PRUEBA DE VULNERABILIDAD EN LOS PUNTOS DE ACCESO INALÁMBRICOS

TRABAJO INTEGRADOR PARA OBTENER EL TITULO DE ESPECIALISTA EN TELECOMUNICACIONES

DIRECTOR:
EDUARDO GÓMEZ VÁSQUEZ

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
ESPECIALIZACIÓN EN TELECOMUNICACIONES
CARTAGENA DE INDIAS D. T. Y C.,
2009

PRUEBA DE VULNERABILIDAD EN LOS PUNTOS DE ACCESO INALÁMBRICOS

ASTRID CALDERÓN HERNÁNDEZ
CRISTHIÁN PADILLA RODRIGUEZ

ASESORES:
ING. ENRIQUE SANTIAGO CHINCHILLA

ING. GONZALO LOPEZ

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
ESPECIALIZACIÓN EN TELECOMUNICACIONES
CARTAGENA DE INDIAS D. T. Y C.,
2009

Cartagena de Indias, D. T. y C., Octubre 27 de 2009

Señores
COMITÉ DE REVISION DE MONOGRAFIA
UNIVERSIDAD TECNOLOGICA DE BOLIVAR

Apreciados señores.

Por medio de la presente nos permitimos informales que la monografía titulada "**PRUEBA DE VULNERABILIDAD EN LOS PUNTOS DE ACCESO INALÁMBRICOS**" ha sido desarrollada de acuerdo a los objetivos establecidos.

Como autores del proyecto consideramos que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

Atentamente,

_____	_____
ASTRID CALDERON HERNANDEZ	**CRISTHIAN PADILLA R**
C.C. N° 45.760.261 CARTAGENA	C.C. N° 73189449 CARTAGENA

Cartagena de Indias, D. T. y C., Octubre 27 de 2009

Señores
COMITÉ DE REVISION DE MONOGRAFIA
UNIVERSIDAD TECNOLOGICA DE BOLIVAR

Apreciados señores.

Por medio de la presente nos permitimos informales que la monografía titulada "**PRUEBA DE VULNERABILIDAD EN LOS PUNTOS DE ACCESO INALÁMBRICOS**" ha sido desarrollada de acuerdo a los objetivos establecidos.

Como director del proyecto considero que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

Atentamente,

_____

EDUARDO GÓMEZ VÁSQUEZ
DIRECTOR MONOGRAFIA

Cartagena de Indias, D. T. y C., Octubre 27 de 2009

NOTA DE ACEPTACION

_____
Firma Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Articulo 105. La Universidad Tecnológica de Bolívar, se reserva el derecho de propiedad intelectual de todos los Trabajos Integradores aprobados y no pueden ser explotados comercialmente sin su autorización.

Cartagena de Indias, D. T. y C., Octubre 27 de 2009

AUTORIZACIÓN

Yo, **ASTRID CALDERON HERNÁNDEZ**, identificada con número de cédula 45.760.261 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi Trabajo Integrador y publicarlo en el catalogo ON LINE de la Biblioteca.

_____

ASTRID CALDERON HERNÁNDEZ
C.C. 45.760261 DE CARTAGENA

Cartagena de Indias, D. T. y C., Octubre 27 de 2009

AUTORIZACIÓN

Yo, **CRISTHIAN PADILLA RODRIGUEZ**, identificado con número de cedula 73.189.449 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi Trabajo Integrador y publicarlo en el catalogo ON LINE de la Biblioteca.

_____

CRISTHIAN PADILLA RODRIGUEZ
C.C. 73.189.449 DE CARTAGENA

AGRADECIMIENTOS

Gracias... es la palabra más adecuada para recompensar todo
El apoyo y la confianza brindada por nuestras familias...
... sin ellos, esta meta hubiese sido más difícil de alcanzar.

A nuestros asesores y todas las personas que nos rodearon,
Por esas palabras de aliento que siempre estuvieron marcando
La senda de la no derrota...

... pero sobre todas las cosas gracias a Dios.
Él con su amor nos llenó de mucha fortaleza
Para no desmayar en los momentos difíciles.

CONTENIDO

Pág.

LISTA DE FIGURAS

GLOSARIO

Primero vamos a explicar una serie de conceptos básicos, que son los que después manejaremos:

- **Red Inalámbrica (Wireless Network):** Sistema de alta velocidad para acceder a Internet sin necesidad de instalar cables.
- **WiFi**: es una de las tecnologías de comunicación inalámbricas más utilizadas hoy en día. Wifi es una abreviatura de Wireless Fidelity, también llamada WLAN (Wireless Lan o red inalámbrica).
- **Punto De Acceso (Access Point – en inglés):** Es un dispositivo inalámbrico central de una red inalámbrica WIFI (Wireless) que por medio de ondas de radio frecuencia (RF) recibe información de diferentes dispositivos móviles y la transmite a través de cable al servidor de la red cableada.
- **El Estándar IEEE 802.11**: proporciona mecanismos de seguridad mediante procesos de autenticación y cifrado. En el modo de red Ad Hoc o conjunto de servicios avanzados, la autenticación puede realizarse mediante un sistema abierto o mediante clave compartida. Una estación de red que reciba una solicitud puede conceder la autorización a cualquier estación, o sólo a aquellas que estén incluidas en una lista predefinida. En un sistema de clave compartida, sólo aquellas estaciones que posean una llave cifrada serán autenticadas.
- **Punto De Acceso WIRELESS-G:** Wireless-G es el novedoso estándar de red inalámbrica de 54 Mbps que proporciona una velocidad casi 5 veces superior que los populares productos Wireless-B (802.11b). El punto de acceso Wireless-G de Linksys permite

conectar dispositivos Wireless-G o Wireless-B a la red. Ya que ambos estándares son incorporados, puede aprovechar la inversión realizada en infraestructura 802.11b y migrar los clientes de red al novedoso y velocísimo estándar Wireless-G a medida que aumentan sus necesidades. Además, para proteger datos y privacidad, puede encriptar todas las transmisiones inalámbricas, incluyendo filtros MAC y configuración basada en explorador Web para facilitar la tarea.

- **SSID**: Nombre de nuestra WLAN (red inalámbrica). Los puestos que deseen conectar por Wireless al Router, tienen que conocer este nombre y colocarlo en el apartado correspondiente de su configuración Wireless.
- **Identificador de Servicios Ampliables — ESSID (Extended Service Set Identifier):** Nombre o código asignado por el fabricante a un enrutador. Puede ser un nombre o código estándar predeterminado asignado por el fabricante a todas las unidades de hardware de ese modelo. Los usuarios pueden optimizar la seguridad cambiándolo a un nombre exclusivo. Similar a un Identificador de Conjunto de Servicio o Service Set Identifier (SSID).
- **ESSID Broadcast**: Hace que nuestro SSID sea público, es decir, cualquiera que entre dentro del radio de acción de nuestro Router, podrá ver nuestro SSID (Y conectarse a nuestra WLAN si no utilizamos encriptación).
- **Dirección de Control de Acceso a Medios — MAC (Media Access Control Address)**: Número exclusivo asignado por el fabricante a cada computadora u otro dispositivo de una red.
- **Filtrado de direcciones MAC**: Permite especificar qué computadores pueden entrar en la red. Cuando se active esta

característica, hay que introducir las direcciones MAC de cada cliente de la red (tarjeta inalámbrica) para permitirles el acceso a la red.

- **Encriptación — Codificación (Encryption):** Codificación de los datos en un código secreto que solamente puede ser decodificado o leído por el software instalado para decodificar la información.
- **Equivalencia de Privacidad Inalámbrica — WEP (Wired Equivalent Privacy)**: Protocolo de seguridad que encripta o codifica los datos transferidos desde y hacia los dispositivos inalámbricos conectados dentro de una red. No provee tanta seguridad como una encriptación WPA. Nos ofrece dos niveles de seguridad, encriptación a 64 o 128 bit. La encriptación usa un sistema de claves. La clave del computador debe coincidir con la clave del Router. **WEP** es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. El WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas. En ningún caso es compatible con IPSec. W.E.P puede usar incluso en implementaciones 802.11a/g/n. Desde un comienzo se conocían las debilidades en cuanto a Seguridad Informática de las Redes Inalámbricas WIFI. Por este motivo se incluyó en el estándar 802.11b un mecanismo de seguridad que permita encriptar la comunicación entre los diversos elementos de una red inalámbrica WIFI. Esta protección se denominó WEP (Wired Equivalent Privacy). En español sería algo así como "Privacidad equivalente a la de una red cableada". El protocolo WEP se basa en el algoritmo de encriptación RC4, con una clave secreta de 40 o 104 bits, combinada con un

Vector de Inicialización (IV) de 24 bits para encriptar el mensaje de texto M y su checksum – el ICV (Integrity Check Value). El mensaje encriptado C se determinaba utilizando la siguiente fórmula: C = [M || ICV(M)] + [RC4(K || IV)]

- **Acceso Protegido para Transferencia Inalámbrica de Datos — WPA (*Wireless Protected Access*)**: Protocolo de seguridad desarrollado para reparar defectos del protocolo WEP. Encripta o codifica los datos transferidos desde y hacia los dispositivos inalámbricos conectados dentro de una red. Ofrece dos tipos de seguridad, con servidor de seguridad y sin servidor. Este método se basa en tener una clave compartida de un mínimo de 8 caracteres alfanuméricos para todos los puestos de la red (Sin servidor) o disponer de un cambio dinámico de claves entre estos puestos (Con servidor). Es una opción más segura, pero no todos los dispositivos Wireless lo soportan. **WPA y WPA2** son dos Protocolos de Encriptación que se desarrollaron para solucionar las debilidades detectadas en el protocolo de encriptación WEP. El nombre de WPA (WIFI Protected Access) que quiere decir en español: Acceso protegido WIFI, es un nombre comercial que promueve la WIFI Alliance. La parte técnica está definida y estipulada en el estándar de seguridad IEEE 802.11i. Aunque se han descubierto algunas pequeñas debilidades en WPA/WPA2 desde su lanzamiento, ninguna de ellas es peligrosa si se siguen unas mínimas recomendaciones de seguridad. La vulnerabilidad más práctica es el ataque contra la clave PSK de WPA/WPA2. Como ya hemos dicho, la PSK proporciona una alternativa a la generación de 802.1X PMK usando un servidor de autenticación. Es una cadena de 256 bits o una frase de 8 a 63 caracteres, usada para generar una cadena utilizando un algoritmo

conocido: PSK = PMK = PBKDF2 (frase, SSID, SSID length, 4096, 256), donde PBKDF2 es un método utilizado en PKCS#5, 4096 es el número de hashes y 256 la longitud del resultado. La PTK es derivada de la PMK utilizando el 4-Way Handshake y toda la información utilizada para calcular su valor se transmite en formato de texto. La fuerza de PTK radica en el valor de PMK, que para PSK significa exactamente la solidez de la frase.

- **Radius**: es el acrónimo de Remote Authentication Dial In User Service. Sus diversas funciones y características están definidas en varias RFC de la IETF. Algunas de las importantes son: RFC 2058, 2138 y 2548. Como su nombre lo indica es un servidor que tiene la función de autenticar a los usuarios que se conectan remotamente.
- **Enrutador — Encaminador — Interfaz (Router):** Dispositivo que conecta dos o más redes. Un enrutador encuentra la mejor vía para transferir la información a través de las redes.
- **Firewall o Cortafuegos**: Programa hardware o software diseñado para impedir que los hackers usen su computadora para enviar información personal sin su autorización. Los programas firewall vigilan los intentos exteriores de acceder a su sistema y bloquean las comunicaciones de y hacia fuentes no autorizadas por el usuario.

1. MARCO TEÓRICO

Desde los comienzos, las redes inalámbricas WIFI fueron creciendo de una manera caótica. En casi todas las organizaciones se instalaron al comienzo 2 o 3 Puntos de Acceso y luego se fueron añadiendo más y más, dando lugar a una arquitectura que se conoce como "Mar de Puntos". Cada Access Point, está conectado por un cable a la red de la empresa y se dedica a transmitir la información de los dispositivos WIFI a la red cableada empresarial. Ningún Access Point, sabe de la existencia de los demás Access Point, aunque sean vecinos. No tienen ningún modo de saberlo...y, a decir verdad, hoy en día tampoco les interesa pues el estándar 802.11 WIFI no lo exige**.**

Así es, por ejemplo**,** que un Punto de Acceso puede estar muy congestionado y hasta colapsado por un gran número de usuarios, mientras el vecino está "aburrido" sin usuarios conectados o muy poquitos y, no tiene ninguna posibilidad de ayudar al Punto de Acceso vecino porque, fundamentalmente, no lo sabe. Lo que es más grave es que nadie lo sabe, ni el administrador de la red. Dijimos que las conexiones de una red inalámbrica wifi son "volátiles" por el hecho de ser "móviles". Entonces la carga de trabajo de cada Access Point, varía permanentemente**.**

En realidad, sin herramientas apropiadas, no sabemos nada de lo que está sucediendo en la red y entonces, siempre vamos "a remolque". Cuando hay quejas de los usuarios o cuando algo no funciona, debemos reaccionar y comenzar a analizar que está sucediendo, o que puede haber sucedido. No sabemos cuantos usuarios hay conectados en un

Momento puntual a cada Access Point, no sabemos con que estándar se está conectando cada uno, por ejemplo, cuantos están utilizando 802.11b y cuantos están utilizando 802.11g, etc.. Todo este desconocimiento y descontrol, no permiten una gestión "predictiva" y profesional de la red inalámbrica WIFI, como es de desear.

Por todo ello, la IETF, creó hace ya varios años, un grupo denominado CAPWAP - *Control and Provisioning of Wireless Access Points* - que está estudiando nuevos estándares para el "gobierno" de los Access Point. La idea es que en las redes inalámbricas WIFI, exista un "cerebro" al cual se conecten todos los Access Points y que éste sepa lo que está sucediendo en cada uno y pueda coordinar sus tareas. En este caso, la arquitectura de la red inalámbrica WIFI, sería centralizada (en vez de un océano o mar de puntos) y funcionaría verdaderamente como un sistema, como una verdadera red y no como recursos independientes y autónomos.

Entonces, toca especificar que funciones y tareas son necesarias para gestionar profesionalmente una red inalámbrica WIFI:

- Funciones y Tareas Requeridas para la Gestión y Control de una Red WIFI
- Instalación y Configuración
- Administración
- Problemas de Conexión y Mantenimiento
- Control del Rendimiento
- Gestión de la Seguridad

Aunque muchos crean lo contario **la Gestión de una Red Inalámbrica WIFI es un proceso permanente y continuo**, las 24 horas del día. Muchos se conforman con el primer paso de la tabla anterior: **Instalan y configuran y creen que ya la red inalámbrica Wifi funcionará sola**. Desgraciadamente no es así, se presentarán continuamente problemas de conexión, de mantenimiento, de seguridad, de rendimiento, etc.

Por lo tanto, existe un Ciclo de Gestión de una Red Inalámbrica WIFI. En primer lugar es necesario **"capturar" información**, saber que está sucediendo en cada Punto de Acceso Inalámbrico y en cada dispositivo wifi y lo que es más importante, aún, que está sucediendo en el aire, en el espectro de RF. Luego, hay que **analizar y comprender** el significado de toda esa información recabada. En tercer lugar hay que **responder, actuar** para corregir o mejorar los problemas que se estén presentando y por último hay que realizar el **análisis forense, sacar conclusiones** para corregir y mejorar nuestra red: reconfigurar Access Points, re-ubicarlos, o cualquier otra medida que resulte de las conclusiones.

ESTÁNDARES WIFI DE CONEXIÓN

A partir del estándar IEEE 802.11/ WIFI se fueron desarrollando otros estándares relacionados con WIFI que han ido introduciendo mejoras y solucionando inconvenientes. Los estándares de WIFI relativos a la transmisión de datos son:

- **Estándar 802.11:** Fue el primero y las velocidades de 1 y 2 Mbps eran muy pequeñas y no permitían implementar aplicaciones

empresariales de envergadura, por lo tanto se crearon nuevos grupos de trabajo para crear otros estándares.

- **Estándar 802.11a:** Permite realizar transmisiones con velocidades máximas de 54 Mbps y opera en una banda de frecuencia superior a los 5 GHz, por lo tanto no es compatible con el estándar 802.11b y el estándar 802.11g. A pesar de ser el "a" es, prácticamente, el más nuevo pues esa banda de frecuencia estaba asignada en muchos países a fuerzas públicas (bomberos, cruz roja, etc.) y recién últimamente está siendo liberada. Es muy útil Por ejemplo para separar el tráfico o para zonas con mucho ruido e interferencias. Además con el estándar 802.11a se pueden llegar a utilizar hasta 8 canales no superpuestos.
- **Estándar 802.11b**: Las conexiones funcionan a una velocidad máxima de 11 Mbps y opera en una banda de 2,4 GHz. Es el más popular pues fue el primero en imponerse y existe un inventario muy grande de equipos y dispositivos que manejan esta tecnología. Además, al ser compatible con el estándar 802.11g permitió la incorporación de éste último a las redes inalámbricas wifi ya existentes**.** Con el estándar 802.11b, sólo se pueden utilizar 3 canales no superpuestos (de los 11 existentes) en la mayoría de los países. En Europa, según los estándares ETSI, se pueden utilizar 4 canales de los 13 existentes. No todos lo Puntos de Acceso Inalámbrico sirven para los 2 sistemas, así que es importante tenerlo en cuenta a la hora de adquirir un Access Point.
- **Estándar 802.11g:** Las conexiones funcionan a una velocidad máxima de 54 Mbps y opera en una banda de 2,4 GHz**.** El estándar 802.11g fue aprobado a mediados del año 2003 y se popularizó rápidamente por su compatibilidad con el estándar 802.11b. Lo que

muchos desconocen es que al mezclar equipos del estándar 802.11b con equipos del estándar 802.11g la velocidad la fija el equipo más lento, o sea que la instalación mixta seguirá funcionando generalmente a velocidades lentas. Respecto de los canales aquí caben las mismas observaciones que para el estándar 802.11b, o sea que con el estándar 802.11g se pueden utilizar 3 Canales no superpuestos de los 11 disponibles y en Europa 4 de los 13 canales disponibles. Los canales que generalmente se utilizan con el estándar 802.11g y con el estándar 802.11b son: "1", "6" y "11" y en Europa: "1", "4", "9" y "13".

- **Estándar 802.11n:** Es un estándar nuevo que aún está en elaboración. Si bien se está trabajando en él desde el año 2004, sólo se ha logrado hasta ahora un borrador, que todavía no es definitivo y que, como suele suceder , puede ser modificado hasta la aprobación final del estándar 802.11n. El objetivo es elaborar un estándar con velocidades de transmisión superiores a 100 Mbps. El proceso se está demorando pues entre los promotores del estándar se han formado dos grupos antagónicos WWiSE y TGn Sync. Ninguno de los dos tiene una mayoría suficiente para imponer su tecnología y por lo tanto están trabadas las negociaciones. En 2005 se creó otro grupo con empresas de ambos bandos para tratar de encontrar algún punto medio. Este grupo es el "Enhanced Wireless Consortium - EWC". En lo único que están los dos grupos de acuerdo es en la utilización de una nueva tecnología conocida como MIMO que permite incrementar el ancho de banda y el alcance en WIFI utilizando Multiplexing. Según se apruebe la propuesta de un grupo u otro, las velocidades podrían variar entre 135 Mbps y 300 Mbps y las bandas de frecuencia serían 10GHz, 20GHz o 40GHz.

- **El Dilema Pre-estándar 802.11n:** En las redes inalámbricas WIFI, el tema de la homologación y certificación de equipos, no es un tema menor. Conviene aclarar, desde ya, y enfatizar que la compra de equipos homologados y certificados por la WiFi Alliance (Organización que agrupa a los fabricantes de productos WiFi) es de vital importancia para garantizar un funcionamiento armónico de los diversos elementos que componen una red inalámbrica wifi. Debido a las demoras que se están produciendo con este estándar, y ante la avidez de los consumidores por instalar redes inalámbricas wifi con velocidades superiores a 54 Mbps, existen algunos fabricantes que desde hace varios meses están ofreciendo productos "supuestamente" del estándar 802.11n. Como se explicó anteriormente, el estándar 802.11n aún no existe y sólo hay un borrador que todavía puede ser modificado una o más veces. Por consiguiente la WiFi Alliance, ha comunicado que no certificará productos respecto del inexistente estándar 802.11n.

Por todo esto es importante dejar claro a todos los usuarios que cualquier producto que compren de 802.11n no es estándar y puede presentar ahora y, aún más en el futuro, problemas de compatibilidad con otros elementos de la red inalámbrica wifi.

LA WI-FI ALLIANCE

Es una asociación constituída en el año 1999 con la finalidad de agrupar a todos los fabricantes de productos WI-FI: Puntos de Acceso inalámbricos, tarjetas cliente WI-FI, software para WI-FI, etc.

Desde el comienzo de la industria, existieron muchos problemas de interoperatividad y compatibilidad en redes inalámbricas wifi, debido a la utilización de equipos de diferentes fabricantes. Es muy común la situación en que en una instalación haya Puntos de Acceso inalámbricos de una marca, y vengan visitas (proveedores o clientes, por ejemplo) con estaciones clientes equipadas con hardware de otros fabricantes.
Para evitar que subsistan estos problemas, la Alianza WI-FI, testea y homologa todos los productos del estándar 802.11 y **les otorga un certificado donde se especifica para cada modelo qué funcionalidades están homologadas.** Este punto es de suma importancia pues permite al consumidor verificar las especificaciones de cada modelo independientemente de las aseveraciones del distribuidor local.

WIFI, el Asesino Silencioso:

Es importante enfatizar que la información se transmite por ondas de RF que viajan por el aire y es imposible evitar que sean "vistas" o "interceptadas", pues el aire es un medio compartido, público. Por este motivo acostumbro a denominar a wifi, como el "asesino silencioso". Muchos nos están "escuchando" las 24 horas del día, pero no los vemos!!!.

Algunos acostumbran a pensar, o a decir, que sus sistemas no corren peligro pues no tienen redes wifi en su organización. Esta aseveración es incorrecta pues, en realidad, los peligros que acabamos de mencionar son de la tecnología Wifi y no de las redes wifi**.** Aunque en la empresa no existan aún redes inalámbricas wifi, es suficiente que hayan algunos

computadores wifi (portátiles ?!) para que nuestros sistemas se tornen más frágiles y vulnerables. No por nada Wifi, es..."el asesino silencioso!!!" .

Según numerosas estadísticas existe muy poca conciencia de todas estas amenazas y peligros, por parte de los usuarios de redes inalámbricas wifi. Por ello todas demuestran que más del 60% de las redes wifi en las grandes ciudades del planeta están abiertas totalmente o, en su defecto, **muy mal protegidas**.

FILTRADO DE DIRECCIONES MAC

Es uno de los métodos de protección de redes inalámbricas wifi, más primitivos y menos eficaz que existen pues tiene muchas desventajas y puntos débiles.

El método de Filtrado de Direcciones MAC / MAC Address, consiste en suministrar a cada Punto de Acceso Inalámbrico un listado de las direcciones MAC de los equipos que están autorizados a conectarse a la red. De esta manera los equipos que no figuren en la lista serán rechazados. Las desventajas de este método son las siguientes:

Si hay muchos Access Points en la organización se producen errores al teclear la dirección MAC repetidamente en todos los Puntos de Acceso. Esto producirá inconvenientes con los usuarios "legales" que son rechazados. Además es muy trabajoso como se vio, la transmisión de la información en Wifi se hace por medio de paquetes. En muchos de estos la Mac Address, que generalmente no va encriptada, y obviamente puede ser capturada por un hacker. Existen programas en Internet que

permiten "imitar" y reemplazar esta Dirección MAC**.** Si esta es capturada por un hacker, toda la seguridad del sistema queda desarticulada.

La Dirección MAC, es una característica del hardware (no del usuario). Si el hardware (PC, PDA, USB, etc.) se pierde o es robado, el que lo encuentre podrá tener libre acceso a la red inalámbrica WIFI pues pasaría el control del filtro.

Seguridad WIFI: WEP (WIRED EQUIVALENT PRIVACY)

Desde un comienzo se conocían las debilidades en cuanto a Seguridad Informática de las Redes Inalámbricas WIFI. Por este motivo se incluyó en el estándar 802.11b un mecanismo de seguridad que permita encriptar la comunicación entre los diversos elementos de una red inalámbrica WIFI. Esta protección se denominó WEP (Wired Equivalent Privacy). En español sería algo así como "Privacidad equivalente a la de una red cableada". El protocolo WEP se basa en el algoritmo de encriptación RC4.

La idea de los promotores del estándar 802.11b consistía en encriptar el tráfico entre Puntos de Acceso y estaciones móviles y compensar así la falta de seguridad que se obtiene al enviar la información por un medio compartido como es el aire. Es así como, todos los Puntos de Acceso y dispositivos WIFI incluyen la opción de encriptar las transmisiones con el Protocolo de Encriptación WEP.

EL MECANISMO DE ENCRIPTACIÓN WEP

Brevemente diremos que hay que establecer una clave secreta en el Punto de Acceso, que es compartida con los clientes WIFI. Con esta clave, con el algoritmo RC4 y con un Vector de Inicialización (IV) se realiza la encriptación de los datos transmitidos por Radio Frecuencia.

A medida que fue aumentando la difusión de las Redes Inalámbricas WIFI, se fueron detectando graves problemas de seguridad informática en el Protocolo de Encriptación WEP, lo que generó hace unos años muy mala prensa a las redes inalámbricas WIFI.

RESUMEN DE DEBILIDADES DEL PROTOCOLO WEP

- El Vector de Inicialización IV, es demasiado corto pues tiene 24 bits y esto ocasiona que en redes inalámbricas WIFI con mucho tráfico se repita cada tanto.
- Hay algunos dispositivos clientes (tarjetas, USB) muy simples que el primer IV que generan es cero y luego 1 y así sucesivamente. Es fácil de adivinar.
- Las claves que se utilizan son estáticas y se deben cambiar manualmente. No es fácil modificarlas frecuentemente.
- No tiene un sistema de control de secuencia de paquetes. Varios paquetes de una comunicación pueden ser robados o modificados sin que se sepa.

Esta situación generó la aparición de múltiples aplicaciones capaces de crackear la seguridad WEP en poco tiempo. Según la capacidad de los equipos utilizados y la habilidad del hacker y el tráfico de la red

inalámbrica WIFI, se puede tardar desde 15 minutos a un par de horas en descifrar una clave WEP.

SEGURIDAD WIFI: WPA (WIFI PROTECTED ACCESS)

WPA y WPA2, son dos Protocolos de Encriptación que se desarrollaron para solucionar las debilidades detectadas en el protocolo de encriptación WEP. El nombre de WPA (WIFI Protected Access) que quiere decir en español: Acceso protegido WIFI, es un nombre comercial que promueve la WIFI Alliance. La parte técnica está definida y estipulada en el estándar de seguridad IEEE 802.11i.

La WiFi Alliance, estaba interesada en buscar una rápida solución a los inconvenientes de WEP. Además se buscaba que la solución WPA, funcionara con los Puntos de Acceso y dispositivos WIFI, ya vendidos a miles y miles de usuarios. Por este motivo se decidió desarrollar dos soluciones. Una rápida y temporal que se denominó WPA y otra más definitiva para aplicar en nuevos Puntos de Acceso, y no en los existentes, que se llamó WPA2.

Los Puntos de Acceso existentes hasta ese momento (2001/2002) ya tenían la capacidad de su hardware ocupada al 90% con diversas funciones, por lo tanto cualquier modificación que se le hiciera al WEP, no podría requerir mucha capacidad de proceso.

Se desarrolló un protocolo temporal denominado TKIP (Temporal Key Integrity Protocol) que es una "envoltura" del WEP y es conocido como WPA. El WPA (primera fase del estándar 802.11i) fue aprobado en Abril de 2003. Desde Diciembre de 2003 fue declarado obligatorio por la WiFi

Alliance. Esto quiere decir que todo Punto de Acceso Inalámbrico que haya sido certificado a partir de esta fecha, ya debe soportar "nativamente" WPA. Todo Punto de Acceso anterior a Diciembre de 2003 puede soportar "nativamente" sólo WEP. Recuerde!: Todos los fabricantes miembros de la WiFi Alliance deben poner gratuitamente a disposición de sus clientes un "parche" para actualizar los Puntos de Acceso antiguos de WEP a WPA.

MEJORAS A LA SEGURIDAD WIFI INTRODUCIDAS EN WPA

- Se incrementó el Vector de Inicialización (IV) de 24 bits a 48.
- Se añadió una función MIC (Message Integrity Check) para controlar la Integridad de los mensajes. Detecta la manipulación de los paquetes.
- Se reforzó el mecanismo de generación de claves de sesión
- Existen 2 versiones de WPA, una "home" o "Personal" que es para uso casero y de pymes, y otra más robusta denominada "Enterprise". No vienen activadas por defecto y deben ser activadas durante la configuración. Los Puntos de Acceso antiguos "emparchados" o actualizados de WEP a WPA se vuelven más lentos, generalmente y, si bien aumenta la seguridad, disminuye el rendimiento

SEGURIDAD WIFI: WPA2 (WIFI PROTECTED ACCESS 2)

WPA2, es el nombre que le dio la WIFI Alliance a la segunda fase del estándar IEEE 802.11i. La seguridad es muchísimo más robusta que la que ofrece WPA. WPA2 ya no se basa en un parche temporal sobre el

algoritmo RC4 y, en su lugar, utiliza el algoritmo de encriptación AES - recomendado por el NIST , de los más fuertes y difíciles de crackear en la actualidad. Este algoritmo de encriptación requiere un hardware más robusto, por lo tanto los Puntos de Acceso antiguos no se pueden utilizar con WPA2. Las primeras certificaciones de Puntos de Acceso compatibles con WPA2, se han hecho en Septiembre de 2004. Esto era voluntario, pero WPA2 es requisito obligatorio para todos los productos WIFI, desde Marzo de 2006.

Hay que tener mucho cuidado con productos anteriores a esas fechas, pues no son capaces de soportar WPA2. Por ejemplo, hay muchos PDA o Palm que se utilizan en redes inalámbricas WIFI que no se pueden utilizar con WPA2. Tampoco los computadores portátiles con Centrino de los primeros modelos soportan WPA2.

La implementación de protección que se aplica en el estándar de seguridad Wifi 802.11i, se conoce con el acrónimo CCMP y está basada, como ya se comentó, en el algoritmo de encriptación AES. El cifrado que se utiliza es simétrico de 128 bits y el Vector de Inicialización (IV) tienen una longitud de 48 bits.

El nuevo estándar exigió cambios en los paquetes que utilizan las redes inalámbricas WIFI para transmitir la información. Por ejemplo en los paquetes de "Beacons" o "Association Request" hubo que incluir datos sobre el tipo de encriptación: WEP, TKIP, CCMP, o sobre el tipo de autenticación: 802.1x (se verá en los próximos capítulos) o contraseña. Esto explica una vez más, porque los Puntos de Acceso y dispositivos Palm o PDA muy antiguos no funcionan con WPA2.

Para finalizar, digamos que al igual que con WPA, existen 2 versiones: **"WPA2 Personal" que sólo requiere contraseña y "WPA2 Enterprise" que requiere 802.1x y EAP**. En el momento de la configuración se debe estipular cual se va a utilizar.

VPN - VIRTUAL PRIVATE NETWORK

Las VPN son una herramienta diseñada para proteger las comunicaciones. Las VPN crean un túnel criptográfico entre 2 puntos. La encriptación se realiza mediante el protocolo IPSec de la IETF.

Cuando se empezó a tomar conciencia de la fragilidad de la seguridad wifi debido a las carencias del protocolo WEP, en algunos sectores se difundió el uso de VPN para reforzar la encriptación**.**

Se "tira" un túnel entre el cliente de la red inalámbrica WIFI y el servidor. De esta manera, queda protegida la conexión con IPSec que es un método de encriptación robusto y muy difícil de hackear**.**
La utilización de las VPN añade bastante seguridad a las redes inalámbricas pero tiene ciertas desventajas. Una de ellas es la económica pues cada túnel tiene un costo para la empresa y cuando se trata de proteger a cientos o miles de usuarios de una red inalámbrica wifi, las VPN se convierten en extremadamente costosas. Otro inconveniente es que las VPN han sido pensadas y diseñadas para conexiones "dial-up" punto a punto, pero las redes inalámbricas WIFI transmiten ondas de RF (irradian) por el aire que es un medio compartido.

DESVENTAJAS AL UTILIZAR VPN EN REDES INALÁMBRICAS WIFI

- Para un número grande de clientes WIFI, suele ser una solución bastante costosa. Se verán soluciones más baratas.
- Ayudaron bastante a mejorar la seguridad WEP, pero ahora que existe WPA y WPA2 no hacen falta
- Están diseñadas para proteger a partir de la capa 3 del modelo OSI, pero las redes inalámbricas WIFI (802.11) funcionan en capa 2.

Resumiendo, las VPN pueden ser una buena solución cuando ya están siendo utilizadas en la organización y se necesita proteger a los primeros usuarios de WIFI. En cuanto se masifica la utilización de las redes inalámbricas WIFI, su gestión se complica y los costos aumentan de manera innecesaria.

SEGURIDAD WIFI: ESTÁNDAR IEEE 802.1X

En los primeros años de este siglo, cuando sólo existía la encriptación WEP y antes que fuera desarrollado el estándar de seguridad 802.11i con la encriptación WPA y WPA2, el IEEE comenzó a buscar soluciones que fueran capaces de mejorar la Seguridad Wifi. El resultado buscado se consiguió adaptando el estándar 802.1x que se había aprobado en 2001 para redes cableadas. En 2004 se finalizó la adaptación para redes inalámbricas WIFI. Este estándar de seguridad en redes se basa en el control de acceso a puertos.

El estándar 802.1x constituye la columna vertebral de la Seguridad WIFI y es imprescindible y muy recomendable su utilización en toda red

empresarial que pretenda lograr una seguridad robusta**.** 802.1x introduce importantes cambios en el esquema de seguridad wifi.

ESTÁNDAR 802.1X: MODIFICACIONES EN SEGURIDAD WIFI

- Se necesita autenticar a los usuarios antes de conectarse a una red inalámbrica WIFI
- La autenticación se realiza con un protocolo conocido como EAP - Extensible Authentication Protocol. Existen varias versiones de EAP:LEAP, TLS, TTLS, PEAP, FAST
- La autenticación se realiza mediante un servidor de tipo RADIUS
- Es de resaltar, algunos cambios de fundamental importancia: En el esquema de 802.1x, se autentica al usuario y no al dispositivo**,** como se hacía, por ejemplo en el filtrado de Direcciones MAC (MAC Address).

Esto es muy importante porque impide que se pueda entrar a la red, aún cuando a uno le roben o pierda su laptop o PDA. La otra diferencia importante es que con 802.1x, el Punto de Acceso no puede "autorizar" a nadie el acceso a la red. La función de autorización recae en el servidor RADIUS.

El esquema básico de funcionamiento según se define en el estándar es el siguiente:

En 802.1x el puerto no se abre y no se permite la conexión hasta que el usuario está autenticado. El estándar define 3 elementos:

- **Servidor de Autenticación:** Es el que verificará las credenciales de los usuarios. Generalmente es un servidor RADIUS.

- **Autenticador:** Es el dispositivo que recibe la información del usuario y la traslada al servidor de autenticación (esta función la cumple el Punto de Acceso)
- **Suplicante:** Es una aplicación "cliente" que suministra la información de las credenciales del usuario al Autenticador. (soft cliente)

PROTOCOLOS DE AUTENTICACIÓN EAP

- **EAP-LEAP**

  a. Desarrollado por Cisco

     Soporta:

     - Autenticación mutua fuerte
     - Credenciales de seguridad
     - Claves dinámicas de encriptación

  b. Requiere Infraestructura de Cisco

  c. Requiere certificado digital en el servidor RADIUS

  d. Sólo soporta las bases de datos de Microsoft: Active Directory y NT Domain

  e. LEAP es vulnerable a ataques de diccionario

- **EAP-TLS**

a) Desarrollado por Microsoft

   Soporta:

   - Autenticación mutua fuerte
   - Credenciales de seguridad
   - Claves dinámicas de encriptación

b) Requiere certificados digitales en todos los usuarios así como un servidor RADIUS

c) Requiere certificado digital en el servidor RADIUS

d) Sólo soporta las bases de datos de Microsoft: Active Directory y NT Domain

- **EAP-TTLS**

a. Desarrollado por Funk Software y Certicom

Emplea:

- Autenticación mutua fuerte
- Credenciales de seguridad
- Claves dinámicas de encriptación

b. Requiere certificados digitales sólo en el servidor RADIUS

c. Se pueden utilizar certificados digitales en los clientes de manera opcional

d. Compatible con las bases de datos de seguridad preexistentes incluyendo:

- Windows Active Directory
- Dominios NT
- Tokens
- SQL
- LDAP
- etc...

SERVIDOR RADIUS

RADIUS es el acrónimo de Remote Authentication Dial In User Service. Sus diversas funciones y características están definidas en varias RFC de

la IETF. Algunas de las importantes son: RFC 2058, 2138 y 2548 . Como su nombre lo indica es un servidor que tiene la función de autenticar a los usuarios que se conectan remotamente.

Originalmente estaba pensado para accesos por líneas cableadas, pero cuando se modificó el estándar 802.1x para seguridad WIFI, se adaptó también como herramienta de autenticación para las redes inalámbricas wifi.
El servidor RADIUS cumple varias funciones en la arquitectura de seguridad de una red inalámbrica WIFI, las cuales se detallan a continuación:

FUNCIONES DEL SERVIDOR RADIUS EN REDES INALÁMBRICAS WIFI

- Recibir pedido de conexión de los usuarios wifi
- Autenticar a los clientes wifi y luego Autorizar su acceso a la red
- Devolver toda la información de configuración necesaria para que el cliente acceda a la red entre ellas la clave
- Para robustecer la seguridad wifi, el servidor RADIUS puede generar claves "dinámicas", es decir que las puede ir cambiando cada tanto. El administrador puede configurar el intervalo

El servidor RADIUS generalmente es un software aunque existen algunos appliance. Las versiones servidor de Windows 2000 y Windows 2003 incluyen un servidor RADIUS, que se denomina IAS - Internet Access Server

El servidor RADIUS tiene la función de Autenticar y de Autorizar a los clientes de WIFI**.** Los servidores RADIUS más completos incluyen una tercera función que es el Accounting, por eso se denominan "AAA" o

En lo que respecta a Seguridad WIFI, los Servidores RADIUS, además de autenticar y autorizar el acceso de usuarios añaden otras ventajas muy relevantes:

- A diferencia de las VPN, protegen la capa 2 pues cifran el canal antes que el usuario sea autenticado y reciba su IP**.** La VPN necesita una dirección IP para autenticar al usuario.
- El servidor RADIUS genera claves dinámicamente, lo que mitiga significativamente las deficiencias del protocolo de encriptación WEP**.**

SUPLICANTES

En el esquema de una red inalámbrica wifi con autenticación, la conexión la debe iniciar el dispositivo móvil, que es el que solicita al Servidor RADIUS, por medio del Punto de Acceso, ser autenticado. Esta tarea la realiza un software "cliente" instalado en el dispositivo móvil, que según se vio en "**Seguridad WIFI: Estándar IEEE 802.1x**" , se denomina "Suplicante", pues es el que "pide" o "solicita" la autenticación.

Existen diversos tipos de suplicantes para redes inalámbricas wifi, algunos muy simples y otros más sofisticados y con diversas funciones. Su elección también requerirá un análisis previo, en el caso de las redes inalámbricas wifi empresariales. Generalmente los muy simples se descargan gratis de internet o vienen incluidos en el CD de los Puntos de

Acceso Inalámbrico. Los más sofisticados deben adquirirse comercialmente y pagar las licencias correspondientes.

Al elegir un Suplicante hay que tener el cuenta, en que sistemas operativos funciona, que EAP soporta, y otras funciones como transparencia para el usuario, si está protegido por contraseña para que los usuarios no puedan modificar la configuración, etc.
Existen también varios Suplicantes para Linux.. Uno de los más conocidos es el "X-Supplicant" que soporta EAP-LEAP, EAP-TLS, EAP TTLS y EAP-PEAP, aunque no funciona bien con el RADIUS DE MICROSOFT, llamado IAS - Internet Access Server.

El Suplicante de Microsoft está incluido en Windows XP, en Windows 2000 y en Windows 2003 y, como ya se comentó, soporta EAP-TLS y EAP- PEAP, versión de Microsoft y requiere certificados digitales en cada uno de los clientes.

PUNTOS DE ACCESO HOSTILES - ROGUE ACCESS POINTS

Existe un problema muy difícil de solucionar en Seguridad WIFI, son los Puntos de Acceso Hostiles o Rogue Access Point, en inglés. En realidad, los Puntos de Acceso hostiles son sólo un capítulo de un tema más amplio y complicado que son las comunicaciones incontrolables o, descontroladas. Son conexiones que se establecen voluntaria o involuntariamente y, por su naturaleza son "temporales" y muchas veces por muy pocos minutos. El problema consiste en que hay que detectarlas "en caliente", es decir mientras están sucediendo. Además, muchas ocurren muy lejos de los "ojos" de la empresa u organización. Por ejemplo, en el aeropuerto, o en la universidad, o en un hotel...

Estas amenazas, o peligros, tienen su origen en la misma esencia de la tecnología WIFI. Las ondas - los paquetes - de RF transmitidas por cada dispositivo están en el aire, que es un medio compartido y no se puede impedir que sean capturadas o "vistas" por extraños. Además, no siempre es necesario un Punto de Acceso para establecer una conexión, pues estas se pueden realizar entre 2 dispositivos WIFI.

Así como nosotros tenemos nuestros puntos de acceso (la cantidad dependerá si somos particulares o empresas) es muy probable (cada día que pasa, es más probable) que nuestros vecinos u otras empresas que estén en el mismo edificio o en la misma manzana (recordar que el alcance de las ondas WIFI, son aprox. 100 mts), tengan sus Access Points. Estos, representan una amenaza permanente - las 24 horas del día - a nuestra red inalámbrica wifi y a nuestros dispositivos cliente wifi (notebooks, PDA, teléfonos celulares Wifi)**,** pero no hay nada que podamos hacer para evitarlos. No podemos impedirles a los vecinos que instalen sus propios Puntos de Acceso y sus propias redes inalámbricas**.** Es un peligro con el que debemos convivir, saber que existe y estar lo más alertas posibles, pues evidentemente, con tantos "vecinos" no sabemos cuales son las intenciones de cada uno y de cada uno de sus empleados.

Básicamente existen 3 fuentes de Puntos de Acceso Hostiles:

- Los vecinos
- "insiders" - empleados de nuestra organización, visitantes, etc.
- Los hackers

Es decir que, además del peligro potencial que representan todos los Access Points instalados en la vecindad (y que si no tenemos herramientas apropiadas para su detección, ni siquiera sabemos que existen) están los que puedan "insertarse" dentro de nuestra organización por parte de empleados o visitantes (proveedores, clientes, etc.) con diversas finalidades: "practicar", facilitar alguna tarea, o hasta robar información. Insisto en que la detección de estos puntos de acceso hostiles es muy complicada y requiere equipos muy sofisticados, sobre todo en organizaciones de gran tamaño como universidades, ministerios, industrias, aeropuertos, hoteles, etc.

Acciones Posibles para Combatir los Puntos de Acceso Hostiles Existen 5 acciones posibles, aunque muchas veces podemos llevarlas a cabo. Estas son:

1. Prevención
2. Detección
3. Bloqueo
4. Localización
5. Eliminación

Como es obvio, no podemos eliminar el access point de un vecino. Pero si podremos **detectarlo y localizarlo** para luego tratar de prevenir. Cuando se trata de un punto de acceso hostil, de un hacker, si tendremos derecho a eliminarlo, después de haberlo detectado y localizado**.**

CONEXIONES WIFI INCONTROLABLES

Como se vio anteriormente, hay muchas conexiones de WIFI, que se establecen entre dispositivos inalámbricos como notebooks o PDAs. Además también se realizan conexiones wifi en hoteles, universidades y aeropuertos con Puntos de Acceso de uso público, denominados HotSpots. Otro alternativa son los casos en que hackers, o simplemente curiosos se entrometen en dispositivos ajenos. Muchas veces estas conexiones son voluntarias, pero en muchos otros casos se establecen "a espaldas" del usuario y sin su conocimiento. Generalmente el hacker o intruso aprovecha la falta de información y conocimientos del usuario desprevenido. Estas conexiones son muy difíciles de evitar y de detectar, especialmente si la víctima no tiene buenos conocimientos de los peligros de wifi y si no se dispone de herramientas adecuadas para la detección y la protección.

2. DISEÑO METODOLÓGICO

2.1. COMPUTADORES FIJOS Y UN PORTÁTIL(ES) CON CONEXIÓN A INTERNET MEDIANTE CABLE

En la actualidad, se han comenzado a utilizar las conexiones inalámbricas. En parte es por moda, pero la verdad es que con un portátil es muy cómodo moverlo por toda la casa y seguir teniendo acceso a Internet (o a una impresora, o a los documentos del computador fijo, o ....).

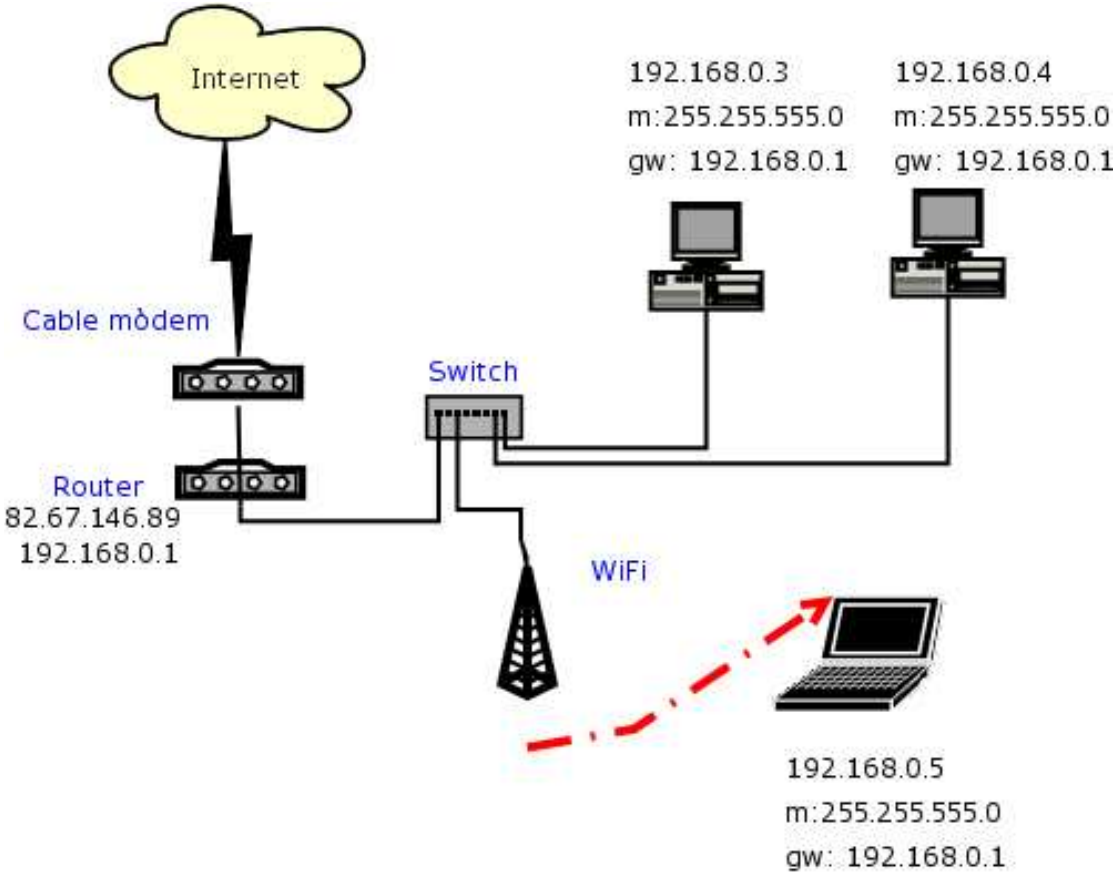

Figura 1: Conexión A Internet Mediante Cable

Fuente: http://www.terra.es/personal/lureyc/redes/ejemplos.html

En lugar de tener tres elementos para conectarlo todo es muy útil utilizar un equipo todo en uno: Para cable Linksys WRT54G (Alrededor de 90 EUR en Setiembre de 2004)

- En el caso de las impresoras hay tres opciones:

Conectar la impresora a uno de los computadores y compartirla (no daré más detalles porque la forma de hacerlo depende bastante del sistema operativo que utilices).

Conectar la impresora al enrutador. Muchos enrutadores incorporan un puerto USB, donde conectar una impresora u otro aparato, entonces basta con seguir las instrucciones del fabricante para compartir la impresora. Si encuentras uno de estos enrutadores no suelen ser más caros que uno normal.

Conectar la impresora como un computador más de la red (con su propia dirección IP). Es desde luego la opción más flexible y útil, el problema es que el precio de las impresoras que se conectan directamente a la red es algo más alto que las normales, y lo que es peor, cuestan algo más de encontrar.

2.2. IDENTIFICACIÓN DE REQUERIMIENTOS

Características

- Configure una red Wireless-G de alta velocidad (borrador 802.11g) en el hogar o la oficina

- Transferencia de datos de hasta 54 Mbps: 5 veces más rápido que Wireless-B (802.11b)
- Compatible con las redes Wireless-B a 11 Mbps
- Seguridad inalámbrica avanzada con encriptación WEP de 128 bits y filtro de MAC

Especificaciones

- Estándares IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE802.3u
- Puertos 1 Auto-Cross Over 10/100 (MDI/MDI-X), potencia
- Botones Reset
- Cableado RJ-45
- LEDs Encendido, actividad, enlace
- Seguridad Web-browser WPA, WEP Encryption, MAC Filtering, SSID Broadcast enable/disable
- WEP 64/128 bit
- Tamaño 186 x 48 x 169 mm
- Peso 46 gr

Contenido

- Punto de acceso Wireless-G
- Antenas desmontables
- Adaptador de corriente
- CD de instalación con guía de usuario
- Cable Ethernet
- Instalación rápida
- Tarjeta de registro

Requerimientos

- PC con procesador 200MHz
- 64MB RAM
- Internet Explorer 4.0 O Netscape Navigator 4.7 ó superior para configuración Web
- CD-ROM
- Windows 98SE, Me, 2000, o XP
- Adaptador Wireless 802.11b con protocolo TCP/IP instalado para PC o adaptador de red con cable de red
- Ethernet y protocolo TCP/IP instalado para PC

2.3. SEGURIDAD WIFI

Con la proliferación del uso de portátiles y PDAs con capacidades inalámbricas WiFi, cada vez es mayor la demanda de conexiones a Wireless Access Points. Las redes Wireless se difunden con rapidez, **a medida que el IEEE va aprobando nuevos estándares WiFi como el 802.11i, 802.11e y 802.11n**

La gran comodidad y ventajas que suponen estas nuevas opciones de conexión inalámbricas han hecho que muchísimos usuarios no se hayan percatado de los peligros a que están expuestas las redes WiFi (al no haber ya una conexión física) si no adoptan las medidas de seguridad aconsejadas por los expertos.

Como se observa en el gráfico, **Existen diversas maneras de poner a prueba la seguridad WiFi de una red inalámbrica.**

Una alternativa consiste en que el intruso intente conectarse a un Access Points de la red inalámbrica para luego ganar acceso a la red corporativa.

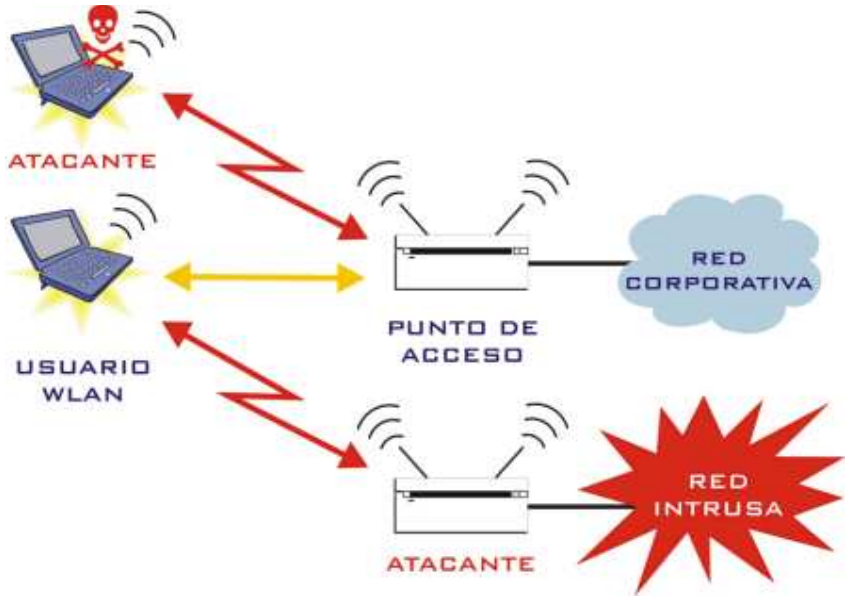

Figura 2: Ejemplo De Un Access Point Pirata
Fuente: http://www.virusprot.com/Whitepap1.html

La otra alternativa consiste en "implantar" un Access Point "pirata" conocido como ROUGE AP para atraer a los usuarios desprevenidos o muy curiosos a una red de hackers o red pirata.

Es preciso comprender que en las redes Wireless la información se transmite por medio de ondas de radio frecuencia y, esta, está en el aire y es imposible impedir que sea observada y/o capturada por cualquiera que se encuentre en un radio aproximado de 100 metros.

En el cuadro siguiente se enumeran los principales peligros que debemos mitigar para mejorar la seguridad WiFi.

- Cualquier otro usuario en un radio aproximado de 100 metros puede ser un "intruso potencial", bien con intención o sin ella.
- ¿Quién nos asegura que nos estamos conectando al servidor que deseamos?

- Como administradores de una red, ¿quién nos asegura que cada uno que intente conectarse a la misma es "de los nuestros"?
- Debemos asegurarnos que, una vez establecida la conexión, esta sea SEGURA, o lo que es lo mismo, ENCRIPTADA**.**

Como se ve en el gráfico de arriba, en las redes inalámbricas WiFi existen 2 tramos por los que viajan los paquetes que llevan la información:

- **Un tramo es inalámbrico (aéreo):** es el que va desde cada equipo WiFi hasta el Access Points.
- **Otro tramo es cableado:** es el que va desde el Access Points hasta el servidor de la organización.

Al no poder impedir de ninguna manera que la información que está en el aire sea vista por cualquiera, esta debe ser protegida por medio de protocolos de encriptación. En la actualidad se utilizan **WEP, WPA y WPA2**.

Pero la encriptación es una protección necesaria, muy necesaria, pero no suficiente pues no sirve para impedir accesos no deseados a nuestra red corporativa.

Durante un tiempo se han intentado diversas soluciones pero luego se iría demostrando su vulnerabilidad, hasta que por fin en abril de 2001 el IEEE (Institute of Electrical and Electronics Engineers) ha fijado un ESTÁNDAR: el IEEE 802.1x que se aplica a todas las redes con o sin cables. En 2004 fue ratificado para redes inalámbricas WiFi.

2.4. SEGURIDAD INALÁMBRICA EN EL ROUTER LINKSYS

CONFIGURACIÓN POR DEFECTO DEL ROUTER

Vamos a analizar la configuración del Router tal y como está después de desenvolverlo y ponerlo a funcionar.

- Dirección IP del Router: 192.168.1.1
- Servidor DHCP Activado. (El servidor DHCP asigna automáticamente una dirección IP dentro de su propio rango a todo aquel computador que lo solicite).
- Wireless activado.
- Difusión ESSID activada.
- SSID: Linksys
- Claves de acceso al Router: Usuario: admin. Contraseña: admin
- Sin filtrado de direcciones MAC
- Sin encriptación.

Es decir, la configuración perfecta para que cualquier vecino un poco avispado tenga completo acceso a nuestro Router, nuestra ADSL e incluso los pcs de nuestra red.

2.5. MEDIDAS DE SEGURIDAD RECOMENDADAS.

Luego según el enrutador, Proteja su Estación Base con una Contraseña / Cambie la Contraseña Predeterminada: Linksys | NETGEAR | Apple AirPort

Si vamos a utilizar el Router Linksys solamente mediante cable debemos desactivar la característica Wireless del Router

Cambiar las claves de acceso por defecto.

- **Linksys**[1]

  Instrucciones Detalladas

  1. Conéctese a su red inalámbrica.
  2. Abra su navegador de Internet y escriba http://192.168.1.1 en el espacio destinado a dirección Web.
  3. Presione la tecla Enter.
  4. Escriba el User Name (Nombre de Usuario) asignado para su red.
  5. Escriba la Contraseña predeterminada o default password.
  6. Presione el botón OK.
  7. Seleccione el enlace de texto Administration.
  8. En el cuadro de Router Password escriba una nueva contraseña y luego vuélvala a escribir.
  9. Haga clic sobre el botón Save Settings.
  10. Haga clic sobre el botón Continue.

Desactivar SSID Broadcast (Difusión).

Siendo uno de los datos que es necesario para poder conectar a nuestra red es importante no estar divulgándolo de manera tan evidente. Incluso sería necesario cambiarle el nombre, puesto que los programas habituales de búsqueda de redes son capaces de identificar la marca del Router, y por tanto deducir el nombre por defecto.

Por tanto en Wireless Network Name (SSID), pondremos otro diferente al definido por defecto.

Desactivar el servidor DHCP.

Si tenemos esta opción activada cualquier computador que tenga su tarjeta de red configurada en "Obtener una ip automáticamente" tendrá acceso a nuestra red.
Sería conveniente no sólo desactivar esta opción sino, también, cambiar la ip local que trae el Router por defecto, ya que siendo 192.168.1.1, es demasiado evidente.

Filtrado de direcciones MAC.

Cada tarjeta de red posee una dirección MAC (Media Access Control), que en teoría es única para cada una de ellas. Está formada por 48 bits que se suelen representar mediante dígitos hexadecimales que se agrupan en seis Por ejemplo, una dirección MAC podría ser E1:B1:CF:3D:4A:AA . Normalmente viene impresa en la tarjeta de red, aunque también se puede consultar mediante el comando ipconfig /all en ms-dos.
Al activar el filtrado de direcciones MAC del Router estamos autorizando el acceso al mismo únicamente a las tarjetas de red que introduzcamos en la lista. Iremos al menú Wireless y dentro de él, al apartado Wireless NetWork Access.

Ninguna de estas medidas por sí sola es segura, todas se pueden saltar. Pero todas ellas combinadas dificultará en extremo que nuestra red sea accesible.

En caso de usar otro tipo de enrutador

- **NETGEAR**[1]

  Instrucciones Detalladas:

  1. Conéctese a su red inalámbrica.
  2. Abra su navegador de Internet y escriba http://www.routerlogin.net en el espacio destinado a dirección Web.
  3. Presione la tecla Enter.
  4. Se abrirá el cuadro de comandos de diálogo NETGEAR.
  5. Haga clic sobre el botón OK.
  6. Escriba el nombre de usuario y la contraseña predeterminada (default password) que probablemente sea "password".
  7. Se abrirá la ventana de Router Manager.
  8. Bajo el título Maintenance seleccione del menú la opción Set Password.
  9. Escriba la contraseña predeterminada originalmente, (nuevamente, es probable que la antigua contraseña sea password). A continuación escriba una contraseña nueva — dos veces.
  10. Haga clic sobre el botón Apply.

- **Apple AirPort**[2]

  Instrucciones Detalladas:

[1] http://www.alertaenlinea.gov/tools/password-protect-netgear-change-password.aspx

[2] http://www.alertaenlinea.gov/tools/password-protect-apple-airport-change-password.aspx

1. Abra su aplicación AirPort Admin Utility (este programa fue previamente instalado desde el CD-ROM cuando usted instaló el dispositivo).
2. Busque el nombre de su red y haga doble-clic o presione el botón Configure que se encuentra en la parte inferior derecha de la pantalla.
3. Aquí nuestro nombre de red es Apple AirPort Express.
4. Ingrese su contraseña y haga clic sobre OK.
5. Se abrirá la ventana de configuración de la Estación Base Configure "Apple AirPort Express". Haga clic sobre la etiqueta AirPort que se encuentra en la parte superior.
6. Nuevamente, usted verá nuestro nombre de red Apple AirPort Express. Su nombre será diferente.
7. Haga clic sobre el botón Change Password.
8. Escriba una contraseña nueva y luego rescríbala para confirmarla. Haga clic sobre el botón Change.
9. Por último, para guardar los cambios asegúrese de hacer clic sobre la opción Update

Ingreso de Contraseña Incorrecta u Olvido de Contraseña

¿No puede recordad la contraseña de su estación base Wi-Fi? Si al ingresar sus contraseñas no puede acceder al menú de configuración de su estación Wi.Fi, intente hacerlo de alguna de las dos siguientes maneras:

Primero, intente ingresar la contraseña predeterminada de fábrica. Esta contraseña predeterminada es la que se le asignó a su estación al momento de despacharla. La siguiente lista incluye algunas contraseñas comúnmente predeterminadas para las marcas más conocidas:

- Contraseña predeterminada para Linksys: admin
- Contraseñas predeterminadas para NETGEAR: 1234 ó password
- Contraseñas predeterminadas para Apple Airport: public o password o admin

- Contraseña predeterminada para DLink: admin
- Contraseña predeterminada para Belkin: admin

Segundo, si no puede ingresar con la contraseña predeterminada, tendrá que reiniciar su estación base. De esta manera restablecerá la contraseña original de la estación base de la lista anterior. El único problema es que también restablecerá el resto de las funciones — incluso la configuración del ISP y otras funciones de seguridad.

Para reiniciar su estación de base, busque un pequeño orificio ubicado en la parte lateral o trasera del aparato— tiene el tamaño de la punta de un bolígrafo. Cuando encuentre este orificio (¡asegúrese de que sea el botón de reinicio!), tome un lápiz o un bolígrafo y presione el botón con la punta manteniéndolo apretado por varios segundos. Para consultar el procedimiento correcto, lea el manual de su aparato o visite el sitio Web de asistencia técnica. Para reiniciar las estaciones base de Apple tendrá que mantener presionado el botón durante 10 segundos, para Linksys durante 30 segundos. Antes de probar este método, verifíquelo con el servicio de asistencia técnica.

2.6. SEGURIDAD INALÁMBRICA. ENCRIPTACIÓN.

Encriptar la conexión Wireless es protegerla mediante una clave, de manera que sólo los computadores cuya configuración coincida con la del Router tengan acceso. Es necesaria para mantener segura nuestra red frente a los intrusos, que en el caso de redes domésticas, muy bien pueden ser nuestros "adorables" vecinos.

El proceso consiste en dos pasos:

- Configurar la encriptación en el Router.
- Configurar la encriptación en la tarjeta de red Wireless de cada computador.

El Router soporta 2 tipos de encriptación:

- **WEP (*Wired Equivalent Privacy)* o Privacidad Equivalente a Cableado**. Nos ofrece dos niveles de seguridad, encriptación a 64 o 128 bit. La encriptación usa un sistema de claves. La clave de la tarjeta de red del computador debe coincidir con la clave del Router.
- **WPA (*Wireless Protected Access*)** Ofrece dos tipos de seguridad, con servidor de seguridad y sin servidor. Este método se basa en tener una clave compartida de un mínimo de 8 caracteres alfanuméricos para todos los puestos de la red (Sin servidor) o disponer de un cambio dinámico de claves entre estos puestos (Con servidor). Es una opción más segura, pero no todos los dispositivos Wireless lo soportan.

Para acceder a la configuración de seguridad Wireless, debemos entrar a la configuración del Router. Para ello introducimos en el navegador la dirección IP la puerta de enlace de nuestra red local (dirección IP del Router).

Por defecto es 192.168.1.1, o podemos averiguarla abriendo una ventana de MS-DOS e introduciendo el comando **ipconfig** o **winipcfg**.

1.- WEP

WEP es un acrónimo de *Wired Equivalent Privacy* o Privacidad Equivalente Cableada. El Router usa encriptación WEP con dos modos diferentes de encriptación; de 64 y de 128 bits. La encriptación usa un sistema de claves. La clave del computador debe coincidir con la clave del Router. Hay dos formas de crear una clave. El modo más sencillo es

crear una clave desde una frase de paso (como una contraseña). El software del Router convertirá la frase en una clave. El método avanzado es teclear las claves manualmente.

Tenemos dos posibilidades de encriptación WEP:

A.- 64-bits (10 hex digits)

B.- 128-bit WEP

Según Microsoft, únicamente se debe utilizar sistema abierto/WEP si ningún dispositivo de red admite WPA. Se recomienda encarecidamente utilizar dispositivos inalámbricos compatibles con WPA y WPA-PSK/TKIP

Nota: una clave de alta seguridad es la que utiliza un conjunto aleatorio de dígitos hexadecimales (para la clave WEP) o caracteres (para WPA-PSK) del mayor tamaño de clave posible

2.- WPA Pre-Shared Key

Técnicamente, WPA-PSK (Wi-Fi Protected Access Pre-Shared Key) significa "Acceso protegido de fidelidad inalámbrica con Clave previamente compartida". La encriptación usa una autenticación de clave previamente compartida con cifrado TKIP (Temporal Key Integrity Protocol, Protocolo de integridad de clave temporal), denominado en adelante WPA-PSK/TKIP.

Según la descripción de Microsoft, WPA-PSK proporciona una sólida protección mediante codificación para los usuarios domésticos de dispositivos inalámbricos. Por medio de un proceso denominado "cambio automático de claves", conocido asimismo como TKIP **(Protocolo De Integridad De Claves Temporales),** las claves de codificación cambian con tanta rapidez que un pirata informático es incapaz de

reunir suficientes datos con la suficiente rapidez como para descifrar el código.

Características mínimas de las amenazas:

- Un atacante puede usar hardware o drivers comodity, no se requiere hardware inalámbrico o dedicado
- Un atacante consume recursos limitados en un dispositivo atacante, así que no es costoso para montar.
- La vulnerabilidad no será mitigada por capas emergentes MAC en mejoras de seguridad, por ejemplo, IEEE 802.11 TGi.
- Los vendedores independientes han confirmado que actualmente no hay defensa en contra de este tipo de ataques a DSSS basadas en WLANs.

  El rango de alcance del ataque puede crecer si se incrementa el poder de transmisión del dispositivo atacante o se usa una antena de alto aumento.

2.7. ROMPER UNA RED INALAMBRICA

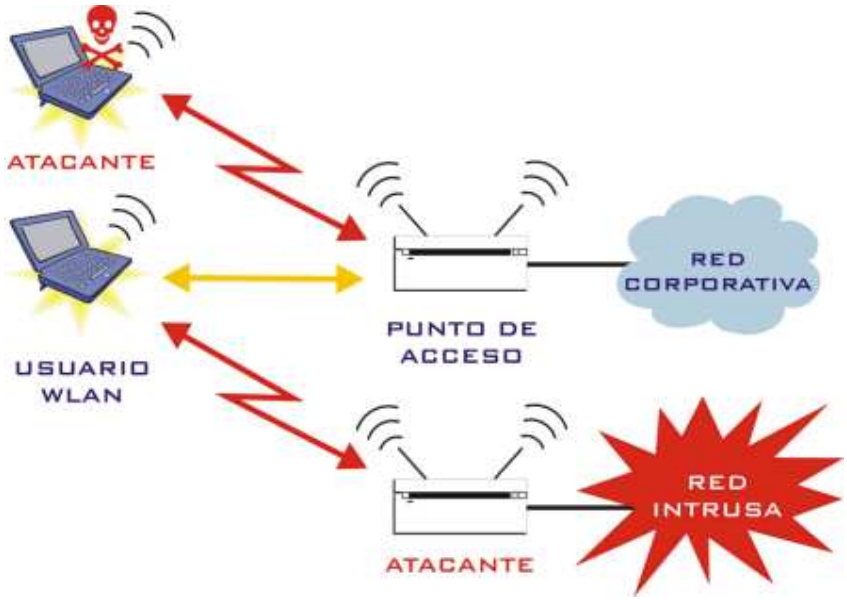

Figura 3: Ejemplo De Un Access Point Pirata
Fuente: http://www.virusprot.com/Whitepap1.html

Para el ejemplo, nosotros nos colocamos desde el punto de vista del intruso e intentaremos descifrar y acceder a una red WiFi, utilizando para ello varias herramientas Windows de libre acceso.

Bien vamos a intentar explicar la (in)seguridad de una red wireless domestica, lo que conseguiremos con esto es aprender a acceder a una red inalámbrica (wireless, wlan...) ajena, que herramientas necesitamos para ello, y así utilizar su ancho de banda para conectarse a Internet, adquirir datos, archivos o simplemente para comprender el tema, y así montar una red segura, aprendiendo de las vulnerabilidades de este tipo de redes.

Es importante, recordarles que meterse en una red ajena y utilizar su ancho de banda reservado para Internet es ilegal.

Adaptadores inalámbricos

Figura 4: Adaptadores Inalámbricos

fuente: http://www.taringa.net/posts/ebooks-tutoriales/2203519/como-crackear-cifrado-wep+seguridad-en-redes-wifi-en-windows.html

Se presentan en muchos formatos, pero sobretodo, para los PCs de sobremesa en PCI y para los pórtatiles en PCMCIA o CARDBUS (parecidos, pero no son lo mismo) y últimamente también aparecen en USB.

Los AP (Access Point)

Normalmente suelen ser un módem-Router (en las conexiones domésticas) ya que son muchos los proveedores de Internet (ISP) que con sus ofertas WiFi ofrecen un Router inalámbrico que al mismo tiempo funcionan como modem. Por lo tanto, no todas las redes inalámbricas tienen por qué tener conexión a Internet, aunque la mayoría la tendrán por lo que he comentado anteriormente.

Hablemos ahora un poco sobre la configuración de routers. Bien, estos routers contienen como un "servidor" que nos permite acceder a su configuración, donde podremos activar a parte de configurar todos los elementos de seguridad (WEP, ACL, DHCP…) de que disponga nuestro Router, también podremos configurar el direccionamiento de los puertos

(NAT), aunque esto ya se aleja del tema de seguridad para entrar en este tipo de redes.

Los Router disponen de un servidor, normalmente Web, aunque también pueden ser por Telnet, o incluso por FTP (para subir archivos de configuración ROM).

Figura 5: Router Linksys

Fuente: http://www.taringa.net/posts/ebooks-tutoriales/2203519/como-crackear-cifrado-

Para acceder a ellos usualmente se pone en la barra de direcciones de nuestro navegador la IP del Router (usualmente 192.168.1.1 o 192.168.1.0) o si preferimos por Telnet pues hacer telnet a la IP. Para entrar a la configuración nos pedirá un User y un password, o simplemente un password, también depende del modelo del Router. Por lo tanto podemos concluir que es muy importante averiguar con que Router estamos tratando y buscar un manual sobre éste en la pagina del fabricante, a no ser que el Router sea nuestro y ya poseamos uno, por lo tanto muy importante leerlo.

Dispositivos inalámbricos

Figura 6: Dispositivos Inalámbricos

Fuente: http://www.taringa.net/posts/ebooks-tutoriales/2203519/como-crackear-cifrado-

¿Que los diferencia? ¿Que hace que sea tan importante su elección?

Aparte de la sensibilidad de recepción, la potencia de salida, la posibilidad de

añadir una antena (conectores...) el estándar o protocolo que utiliza (IEEE 802.11a/b/g), la posibilidad de calibrar la potencia de emisión... etcétera.

Bien, pues aparte de todo esto, una diferencia muy importante y que no nos la especifican ni en la caja, ni en el manual de instrucciones ni en ningún sitio, es el CHIPSET[3].

Existen distintos chipsets, los más "famosos" son:

- Intersil Prism
- Atheros
- Hermes u Orinoco
- Cisco Aironet
- TI (Texas Intruments)
- Realtek
- Symbol
- Atmel

Pues bien, la cuestión, está en averiguar que chipset incorpora nuestra tarjeta.
Se añade una pequeña dificultad y es que cada fabricante (Conceptronic, Intel, Dlink …) cada modelo (c54C, 2200BG, 520G) e incluso cada revisión (-G520+, 2200BG+) no tienen por qué tener el mismo chipset, es decir diferentes fabricante pueden coincidir en dos modelos en el mismo chipset, aunque sean diferentes fabricantes, es como si el mundo de los chipsets no estuviese ligado al de los fabricantes.

[3] http://www.linux-wlan.org/docs/wlan_adapters.html.gz

Bien como en este post, hablamos para Windows, recomendare una tarjeta que tenga un chipset Atheros o Realtek[4], que según la pagina Web del programa AirCrack[5], tiene una compatibilidad 100%.

2.8. CAPTURANDO PAQUETES Y AVERIGUANDO EL CIFRADO

El programa que recomiendo en Windows para averiguar el cifrado Wep, es el Aircrack muy fácil de utilizar e intuitivo.
Y además porque incluye el Airodump, un programa para capturar paquetes, también muy fácil de utilizar.

Antes que nada una descripción de lo que haremos, en dos líneas:

1. Capturaremos paquetes con el Airodump[6].
2. Una vez con suficientes paquetes validos, averiguaremos el cifrado.

---

[4] http://www.wildpackets.com/support/hardware/airopeek

[5] Para romper una contraseña de 104 bits WEP ocupando la suite Aircrack es necesario obtener entre 500,000 y 2 millones de paquetes validos esto toma como mínimo unos 10 minutos. Ahora investigadores Alemanes extendiendo el algoritmo de Andreas Klein han logrado reducir la cantidad de paquetes necesarios para crackear una red inalámbrica con seguridad WEP a 85,000 paquetes los que significa una reducción en el tiempo de crackeo a menos de un minuto (impresionante!!!).

[6] Descargar el programa:
link 1: http://www.aircrack-ng.org/doku.php
link 2: (versión vieja) http://foro.seguridadwireless.net/index.php/topic,6918.0.html
link 3: (suite aircrack-ptw) http://foro.seguridadwireless.net/index.php/topic,7220.0.html
si no encontrar los archivos esenciales:
[/list]
[li]Peek.dll[/li]
[li]Peek5.sys[/li]
[li]MSVCR70.dll[/li]
[/list]

Una vez tengamos el Airodump extraído y nuestra tarjeta con los drivers compatibles instalados, ya lo tenemos todo para empezar a esnifar la red.

1. Así que ejecutamos el Airodump.exe, una vez abierto detectara todas las tarjeta habilitadas en el sistema de forma automática, introducimos el numero que hay a la izquierda de la tarjeta inalámbrica.
2. El siguiente paso es seleccionar el tipo de interfaz de la red, (Atheros, Aironet / Orinoco Realtek), pues depende cada uno del driver y de la tarjeta que tenga.
3. El siguiente paso es elegir el canal. Si pones cero, dará por entendido que no quieres filtrar ningún canal y los esnifara todos, útil si no sabes el canal de la red que quieres esnifar.
4. El siguiente es el nombre del archivo donde guardara los paquetes, no hace falta poner ninguna extensión, ya que automáticamente ya la crea.
5. El siguiente sirve para filtrar MACs, es decir el programas solo aceptara los paquetes de la MAC que escribas, el formato debe ser 00:00:00:00:00, es decir hay que añadir los dos puntos ":". Por supuesto para no filtrar ninguna y procesar todos los paquetes de todas las MACs, se tiene que escribir una "p" y listo. Se puede combinar con el filtrado por canales sin problemas.
6. Por último si todo ha ido bien, empezara a capturar paquetes. Pues bien dependiendo de la cantidad de tráfico que haya, puedes tardar más tiempo o menos, es lógico a mayor cantidad de tráfico mas IVs nos llegaran.

Mas o menos con un millon de IVs es suficiente para una llave de 128 bits (104 bits reales) para una de 64 pues la mitad, claro que se recomienda que por si acaso no se pare de capturar paquetes y llega al millon, pues en vez de detenerlo y pasar a crackearlo, se toma el archivo.cap que por momentos ira creciendo y se hace una copia de él en la misma carpeta, todo esto sin parar el airodump.

7. A veces, como el crackear un cifrado no es una ciencia totalmente cierta, pues el programa nos muestra un desagradable mensaje, eso si muy educado que dice "No luck, sorry" y como se había detenido el airodump se tiene que empezar a capturar mas paquetes, pero desde cero.

Si observamos que capturamos muy poco o si simplemente no cogemos ningun IVs, podria ser por esto:

- Asegurémonos que es WEP y no WPA
- Que no estemos demasiado lejos y solo te lleguen los Beacon Frames
- Si nuestra tarjeta no es compatible con el 802.11g, y el AP solo emite en 802.11g y no en 802.11b, no funcionará.
- Si aparte de esa red existen otra, prueba a especificar la MAC del AP (BSSID).
- También puede ser que nuestro driver este mal instalado. Revisarlo.

2.9. CRACKEANDO CON AIRCRACK

Aircrack es una colección de herramientas para la auditoría de redes inalámbricas:

- airodump: programa para la captura de paquetes 802.11
- aireplay: programa para la inyección de paquetes 802.11

- aircrack: crackeador de claves estáticas WEP y WPA-PSK
- airdecap: desencripta archivos de capturas WEP/WPA

Aircrack está incluido en el Troppix LiveCD, que incluye los controladores {Prism2 / PrismGT / Realtek / Atheros / Ralink} parcheados para la inyección de paquetes, así como los controladores acx100 e ipw2200 (Centrino b/g) .

Recibo el mensaje "cygwin1.dll not found" cuando inicio aircrack.exe.[7]

Para usar aircrack, arrastra el/los archivo(s) de captura .cap o .ivs sobre aircrack.exe. Si quieres pasarle opciones al programa deberás abrir una consola de comandos (cmd.exe) e introducirlas manualmente; también hay una GUI para aircrack, desarrollada por hexanium.

C:\TEMP> aircrack.exe -n 64 -f 8 out1.cap out2.cap

Crackear una clave WEP estática

La idea básica es capturar tanto tráfico encriptado como sea posible usando airodump. Cada packete de datos WEP tiene asociado un Vector de Inicialización (IV) de 3-bytes: después de recoger un número suficiente de paquetes de datos, ejecuta aircrack sobre el archivo de captura resultante. Entonces aircrack ejecutará un conjunto de ataques de tipo estadístico desarrollados por un talentoso hacker llamado **KoreK**.

[7] Puedes descargar esta librería de:http://100h.org/wlan/aircrack/.

Mi clave WEP es la correcta

Hay dos modos de autenticación WEP:

- **Open-System Authentication**: Este es el predeterminado. El AP acepta todos los clientes, y **nunca comprueba** la clave: siempre concede la asociación . De todas formas, si tu clave es incorrecta no podrás recibir o enviar paquetes (porque fallará la desencriptación), y pot tanto DHCP, ping, etc. acabarán interrumpiéndose.
- **Shared-Key Authentication**: el cliente debe encriptar la petición antes de que le sea concedida la asociación por el AP. Este modo tiene fallas y provoca la recuperación de la clave, por lo que nunca está activado de modo predeterminado.

En resumen, sólo por que parezca que te conectas de forma satisfactoria al AP no significa que tu clave WEP sea la correcta! Para comprobar tu clave WEP, debe desencriptar un archivo de captura con el programa airdecap.

IVs para crackear WEP

El crackeo WEP no es una ciencia exacta. El número de IVs necesarios depende de la longitud de la clave WEP, y también de la suerte. Normalmente, una clave WEP de 40-bit puede ser crackeada con 300.000 IVs, y una de 104-bit con 1.000.000 de IVs; **teniendo mala suerte se pueden necesitar dos millones de IVs, o más.**

No hay ninguna manera de saber la longitud de la clave WEP: esta información está oculta y nunca es anunciada, guardada bien en packetes de gestión, bien en paquetes de datos; como consecuencia, airodump no puede reportar la longitud de la clave WEP. Por ese motivo, se recomienda ejecutar aircrack dos veces: cuando tienes 250.000 IVs, inicias aircrack con "-n 64" para crackear la WEP de 40-bit. Si no la sacas, vuelves a iniciar aircrack (sin la opción -n) para crackear la WEP de 104-bit.

No consigo IVs!

Posibles motivos:

- Te encuentras demasiado lejos del punto de acceso.
- No hay tráfico en la red escogida.
- Hay tráfico de tipo G pero estás capturando en modo B.
- Hay algún problema con tu tarjeta (¿problema de firmware ?)
- Los beacons sólo son "paquetes anuncio" sin encriptar. No sirven para el crackeo WEP.

No hay una versión de aireplay para Windows

El controlador PEEK no soporta la inyección de paquetes 802.11; **No** portaré aireplay a Win32. De todos modos, hay alternativas comerciales:

- Tarjetas Prism: http://www.tuca-software.com/transmit.php
- Tarjetas Atheros:
  http://www.tamos.com/htmlhelp/commwifi/pgen.htm

Compatibilidad de mi tarjeta con airodump / aireplay

Antes de nada, busca en Google para averiguar cuál es el chipset de tu tarjeta. Por ejemplo, si tienes una Linksys WPC54G busca por "**wpc54g chipset Linux**".

El controlador PEEK no reconoce mi tarjeta.

Los controladores de Windows arriba mencionados no reconocen algunas tarjetas, incluso teniendo el chipset correcto. En este caso, abre el administrador de dispositivos, selecciona tu tarjeta, "Actualizar el controlador", selecciona "Instalar desde una ubicación conocida", selecciona "No buscar, seleccionaré el controlador a instalar", haz click en "Utilizar disco", introduce la ruta donde ha sido descomprimido el archivo, deselecciona "Mostrar hardware compatible", y elige el controlador.

Tarjeta a comprar

El mejor chipset a día de hoy es Atheros; está muy bien soportado por ambos Windows y Linux. El último parche madwifi hace posible inyectar en bruto paquetes 802.11 tanto en modo Infraestructura (Managed) como Monitor a velocidades b/g.

Ralink hace buenos chipsets, y ha sido **muy** cooperativo con la comunidad open-source para desarrollar controladores GPL. Ahora la inyección de paquetes está completamente soportada bajo Linux con tarjetas PCI/PCMCIA RT2500, y también funciona en dispositivos USB RT2570.

*Nota: hay algunos modelos más baratos con nombre parecido (WG511, WG311, DWL-650+ y DWL-G520+); esas tarjetas **no están basadas***

en Atheros . Además, el controlador Peek no soporta las tarjetas Atheros recientes, por lo que deberás usar CommView WiFi en su lugar.

Airodump en Windows

Antes de nada, asegúrate de que tu tarjeta es compatible (mira la tabla de más arriba) y de que tienes instalado el controlador adecuado. También debes descargar peek.dll y peek5.sys y ponerlos en el mismo directorio que airodump.exe.

A la hora de ejecutar airodump, deberías especificar:

- El número identificador de la interfaz de red, que debe ser elegido de la lista mostrada por airodump.
- El tipo de interfaz de red ('o' para HermesI y Realtek, 'a' para Aironet y Atheros).
- El número de canal, entre 1 y 14. También puedes especificar 0 para alternar entre todos los canales.
- El prefijo de salida. Por ejemplo, si el prefijo es "foo", entonces airodump creará foo.cap (paquetes capturados) y foo.txt (estadísticas CSV). Si foo.cap existe, airodump continuará la captura añadiéndole los paquetes.
- La opción "sólo IVs". Debe ser 1 si solamente quieres guardar los IVs de los paquetes de datos WEP. Esto ahorra espacio, pero el archivo resultante (foo.ivs) sólo será útil para el crackeo WEP.

Para parar de capturar paquetes presiona Ctrl-C. Puede que te salga una pantalla azul, debido a un bug en el controlador PEEK por no salir limpiamente de modo monitor. También puede que el archivo resultante de la captura está vacío. La causa de este bug es desconocida.

Airodump oscila entre WEP y WPA.

Esto ocurre cuando tu controlador no desecha los paquetes corruptos (los que tienen CRC inválido). Si es un Centrino b, simplemente no tiene arreglo; ve y compra una tarjeta mejor. Si es una Prism2, prueba a actualizar el firmware.

Significado de los campos mostrados por airodump

Airodump mostrará una lista con los puntos de acceso detectados, y también una lista de clientes conectados o estaciones ("stations"). Aquí hay un ejemplo de una captura de pantalla usando una tarjeta Prism2 con HostAP:

```
BSSID          PWR  Beacons   # Data  CH  MB  ENC   ESSID

00:13:10:30:24:9C  46      15    3416   6  54. WEP   the ssid
00:09:5B:1F:44:10  36      54       0  11  11 OPN   NETGEAR

BSSID          STATION         PWR  Packets  Probes

00:13:10:30:24:9C  00:09:5B:EB:C5:2B   48      719  the ssid
00:13:10:30:24:9C  00:02:2D:C1:5D:1F  190       17  the ssid
```

Field	Description
BSSID	Dirección MAC del punto de acceso.
PWR	Nivel de señal reportado por la tarjeta. Su significado depende del controlador, pero conforme te acercas al punto de acceso o a la estación la señal aumenta. Si PWR == -1, el controlador no soporta reportar el nivel de señal.
Beacons	Número de paquetes-anuncio enviados por el AP. Cada punto de acceso envía unos diez beacons por segundo al ritmo (rate) mínimo (1M), por lo que normalmente pueden ser recogidos desde muy lejos.

# Data	Número de paquetes de datos capturados (si es WEP, sólo cuenta IVs), incluyendo paquetes de datos de difusión general.
CH	Número de canal (obtenido de los paquetes beacon). Nota: algunas veces se capturan paquetes de datos de otros canales aunque no se esté alternando entre canales debido a las interferencias de radiofrecuencia.
MB	Velocidad máxima soportada por el AP. Si MB = 11, entonces se trata de 802.11b, si MB = 22 entonces es 802.11b+ y velocidades mayores son 802.11g.
ENC	Algoritmo de encriptación en uso. OPN = sin encriptación, "WEP?" = WEP o mayor (no hay suficiente datos para distinguir entre WEP y WPA), WEP (sin la interrogación) indica WEP estática o dinámica, y WPA si TKIP o CCMP están presentes.
ESSID	Conocida como "SSID", puede estar vacía si el ocultamiento de SSID está activo. En este caso airodump tratará de recuperar el SSID de las respuestas a escaneos y las peticiones de asociación.
STATION	Dirección MAC de cada estación asociada. En la captura de más arriba se han detectado dos clientes (00:09:5B:EB:C5:2B y 00:02:2D:C1:5D:1F).

Usar Ethereal para capturar paquetes 802.11

Bajo Linux, simplemente prepara la tarjeta para modo Monitor con el script airmon.sh. Bajo Windows, Ethereal NO PUEDE capturar paquetes 802.11 .

Ethereal decodificar paquetes de datos WEP

Sí. Ve a Editar -> Preferencias -> Protocolos -> IEEE 802.11, selecciona 1 en la "WEP key count" e introduce tu clave WEP debajo.

Cambiar mi dirección MAC

Esta operación solamente es posible bajo Linux. Por ejemplo, si tienes una tarjeta Atheros:

```
ifconfig ath0 down
ifconfig ath0 hw ether 00:11:22:33:44:55
ifconfig ath0 up
```

Si no funciona, intenta sacar y re-insertar la tarjeta.

Uso aircrack

Usage: aircrack [options] <capture file(s)>

Se puede especificar múltiples archivos de entrada (tanto en formato .cap como .ivs). También puedes ejecutar airodump y aircrack al mismo tiempo: aircrack se auto-actualizará cuando haya nuevos IVs disponibles.

Aquí hay un sumario con todas las opciones disponibles:

Opción	Param.	Descripción
-a	amode	Fuerza el tipo de ataque (1 = WEP estática, 2 = WPA-PSK).
-e	essid	Si se especifica, se usarán todos los IVs de las redes con el mismo ESSID. Esta opción es necesaria en el caso de que el ESSID no esté abiertamente difundido en un crackeo WPA-PSK (ESSID oculto).
-b	bssid	Selecciona la red elegida basándose en la dirección MAC.
-p	nbcpu	En sistemas SMP , especifica con esta opción el número de CPUs.
-q	*none*	Activa el modo silencioso (no muestra el estado hasta que la clave es o no encontrada).
-c	*none*	(crackeo WEP) Limita la búsqueda a caracteres alfanuméricos solamente (0x20 - 0x7F).
-d	start	(crackeo WEP) Especifica el comienzo de la clave WEP (en hex), usado para depuración.
-m	maddr	(crackeo WEP) Dirección MAC para la que filtrar los paquetes de datos WEP. Alternativamente, especifica -m ff:ff:ff:ff:ff:ff para usar todos y cada uno de los IVs, indiferentemente de la red que sea.
-n	nbits	(crackeo WEP) Especifica la longitud de la clave: 64 para WEP de 40-bit , 128 para WEP de 104-bit , etc. El valor predeterminado es 128.
-i	index	(crackeo WEP) Conserva sólo los IVs que tienen este índice de clave (1 a 4). El comportamiento predeterminado es ignorar el índice de la clave.
-f	fudge	(crackeo WEP) De forma predeterminada, este parámetro está establecido en 2 para WEP de 104-bit y en 5 para WEP de 40-bit. Especifica un valor más alto para elevar el nivel de fuerza bruta: el crackeo llevará más tiempo, pero con una mayor posibilidad de éxito.
-k	korek	(crackeo WEP) Hay 17 ataques de tipo estadístico de korek. A veces un ataque crea un

		enorme falso positivo que evita que se obtenga la clave, incluso con grandes cantidades de IVs. Prueba -k 1, -k 2, ... -k 17 para ir desactivando cada uno de los ataques de forma selectiva.
-x	*none*	(crackeo WEP) No aplicar fuerza bruta sobre los dos últimos keybytes.
-y	*none*	(crackeo WEP) Éste es un ataque de fuerza bruta experimental único que debería ser usado cuando el método normal de ataque falle con más de un millón de IVs.
-w	words	(WPA cracking) Ruta hacia la lista de palabras.

Implementar una opción para reanudar en aircrack

No hay planes de implementar esta capacidad.

Crackear un red WPA-PSK

Debes capturar hasta que se produzca un "saludo" (Handshake) entre un cliente inalámbrico y el punto de acceso. Para forzar al cliente a reautenticarse puedes iniciar un ataque de deautenticación con aireplay. También es necesario un buen diccionario[8].

Para tu información. No es posible pre-computar grandes tablas de Pairwise Master Keys como hace rainbowcrack, puesto que la contraseña está entremezclada con el ESSID.

Crackeando WPA en el futuro

[8] Ver http://ftp.se.kde.org/pub/security/tools/net/Openwall/wordlists/

Es extremadamente improbable que WPA sea crackeado del modo que lo ha sido WEP.

El mayor problema de WEP es que la clave compartida está adjunta en el IV; el resultado está vinculado directamente con el RC4. Esta construcción simple superpuesta es propensa a un estaque de tipo estadístico, ya que los primeros bytes del texto cifrado están fuertemente correspondidos con la clave compartida (ver el papel de Andrew Roos). Existen básicamente dos contramedidas a este ataque: 1. mezclar el IV y la clave compartida usando una función para la codificación o 2. Descartar los primeros 256 bytes de la salida del RC4.

Ha habido alguna desinformación en las noticias acerca de las fallas de TKIP:

Por ahora, TKIP es razonablemente seguro por sí solo viviendo un tiempo prestado ya que se apoya en el mismo algoritmo RC4 en el que se apoyó WEP.

Realmente, TKIP (WPA1) **no es** vulnerable: para cada paquete, el IV de 48-bit está mezclado con la clave temporal pairwise de 128-bit para crear una clave RC4 de 104-bit, por lo que no hay ninguna correlación de tipo estadístico . Es más, WPA proporciona contramedidas ante ataques activos (reinyección de tráfico), incluye un mensaje de integridad de código más fuerte (Michael), y tiene un protocolo de autenticación muy robusto ("saludo" de 4 fases). La única vulnerabilidad a tener en cuenta es el ataque con diccionario, que falla si la contraseña es lo suficientemente robusta.

WPA2 (aka 802.11i) es exactamente lo mismo que WPA1, excepto que usa CCMP (////AES in counter mode////) en lugar de RC4 y HMAC-SHA1 en lugar de HMAC-MD5 para el EAPOL MIC. Como apunte final, WPA2 es un poco mejor que WPA1, pero ninguno de los dos será crackeado en un futuro cercano.

¡Tengo más de un millón de IVs, pero aircrack no encuentra la clave!

Posibles motivos:

- Necesitas capturar más IVs. normalmente, una WEP de 104-bit puede ser crackeada con aproximadamente un millón de IVs, aunque a veces se necesitan más IVs.

- Si todos los votos (votes) parecen iguales, o si hay muchos votos negativos, entonces el archivo con la captura está corrupto, o la clave no es estática (¿se está usando EAP/802.1X ?).

- Un falso positivo evitó que se obtuviera la clave. Prueba a desactivar cada ataque korek (-k 1 .. 17), sube el nivel de fuerza bruta (-f) o prueba con el ataque inverso experimental único (-y).

He encontrado una clave, ¿cómo desencripto un archivo de captura ?

Puedes usa el programa airdecap :

uso: airdecap [opciones] <archivo pcap>

-l : no elimina la cabecera del 802.11

-b bssid : filtro de dirección MAC del punto de acceso
-k pmk : WPA Pairwise Master Key en hex
-e essid : Identificador en ascii de la red escogida
-p pass : contraseña WPA de la red escogida
-w key : clave WEP de la red escogida en hex

ejemplos:

airdecap -b 00:09:5B:10:BC:5A open-network.cap
airdecap -w 11A3E229084349BC25D97E2939 wep.cap
airdecap -e "el ssid" -p contraseña tkip.cap

Recupero mi clave WEP en Windows

Puedes usar el programa WZCOOK que recupera las claves WEP de la utilidad de XP Wireless Zero Configuration. Éste es un software experimental, por lo que puede que funcione y puede que no, dependiendo del nivel de service pack que tengas.

2.10. CÓMO PROTEGER LA RED INALÁMBRICA

El acceso inalámbrico a Internet puede ofrecerle conveniencia y movilidad. Pero hay algunos pasos que usted debería seguir para proteger su red inalámbrica y las computadoras conectadas a la misma.

- Use encriptación para codificar o encriptar las comunicaciones en la red. Si tiene la opción, use el Acceso Protegido para Transferencia Inalámbrica de Datos o WPA (por su acrónimo del inglés Wi-Fi Protected Access) que es un sistema de encriptación más potente que

el sistema de Equivalencia de Privacidad Inalámbrica o WEP (por su acrónimo del inglés Wired Equivalent Privacy).

- Use software antivirus y antiespía y también active el firewall.
- Casi todos los enrutadores inalámbricos (Wireless routers) tienen un mecanismo llamado identificador de emisión (identifier broadcasting). Desactive el mecanismo del identificador de emisión para que su computadora no emita una señal a todas las terminales que estén en las cercanías anunciando su presencia.
- Cambie la configuración predeterminada del identificador de su enrutador asignado por el fabricante del dispositivo (router's pre-set password for administration) para que los hackers no puedan utilizarlo para intentar acceder a su red.
- Cambie la contraseña predeterminada de instalación del enrutador por una nueva contraseña que solamente usted conozca. Cuanto más extensa sea la contraseña, más difícil será descifrarla.
- Solamente permita el acceso a su red inalámbrica a computadoras específicas.
- Apague su red inalámbrica cuando sepa que no la va a utilizar.
- No dé por supuesto que los hot spots públicos o puntos de acceso público a Internet son seguros. Debería tener en cuenta que otras personas pueden acceder a cualquier información que usted vea o envíe a través de una red inalámbrica pública.

Cada vez más son más los usuarios de computadoras que se interesan en la conveniencia y movilidad que brinda el acceso inalámbrico a Internet. Actualmente, las personas que viajan por negocios usan computadoras portátiles para mantenerse en contacto con sus oficinas; los turistas mandan fotos a sus amigos desde sus lugares de vacaciones

y los compradores hacen sus pedidos cómodamente sentados en el sofá de sus casas. Una red inalámbrica (Wireless network) puede conectar varias computadoras ubicadas en distintas partes de su casa o negocio sin enredos de cables y le permite trabajar en una computadora portátil desde cualquier lugar dentro del área de la red.

Generalmente, para acceder a Internet sin cables es necesario tener instalada una conexión de banda ancha, esto se llama "punto de acceso" (Access point), como por ejemplo una línea de cable o DSL que funciona conectada a un módem. Para instalar la red inalámbrica, usted conecta el punto de acceso a un enrutador inalámbrico (Wireless Router) que emite una señal al aire que en algunas oportunidades tiene un radio de emisión de hasta varios cientos de pies. Cualquier computadora que esté equipada con una tarjeta de cliente inalámbrico (Wireless client card) que se encuentre dentro del radio de emisión del enrutador puede captar la señal del aire y acceder a Internet.

El aspecto negativo de una red inalámbrica es que, a menos que usted tome ciertas precauciones, cualquier usuario que tenga una computadora preparada para acceder a Internet sin cable puede usar su red. Esto significa que sus vecinos, o en el peor de los casos los ciber-delincuentes o hackers que andan al acecho cerca de su computadora, podrían "colgarse" de su red, o hasta podrían lograr acceder a la información almacenada en su computadora. Si una persona no autorizada usa su red para cometer un delito o enviar mensajes electrónicos spam, la actividad puede ser rastreada hasta su cuenta de usuario. Afortunadamente, hay algunos pasos que usted puede seguir

para proteger su red inalámbrica y las computadoras conectadas a la misma.

Pasos preventivos

- **Use encriptación**. La manera más efectiva de proteger su red inalámbrica contra los intrusos es encriptar o codificar las comunicaciones en red. La mayoría de los enrutadores inalámbricos, puntos de acceso y estaciones base tienen un mecanismo de encriptación incorporado. Si su enrutador inalámbrico no tiene esta función de encriptación, considere conseguir uno que sí la tenga. Los fabricantes de enrutadores inalámbricos frecuentemente despachan sus aparatos con la función de encriptación desactivada y usted debe activarla. En el manual de instrucciones de su enrutador inalámbrico debería encontrar la descripción del procedimiento para instalarla. Si no fuera así, consulte el sitio Web del fabricante del enrutador. Hay dos tipos principales de encriptación: Acceso Protegido para Transferencia Inalámbrica de Datos o WPA (por su acrónimo del inglés Wi-Fi Protected Access) y Equivalencia de Privacidad Inalámbrica o WEP (por su acrónimo del inglés Wired Equivalent Privacy). Su computadora, enrutador y demás equipo deben utilizar la misma encriptación. El sistema WPA provee una encriptación más potente; si tiene la opción, use este sistema ya que está diseñado para protegerlo contra la mayoría de los ataques de los hackers. Algunos modelos más antiguos de enrutadores solamente ofrecen encriptación WEP, lo que es mejor que no tener ningún tipo de encriptación. Este sistema de encriptación o codificación debería proteger su red inalámbrica contra las intrusiones accidentales de

vecinos o contra los ataques de hackers menos sofisticados. Si usa el sistema de encriptación WEP, configúrelo al nivel de seguridad más alto.

- **Use software antivirus y antiespía y también active el firewall.** Las computadoras conectadas a una red inalámbrica necesitan tener la misma protección que las computadoras conectadas a Internet por medio de un cable. Instale en su computadora un software antivirus y antiespía y manténgalos actualizados. Si su computadora fue entregada con el firewall o cortafuegos desactivados, actívelo.
- **Desactive el identificador de emisión.** Casi todos los enrutadores inalámbricos (Wireless routers) tienen un mecanismo llamado identificador de emisión (identifier broadcasting). Este mecanismo emite una señal a todas las terminales que estén en las cercanías anunciando su presencia. No es necesario que usted emita esta información si la persona que está usando la red ya sabe que está disponible. Los hackers pueden usar el identificador de emisión para acceder a redes inalámbricas vulnerables. Si su enrutador inalámbrico se lo permite, desactive el mecanismo del identificador de emisión.
- **Cambie la configuración predeterminada del identificador de su enrutador (router's pre-set password for administration).** Probablemente, el identificador de su enrutador sea un código o nombre de identificación (ID) estándar predeterminado que fue asignado por el fabricante para todas las unidades de hardware de ese modelo. Aunque su enrutador no esté emitiendo la señal de su identificador a todo el mundo, los hackers conocen los códigos o nombres de identificación predeterminados y pueden usarlos para intentar acceder a su red. Cambie el identificador de su enrutador por

un código que solamente usted conozca, y recuerde que para que su enrutador y su computadora puedan comunicarse entre sí, debe configurar el mismo código de identificación o ID en ambos. Use una contraseña que tenga por lo menos 10 caracteres: Cuanto más extensa sea su contraseña o código de identificación, más difícil resultará que los hackers logren acceder a su red.

- **Cambie la contraseña predeterminada de instalación del enrutador.** Probablemente, el fabricante de su enrutador inalámbrico le asignó una contraseña estándar predeterminada (pre-set password for administrator) para permitir la instalación y operación del enrutador. Los hackers conocen estas contraseñas predeterminadas, por lo tanto, cámbiela por una contraseña nueva y que solamente usted conozca. Cuanto más extensa sea la contraseña, más difícil será descifrarla.
- **Solamente permita el acceso a su red inalámbrica a computadoras específicas.** Cada computadora habilitada para comunicarse con una red tiene asignada una dirección exclusiva de Control de Acceso a Medios o MAC (por su acrónimo del inglés, Media Access Control). Generalmente, los enrutadores inalámbricos tienen un mecanismo que permite que solamente los aparatos con una dirección MAC particular puedan acceder a la red. Algunos hackers han imitado domicilios MAC, por lo tanto no se confíe solamente en esta medida de protección.
- **Apague su red inalámbrica cuando sepa que no la va a utilizar**. Los hackers no pueden acceder a un enrutador inalámbrico cuando está apagado. Si usted apaga el enrutador cuando no lo usa, está limitando la cantidad de tiempo de vulnerabilidad a los ataques de los hackers.

- **No dé por supuesto que los hot spots públicos son seguros.** Muchos bares, hoteles, aeropuertos y otros establecimientos públicos ofrecen redes inalámbricas para sus clientes. Estos hot spots o puntos de acceso a Internet son convenientes, pero no siempre son seguros. Consulte con el propietario del establecimiento para verificar cuáles son las medidas de seguridad implementadas.
- **Tenga cuidado con el tipo de información a la que accede o que envía desde una red inalámbrica pública.** Para evitar riesgos, debería tener en cuenta que otras personas pueden acceder a cualquier información que usted vea o envíe a través de una red inalámbrica pública. A menos que usted pueda verificar que un "hot spot" haya implementado medidas de seguridad efectivas, lo mejor es evitar el envío o recepción de información delicada a través de la red.

CONCLUSION

A consecuencia de esta realidad que nos plantea la tecnología 802.11 de las redes inalámbricas WiFi, se pueden extraer los siguientes Riesgos y Conclusiones de **extremada importancia:**

- Constituyen una vía de penetración fácil a PC, PDA y redes empresariales, aún para hackers con escasos conocimientos. Rompen la seguridad perimetral, pues a través de los dispositivos inalámbricos WiFi, es muy sencillo "escalar" al corazón de los sistemas.

- Sirven de puerta de entrada de Virus Informáticos, Spyware, Keyloggers que además de infectar el perímetro, pueden robar información valiosa y contraseñas.

- Son uno de los puntos más débiles en los esquemas de seguridad modernos, donde los dispositivos WiFi como notebooks y PDA, crecen incesantemente.

- La redes 802.11 son como un arma de doble filo, por un lado está la parte buena:[/list]

  - Su ahorro en cableado

  - Su movilidad

  - Etcétera...

Pero por otro lado también son muy vulnerables (por ahora). Y por lo tanto se puede atentar fácilmente contra nuestra privacidad, a no ser que tengamos conocimientos elevados sobre redes.

- El mito "No tenemos redes inalámbricas WiFi, así que WiFi no es nuestro problema" queda totalmente desvirtuado. TODA ORGANIZACIÓN QUE TENGA DENTRO DE SUS PAREDES ALGÚN EQUIPO WIFI: NOTEBOOKS, PDA, PALM, ESTÁ EXPUESTO A ATAQUES INALÁMBRICOS.

Para acabar comentar, algunos puntos muy básicos que debemos tener en cuenta para proteger nuestra red:

- Activar el cifrado WEP, cuantos mayor longitud (mas bits) mejor, cambiarlo frecuentemente.
- Desactivar el broadcasting, emisión de frames de autenticación.
- Ocultar el ESSID y cambiar su nombre.(la longitud en este caso no importa)
- Activar ACL (filtrado de MACs)
- Desactivar el DHCP del Router y cambiar su pass de acceso, así como actualizar su firmware.

BIBLIOGRAFÍA

1. Eduardo Tabacman. *Seguridad en Redes Wireless*. En las memorias de la I Jornada de Telemática "Comunicaciones Inalámbricas, Computación Móvil". ACIS, Bogotá (Colombia), Noviembre 13 y 14 de 2003.

2. Dennis Fisher. *Study Exposes WLAN Security Risks*. Marzo 12 de 2003. http://www.eweek.com/ print_article/ 0,3048,a=38444,00.asp

3. Paul Congdon. *IEEE 802.1x Overview Port Based Network Access Control.* Marzo de 2000. http://www.ieee802.org/1/files/public/docs2000/ P8021XOverview.PDF

4. Suhdir Nath. *802.1x Overview.* Noviembre de 2003 http:// www.cisco.com/warp/public/732/ Tech/security/docs/ 8021xoverview.ppt

Referencias Web:

1. http://www.adslayuda.com/wag54g.html
2. http://www.taringa.net/posts/ebooks-tutoriales/2203519/como-crackear-cifrado-wep+seguridad-en-redes-wifi-en-windows.html
3. http://www.redestelecom.es/Firmas/200806020015/Localizacion-de-puntos-de-acceso-inalambrico-vulnerables.aspx

4. http://www.seguridaddigital.info/index.php?option=com_content&task=view&id=143&Itemid=26
5. http://www.adslnet.es/index.php/manuales-tutoriales-de-configuracion-del-router-linksys-wag354gcw/
6. http://www.virusprot.com/Whitepap1.html
7. http://www.canariaswireless.net/modules.php?name=News&file=article&sid=599
8. http://wiki.universidadlibre.org.ar/index.php?title="Wireless"
9. http://www.alertaenlinea.gov/topics/wireless-security.aspx
10. http://www.adslayuda.com/n1505-La-inseguridad-de-la-encriptacion-WEP-.html
11. http://www.slideshare.net/mark83/introduccin-a-la-seguridad-en-redes-inalmbricas
12. http://www.terra.es/personal/lureyc/redes/wifi.html
13. http://www.terra.es/personal/lureyc/redes/ejemplos.html
14. http://aircrack.red-inalambrica.net/descargar-aircrack-ng-windows-linux-y-zaurus
15. http://gabaon.bravehost.com/aircrack_doc_es.htm