

FinIntrusion Kit ha sido diseñado y desarrollado por especialistas en sistemas de intrusión de TI de primer nivel mundial, con más de 10 años de experiencia en su campo gracias a su participación en varios Tiger Teams (Red Teams), tanto del sector privado como de agencias gubernamentales, valorando la seguridad de distintas redes y organizaciones.

FinIntrusion Kit es el resultado de un kit operativo **actualizado y encubierto** a la vez, que puede utilizarse en la mayoría de **operaciones de intrusión de TI**, tanto en áreas defensivas como ofensivas. Entre nuestros clientes hay **departamentos militares especializados en guerra cibernética, agencias de inteligencia, departamentos de inteligencia policial y otras fuerzas y cuerpos de seguridad**.

Ejemplo De Uso 1: Unidad Técnica De Vigilancia

FinIntrusion Kit se utilizó para quebrantar **el cifrado WPA** de la red inalámbrica del hogar de un objetivo y para monitorear sus **credenciales de acceso al correo web (Gmail, Yahoo, etc.) y a redes sociales (Facebook, MySpace, etc.)**. lo que permitió a los investigadores **monitorizar de forma remota** estas cuentas desde los cuarteles centrales sin necesidad

DE UN VISTAZO	
Uso:	· Operaciones estratégicas · Operaciones tácticas
Capacidades:	· Romper cifrados WEP/WPA · Monitorizar redes (incluyendo sesiones SSL) · Ataques de intrusión de TI
Contenido:	· Hardware/Software

de acercarse al objetivo.

Ejemplo De Uso 2: Seguridad De TI

Varios clientes han utilizado FinIntrusion Kit para **quebrantar con éxito la seguridad** de redes y sistemas informáticos con finalidades **ofensivas y defensivas** utilizando diversas técnicas y herramientas.

Ejemplo De Uso 3: Casos De Uso Estratégico

FinIntrusion Kit se suele utilizar para acceder de forma remota a cuentas de correo electrónico y servidores de objetivos (p. ej. blogs o grupos de discusión) y monitorear sus actividades controlando, entre otros, elementos como los registros de acceso.

Descripción General De Funciones

- Descubre **redes WLAN (802.11) y dispositivos Bluetooth®**.
- Recupera contraseñas WEB (de 64 y 128 bits) en **entre 2 y 5 minutos**.
- **Descifra contraseñas WPA1 y WPA2** utilizando ataques con diccionarios.
- Monitorea de manera activa redes de LAN (por cable e inalámbricas) y **extrae nombres de usuario y contraseñas incluso en sesiones con cifrado TLS/SSL**.
- Emula **puntos de acceso inalámbrico hostiles (802.11)**.
- **Entra de forma Remota en cuentas de correo electrónico** utilizando técnicas de intrusión basadas en la red, el sistema y la contraseña.
- **Evaluación y validación de la seguridad de la red**.

Encontrará la lista completa de funciones en las Especificaciones del producto



FININTRUSION KIT

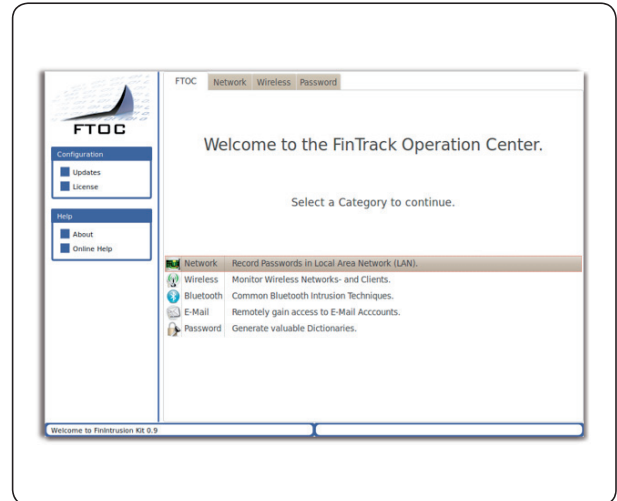
Componentes Del Producto



FinIntrusion Kit – Unidad Táctica Encubierta

Componentes básicos para la intrusión de TI :

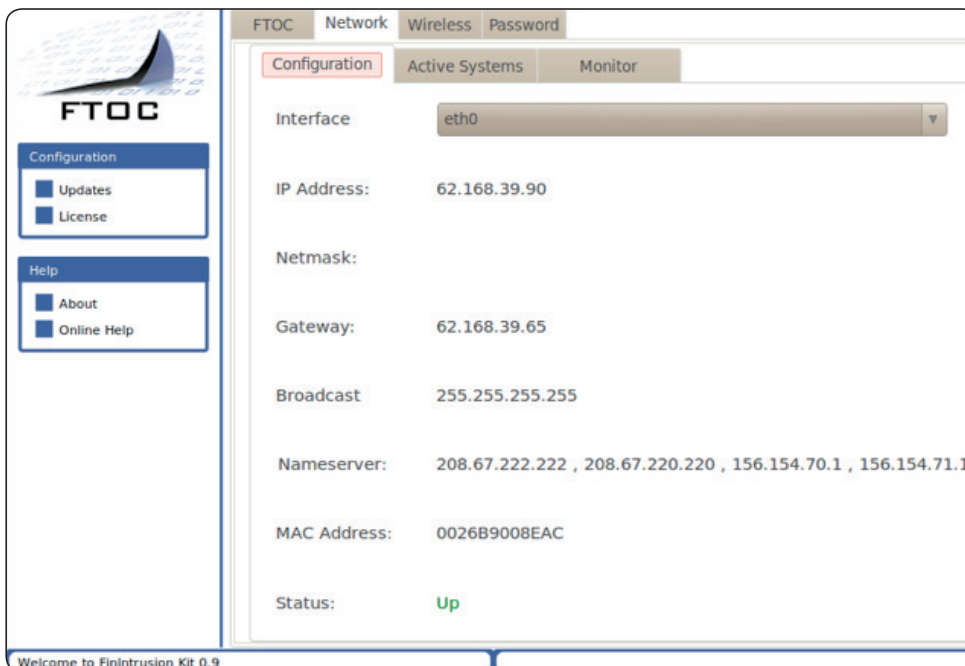
- Adaptador WLAN de gran potencia
- Adaptador Bluetooth de gran potencia
- Antenas 802.11
- Muchos dispositivos habituales de intrusión de TI



FinTrack Operation Center

- Interfaz gráfica de usuario para automatizar ataques de intrusión de sistemas de TI .

Monitorización automática de LAN/WLAN



Rastreador activo de contraseñas de redes LAN y WLAN

Captura incluso datos con cifrado SSL de servicios como correo Web, portales de vídeo, banca en línea y muchos más.

