ISEC Lab #5

Análisis de redes wireless

Parte 1
Herramientas y técnicas de ataque

Vicente Aguilera Díaz
vaguilera<arroba>isecauditors.com

1 Introducción

En esta ocasión dedicamos el ISECLab a las redes wireless. En concreto nos centraremos en algunas de las herramientas de auditoría más conocidas, y veremos como pueden ser utilizadas para analizar y/o atacar este tipo de redes, así como las soluciones disponibles actualmente para hacer frente a los problemas aquí identificados.

El artículo “Análisis de redes wireles” consta de dos partes:

- Parte 1: Herramientas y técnicas de ataque
- Parte 2: Medidas de seguridad

El objetivo de esta primera parte del artículo es mostrar la inseguridad de las redes w¡reless incluso tras la adopción de ciertas medidas de protección, lo que nos llevará a la conclusión de que en estas redes, y debido a su naturaleza, deberemos prestar más atención que nunca al aspecto de la seguridad.

2 Ataques a los sistemas básicos de protección

Si realizamos un pequeño estudio sobre las redes wireless de nuestra ciudad y analizamos las medidas de seguridad adoptadas, nos sorprenderemos de los resultados obtenidos: la mitad de las redes no disponen de encriptación (WEP y/o WPA), la mayoría emiten el SSID en broadcast, algunas utilizan SSIDs por defecto o fácilmente predecibles, no han habilitado el filtrado por MAC, etc. Es decir, podemos señalar que nos encontramos ante redes desprotegidas en la mayoría de casos o, cuando menos, inseguras.

En este escenario, podemos definir como medidas de protección de carácter básico, las siguientes:

- Habilitar protecciones WEP y/o WPA.
- Activar el filtrado por MAC
- Deshabilitar el broadcast del SSID.
- Utilizar un SSID complejo.
- Deshabilitar el DHCP.

Por supuesto, es mejor adoptar ciertas medidas (aunque sean básicas) que no adoptar ninguna y dejar nuestra seguridad en manos de la buena suerte. No obstante, en los siguientes apartados se exponen herramientas y técnicas que dejan en evidencia la adopción de estas medidas, por lo que podemos avanzar que no resultan suficientes.

2.1 Obtención de claves WEP

WEP surgió como una primera medida de protección que garantizaba (o eso se pretendía...) la confidencialidad de los datos en una red inalámbrica. No obstante, como veremos, este mecanismo de protección resulta insuficiente.

Las debilidades de WEP se pueden agrupar en las siguientes categorías:

- Sniffing: Las estaciones emiten en determinadas franjas de frecuencia, pero las tarjetas y antenas pueden capturar tráfico de toda la banda. Esto permite capturar el tráfico de la celda (zona de actuación de un AP) e identificar estaciones. Además, se emite de forma omnidireccional por lo que resulta más fácil capturar este tráfico.
- IV: vector de inicialización. Longitud de 24 bits (2^24 = 16.777.216 combinaciones posibles) : se reutiliza en un corto periodo de tiempo (muy pocas horas), y dependiendo del numero de dispositivos que compartan la clave (K) se reduce el tiempo de colisión.
- Sistema de claves. WEP no define la gestión de claves (número de claves diferentes utilizadas en una red, frecuencia de cambio, etc.), por lo que normalmente se suele compartir la clave por todas las estaciones y el cambio de claves se realiza de forma manual.
- Sistema de integridad: Formando parte del texto cifrado (RC4) se encuentra un CRC32 del mensaje antes de ser cifrado. Este sistema permite que alguien pueda alterar o generar un mensaje y asignar un CRC32 que sea coherente, por lo que será aceptado como válido. La solución pasaría por utilizar funciones hash.

WEP se encuentra definido en el estándar 802.11, por lo que las vulnerabilidades de WEP afectan a todos los estándares 802.11x.

Veamos como intenta garantizar WEP la privacidad de los mensajes.

WEP utiliza el sistema de cifrado RC4 de RSA, cuya semilla se crea concatenando el vector de inicialización (IV) y la clave compartida por los clientes (K).

Se genera un CRC (checksum de 32 bits) para detectar modificaciones involuntarias sobre el texto en claro (M) y se cifra (M y CRC) realizando la operación lógica XOR con la semilla creada anteriormente. A continuación se transmite el IV (en claro) junto con el mensaje cifrado (C). El receptor lee el IV en claro, lo concatena a la clave compartida y si valida el CRC entonces se acepta como válido el paquete.

Veamos esto de forma esquemática:

```
     Texto en claro (M) + CRC

     RC4 (IV,K)

XOR  ----------------------------

IV + Texto cifrado (C)
```

Habíamos comentado que una de las debilidades de WEP era el uso de un vector de inicialización de 24 bits, cosa que provocaba que se llegara a reutilizar un mismo IV en poco tiempo. Supongamos colisión de dos IV y el uso de la misma clave:

```
     M1              M2

     RC4(IV,K)       RC4(IV,K)

XOR  ---------       ---------

     C1              C2
```

En estas condiciones se produce el hecho que se detalla a continuación:

```
     C1         M1

     C2         M2

XOR  --         --

     C          C
```

Es decir, el resultado de realizar la operación lógica XOR entre dos mensajes cifrados coincide con el resultado de realizar la XOR entre los dos mensajes en claro.

Lo que quiere decir que si en una colisión se conoce un texto en claro (M1), es fácilmente obtenible otro texto en claro (M2) simplemente haciendo la siguiente operación:

```
M2 = XOR (M1, C)
```

Existen técnicas de ataque que permiten obtener directamente la clave WEP, lo que permite descifrar cualquier mensaje que haya utilizado esa misma clave. En 2001, Stubblefield, Ioannidis y Rubin implementaron un sistema que se aprovechaba de las deficiencias de RC4 con este propósito.

Existe un gran número de herramientas que facilitan toda esta tarea. Los pasos a seguir son:

1. Capturar el suficiente número de paquetes

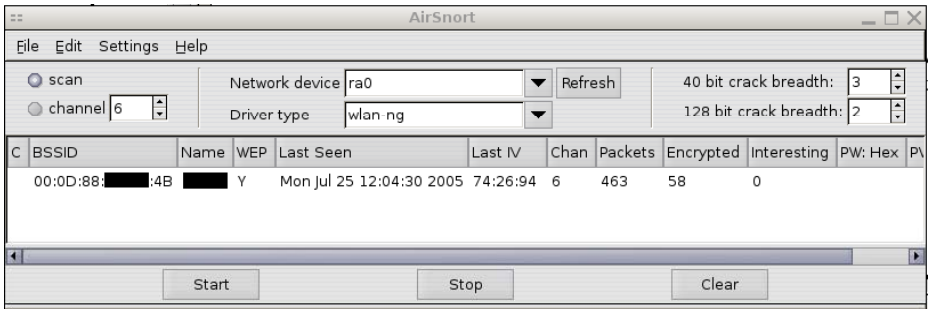
Es necesario activar el modo monitor en nuestra tarjeta. Normalmente las herramientas (como kismet) activan este modo de forma automática. En todo caso, podemos activar este modo de forma manual (si lo soporta nuestra tarjeta) mediante las wireless tools a través del comando:

iwconfig <wifi interface> mode monitor

Algunas de las herramientas que podemos utilizar para capturar tráfico son:

- **Ethereal**: Es un analizador de protocolos y permite obtener información detallada sobre el contenido de cada paquete (parámetros WEP, IV, dirección origen y destino, BSSID, flags activados, etc.)
- **AirSnort**: Además de capturar tráfico de redes wireless, permite recuperar claves de encriptación. AirSnort opera en modo pasivo monitorizando las transmisiones y obteniendo la clave de encriptación cuando se ha capturado el suficiente número de paquetes.

  Deberemos tener configurada la tarjeta en modo promiscuo (monitor) y seleccionar previamente el canal del que se desea capturar tráfico. El canal puede ser identificado fácilmente mediante una herramienta que permita escanear redes wireless.



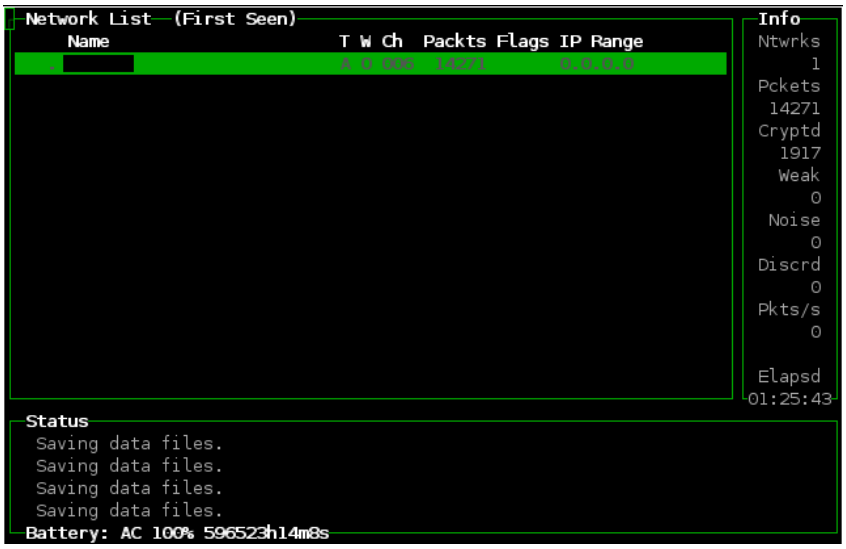
- **Airodump**: Es una de las herramientas que componen Aircrack. Airodump es la herramienta encargada de capturar tráfico 802.11.

```
BSSID              CH  MB  ENC  PWR  Packets   LAN IP / # IVs   ESSID

00:0D:88:[redacted]:4B   6  54  WPA   -1    14255             1916   [redacted]
```

  Veremos que existen muchos menos IVs que paquetes capturados. Esto se debe a que el IV no se transmite en todos los paquetes. Si capturamos el tráfico con ethereal observaremos que muchos paquetes son del tipo "Beacon frame" (anuncian el SSID), y sólo en los paquetes de datos obtendremos esta información.

- **Kismet**: Una de las herramientas más completas. Permite detectar redes, capturar tráfico e incluso actuar como IDS (Intrusión Detection System). Entre las capacidades de Kismet también cuenta con obtención de SSIDs ocultos y decodificación de paquetes WEP en tiempo de ejecución.



Si monitorizando la red observamos que no existe mucho tráfico (lo que provoca que necesitemos mucho más tiempo para conseguir capturar el número de paquetes necesario), se pueden utilizar técnicas para generar más tráfico en la red. Por ejemplo:

- **Ataques de repetición**: WEP no utiliza el concepto de estado, por lo que no puede conocer características sobre la situación de un paquete. De esta forma es posible volver a enviar paquetes capturados (aunque se encuentren cifrados se descifrarán correctamente puesto que han sido cifrados por una estación que conocía la clave WEP), provocando de esta manera la generación de más IV.

  Una herramienta que nos permite realizar esta operación es "aireplay" (incluida en Aircrack).

En cualquier caso, independientemente de la herramienta utilizada, el resultado debe ser un fichero que contiene el tráfico capturado.

2. Obtener la clave

A partir del tráfico capturado con encriptación WEP, existen un gran número de herramientas que permiten deducir la clave WEP.

A continuación se enumeran algunas de estas herramientas:

- **Aircrack**: Es un conjunto de herramientas para auditar redes wireless. Incluye:
  - airodump: captura paquetes 802.11
  - aireplay: inyecta paquetes 802.11
  - aircrack: rompe claves WEP y WPA-PSK
  - airdecap: descifra ficheros WEP/WPA capturados
- **WEPCrack**: Desarrollada en Perl, permite romper claves WEP utilizando las deficiencias descubiertas en la planificación de las claves en RC4. Compuesta por:
  - pcap-getIV.pl - Extrae IV y la información necesaria para obtener la clave WEP, a partir de la captura de tráfico o de un fichero con tráfico ya capturado. La salida la deja en un fichero IVFile.log
  - WeakIVGen.pl - Genera datos de test para comprobar el éxito de WEPCrack.pl
  - WEPCrack.pl - Intenta obtener la clave WEP a partir de la información almacenada en el fichero IVFile.log
- **Weplab**: Esta herramienta permite romper claves WEP utilizando distintas técnicas:
  - Fuerza bruta: utilizando todas las claves posibles. También es posible restringir el espacio de claves que se analizan, creando espacios personalizables y mucho más pequeños (por ejemplo: 7F:7F:7F... analizaría el espacio de claves formadas por caracteres ascii planos).
  - Diccionario: utilizando un diccionario con palabras de uso común y analizando cada una como posible clave.
  - Ataques estadísticos: utilizando distintas técnicas (FMS, Korek, ...), que permiten romper claves de longitud 64 bits con 100.000 paquetes y claves de 128 bits utilizando 300.000 paquetes.

Otras herramientas conocidas y que tienen el mismo objetivo son “dwepbrack” y “wepattack”.

3. Incorporar nuestra estación a la red

El objetivo de un intruso es el de disponer de acceso a la red atacada. Para conseguirlo deberá conocer ciertos parámetros de la red (direccionamiento IP, máscara de red, y dirección IP del gateway si desea hacer uso de la conexión a Internet).

Ahora bien, nos podemos encontrar con dos situaciones:

- **DHCP habilitado**: Si el responsable de la red ha habilitado DHCP, el intruso lo tiene muy fácil. Simplemente debe configurar su tarjeta para que utilice DHCP y el servidor le asignará de forma automática una IP válida (así como el resto de parámetros de la red).
- **DHCP deshabilitado**: Ya que no se pueden obtener los parámetros de la red de forma automática, es necesario identificar esta información a partir del tráfico capturado. Como ya disponemos de la clave WEP, es posible descifrar alguno de estos paquetes y visualizar su contenido, obteniendo de esta forma la información que necesitamos.

  Una herramienta que permite visualizar tráfico en claro a partir de tráfico WEP encriptado es ”decrypt” (incluida en Airsnort). Su uso es muy sencillo. A partir de un fichero capturado con tráfico encriptado genera otro fichero con el tráfico en claro y que puede ser mostrado por un analizador de protocolos como Ethereal.

2.2 Evasión del filtrado por MAC

Los APs disponen de una lista de direcciones MAC de las estaciones a las que se les permite su asociación. De tal forma que si una estación intenta asociarse utilizando el SSID de la red, el AP valida si su MAC coincide con alguna de la lista y si no se encuentra la rechaza.

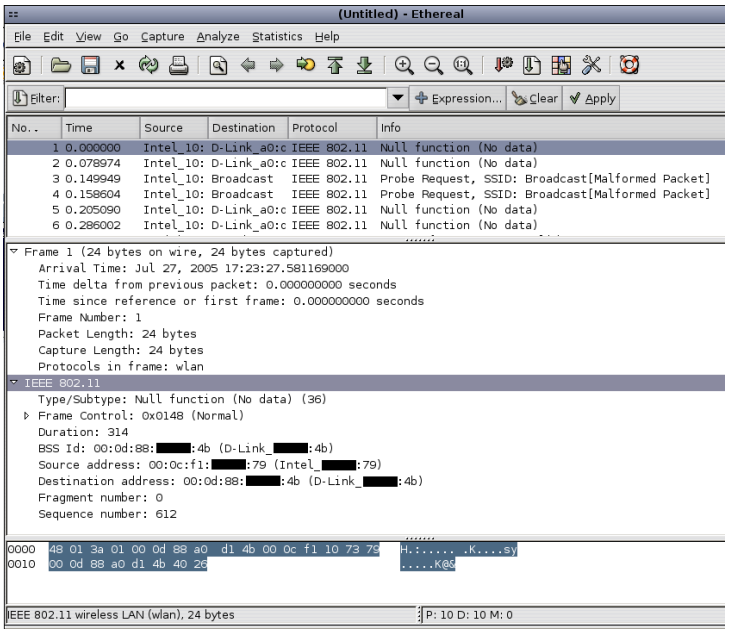
Así, el objetivo para un intruso sería obtener la MAC de un cliente válido y suplantar esa estación utilizando su dirección MAC. Estos dos pasos se comentan a continuación:

1. Obtener la MAC de un cliente válido

Resulta fácil obtener la MAC de un cliente válido (reconocido por el AP). La dirección MAC se transmite en claro en todos los paquetes. Por lo tanto, basta con monitorizar el tráfico y analizar su contenido. Para esta tarea podemos utilizar una de las siguientes herramientas:

- Ethereal

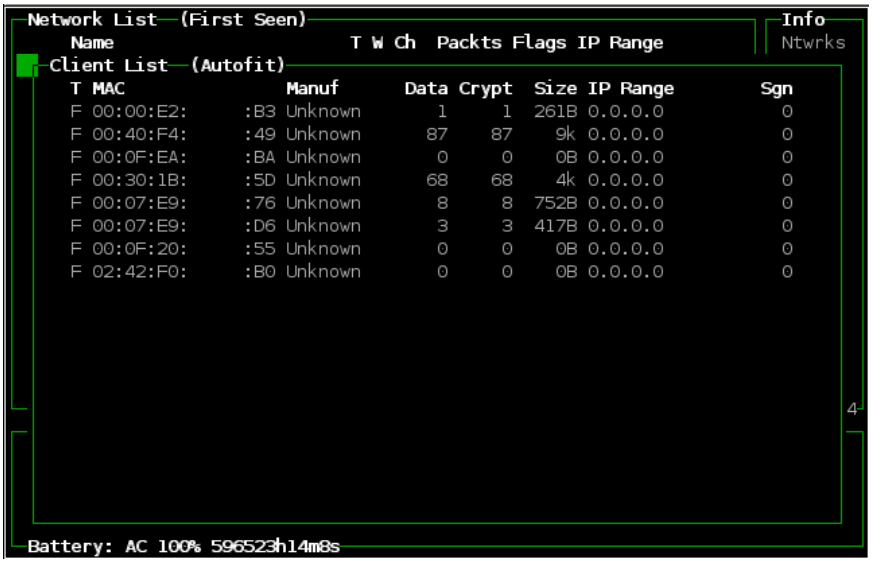
Podemos capturar tráfico 802.11 directamente con Ethereal o cargar el contenido de capturas de tráfico realizadas con otras herramientas (cuyo formato sea reconocido por Ethereal).



- Kismet

Kismet permite identificar las estaciones asociadas en una red wireless (todas comparten el mismo SSID) y mostrar información sobre las mismas como su dirección MAC (entre otra información).

En la siguiente captura se muestra como ejemplo un listado de las estaciones asociadas a una red wireless detectada por Kismet:



2. Suplantar la MAC del cliente

Una vez identificada la MAC de un cliente, simplemente modificaremos nuestra MAC por la del cliente (víctima) que queremos suplantar, evadiendo la restricción impuesta por las ACLs (el filtrado de MAC).

Para modificar nuestra MAC basta con ejecutar lo siguiente:

#ifconfig <wifi interface> hw ether <MAC address>

En estos momentos disponemos de tres opciones:

- Esperar a que la víctima se desconecte. Generalmente, un intruso esperará a que el cliente a suplantar se haya desconectado de la red para llevar a cabo su conexión. Podemos decir que sería la forma más limpia.
- Incorporarnos a la red coexistiendo con la víctima. Es posible que dos estaciones compartan la MAC y coexistan en la misma red (esta técnica se conoce como piggybacking).
- Forzar la desconexión de la víctima. El intruso puede provocar la disociación de la víctima con el AP y forzar de esa forma la expulsión de la red. En este caso, y si se realiza de forma repetida, cabe la posibilidad de que la víctima se percate del ataque.

2.3 Obtención de SSIDs ocultos

El estandar 802.11 sólo cifra los paquetes de datos, por lo que el SSID puede ser obtenido simplemente mediante monitorización de la red. No obstante, se puede desactivar la opción de transmitir en broadcast el SSID, de forma que no se esté transmitiendo continuamente el SSID haciendo más difícil su identificación.

Aún así es posible capturar el SSID utilizado (ya que se transmite en claro en las tramas de reautenticación y reasociación) empleando, por ejemplo, alguno de los métodos siguientes:

- Método pasivo: monitorización del tráfico

Los clientes envían el SSID cuando se intentan asociar a la red. La idea es monitorizar el tráfico de la red con el objetivo de capturar el tráfico enviado por un cliente que se intenta conectar. En ese momento transmitirá el SSID.

- Método activo: provocar una reasociación con el AP

Si el cliente transmite el SSID al intentar asociarse a un AP, la idea consiste en provocar la disociación (suplantando al AP) de alguno de los clientes ya existentes, con el objetivo de que vuelva a asociarse y podamos obtener el SSID, capturando el tráfico, cuando lo transmita la estación.

La disociación de un cliente sólo la puede provocar el AP con el que se encuentra asociado, por lo que suplantar al AP se convierte en una tarea imprescindible. Pero para poder suplantar a un AP, primero debemos ser capaces de actuar como un AP.

Para convertirnos en AP disponemos de dos opciones:

- configurar la tarjeta en modo "master" (tarjetas con chipset Prism2, Atheros y quizás dentro de poco Ralink tras haber liberado el driver con licencia GPL) simulando un AP, o
- convertir nuestro linux en un AP. Si queréis ampliar información y bajaros los drivers y utilidades: http://hostap.epitest.fi/

En cualquier caso, para provocar la reasociación de los clientes será necesario llevar a cabo dos tipos de ataques:

- MAC Spoofing: para suplantar al AP deberemos obtener su MAC. Esta identificación se realiza de forma fácil y rápida mediante la utilización de algún escáner que detecte dispositivos wifi (ver listado de herramientas en el apartado 4). Una vez identificada, asignaremos a nuestra tarjeta dicha MAC.

- Management Frames Spoofing: Para llevar a cabo ataques de disociación y des-autenticación. El objetivo es provocar la disociación de todos los clientes (enviando tramas específicas a la dirección de broadcast), de un nodo, o de un dispositivo cliente. Si monitorizamos el tráfico tras la disociación podremos capturar la MAC de los clientes al intentar asociarse de nuevo al AP.

Existen herramientas que llevan a cabo esta operación (como por ejemplo “deauth”, que forma parte del proyecto void11, y “essid_jack”, que forma parte de airjack).

2.4 DoS

Las redes wireless no se encuentran exentas de sufrir ataques de negación de servicio, ya sea a nivel de toda la red (ataques dirigidos contra con los AP) o a nivel de determinadas estaciones.

Debemos diferenciar entre los ataques llevados a cabo por un usuario que se encuentra asociado y autenticado (en este caso los ataques de DoS no se diferencian con los de una red cableada) o por un intruso que no se encuentra asociado a la red wireless.

Veamos algunos de los ataques de DoS que pueden sufrir este tipo de redes:

- Interferencias

Un ataque de DoS exclusivo de estas redes consiste en generar tráfico en la misma frecuencia en la que trabaja la red wifi para degradar el rendimiento de la misma. Por ejemplo, si los dispositivos wifi operan en la banda de los 2.4GHz, si se acerca un microondas (que también opera en la misma banda) a uno de los clientes y se pone en funcionamiento, la señal de la red wifi se degrada debido a las interferencias con las ondas de radio emitidas por el microondas.

Pero este hecho puede ocurrir también de forma involuntaria, por ejemplo con teléfonos inalámbricos, transmisores u otros equipos bluetooth que operen en la misma frecuencia y de forma próxima al AP o a la estación.

Conviene recordar que también pueden existir interferencias internas producidas por rebotes de la señal (paredes, techo, ...) y que pueden afectar en la degradación del nivel de la señal.

- Network DoS

Consiste en suplantar un AP (utilizando su dirección MAC) e inundando la red con paquetes de disociación. De esta forma, el atacante provoca que las estaciones autenticadas pierdan la conexión. Si el envío de estos paquetes se realiza de forma constante no se permitirá que las estaciones de la celda gestionada por el AP suplantado puedan mantener la conexión.

Existen herramientas que llevan a cabo esta operación (como por ejemplo “deauth”, que forma parte del proyecto void11, y “airjack”)

- AP DoS

En esta ocasión el ataque se dirige contra los AP, inundándolos con paquetes de autenticación con direcciones aleatorias de estaciones. Este hecho provoca que algunos AP no ofrezcan servicio tras un elevado número de peticiones de autenticación.

Existen herramientas que llevan a cabo esta operación (como por ejemplo “auth”, que forma parte del proyecto void11).

3 Conclusiones y recomendaciones

Como habréis podido observar las redes wireless son, por naturaleza, más inseguras que las redes cableadas. En estas últimas, la restricción física de la conexión cableada impone un filtro añadido del que no disponen las redes wireless.

Hemos comentado algunas de las herramientas más utilizadas en el análisis de este tipo de redes, y como pueden ser usadas para permitir romper ciertas protecciones. Asimismo, hemos observado que muchas de las deficiencias aprovechadas por estas herramientas son debidas al protocolo WEP.

Pero... ¿podemos concluir que estas redes son inseguras? La respuesta debe ser que estas redes pueden ser tan seguras (o inseguras) como lo puedan ser las redes cableadas. Claro está que para conseguirlo hemos de adoptar nuevas medidas de seguridad y superar las deficiencias de WEP.

En cuanto a las soluciones y recomendaciones a los problemas aquí planteados os remito a la segunda parte de este artículo “Medidas de seguridad”.

4 Herramientas

Sniffers	
Herramienta	URL
ethereal	http://www.ethereal.com/
airsnort	http://airsnort.shmoo.com/
airtraf	http://airtraf.sf.net/
airodump	Incluida en Aircrack (ver enlace más abajo)

Scanners	
Herramienta	URL
Kismet	http://www.kismetwireless.net
gtkscan	http://sourceforge.net/projects/wavelan-tools/

Crackers	
Herramienta	URL
aircrack	http://www.cr0.net:8040/code/network/aircrack/
wepcrack	http://sourceforge.net/projects/wepcrack/
dwepcrack	http://www.e.kth.se/~pvz/wifi/
wepattack	http://wepattack.sf.net
weplab	http://weplab.sourceforge.net/
wpa_attack	http://www.tinypeap.com/html/wpa_cracker.html

Packet injection	
Herramienta	URL
updflood	http://www.foundstone.com/resources/stress_testing.htm
airpwn	http://sourceforge.net/projects/airpwn
aireplay	Incluida en Aircrack (ver enlace más arriba)
airjack	http://sourceforge.net/projects/airjack/

Utilities	
Herramienta	URL
fakeap	http://www.blackalchemy.to/project/fakeap/
decrypt	Incluída en AirSnort (ver enlace más arriba)
WLAN tools	http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html
void11	http://www.wlsec.net/void11/
essid_jack	Incluida en Airjack (ver enlace más arriba)
hostap	http://hostap.epitest.fi/

5 Enlaces de Interés

- Weaknesses in the Key Scheduling Algorithm of RC4:
  http://www.wisdom.weizmann.ac.il/~itsik/RC4/Papers/Rc4_ksa.ps
- Wardriving Tools:
  http://www.wardrive.net/wardriving/tools
- The Unofficial 802.11 Security Web Page
  http://www.drizzle.com/~aboba/IEEE/

6 Glosario

- **ACL** (Access Control List): Método de filtrado mediante el cual sólo se permite unirse a la red a determinadas direcciones MAC.

- **AP** (Access Point): Dispositivo hardware o software que actúa como concentrador de comunicaciones entre dispositivos wireless y que los conecta a una red cableada.

- **CRC** (Cyclic Redundancy Check): Una de las técnicas más usadas para detectar errores durante la transmisión de datos. Al emplear esta técnica se añaden secuencias de n bits a cada frame con información redundante y que permite detectar errores durante el envío.

- **IV** (Initialization Vector)**:** Campo no cifrado de 24 bits de longitud que viaja en la cabecera de los paquetes de datos. Junto con la clave compartida sirve como semilla para el algoritmo de cifrado RC4.

- **SSID** (Service Set Identifier): Nombre público (máximo 32 caracteres alfanuméricos) de una red wireless. Todos los dispositivos wireless de una WLAN deben utilizar el mismo SSID para comunicarse entre ellos. Podemos encontrar dos variantes:

  - **BSSID** (Basic SSID): utilizado por clientes en redes ad-hoc (en las que no hay un AP).
  - **ESSID** (Extended SSID): utilizado en redes en infraestructura (con la presencia de un AP).

- **WEP** (Wired Equivalent Privacy): Protocolo de seguridad para redes wireless definido en el estándar 802.11, diseñado para proporcionar el mismo nivel de seguridad que el ofrecido por las redes cableadas.

- **WLAN** (Wireless Local-Area Network):
  Tipo de red de área local que utiliza ondas de radio de alta frecuencia en lugar de cables para la comunicación entre nodos.

- **WPA** (Wi-Fi Protected Access): Estándar diseñado para mejorar las capacidades de seguridad ofrecidas por WEP. Incluye dos mejoras importantes: cifrado de datos mejorado con TKIP (Temporal Key Integrity Protocol) y autenticación de usuarios a través de EAP (Extensible Authentication Protocol).