **11. Nikto**

[Nikto2](https://www.cirt.net/Nikto2) es un escáner web gratuito y de código abierto para realizar pruebas rápidas e integrales con elementos en la web.

Para ello, Nikto busca más de 6500 archivos potencialmente peligrosos, versiones de programas obsoletos, configuraciones de servidor vulnerables y problemas específicos de un servidor.

## **12. Yersinia**

[Yersinia](http://www.yersinia.net/) (denominado así, por el nombre de una bacteria), es una utilidad de red también diseñada para explotar protocolos de red vulnerables pretendiendo ser un sistema de red seguro que analiza y prueba el marco en el que se encuentra.

Cuenta con ataques para IEEE 802.1Q, Hot Standby Router Protocol (HSRP), Cisco Discovery Protocol (CDP), etc.

## **13. Escáner Burp Suite**

[Burp Suite Scanner](https://portswigger.net/burp) es una plataforma GUI integrada profesional para probar las vulnerabilidades de seguridad de las aplicaciones web.

Incluye todas las herramientas de prueba y penetración en una edición comunitaria (gratuita) y exista una edición profesional (por 349 dólares año).

## **14. Hashcat**

[Hashcat](https://hashcat.net/hashcat/) es conocido entre la comunidad de expertos en seguridad, como la herramienta de recuperación y descifrado de contraseñas más rápida y avanzada del mundo.

Es de código abierto y cuenta con un motor de reglas en el kernel, más de 200 tipos de Hash diferentes, un sistema de evaluación comparativa integrado, etc.

## **15. Maltego**

[Maltego](https://www.paterva.com/web7/buy/maltego-clients.php) es un software propietario, pero se usa ampliamente en el análisis forense de código abierto.

Es una herramienta de análisis de enlaces GUI que proporciona minería de datos en tiempo real junto con conjuntos de información ilustrados utilizando gráficos basados en nodos y conexiones de múltiples órdenes.

## **16. BeEF (el framework de explotación del navegador)**

[BeEF](http://beefproject.com/), como su nombre lo indica, es una herramienta de penetración que se centra en las vulnerabilidades del navegador.

Con BeEF puedes evaluar la seguridad de un entorno de destino utilizando vectores de ataque desde el lado del cliente.

## **17. Fern Wifi Cracker**

[Fern Wifi Cracker](https://github.com/savio-code/fern-wifi-cracker) es una herramienta de seguridad inalámbrica GUI basada en Python para auditar las vulnerabilidades de la red.

Con Fern Wifi Cracker vas a poder descifrar y recuperar claves WEP/WPA/WPS, así como realizar varios ataques de red sobre redes basadas en Ethernet.

## **18. GNU MAC Changer**

[GNU MAC Changer](https://github.com/alobbs/macchanger) es una utilidad de red que agiliza y facilita la manipulación de las direcciones MAC de las interfaces de red.

## **19. Wifite2**

[Wifite2](https://github.com/derv82/wifite2) es una herramienta de auditoría de red inalámbrica gratuita y de código abierto basada en Python diseñada para funcionar perfectamente con distribuciones de prueba de lápiz.

Es una reescritura completa de Wifite y por lo tanto, presenta un rendimiento mejorado.

Hace un buen trabajo para descifrar puntos de acceso ocultos, descifrar contraseñas WEP débiles utilizando una lista de técnicas de descifrado, etc.

## **20 .Pixiewps**

[Pixiewps](https://github.com/wiire-a/pixiewps) es una herramienta offline de fuerza bruta basada en C para explotar implementaciones de software con poca o ninguna entropía.

Fue desarrollado por **Dominique Bongard** en 2004 para utilizar con la intención de educar a los estudiantes.

Dependiendo de la fuerza de las contraseñas que intentes descifrar, Pixiewps puede hacer el trabajo en cuestión de segundos o minutos.