Seguridad Wireless: Auditoria con CommView para Wi-Fi

Proyecto final de carrera

Titulación: Ingeniero Técnico en Informática de Sistemas

Autor: D. Benjamín Siale Ripeu

Director: Juan V. Oltra Gutiérrez

15 de Julio de 2011

Índice general

Índice de figuras

Capítulo 1

Introducción

En los últimos años, el despliegue de tecnologías inalámbricas ha tenido un crecimiento exponencial. El desarrollo de la sociedad de la información y la comunicación ha contribuido a ello. Entre las nuevas tecnologías desplegadas, sobresalen las comunicaciones mediante teléfonos móviles, ordenadores portátiles y otros dispositivos de comunicación inalámbrica. Una red Wi-Fi, al igual que ocurre con cualquier tipo de red inalámbrica, es una red en principio insegura puesto que el medio de transmisión es el aire y las señales viajan libres, de manera que cualquier individuo equipado con una antena de las características adecuadas podría recibir la señal y analizarla. Sin embargo, esa capacidad de recibir la señal no equivale a poder extraer la información que contiene, siempre y cuando se tomen las medidas oportunas, como el cifrado de la misma.Las tecnologías inalámbricas (Wireless, en inglés) han contribuido en gran manera a otro fenómeno que es la movilidad. Esta ha cambiado en el último par de años, sin que muchos lo perciban, la estructura y la topología de las redes empresariales. Los dispositivos de almacenamiento de información que antes eran fijos y estaban protegidos por las defensas perimetrales, ahora son móviles.PC portátiles, PDAs y teléfonos celulares portan, muchas veces, archivos con información confidencial de las organizaciones. A lo largo de este trabajo se verán las distintas características de las redes wi-Fi, así como conceptos generales sobre seguridad, medidas a tomar para tener una red inalámbrica más segura.

1.1. Objetivos

1.- Estudio del protocolo de comunicaciones wireless en redes de área local. El uso de redes Wi-Fi en entornos tanto domésticos como laborales ha estado aumentando durante estos últimos años hasta establecerse como un sistema de comunicaciones y acceso a Internet habitual para permitir la conexión a estaciones móviles o evitar el cableado. Debido a lo reciente de esta tecnología aún no recibe la debida atención a nivel académico, por lo que el estudio de dicha tecnología mejorará la formación del alumno como ingeniero en informática.

2.- Análisis del nivel de seguridad en redes Wi-Fi. Tanto a nivel teórico como práctico se realizará un estudio y análisis del nivel de seguridad de este tipo de redes, mostrando vulnerabilidades y ataques posibles en función de los distintos parámetros que se pueden ajustar en los routers wireless. Con esto se aprenderán las contramedidas que pueden ser aplicadas para mejorar la seguridad de las redes wireless.

3.- CommView para Wi-Fi . Bajo el SO Linux tenemos varios programas para la auditoria de las redes Wi-Fi tales como Backtack,wifislax,wifiway,etc. . . Que sirven para comprobar y de alguna manera fortalecer nuetras Wlan con los distintos comandos que integran suite como esta para windows:Commview.

4.-La facilidad de romper la seguridad de una red Wi-Fi. Mediante el uso de los programas adecuados y el conocimiento de ciertos comandos se verá lo facil que puede resultar romper la segurida de una red Wi-fi cifrada mediante claves WEP.

Capítulo 2

Redes Inalámbricas

2.1. Introduccion a las redes inalámbricas

Durante los últimos años han surgido y se han hecho con gran popularidad nuevas tecnologías inalámbricas como WIFI, WIMAX, GSM, Bluetooth, Infrarrojos, etc, siendo los dispositivos inalámbricos una de las grandes revoluciones tecnológicas de los últimos tiempos.
Las tecnologías inalámbricas o wireless, han conseguido esa popularidad gracias a la movilidad que permiten, llegando a cambiar la estructura y topología de las redes empresariales. Los dispositivos de almacenamiento de información que antes eran fijos ahora pueden ser portados y cambiar su conexión a distintas redes de una manera sencilla.

Es probable que en un futuro cercano todos los dispositivos que hoy utilizamos se unifiquen, pudiendo pasar a llamarse Terminales Internet, en los que se reunirían funciones de teléfono, agenda, reproductor multimedia, ordenador personal, etc.

Cada una de las tecnologías inalámbricas indicadas en el comienzo de este apartado tiene su ámbito de aplicación, sus ventajas y debilidades. A pesar de que nos centraremos en el estudio de las Redes Wi-Fi es conveniente conocer los distintos tipos de redes inalámbricas existentes en el cual se incluye la tecnología Wi-Fi. A continuación se muestra la clasificación de cada tipo de redes wireless.

Redes Inalámbricas Personales. Dentro de estas redes podemos integrar a dos principales actores: · Infrarrojos. Estas redes son muy limitadas dado su corto alcance, su necesidad de visión sin obstáculos entre los dispositivos que se comunican y su baja velocidad (hasta 115 Kbps). Se utilizan principalmente en ordenadores portátiles, PDAs, teléfonos móviles e impresoras. ·

Bluetooth. Es el estándar de comunicación entre pequeños dispositivos de uso personal, como PDAs o teléfonos móviles. Funciona en la banda de 2.4 GHz que no requiere licencia y tiene un alcance de entre 10 y 100 metros, según el dispositivo.

Redes Inalámbricas de Consumo.

También distinguimos dos tipos: · Redes CDMA y GSM. Son los estándares de telefonía móvil americano y europeo y asiático respectivamente. · WIMAX. Es una tecnología wireless que ha sido concebida y desarrollada para suministrar servicios de Banda Ancha en tramos de pocos kilómetros, como campus universitarios, urbanizaciones, etc. El rango típico de WIMAX es de 3 a 10 kilómetros, aunque puede alcanzar más de 40.

Redes Inalámbricas de Área Local.

Las WLAN, Redes Inalámbricas de Área Local, o Redes Wi-Fi serán el tipo de redes en el que se basa el presente proyecto, por lo tanto, a continuación se describirán detalladamente sus características, los elementos que las componen y su seguridad.

2.2. Redes Wi-Fi

Wi-Fi, es un conjunto de estándares para redes inalámbricas de área local (WLAN) basado en las especificaciones IEEE 802.11.
Fue creada por la Wi-Fi Alliance (anteriormente WECA, Wireless Ethernet Compability Alliance), la organización comercial que prueba y certifica que los equipos cumplen los estándares 802.11.

Figura 2.1: Simbolo Wi-Fi Alliance

su nombre no es un acrónimo de Wireless Fidelity, a pesar de que en sus comienzos se añadió junto con el nombre Wi-Fi la frase (The Standard for Wireless Fidelity) con el fin de dar significado al mismo, sino que fue creado como un juego de palabras relacionado con Hi-Fi (High

Fidelity). Resaltando sus principales características, se podría decir que las Redes Inalámbricas Wi-Fi son muy fáciles de adquirir, no tanto de configurar y muy difíciles de proteger.

2.2.1. WLAN vs LAN

La norma IEEE 802.11 fue diseñada para sustituir a las capas físicas y de enlace de las redes Ethernet (802.3) especificando su funcionamiento en redes WLAN (redes wireless de área local), por lo que las redes Wi-Fi y las Ethernet son idénticas salvo en el modo en el que los terminales acceden a la red, lo que supone compatibilidad entre ambas. Las principales diferencias entre las redes cableadas Ethernet y las redes inalámbricas Wi-Fi son:

Medio de transmisión. Mientras las redes cableadas utilizan un medio exclusivo como es el cable, las redes Wi-Fi utilizan el aire, un medio compartido.

Señalización. Ethernet utiliza señales eléctricas y Wi-Fi ondas de Radio Frecuencia.

Seguridad. Al utilizar cableado Ethernet "no permite", al menos tan fácilmente, que la información sea vista por extraños. Sin embargo con las redes inalámbricas la información puede ser capturada por cualquiera.

La comodidad conseguida gracias a la movilidad que ofrece la tecnología Wi-Fi, junto con la supresión del cableado son sin duda alguna los puntos fuertes de este tipo de redes. Sin embargo a su vez aparecen desventajas como la pérdida de velocidad en comparación con redes cableadas, debida a las interferencias y pérdidas de señal que el medio puede provocar.

Como se verá más adelante el principal problema que surge en las redes WLAN es la debilidad de su seguridad, ya que con las herramientas apropiadas en pocos minutos la contraseña de red se puede ver comprometida si no es correctamente protegida. Con el fin de solucionar este problemas la Wi-Fi Alliance hizo pública la clave WPA y posteriormente la WPA2, un nuevo tipo de clave mucho más robusta que las WEP, pero todo esto será explicado con más detenimiento en el apartado de seguridad.

2.2.2. IEEE 802.11

Las redes de área local inalámbricas (WLAN) son una alternativa a las redes de área local cableadas. Esta tecnología utiliza ondas electromagnéticas (radio o infrarrojos) para transmitir datos, eliminando la necesidad de cables. Sin embargo, WLAN presenta una serie de inconvenientes frente a las redes cableadas, como tener una tasa de transmisión menor y una interfaz radio con condiciones cambiantes, que pueden afectar a la transmisión de datos a través del medio inalámbrico (e.g. aumentando la probabilidad de error).
El estándar más utilizado de WLAN es IEEE 802.11, al que se le han ido añadiendo nuevos estándares (e.g. IEEE 802.11a/b/g/e/i) a éste, cuyos objetivos principales se exponen a continuación:

Aumento de la tasa de transmisión: las redes inalámbricas tienen un ancho de banda limitado y son más sensibles a factores ambientales o externos (obstáculos, interferencias) que las redes cableadas. Estos factores disminuyen la tasa de transmisión, de tal forma que se hace necesaria la inclusión de mecanismos que permitan la adaptación a las condiciones del canal.

Mejorar la seguridad: controlar el acceso al medio inalámbrico resulta más complicado que acceder al medio en las redes cableadas, ya que cualquier usuario con una tarjeta de red inalámbrica puede acceder a él. Por tanto, hay que dotar a las redes WLAN de mecanismos de seguridad para evitar que un usuario no autorizado pueda entrar a nuestra red.

Garantizar los requisitos de Qos: se tienen que cumplir los requisitos de QoS demandados por las aplicaciones. Como resultado, el tráfico será tratado de forma diferente según sus requisitos de calidad de servicio.

Controlar el acceso al medio: hay que gestionar el acceso al medio, de forma que los distintos usuarios conectados a la red lo puedan compartir de manera eficiente.

2.2.2.1. Componentes de IEEE 802.11

Como se puede observar en la figura 2.1, IEEE 802.11 tiene cuatro componentes principales:

1. Estaciones. Las estaciones (STAs) son dispositivos que actúan como origen y destino de los datos transmitidos. El objetivo de las redes inalámbricas es permitir la transmisión de datos entre estaciones. Como se verá posteriormente, para el caso de IEEE 802.11e las denominaremos QSTAs ya que soportan calidad de servicio.

2. Medio inalámbrico. El medio inalámbrico es el soporte que permite la transferencia de datos entre estaciones. El estándar permite dos tecnologías diferentes para la propagación de la señal, radiofrecuencia e infrarrojos, siendo ésta última la más utilizada

3. Punto de acceso. Un Punto de Acceso (AP) es una estación que permite conectar otras estaciones al sistema de distribución. Los puntos de acceso se sitúan de forma que puedan proporcionar la cobertura necesaria para dar servicio a los terminales que no tienen comunicación directa, aumentando su radio de cobertura. Además, el AP centraliza todas las comunicaciones entre STA, ya que, si dos estaciones quieren comunicarse entre sí, deben hacerlo a través del AP. Por tanto, el radio de cobertura de un AP limita la distancia a la cuál puede comunicarse una determinada estación. Sin embargo, es posible aumentar la cobertura de la red mediante un sistema de distribución, punto que se abordará a continuación.

4. Sistema de distribución. Un sistema de distribución está formado por varios puntos de acceso conectados entre sí mediante alguna tecnología, de forma que se pueda obtener un área de cobertura mayor. Los puntos de acceso deben comunicarse para gestionar la movilidad de las estaciones. La tecnología más habitual en los sistemas de distribución es Ethernet, aunque se pueden utilizar otras tecnologías, incluso el estándar IEEE 802.11 creando un Sistema de Distribución Inalámbrico (WDS). Cuando una estación móvil se mueve de una zona de cobertura de un AP a la de otro (roaming), se hace evitando los cortes en la comunicación y la pérdida de cobertura.

2.2.2.2. Protocolos IEEE 802.11

Desde 1997, cuando se certificó el primer estándar 802.11 con una velocidad de transferencia máxima de 2 Mbps, han ido surgiendo nuevos estándares que permiten velocidades cada vez mayores y con distintas bandas de frecuencias, alcanzando hoy en día hasta 300 Mbps. A continuación se describen los diferentes protocolos para redes Wi-Fi que han sido certificados como estándares desde la aparición del IEEE 802.11

802.11 legacy

Publicado en 1997, es la versión original del estándar IEEE 802.11. Permitía dos velocidades teóricas de transmisión, 1 y 2 Mbps, mediante señales infrarrojas en la banda ISM (Industrial, Scientific and Medical, de uso no comercial) a 2,4 GHz. Este estándar definía el protocolo CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) como método de acceso. Una parte importante de la velocidad de transmisión se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo que produjo dificultades de interoperabilidad entre equipos de diferentes marcas y rechazo entre los consumidores. En la actualidad no se fabrican productos sobre este estándar.

802.11a

Creado en 1997, no fue aprobado hasta 1999, cuando lo hizo junto con el 802.11b, y apareció en el mercado en productos en el 2001. Este estándar utiliza el mismo protocolo de base que el estándar original, pero opera en la banda de 5 GHz y utiliza 52 subportadoras OFDM (Orthogonal Frequency Division Multiplexing) con una velocidad máxima de 54 Mbps, lo que hace que sea un estándar práctico para redes inalámbricas con velocidades reales de unos 20 Mbps. No puede interoperar con equipos del estándar 802.11b, a menos que dicho equipo implemente ambos estándares. Un punto a favor para este protocolo es que al utilizar la banda de frecuencias de 5 GHz se presentan muchas menos interferencias, debido a que la banda de 2.4 GHz es utilizada por una gran cantidad de aparatos domésticos. Como contrapartida esta banda restringe el uso de los equipos a puntos en línea de vista, lo que requiere una instalación de un mayor número de puntos de acceso y a una cobertura menor. Algo que priori es negativo puede suponer una ventaja en instalaciones donde se desea que el rango de cobertura sea pequeño. Este protocolo conserva su velocidad máxima de 54 Mbps en un rango de 30 metros en el exterior y de 12

metros en el interior.

802.11b

Certificado en 1999, corrige las principales debilidades del estándar original y es el primer protocolo de la familia en ser aceptado por los consumidores. Permite una velocidad máxima de transmisión de 11 Mbps trabajando en la misma banda de frecuencia de 2.4 GHz. También utiliza el método de acceso CSMA/CA lo que reduce en la práctica la velocidad máxima de transmisión a 5.9 Mbps sobre TCP y a 7.1 Mbps sobre UDP.

802.11c

Es menos usado que los primeros dos, pero por la implementación que este protocolo refleja. El protocolo 'c' es utilizado para la comunicación de dos redes distintas o de diferentes tipos, así como puede ser tanto conectar dos edificios distantes el uno con el otro, así como conectar dos redes de diferente tipo a través de una conexión inalámbrica. El protocolo 'c' es más utilizado diariamente, debido al costo que implica las largas distancias de instalación con fibra óptica, que aunque más fidedigna, resulta más costosa tanto en instrumentos monetarios como en tiempo de instalación. "El estándar combinado 802.11c no ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos capa 2 del modelo OSI)".

802.11d

Es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.

802.11e

La especificación IEEE 802.11e ofrece un estándar inalámbrico que permite interoperar entre entornos públicos, de negocios y usuarios residenciales, con la capacidad añadida de resolver las necesidades de cada sector. A diferencia de otras iniciativas de conectividad sin cables, ésta puede considerarse como uno de los primeros estándares inalámbricos que permite trabajar en entornos domésticos y empresariales. La especificación añade, respecto de los estándares 802.11b y 802.11a, características QoS y de soporte multimedia, a la vez que mantiene compatibilidad

con ellos. Estas prestaciones resultan fundamentales para las redes domésticas y para que los operadores y proveedores de servicios conformen ofertas avanzadas. El documento que establece las directrices de QoS, aprobado el pasado mes de noviembre, define los primeros indicios sobre cómo será la especificación que aparecerá a finales de 2001. Incluye, asimismo, corrección de errores (FEC) y cubre las interfaces de adaptación de audio y vídeo con la finalidad de mejorar el control e integración en capas de aquellos mecanismos que se encarguen de gestionar redes de menor rango. El sistema de gestión centralizado integrado en QoS evita la colisión y cuellos de botella, mejorando la capacidad de entrega en tiempo crítico de las cargas. Estas directrices aún no han sido aprobadas. Con el estándar 802.11, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso: (EDCA) Enhanced Distributed Channel Access, equivalente a DCF. (HCCA) HCF Controlled Access, equivalente a PCF.

En este nuevo estándar se definen cuatro categorías de acceso al medio (Ordenadas de menos a más prioritarias).

Background(AC-BK) Best Effort(AC-BE) Video (AC-VI) Voice (AC-VO)

Para conseguir la diferenciación del tráfico se definen diferentes tiempos de acceso al medio y diferentes tamaños de la ventana de contención para cada una de las categorías.

802.11f

Es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el protocolo IAPP que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como itinerancia.

802.11g

En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Que es la evolución del estándar 802.11b, Este utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero

opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22.0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación que fue dada aprox. el 20 de junio del 2003. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas o equipos de radio apropiados.

Interacción de 802.11g y 802.11b.

802.11g tiene la ventaja de poder coexistir con los estándares 802.11a y 802.11b, esto debido a que puede operar con las Tecnologías RF DSSS y OFDM. Sin embargo, si se utiliza para implementar usuarios que trabajen con el estándar 802.11b, el rendimiento de la celda inalámbrica se verá afectado por ellos, permitiendo solo una velocidad de transmisión de 22 Mbps. Esta degradación se debe a que los clientes 802.11b no comprenden OFDM.

Suponiendo que se tiene un Access Point que trabaja con 802.11g, y actualmente se encuentran conectados un cliente con 802.11b y otro 802.11g, como el cliente 802.11b no comprende los mecanismos de envío de OFDM, el cual es utilizados por 802.11g, se presentarán colisiones, lo cual hará que la información sea reenviada, degradando aún más nuestro ancho de banda.

Suponiendo que el cliente 802.11b no se encuentra conectado actualmente, el Access Point envía tramas que brindan información acerca del Access Point y la celda inalámbrica. Sin el cliente 802.11b, en las tramas se verían la siguiente información:

NON-ERP present: no

Use Protection: no

ERP (Extended Rate Physical), esto hace referencia a dispositivos que utilizan tasas de transferencia de datos extendidos, en otras palabras, NON-ERP hace referencia a 802.11b. Si fueran ERP, soportarían las altas tasas de transferencia que soportan 802.11g.

Cuando un cliente 802.11b se asocia con el AP (Access Point), éste último alerta al resto

de la red acerca de la presencia de un cliente NON-ERP. Cambiando sus tramas de la siguiente forma:

NON-ERP present: yes

Use Protection: yes

Ahora que la celda inalámbrica sabe acerca del cliente 802.11b, la forma en la que se envía la información dentro de la celda cambia. Ahora cuando un cliente 802.11g quiere enviar una trama, debe advertir primero al cliente 802.11b enviándole un mensaje RTS (Request to Send) a una velocidad de 802.11b para que el cliente 802.11b pueda comprenderlo. El mensaje RTS es enviado en forma de unicast. El receptor 802.11b responde con un mensaje CTS (Clear to Send).

Ahora que el canal está libre para enviar, el cliente 802.11g realiza el envío de su información a velocidades según su estándar. El cliente 802.11b percibe la información enviada por el cliente 802.11g como ruido.

La intervención de un cliente 802.11b en una red de tipo 802.11g, no se limita solamente a la celda del Access Point en la que se encuentra conectado, si se encuentra trabajando en un ambiente con múltiples AP en Roaming, los AP en los que no se encuentra conectado el cliente 802.11b se transmitirán entre sí tramas con la siguiente información:

NON-ERP present: no

Use Protection: yes

La trama anterior les dice que hay un cliente NON-ERP conectado en uno de los AP, sin embargo, al tenerse habilitado Roaming, es posible que éste cliente 802.11b se conecte en alguno de ellos en cualquier momento, por lo cual deben utilizar los mecanismo de seguridad en toda la red inalámbrica, degradando de esta forma el rendimiento de toda la celda. Es por esto que los clientes deben conectarse preferentemente utilizando el estándar 802.11g. Wi-Fi (802.11b / g)

802.11h

Aparece en 2003 como una modificación del 802.11a con el fin de resolver los problemas derivados de la coexistencia de las redes Wi-Fi con sistemas de radares y satélites, debido a que la banda de 5 GHz era utilizada generalmente por sistemas militares. Este nuevo protocolo proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión mediante las siguientes funcionalidades:

DFS (Dynamic Frequency Selection): Permite evitar interferencias con sistemas de radar y ase-

gurar una utilización uniforme de los canales disponibles.

TPC (Transmitter Power Control): Asegura que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite. **802.11i**

Este protocolo está dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación, abarcando los protocolos 802.1x, TKIP (Protocolo de Claves Integra-Seguras-Temporales), y AES (Estándar de Cifrado Avanzado).

802.11j

Es equivalente al 802.11h, en la regulación Japonesa

802.11k

Permite a los conmutadores y puntos de acceso inalámbricos calcular y valorar los recursos de radiofrecuencia de los clientes de una red WLAN, mejorando así su gestión. Está diseñado para ser implementado en software, para soportarlo el equipamiento WLAN sólo requiere ser actualizado. Y, como es lógico, para que el estándar sea efectivo, han de ser compatibles tanto los clientes (adaptadores y tarjetas WLAN) como la infraestructura (puntos de acceso y conmutadores WLAN).

802.11n

En enero de 2004, el IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y unas 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO Multiple Input-Multiple Output, que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas (3). Existen también otras propuestas alternativas que podrán ser consideradas. El estándar ya está redactado, y se viene implantando desde 2008. A principios de 2007 se aprobó el segundo boceto del estándar. Anteriormente ya había dispositivos adelantados al protocolo y que ofrecían de forma no oficial este estándar (con la promesa de actualizaciones para cumplir el estándar cuando el definitivo estuviera implantado). Ha sufrido

una serie de retrasos y el último lo lleva hasta noviembre de 2009. Habiéndose aprobado en enero de 2009 el proyecto 7.0 y que va por buen camino para cumplir las fechas señaladas.[2] A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

El estándar 802.11n fue ratificado por la organización IEEE el 11 de septiembre de 2009 con una velocidad de 600 Mbps en capa física.

802.11p

Este estándar opera en el espectro de frecuencias de 5.9 GHz, especialmente indicado para automóviles. Será la base de las comunicaciones dedicadas de corto alcance (DSRC) en Norteamérica. La tecnología DSRC permitirá el intercambio de datos entre vehículos y entre automóviles e infraestructuras en carretera.

802.11r

También se conoce como Fast Basic Service Set Transition, y su principal característica es permitir a la red que establezca los protocolos de seguridad que identifican a un dispositivo en el nuevo punto de acceso antes de que abandone el actual y se pase a él. Esta función, que una vez enunciada parece obvia e indispensable en un sistema de datos inalámbricos, permite que la transición entre nodos demore menos de 50 milisegundos. Un lapso de tiempo de esa magnitud es lo suficientemente corto como para mantener una comunicación vía VoIP sin que haya cortes perceptibles.

802.11s

Define la interoperabilidad de fabricantes en cuanto a protocolos Mesh (son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas, la topología Ad-hoc y la topología infraestructura.). Bien es sabido que no existe un estándar, y que por eso cada fabricante tiene sus propios mecanismos de generación de mallas.

802.11v

IEEE 802.11v servirá para permitir la configuración remota de los dispositivos cliente. Esto permitirá una gestión de las estaciones de forma centralizada (similar a una red celular) o distribuida, a través de un mecanismo de capa 2. Esto incluye, por ejemplo, la capacidad de la red para supervisar, configurar y actualizar las estaciones cliente. Además de la mejora de la gestión, las nuevas capacidades proporcionadas por el 11v se desglosan en cuatro categorías: mecanismos de ahorro de energía con dispositivos de mano VoIP Wi-Fi en mente; posicionamiento, para proporcionar nuevos servicios dependientes de la ubicación; temporización, para soportar aplicaciones que requieren un calibrado muy preciso; y coexistencia, que reúne mecanismos para reducir la interferencia entre diferentes tecnologías en un mismo dispositivo.

802.11w

Todavía no concluido. TGw está trabajando en mejorar la capa del control de acceso del medio de IEEE 802.11 para aumentar la seguridad de los protocolos de autenticación y codificación. Las LANs inalámbricas envía la información del sistema en tramas desprotegidos, que los hace vulnerables. Este estándar podrá proteger las redes contra la interrupción causada por los sistemas malévolos que crean peticiones desasociadas que parecen ser enviadas por el equipo válido. Se intenta extender la protección que aporta el estándar 802.11i más allá de los datos hasta las tramas de gestión, responsables de las principales operaciones de una red. Estas extensiones tendrán interacciones con IEEE 802.11r e IEEE 802.11u.

802.11y

Este estandar Publicado en noviembre de 2008, y permite operar en la banda de 3650 a 3700 MHz (excepto cuando pueda interferir con una estación terrestre de comunicaciones por satélite) en EEUU, aunque otras bandas en diferentes dominios reguladores también se están estudiando. Las normas FCC para la banda de 3650 MHz permiten que las estaciones registradas operen a una potencia mucho mayor que en las tradicionales bandas ISM (hasta 20 W PIRE). Otros tres conceptos se añaden: Contention Base Protocol (CBP), Extended Channel Switch Announcement (ECSA), y Dependent Station Enablement (DSE). CBP incluye mejoras en los mecanismos de detección de portadora. ECSA proporciona un mecanismo para que los puntos de acceso (APs) notifiquen a las estaciones conectadas a él de su intención de cambiar de canal o ancho de banda. Por último, la DSE se utiliza para la gestión de licencias.

Protocolo propietario:802.11G+ o Super G

Super G es una tecnología propietaria de la empresa Atheros que mejora el rendimiento de las redes WLAN IEEE 802.11g mediante técnicas de compresión y unión de interfaces de red (Channel Bonding). El Throughput límite en la velocidad de transmisión al usar Super G puede estar entre los 40 Mbit/s y los 60 Mbit/s con una tasa de señalización de 108 Mbit/s, lo cual se consigue uniendo dos canales 802.11g de 54 Mbit/s.

Otros proveedores anuncian sus productos Super G como Tecnología 108G, 108 Mbit/s 802.11g, y Xtreme G. Entre los fabricantes que han licenciado la tecnología Super G de Atheros se encuentran Airlink 101, Clipsal, D-Link, Intelbras, Netgear, Nortel Networks, Planex, SMC, Sony, TRENDnet, SparkLAN, Toshiba y ZyXEL. En general, los productos Super G de distintos proveedores son interoperables en modo Super G.

Este tipo de extensiones 802.11g no estándar de unión de interfaces de red, como Super G, han recibido muchas críticas por crear interferencias en todos los canales Wi-Fi, provocando problemas potencialmente a otros dispositivos inalámbricos en la misma banda, como redes inalámbricas cercanas, teléfonos inalámbricos, monitores para bebé y dispositivos Bluetooth. Sin embargo, Atheros afirma que en escenarios reales con separaciones físicas y muros, no se experimentarán interferencias entre redes cercanas y redes Super G.

Super G es uno de los muchos enfoques desarrollados para incrementar el rendimiento de los dispositivos inalámbricos 802.11g, como el Modo de Alta Velocidad 125 de Broadcom, extensiones basadas en MIMO de Airgo Networks, y Nitro de Conexant.

Atheros también ha adoptado esta tecnología a sus chipsets 802.11a/g, anunciándolo como Super AG.

2.3. Dispositivos

2.3.1. AP/WAP-Puntos de Acceso Wireless

Los puntos de acceso en redes Wi-Fi son los elementos que interconectan los distintos dispositivos de comunicación inalámbrica para formar una red wireless. Habitualmente estos dispositivos pueden conectarse a redes cableadas, permitiendo intercambiar información entre dispositivos cableados y wireless. De la misma manera, distintos puntos de acceso pueden ser conectados permitiendo realizar roaming. Son los encargados de crear la red, permaneciendo a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada. Estos dispositivos tienen direcciones IP asignadas, para poder ser configurados. Desde un único punto de acceso se puede dar soporte a un grupo de usuarios y trabajar en un rango desde unos 30 a varios cientos de metros, siempre en función de las antenas utilizadas. Los Puntos de Acceso pueden ser agrupados en dos categorías: Puntos de Acceso Robustos. Son bastante inteligentes e incorporan funciones adicionales de gestión y seguridad, como Firewall, Site Survey o no emitir el ESSID (algo que se comentará más adelante). Además son más costosos y complicados de gestionar y suelen sobrecargar el tráfico. En algunos casos disponen de slots libres para futuras actualizaciones. Puntos de Acceso Básicos. Son más económicos y sencillos de gestionar y configurar, además suele ser más sencillo compatibilizarlos con otras marcas.

Figura 2.2: Punto de Acceso

2.3.2. Routers

Los routers reciben la señal de la línea que ofrezca el operador de telefonía y se encargan de todos los problemas relacionados a la recepción de la señal, como el control de errores y la extracción de la información, para que los diferentes niveles de red puedan trabajar. Los routers trabajan de manera conjunta con los puntos de acceso wireless, funcionando estos últimos a modo de emisor remoto, es decir, en lugares donde la señal wifi del router no tenga suficiente radio. Otros dispositivos como hubs o switches también pueden encargarse de la distribución de la señal, pero no pueden encargarse de las tareas de recepción. Hoy en día la mayoría de los Puntos de Acceso incluyen las funcionalidades de los Routers, por lo que estos se están viendo sustituidos.

Figura 2.3: Router

2.3.3. Tipos de tarjetas Wi-Fi

Son los dispositivos encargados de la recepción de información en estaciones de redes Wi-Fi. Una de las principales características que las diferencian entre sí es el tipo de interfaz que utilizan, es decir, el puerto de conexión de la tarjeta. A continuación se describen los diferentes tipos de tarjetas en función de la interfaz que utilizan:

PCI:

Peripherial Component Interconnect, bus de interconexión de componentes periféricos, que conecta directamente a la placa base de la computadora dispositivos periféricos (bus local). Permite configurar el dispositivo de manera dinámica y suele ser utilizado en ordenadores de sobremesa. Habitualmente suele disponer de conectores para antenas.

Mini PCI:

Este tipo de tarjetas posee características semejantes a las PCI, pero su tamaño es mucho menor, se utiliza en portátiles y no dispone de conectores para antenas.

PCMCIA:

Personal Computer Memory Card Internacional Association, es un dispositivo utilizado habitualmente en portátiles, la mayoría de estas tarjetas solo son capaces de llegar a la tecnología 802.11b, no permitiendo disfrutar de una velocidad de transmisión demasiado elevada. Las tarjetas PCMCIA también reciben el nombre de PC Card si son de 16 bits o CARD BUS si son de 32 de bits.

USB:

Universal Serial Bus, provee un estándar de serie para conectar dispositivos a un PC. Hoy en día el USB se ha convertido en el método de conexión más usado, debido a su dinamismo, desplazando otros estándares de conexión. Las tarjetas wireless USB son fáciles de instalar, sin embargo, en algunos casos no son tan potentes como las anteriores, esto es en cuanto a velocidad, encriptación o alcance. Pueden ser utilizadas tanto en portátiles como en PCs de sobremesa, y además existe una gran variedad de modelos que implementan los distintos protocolos 802.11, incluso algunos todavía no estandarizados.

CENTRINO:

Centrino Mobile Technology es una iniciativa de Intel para promocionar una combinación prestablecida de CPU, chipset de la placa base e interfaz de red inalámbrica en el diseño de ordenadores personales portátiles. La interfaz de red es del tipo Intel PRO/Wireless 2100 (802.11b) o PRO/-Wireless 2200 (802.11g). Todo lo mencionado correspondía simplemente al tipo de interfaz que utiliza la tarjeta Wi-Fi, sin embargo a la hora de considerar una tarjeta wireless, sobre todo para la tarea de auditorías, es conocer el chipset y los drivers que utiliza, que no tienen porque ser desarrollados por la compañía que ha fabricado la tarjeta Wi-Fi.

Figura 2.4: Tarjeta Wi-Fi

2.3.4. Tipos de antenas

Habitualmente las placas de red inalámbricas disponen de antenas incorporadas diseñadas para un uso en interiores y con un rango de alcance bastante reducido. Para un proceso de auditoría o para cubrir mayores superficies, como pueden ser edificios o vecindarios resultaría conveniente utilizar antenas especializadas. Las características de una antena pueden ser clasificadas, además de por su alcance, según su:

Patrón de radiación:

Omnidireccionales: Cubren áreas grandes, intentando que la radiación sea pareja en 360º. Bidireccionales: Buenas para pasillos y corredores dado que radia o recibe la mayoría de la energía en dos direcciones. Unidireccionales o Direccionales: Son las más apropiadas en conexiones punto a punto o para clientes de una antena omnidireccional.

Ganancia:

Es el cociente entre la intensidad de campo producida por la antena y la intensidad de campo que produciría en el mismo punto un radiador isotópico que absorbiera del emisor la misma potencia de RF. La ganancia de las antenas se mide en dBi. Considerando estas dos características, a continuación se describen los distintos tipos de antenas existentes:

Vertical:

Es una antena omnidireccional con ganancias que van desde los 3 dBi hasta los 17 dBi. Por ser omnidireccionales son antenas buenas en la radiación en plano horizontal.

Yagi:

La antena Yagi es una antena direccional inventada por el Dr. Hidetsugu Yagi de la Universidad Imperial de Tohoku y su ayudante, el Dr. Shintaro Uda (de ahí al nombre Yagi-Uda). Esta invención de avanzada a las antenas convencionales, produjo que mediante una estructura simple de dipolo, combinado con elementos parásitos, conocidos como reflector y directores, logró construir una antena de muy alto rendimiento.

Es un tipo de antena unidireccional de alta ganancia. Se asemeja a una antena clásica de TV, las Yagis pueden alcanzar ganancias de entre 12 y 18 dBi y son más fáciles de apuntar que las antenas parábolicas.

Parabólica:

Las antenas parabólicas tienen una ganancia muy alta, de hasta 27 dBi en antenas comerciales Wi-Fi, pero debido a que la radiación que propaga o puede recibir es muy estrecha no es apropiada para usuarios que no ven directamente la antena. Al igual que las Yagi, las antenas parabólicas son más apropiadas para conexiones punto a punto, como conexiones entre edificios, o para utilizarlas conjuntamente con antenas verticales de alta ganancia.

2.3.5. Modos de funcionamiento

Los dispositivos encargados de la comunicación Wi-Fi, Puntos de Acceso o Tarjetas de Red, pueden utilizar diferentes tipos de funcionamiento:

Modo Managed. Modo en el que las Tarjetas Wi-Fi se conectan al AP para que éste último le sirva de concentrador. La Tarjeta de Red sólo se comunicará con el Punto de Acceso.

Modo Master. Es el modo de funcionamiento del Punto de Acceso, pero las Tarjetas de Red también pueden entrar en este modo si disponen del firmware apropiado o si están conectadas a una máquina que se puede encargar de realizar la funcionalidad requerida.

Modo Ad-Hoc. Los dispositivos utilizan este método cuando la red a la que pertenecen es de topología Ad-Hoc, que será descrita a continuación, por lo que se deben preparar para recibir y enviar paquetes a todos los miembros de la red.

Modo Monitor. También denominado RFMON, con este modo el dispositivo es capaz de capturar todo el tráfico que circula por la red, incluso los paquetes que no van dirigidos hacia él, es decir el firmware de la tarjeta pasa cualquier paquete recibido al controlador software. Como se verá más adelante, este modo es el utilizado por los atacantes para vulnerar la seguridad de los protocolos de cifrado de la red.

Modo Repeater. El dispositivo reenvía los paquetes recibidos de otros nodos inalámbricos.

Modo Secondary. Utilizado como backup de otro dispositivo que funciona en modo Master o Repeater.

Modo Auto. Con este modo el dispositivo se configura de manera automática, empezando por Ad-Hoc y siguiendo en Manager.

2.3.6. Tipos de topologias

Con topología nos referimos a la disposición lógica de los dispositivos, aunque la disposición física también puede verse influida. En las redes Wireless existen los siguientes tipos de topologías:

Topología Ad-Hoc

Cada dispositivo se puede comunicar con todos los demás, es decir, cada nodo forma parte de una red Peer to Peer, de igual a igual, formando una especie de red de grupos de trabajo. A más dispersión geográfica de cada nodo más dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre sí, pero un gran número de dispositivos conectados a la red pueden hacer que el rendimiento se vea reducido.

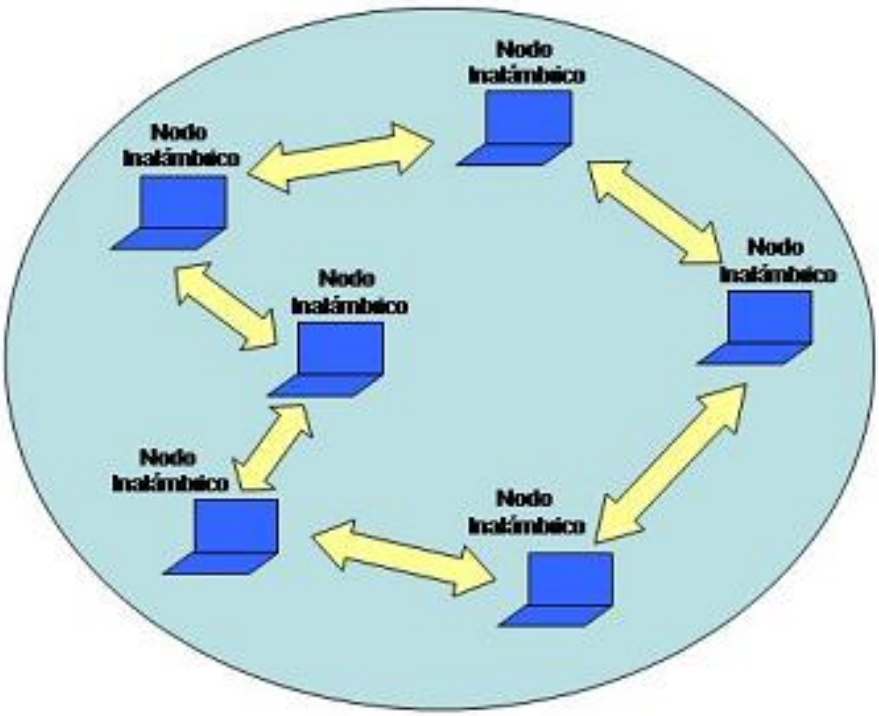


Figura 2.5: Topologia Ad-hoc

Topología Infraestructura

Contrario al modo ad hoc donde no hay un elemento central, en el modo de infraestructura hay un elemento de "coordinación": un punto de acceso o estación base. Si el punto de acceso se conecta a una red Ethernet cableada, los clientes inalámbricos pueden acceder a la red fija a través del punto de acceso. Para interconectar muchos puntos de acceso y clientes inalámbricos, todos deben configurarse con el mismo SSID.

Esta solución ofrece la conexión entre redes con hilos e inalámbricas. Está especialmente indicada para incorporar a una red con cables equipos con conexión inalámbrica, permitiendo la ampliación de la red. Es importante resaltar que, a diferencia del modo ad-hoc, los equipos inalámbricos no hablan directamente entre sí, sino que lo hacen a través de la unidad base, lo que ofrece más seguridad (gracias a la gestión ofrecida por la unidad base) y conectividad con los terminales situados en la red con cables.

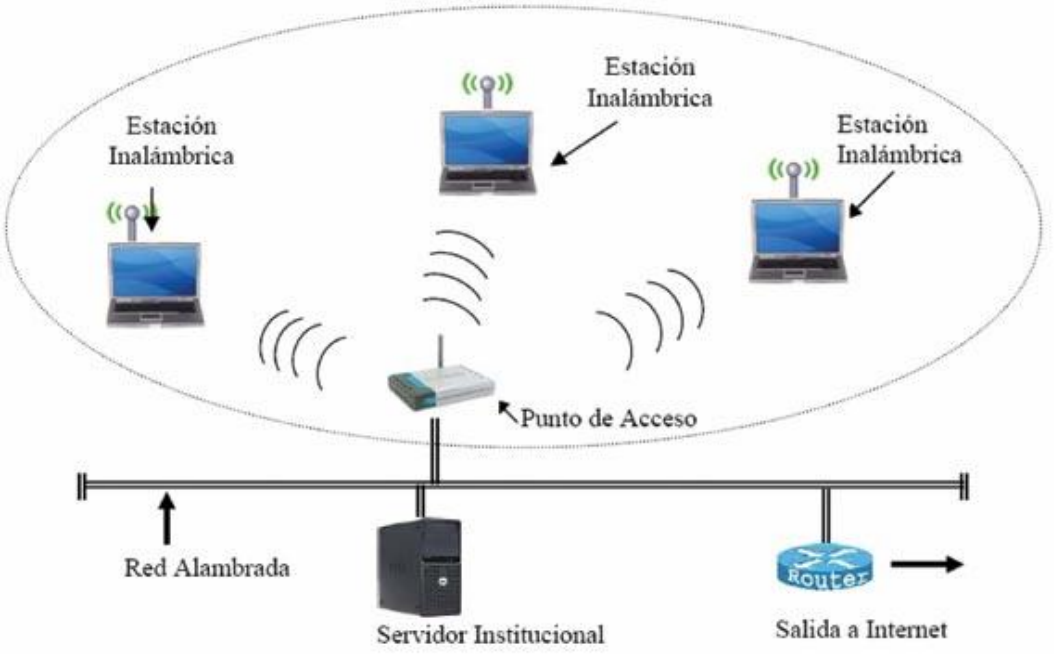


Figura 2.6: Topologia Infraestructura

Topología Mesh

Las redes Mesh, o redes acopladas, son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas. Básicamente son redes con topología de infraestructura, pero que permiten unirse a la red a dispositivos que están fuera del rango de cobertura del Punto de Acceso pero dentro del de algún dispositivo móvil asociado a la red.

También permiten la comunicación entre los dispositivos móviles independientemente del Punto de Acceso. Para hacer esto posible un protocolo de enrutamiento se encarga de transmitir la información hasta su destino con el mínimo número de saltos.

Figura 2.7: Topología Mesh

2.4. Transmisión de la información

2.4.1. Tipos de paquetes

La información en las redes Wi-Fi es transmitida por RF, Radio Frecuencias, a través del aire, en forma de paquetes. El estándar IEE 802.11 define distintos tipos de paquetes con diversas funciones. Hay 3 tipos diferentes de paquetes que pasaremos a analizar de manera breve a continuación.

2.4.1.1. Paquetes de Management

Establecen y mantiene la comunicación.

Association Request. Incluye información necesaria para que el Punto de Acceso considere la posibilidad de conexión. Uno de los datos principales es el ESSID o nombre de la red inalámbrica al que se intenta conectar.

Association Response. Paquete enviado por el AP avisando de la aceptación o denegación de la petición de conexión. Beacon. Los Puntos de Acceso Wi-Fi envían paquetes periódicamente para anunciar su presencia y que todas las estaciones que estén en el rango de cobertura sepan que el AP está disponible. Estos paquetes se denominan "Beacons" y contienen varios parámetros, entre ellos el ESSID del Punto de Acceso.

Probe Request. Lo envían las estaciones para buscar redes Wi-Fi de forma activa, ya que se indicarán tanto el ESSID como la frecuencia de dichas redes.

Probe Response. Son paquetes de respuesta ante los Probe Request, enviados por el AP, confirmando o rechazando transacciones.

Authentication. Paquete por el que el Punto de Acceso acepta o rechaza a la estación que pide conectarse. Como se verá en el apartado de seguridad existen redes WiFi abiertas donde no se requiere autenticación y otras protegidas donde se intercambian varios paquetes de autenticación con desafíos y respuestas para verificar la identidad del cliente.

Desauthentication. Lo envía el Punto de Acceso para eliminar una autenticación existente.

Disassociation. Es enviado por una estación cuando desea terminar la conexión, de esta manera el AP sabe que puede disponer de los recursos que había asignado a esta estación.

2.4.2. Calidad de la señal

Las ondas de RF transmitidas por las redes WiFi son atenuadas e interferidas por diversos obstáculos y ruidos. Lo que se transmite es energía, y esta es absorbida y reducida. A medida que nos alejemos del Punto de Acceso la calidad de la señal se verá atenuada debido a la presencia de paredes o a las transmisiones de otros dispositivos. Las velocidades teóricas de los distintos estándares, en la práctica, son mucho menores, pues la velocidad de transmisión de una red inalámbrica Wi-Fi, será función de la distancia, los obstáculos y las interferencias, que pueden depender del tipo de construcción del edificio, micro-ondas, teléfonos inalámbricos, dispositivos Bluetooth, elementos metálicos, peceras , humedad del ambiente, etc., que se encuentren en el radio de acción del dispositivo Wi- Fi.

Como se comentó en el apartado de estándares 802.11, estos factores afectan a los estándares que actúan en la banda de 2.4 GHz. El 802.11a que actúa en la banda de 5 GHz evita gran cantidad de interferencias, pues no es utilizada prácticamente por ningún dispositivo inalámbrico doméstico.

Además las velocidades se verán afectadas por un hecho básico: Los usuarios de un Punto de Acceso deben compartir el ancho de banda, es decir, a mayor número de usuarios menor será el ancho de banda disponible para cada uno.

Un método para aumentar la capacidad de una Red Wi-Fi, es el uso de celdas, siendo una celda el área que cubre la señal de un AP, de tamaño reducido de manera conjunta, es decir, utilizar simultáneamente múltiples micro-celdas, consiguiendo así mejorar la calidad de la señal para los usuario de la red. Este concepto se desarrolla más profundamente a continuación.

2.5. Seguridad en Redes WiFi

Las redes wireless, a diferencia de las redes cableadas, poseen un punto débil en seguridad en el medio utilizado para la transmisión. Mientras las redes Ethernet utilizan un medio privado como el cable, las redes inalámbricas utilizan el aire, un medio compartido y altamente inseguro. Como se verá en los próximos capítulos el hecho de no disponer de redes WiFi en una organización, o tenerlas bien aseguradas, no tiene por que suponer que el sistema sea seguro, ya que con que exista algún dispositivo Wi-Fi, como portátiles con tarjetas de red inalámbricas, el sistema se torna vulnerable y frágil. Es decir, el peligro no reside realmente en las propias redes, sino en la tecnología Wi-Fi.

A lo largo de los siguientes puntos se describirán más profundamente las posibles medidas de seguridad y ataques con el fin de que el lector sea consciente del nivel de seguridad e inseguridad a la que puede estar sometida una red Wi-fi.

Los tres aspectos fundamentales que se deben tener en cuenta al diferenciar una red WiFi de una cableada, son:

Autenticación y control de acceso.

Los métodos que se emplean son los siguientes:

a. SSID (Service Set Identifier): Contraseña (WEP: Wired equivalent Protocol).

b. Seguridad por restricción de direccionamiento MAC (Múmero de seis octetos que identifca univocamente a la tarjeta):

c. Contraseñas no estáticas: -Periódicas: -OTP (One Time Password): Contraseñas de un solo uso, conocidas como token flexibles.

d. 802.1x: Este estándar no fue presentado para WiFi, sino para el acceso seguro PPP. Se trata del método más seguro actualmente. La arquitectura 802.1x está compuesta por tres partes: Solicitante: Generalmente se trata del cliente WiFi Auenticador: Suele ser el AP (Punto de acceso), que actúa como mero traspaso de datos y como bloqueo hasta que se autoriza su acceso (importante esto último). Servidor de autenticación: Suele ser un Servidor RADIUS (Remote Authentication Dial In User Service) o Kerberos, que intercambiará el nombre y credencial de cada usuario. El almacenamiento de las mismas puede ser local o remoto en otro servidor de LDAP, de base de datos o directorio activo. Otra de las grandes ventajas de emplear 802.1x es que el servidor de autenticación, permite también generar claves de cifrado OTP muy robustas, tema en particular que ya lo posiciona como imprescindible en una red WiFi que se precie de

segura.

e. 802.11i (esto en realidad aplica también a confidencialidad): El Task Group de IEEE 802.11i se conformó en el año 2001 con la intención de analizar una arquitectura de seguridad más robusta y escalable, debido a la inminente demanda del mercado en este tema y en julio de 2004 aprobó este estándar. Por su parte la WiFi Alliance lo lanzó al mercado en septiembre de ese año.

En forma resumida, este nuevo estándar, propone a 802.1x como protocolo de autenticación, pudiendo trabajar con su referencia EAP (Extensible Authentication Protocol: RFC 2284), este último proporciona una gran flexibilidad (sobre todo a los fabricantes) en la metodología de autenticación.

Previo al estándar, varios fabricantes ofrecieron métodos de autenticación: LEAP, PEAP, EAP/TLS, EAP/TTLS. Lo importante es el grado de flexibilidad que el estándar 802.11i ofrece hacia los mismos, pues soporta a la mayoría de ellos.

Cifrado.

a. WEP: Protocolo extremadamente débil y actualmente en desuso.

b. Las deficiencias de WEP, se están tratando de solucionar en la actividad de cifrado, a través del protocolo TKIP (Temporal Key Integrity Protocol). Esta propuesta aparece a finales de 2002 y propone tres mejoras importantes:

- Combinación de clave por paquete: Generando trillones de claves diferentes, una para cada paquete. -VI (Vector de inicialización) de 48 bits: Este tema era una de las mayores debilidades de WEP al emplear sólo 24 bits.

- MIC (Message Integrity Check): Se plantea para evitar el conocido ataque inductivo o de hombre del medio. Y propone descartar todo mensaje que no sea validado.

c. Microsoft ofrece otra alternativa que inicialmente denominó SSN (Simple Security Network), el cual es una implementación de TKIP al estilo Microsoft. SSN lo adoptó 802.11i renombrándolo como WPA (WiFi Protected Access), en el año 2004 aparece WPA2 que es la segunda generación del WPA . Este ya proporciona encriptación con un fuerte algoritmo llamado AES (Norma de Encriptación Avanzada) y está contemplado en IEEE 802.11i . En realidad 802.11i propone un “Mix” de funciones criptográficas cuyo eje central es AES, y lo bautiza como CCMP, su nombre completo proviene el “Counter mode” (CTR) que habilita la encriptación de datos y el Cipher Block Chaining Message Authentication Code (CBCMAC) para proveer integridad, y de ahí su extraña sigla CCMP. La mayoría de los fabricantes están migrando hacia

este algoritmo y se aprecia que será el estándar que se impondrá en el muy corto plazo.

VPNs.

La última opción que se menciona aquí es la aplicación de VPNs. Esta alternativa no responde a ningún estándar de WiFi, pero se trata de llevar al wireless toda la experiencia y solidez que tiene hoy esta tecnología. Existen muchos tipos de VPNs, que es una opción muy válida y de hecho se está implementado cada vez con mayor frecuencia en las opciones de wireless.

2.6. Protocolos de Seguridad

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal.

Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior. El canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos).

Las mismas precauciones que tenemos para enviar datos a través de Internet deben tenerse también para las redes inalámbricas. Conscientes de este problema, el IEEE publicó un mecanismo opcional de seguridad, denominado WEP, en la norma de redes inalámbricas 802.11. Pero WEP, desplegado en numerosas redes WLAN, ha sido roto de distintas formas, lo que lo ha convertido en una protección inservible. Para solucionar sus deficiencias, el IEEE comenzó el desarrollo de una nueva norma de seguridad, conocida como 802.11i, que permitiera dotar de suficiente seguridad a las redes WLAN. La idea de proteger los datos de usuarios remotos conectados desde Internet a la red corporativa se extendió, en algunos entornos, a las redes WLAN No ajena a las necesidades de los usuarios, la asociación de empresas Wi-Fi decidió lanzar un mecanismo de seguridad intermedio, el resultado, en 2003, fue WPA. Analizaremos las características de los mecanismos de seguridad WEP, WPA y WPA2.

2.6.1. WEP

Características y funcionamiento.

WEP (Wired Equivalent Privacy, privacidad equivalente al cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN. Estudiamos a continuación las principales características de WEP. WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso.

El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

El algoritmo de encriptación utilizado es RC4 con claves (seed), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente.

El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante. El algoritmo de encriptación de WEP es el siguiente: Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, Integrity Check Value).

El PRNG (Pseudo-Random Number Generator) de RC4 genera una secuencia de caracteres pseudoaleatorios (keystream), a partir del seed, de la misma longitud que los bits obtenidos en el punto 1. Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (frame body) de la trama IEEE 802.11.
El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV y la clave secreta, tendrá entonces el seed y con ello podrá generar el keystream. Realizando el XOR entre los datos recibidos y el keystream se obtendrá el mensaje sin cifrar (datos y CRC-32). A continuación se comprobara que el CRC-32 es correcto.

Debilidad del vector de inicialización.

La implementación del vector de inicialización (IV) en el algoritmo WEP tiene varios problemas de seguridad. Recordemos que el IV es la parte que varía de la clave (seed) para impedir que un posible atacante recopile suficiente información cifrada con una misma clave.

Sin embargo, el estándar 802.11 no especifica cómo manejar el IV. Según se indica que debería cambiarse en cada trama para mejorar la privacidad, pero no obliga a ello. Queda abierta a los fabricantes la cuestión de cómo variar el IV en sus productos. La consecuencia de esto es que buena parte de las implementaciones optan por una solución sencilla: cada vez que arranca la tarjeta de red, se fija el IV a 0 y se incrementa en 1 para cada trama. Y esto ocasiona que las primeras combinaciones de IVs y clave secreta se repitan muy frecuentemente. Más aún si tenemos en cuenta que cada estación utiliza la misma clave secreta, por lo que las tramas con igual clave se multiplican en el medio.

Por otro lado, el número de IVs diferentes no es demasiado elevado (16 millones aprox.), por lo que terminarán repitiéndose en cuestión de minutos u horas. El tiempo será menor cuanto mayor sea la carga de la red. Lo ideal sería que el IV no se repitiese nunca, pero como vemos, esto es imposible en WEP. La cantidad de veces que se repite un mismo IV dependerá de la implementación elegida para variar el IV por el fabricante (secuencial, aleatoria, etc.) y de la carga de la red. Observemos que es trivial saber si dos tramas han sido cifradas con la misma clave, puesto que el IV se envía sin cifrar y la clave secreta es estática. La longitud de 24 bits para el IV forma parte del estándar y no puede cambiarse. Bien es cierto que existen implementaciones con claves de 128 bits (lo que se conoce como WEP2), sin embargo, en realidad lo único que

se aumenta es la clave secreta (104 bits) pero el IV se conserva con 24 bits. El aumento de la longitud de la clave secreta no soluciona la debilidad del IV.

¿Qué podemos hacer una vez hemos capturado varias tramas con igual IV, es decir, con igual keystream? Necesitamos conocer el mensaje sin cifrar de una de ellas. Haciendo el XOR entre un mensaje sin cifrar y el mismo cifrado, nos dará el keystream para ese IV. Conociendo el keystream asociado a un IV, podremos descifrar todas las tramas que usen el mismo IV. El problema es entonces conocer un mensaje sin cifrar, aunque esto no es tan complicado, porque existen tráficos predecibles o bien, podemos provocarlos nosotros (mensajes ICMP de solicitud y respuesta de eco, confirmaciones de TCP, etc.) .

Con lo que hemos descrito no podemos deducir la clave secreta, aunque sí es posible generar una tabla con los IVs de los que sabemos su keystream, la cual permitirá descifrar cualquier mensaje que tenga un IV contenido en la tabla.

Sin embargo, podemos llegar a más y deducir la clave secreta. Una nueva vulnerabilidad del protocolo WEP permite deducir la clave total conociendo parte de la clave (justamente, el IV que es conocido). Para ello necesitamos recopilar suficientes IVs y sus keystreams asociados obtenidos por el procedimiento anterior.

Otras debilidades de WEP.

WEP también adolece de otros problemas además de los relacionados con el vector de inicialización y la forma de utilizar el algoritmo RC4.

Entre los objetivos de WEP, como comentamos más arriba, se encuentra proporcionar un mecanismo que garantice la integridad de los mensajes. Con este fin, WEP incluye un CRC-32 que viaja cifrado. Sin embargo, se ha demostrado que este mecanismo no es válido y es posible modificar una parte del mensaje y a su vez el CRC, sin necesidad de conocer el resto. Esto permitiría, por ejemplo, modificar algún número de la trama sin que el destino se percatara de ello. En lugar del algoritmo de CRC se recomienda como ICV (Integrity Check Value) un algoritmo diseñado para tal fin como SHA1-HMAC.

El estándar IEEE 802.11 incluye un mecanismo de autentificación de las estaciones basado en un secreto compartido. Para ello se utiliza la misma contraseña de WEP en la forma que describimos a continuación. Una estación que quiere unirse a una red, solicita al punto de acceso autentificación. El punto de acceso envía un texto en claro a la estación y ésta lo cifra y se lo devuelve. El punto de acceso finalmente descifra el mensaje recibido, comprueba que su ICV es correcto y lo compara con el texto que envió.

El mecanismo anterior de autentificación de secreto compartido tiene el problema de enviar por la red el mismo texto sin cifrar y cifrado con la clave WEP (esta clave coincide con la utilizada para asegurar la confidencialidad). El estándar es consciente de esta debilidad y aconseja no utilizar el mismo IV para el resto de transmisiones. Sin embargo, tanto si las implementaciones repiten ese IV como sino, el mecanismo ofrece información que podría ser aprovechada para romper la clave WEP utilizando las debilidades del vector de inicialización explicadas más arriba.

WEP no incluye autentificación de usuarios. Lo más que incluye es la autentificación de estaciones descrita (podrán entrar aquellas estaciones que en su configuración tengan almacenada la clave WEP). El sistema de autentificación descrito es tan débil que el mejor consejo sería no utilizarlo para no ofrecer información extra a un posible atacante. En este caso tendríamos una autentificación de sistema abierto, es decir, sin autentificación.

Entre la larga lista de problemas de seguridad de WEP se encuentra también la ausencia de mecanismos de protección contra mensajes repetidos (replay). Esto permite que se capture un mensaje y se introduzca en la red en un momento posterior. El paquete podría ser, por ejemplo, el que contiene la contraseña de un usuario para utilizar un determinado servicio.

Todos los problemas comentados unidos a las características propias de WEP como es la distribución manual de claves y la utilización de claves simétricas, hacen que este sistema no sea apropiado para asegurar una red inalámbrica. El estudio de N. Borisov, I. Goldberg y D. Wagner explica razonadamente que ninguno de los objetivos planteados por WEP se cumplen.

Alternativas a WEP.

Las vulnerabilidades explicadas de WEP son motivos más que suficientes para utilizar otros mecanismos de seguridad en redes WLAN.

Aunque no forma parte del estándar, los fabricantes de productos Wi-Fi decidieron ofrecer la posibilidad de utilizar claves del doble de longitud (de 64 bits a 128 bits). WEP utilizado con claves de 128 bits es lo que se conoce generalmente como WEP2. Sin embargo, debemos observar que la longitud del vector de inicialización sigue siendo de 24 bits (las tramas IEEE 802.11 no contemplan un mayor número de bits para enviar el IV), por lo que lo único que se ha aumentado es la clave secreta (de 40 bits a 104 bits). Debido a que la longitud del IV y su forma de utilizarlo no varían, las debilidades del IV pueden seguir siendo aprovechadas de la misma manera. WEP2 no resuelve los problemas de WEP.

Otra variante de WEP utilizada en algunas implementaciones es WEP dinámico. En este caso se busca incorporar mecanismos de distribución automática de claves y de autentificación de usuarios mediante 802.1x/EAP/RADIUS. Requiere un servidor de autentificación (RADIUS normalmente) funcionando en la red. En el caso de que la misma clave (clave secreta + WEP) no se utilice en más de una trama, este mecanismo sería suficiente para compensar las principales debilidades de WEP.

Sin embargo, la solución preferida por las empresas como alternativa a WEP ha sido la utilización de VPNs, de la misma manera que se haría si los usuarios estuviesen conectados remotamente a la oficina. La tecnología de VPNs está suficiente probada y se considera segura, aunque no ha sido diseñada específicamente para redes WLAN. Tiene como inconveniente la falta de interoperatibilidad entre dispositivos de distintos fabricantes.

2.6.2. WAP

WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar. WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible.

Características de WPA.

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación. WPA incluye las siguientes tecnologías:

IEEE 802.1X. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las ramas de un switch, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS (Remote Authentication Dial-In User Service). Si la autorización es positiva, entonces el punto de acceso abre el puerto.

El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).

EAP.Definido en la RFC 2284, es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad.

EAP fue diseñado originalmente para el protocolo PPP (Point-to-Point Protocol), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP over LAN) [10]. TKIP (Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama. MIC (Message Integrity Code) o Michael. Código que verifica la integridad de los datos de las tramas.

Mejoras de WPA respecto a WEP.

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados.

El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (replay). Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

WPA puede funcionar en dos modos:

Con servidor AAA, RADIUS normalmente.

Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.

Con clave inicial compartida (PSK).

Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

2.6.3. WAP2

WPA2 (Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2) es un sistema para proteger las redes inalámbricas (WI-FI); creado para corregir las vulnerabilidades detectadas en WPA.

WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.El estándar 802.11i fue ratificado en junio de 2004. La alianza WI-FI llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise.

Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2. "WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público.

Los productos que son certificados para WPA2 le dan a los gerentes de TI la seguridad que la tecnología cumple con estándares de interoperatividad" declaró Frank Hazlik Managing Director de la Wi-Fi Alliance. Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i.

Arquitectura WPA/WPA2 PSK

Tanto WPA-PSK como WPA2-PSK adolecen de vulnerabilidad y es posible atacar estas tecnologías con el objetivo de poder hacer uso de la red e incluso escuchar y analizar el tráfico que por ella se propaga. En este articulo se pretenden reflejar por qué y dónde es vulnerable WPA-PSK y WPA2-PSK, cómo explotar esta vulnerabilidad y cómo proteger adecuadamente la red.

Para entender las vulnerabilidades hemos primero de analizar el proceso de asociación de un cliente a la red wireless. Independientemente del sistema de seguridad que se elija para la red (WEP, WPA-PSK o WPA2-PSK), el proceso de asociación es siempre el mismo. Este proceso va a depender de si el punto de acceso está emitiendo tramas "Beacon Frame" para el anuncio de la red mediante la publicación de su ESSID [Extended Service Set Indentifier] o no.

Si el punto de acceso está emitiendo tramas "Beacon frame" el cliente se conecta a la red en dos fases, una primera Fase de Autenticación, que podrá ser abierta o con clave compartida, y una segunda Fase de Asociación.

En el supuesto caso de que el punto de acceso no esté emitiendo "Beacon frames" existe una Fase de Prueba inicial dónde el cliente envía el ESSID de la red wireless a la que quiere conectarse esperando que el punto de acceso responda y así iniciar las fases de Autenticación y Asociación. Todo este proceso, para una conexión WPA2-PSK puede verse en la imagen siguiente. En ella se pueden ver las tres fases descritas. La única diferencia con una red Abierta o WEP, es que punto de acceso y cliente acuerdan la política de seguridad a seguir, siendo ésta la primera fase del proceso de autenticación de una red WPA/WPA2.

Esta forma de funcionar es importante conocerla, pues como puede verse en al imagen, el cliente se conecta inicialmente a la red sin que haya comenzado el proceso de autenticación WPA/WPA2, tanto si es por medio de PSK como si no, por lo que el tráfico enviado todavía no está siendo cifrado. Debido a esta situación un atacante podría mandar una trama de des-asociación a un cliente de la red provocando que éste se desasocie e inicie un proceso de asociación nuevamente y un nuevo proceso de autenticación WPA/WPA2. A esto se le conoce como el ataque 0 o de des-asociación.

Este proceso de re-autenticación se realizaría únicamente si la conexión se tratase de WPA/WPA2 empresarial, es decir, la conexión está configurada utilizando 802.1x para la autenticación del puerto y EAP [Extended Authetication Protocol] contra un servidor RADIUS [Remote Authentication Dial-In Service] para autenticar la conexión. En el caso de WPA/WPA2 con PSK se pasa directamente a la fase de intercambio de claves.

En la fase de Intercambio de claves el cliente y el AP utilizan la PSK para generar un clave llamada PMK [Pairwise Master Key]. Esta PMK es una derivada cuando el sistema es WPA/WPA2 empresarial pero es la misma PSK en los entornos WPA/WPA2 PSK.

Con la PMK se genera una clave de cifrado para cada proceso de autenticación de un cliente llamada PTK que básicamente se genera a partir de dos números aleatorios, uno de ellos generado por el cliente y el otro por el punto de acceso que intercambian para obtener ambos la misma clave PTK. Este proceso se llama 4-way-Handshake.

Una vez que el cliente está autenticado, el protocolo TKIP utiliza 6 claves de cifrado por cada sesión, 4 de ellas son utilizadas para comunicaciones unicast y 2 para comunicaciones broadcast. Estas claves son únicas por cliente y sesión y se cambian periódicamente. Estas claves se generan a partir de derivadas de las direcciones MAC, ESSID y la PTK.

2.7. Medidas de Seguridad

2.7.1. ACL-Filtro de Direcciones MAC

La dirección MAC (Media Access Control) es un número que identifica las interfaces físicas de los dispositivos que pueden establecer comunicaciones, esto es, tanto Tarjetas de Red como Puntos de Acceso, Routers, etc, suministrados por el fabricante.

El método ACL, Access Control List, consiste en suministrar a cada Punto de Acceso Wi-Fi un listado con las direcciones MAC de los equipos que están autorizados a conectarse a la red. De esta manera los equipos que no figuren en esta lista serán rechazados.

Es uno de los métodos de protección de Redes Wi-Fi más primitivos y menos eficaces que existen debido a una gran cantidad vulnerabilidades y desventajas:
Incomodidad producida y amenaza de errores debido a la configuración manual de cada Punto de Acceso. Al tener que teclear en cada AP las direcciones permitidas aumenta la carga de trabajo de los administradores y un error en la introducción de una dirección puede hacer que usuarios que deberían ser aceptados se rechacen. Además el listado de direcciones permitidas deberá ser actualizado en todos los Puntos de Acceso de la red cada vez que se que quiera dar de alta o de baja a un usuario, algo realmente incómodo en organizaciones con varios Puntos de Acceso.

Facilidad de detección de direcciones MAC permitidas. Al enviarse la dirección MAC sin encriptar en una gran cantidad de paquetes, esta puede ser capturada por un atacante y reemplazar la suya por una permitida en el Punto de Acceso de una manera muy sencilla, quedando toda la seguridad del sistema comprometida.

Seguridad basada en autenticación de dispositivos. El método no autentica al usuario, sino al dispositivo, por lo que en caso de que este caiga en manos de un usuario "no admitido" podrá pasar el control del filtro.

Por todo esto el método de Filtrado de Direcciones MAC no soluciona los problemas de seguridad en Redes Wi-Fi, pero puede ser utilizado como método adicional, según las condiciones

del sistema donde se implante, es decir, cuando la red no esté formada por múltiples Puntos de Acceso y se produzcan pocas variaciones en las listas de direcciones permitidas.

2.7.2. Deshabilitado del Servidor DHCP

El Punto de Acceso puede asignar las direcciones dinámicamente a todos los clientes que se conecten, pero si deshabilitamos esta opción y permitimos el acceso sólo a determinadas direcciones IP, un extraño que se asocie al AP y no disponga de los parámetros de configuración correctos, como dirección IP, dirección de la puerta de enlace, etc., tendrá una conectividad a la red nula.
Esta medida es semejante a la de filtrado de direcciones MAC, con la diferencia de que las direcciones IP pueden ser enviadas cifradas, con lo que el atacante encontrará más problemas a la hora de acceder a la red.

2.7.3. CNAC-Ocultamiento del ESSID

El ESSID (Extended Service Set IDentifier) es un código formado por un máximo de 32 caracteres alfanuméricos incluido en todos los paquetes de una Red Wi-Fi para identificarlos como parte de esa red, a menudo conocido simplemente como nombre de la red.

El método CNAC, Closed Network Access Control, de los más básicos para la protección de una red inalámbrica, está basado en desactivar el broadcast del ESSID en las tramas beacon utilizadas para que las estaciones detecten los Puntos de Acceso, por lo que impide que los dispositivos que no conocen el ESSID puedan asociarse a la red.

El primer paso para atacar una red es detectar la misma, con esta medida de protección un usuario "medio" no podrá detectar nuestra red, sin embargo es una técnica de protección que al igual que las anteriores debe ser utilizada como una medida adicional al uso de otras, ya que con las herramientas apropiadas el ESSID puede ser descubierto de manera sencilla.

2.7.4. VPN-Redes Privadas Virtuales

Las Redes Privadas Virtuales permiten proteger las comunicaciones creando un túnel criptográfico entre los dos extremos, realizando una encriptación mediante el protocolo IPSec de la IETF, un método de encriptación robusto y muy difícil de comprometer.

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. A pesar de que WEP se puede utilizar de manera conjunta con VPN, es algo opcional, pues no añade seguridad adicional a IPSec.

A pesar de la seguridad añadida a las redes inalámbricas, este método tiene algunas ventajas. La principal es la económica, ya que cada túnel tiene un costo, por lo que en redes con una gran cantidad de usuarios las VPN se convierten en una solución extremadamente costosa. Otra gran desventaja es que las VPN han sido diseñadas para conexiones punto a punto y las Redes Wi-Fi transmiten ondas de Radio Frecuencia por un medio compartido, como es el aire. Las VPN protegen a partir de la capa 3 del modelo OSI, pero las Redes Wi-Fi funcionan en la capa 2.

En definitiva, esta es una medida de protección que fue utilizada durante un tiempo para solventar los problemas de seguridad del protocolo WEP, pero con la aparición de los nuevos protocolos WPA y WPA2 las VPN en Redes Wi-Fi cayeron en desuso.

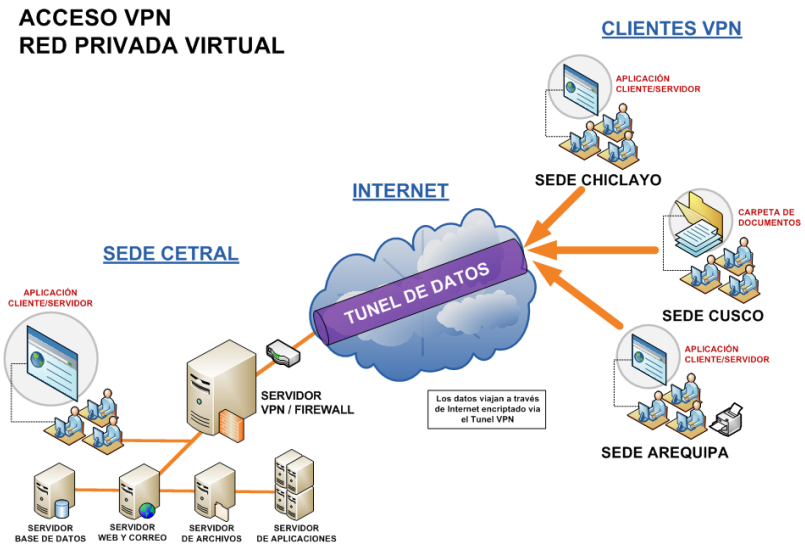


Figura 2.8: Red privada virtual

2.7.5. Mecanismos de Autenticación básicos

OSA (Open System Authentication)

Es el mecanismo de autenticación definido por el estándar 802.11 y consiste en autenticar todas las peticiones que reciben. El principal problema de este mecanismo es que no realiza ninguna comprobación y, además, todas las tramas de gestión son enviadas sin ningún tipo de cifrado, incluso cuando se ha activado WEP.

SKA (Open Shared Key Authentication)

Es el método mediante el cual ambos dispositivos disponen de la misma clave de encriptación. El dispositivo móvil pide al AP autenticarse, éste último le envía una trama y si se la devuelve correctamente codificada, le permite la asociación.

Autenticación de Usuarios-802.1x

Antes de que apareciese el estándar de seguridad 802.11i con la encriptación WPA y WPA2, el IEEE buscaba soluciones que fueran capaces de mejorar la pobre seguridad ofrecida por el protocolo WEP. Una de estas soluciones fue adaptar el estándar 802.1x que había sido aprobado en 2001 para redes cableadas, siendo aprobado para redes inalámbricas Wi-Fi en 2004.
Anteriormente, en la descripción de los protocolos WPA y WPA2, se hizo referencia a este estándar de seguridad, que se basa en el control de acceso a puertos y constituye la columna vertebral de la Seguridad Wi-Fi, siendo imprescindible en redes donde se desee lograr una seguridad robusta.

802.1x introduce importantes cambios en el esquema existente de la seguridad en estas redes. En otros métodos, como el filtrado de Direcciones MAC, antes comentado, la autenticación se realizaba sobre el dispositivo. Con 802.1x esto cambia y la autenticación se realiza sobre el usuario. Este cambio es realmente importante porque impide el acceso a usuarios no permitidos, no a dispositivos no permitidos, solucionando los problemas que se plantearon en el apartado de Filtro de Direcciones MAC, como la suplantación de direcciones o la pérdida de dispositivos.
El otro gran cambio introducido es, que con 802.1x, el Punto de Acceso no es el encargado de autorizar los accesos a la red, esta función recae sobre un servidor de tipo RADIUS, mediante un protocolo conocido como EAP (Extensible Authentication Protocol).

En 802.1x el puerto no se abre, no permitiendo la conexión, hasta que el usuario esté autenticado. Este proceso de autenticación se realiza mediante 3 elementos:

Servidor de Autenticación.

Generalmente es un servidor RADIUS, y se encarga de verificar las credenciales de los usuarios.

Autenticador.

Es el dispositivo que recibe la información del usuario y se la traslada al Servidor de Autenticación, es decir, el Punto de Acceso.

Suplicante.

Es una aplicación cliente que suministra la información de las credenciales del usuario al Autenticador. Con el fin de poder comprender el funcionamiento de esta medida de seguridad, a continuación, se describirán de manera más extensa qué son los servidores RADIUS, el protocolo EAP y el funcionamiento de las aplicaciones suplicantes.

Servidor RADIUS

RADIUS, Remote Authentication Dial In User Service, es un servidor que tiene la función de autenticar a los usuarios que se conectan remotamente. Originalmente estaba pensado para ser usado con redes cableadas, pero fue adaptado como herramienta de autenticación para Redes Wi-Fi cuando se modificó el estándar 802.1x.

Los Servidores RADIUS se encargan de gestionar la seguridad de las Redes WLAN casi por completo, recibiendo las peticiones de conexión y autenticando y autorizando el acceso a los usuarios WiFi, devolviendo además la información necesaria para que el cliente pueda asociarse a la red, entre ellas la clave. Además puede generar claves dinámicas, es decir, puede cambiarlas cada un cierto tiempo, determinado por el administrador, mitigando así significativamente las deficiencias del protocolo de encriptación WEP. Los servidores más completos incluyen otra función adicional, el "Accounting", denominándose "AAA" o "Triple A" (Autenticación, Autorización y Accounting).

Otra ventaja añadida por los Servidores RADIUS es que, a diferencia de las VPN, protegen la capa 2 del modelo OSI, la utilizada por las redes 802.11, pues cifran el canal antes que el usuario sea autenticado y reciba su IP. Las VPN necesitaban una dirección IP para poder autenticar al usuario.

Protocolo EAP

Para robustecer la seguridad wifi, el protocolo EAP, Extensible Authentication Protocol, se utiliza en la autenticación de usuarios. De este protocolo existen diferentes versiones, lo que supone complicaciones, pues cada una tiene sus limitaciones y, cada una soporta diferentes plataformas. Esto obliga el encargado de la seguridad de la Red Wi-Fi, a analizar detenidamente que protocolo EAP se va a utilizar para autenticar con el RADIUS-802.1x. Como punto en común, todos los protocolos EAP, requieren la existencia de un certificado digital en el servidor RADIUS para asegurar que nos estamos conectando a nuestra red.

protocolos EAP existentes:

EAP-LEAP. Desarrollado y patentado por Cisco. Una de sus limitaciones consiste en el requerimiento de infraestructura Cisco y un Servidor RADIUS "LEAP aware", es decir, no sirve cualquier servidor RADIUS. Además, se desaconseja su utilización debido a una vulnerabilidad, descubierta en 2003, explotable mediante ataque de diccionario.

EAP-TLS. Desarrollado por Microsoft. Un requisito, visto por muchos como un inconveniente, es que requiere un Certificado Digital en cada dispositivo cliente. Sin embargo, esto no resulta un inconveniente para organizaciones que ya tengan implantado un sistema de PKI (Infraestructura de Clave Pública). Otra limitación es que sólo soporta bases de datos de Microsoft, como Active Directory, y no soporta ni SQL ni LDAP.

EAP-TTLS. Desarrollado por programadores independientes, con la idea de crear un protocolo EAP flexible. Su principal ventaja es su funcionamiento con cualquier plataforma y Sistema Operativo, siendo además compatible con otros EAP y múltiples bases de datos como SQL y LDAP.

EAP-PEAP. Proyecto conjunto de Cisco, Microsoft y RCA, desarrollado para poder suministrar un protocolo más flexible que los dos primeros. Es muy similar al EAP-TTLS y existen dos versiones, una de Cisco y otra de Microsoft, muy similares pero no iguales.

EAP-FAST. Creado también por Cisco. Existen dos versiones de este protocolo, una sencilla con una seguridad no muy robusta, y otra muy similar a los otros EAP. EAP-FAST es compatible con EAP-LEAP y soporta Active Directory y LDAP.

2.8. Políticas de Seguridad

Sólo mediante tecnología no se puede garantizar un nivel de seguridad alto, ya que los usuarios de la Red Wi-Fi pueden comprometerla conectándose a Puntos de Acceso que no pertenecen a la red y facilitar información confidencial a extraños. Ataques de este tipo se verán a continuación, de la misma manera que se podrá comprobar la debilidad de la mayoría de medidas de seguridad que han sido descritas a lo largo de este capítulo. Por lo tanto, se hace necesario para completar un sistema de seguridad que existan ciertas políticas y guías de buenas prácticas, así como ciertos conocimientos sobre seguridad por parte de los usuarios.

El NIST, Nacional Institute of Standards and Technology, entre las principales recomendaciones que se incluyen en uno de sus documentos sobre la implementación de Redes Wi-Fi en las dependencias del gobierno de USA, hay una que aconseja desarrollar políticas de seguridad para wireless antes de comprar los equipos. Esta recomendación, en la práctica, casi nunca es llevada a cabo, la mayoría de organizaciones en primer lugar compran los dispositivos wireless y más tarde, cuando aparecen los problemas, deciden establecer políticas que regulen y controlen la utilización de las Redes Wi-Fi.

Las políticas que se deben establecer para la utilización de Redes Wi-Fi se deben referir básicamente al uso de los recursos wifi cuando los empleados se encuentran fuera de la organización, como podrán utilizar dichos recursos tanto los empleados de la organización como usuarios externos a la organización o el control de modificaciones en la topología de la red.
Algunas de las políticas más relevantes que se aconsejan establecer en organizaciones son:

Verificar que los usuarios están debidamente entrenados en el uso de tecnología Wi-Fi y conocen los riesgos asociados a su utilización
Cambiar el ESSID por defecto
Desactivar la opción de broadcast del ESSID, uso del método de protección CNAC.

Verificar que en el ESSID no contiene datos de la organización que podrían ser utilizados por un atacante.
Desarrollar una política de instalación de actualizaciones y parches en Puntos de Acceso y clientes de la red.
Desarrollar una política de contraseñas para Puntos de Acceso y clientes.
Desarrollar una política de configuración de los Puntos de Acceso.
Desarrollar una política de autenticación de usuarios.
Realizar auditorías periódicas sobre los Puntos de Acceso para comprobar que los parámetros de configuración no han sido modificados.
Realizar auditorías periódicas sobre el Sistema de Seguridad de la Red.

Como se indicaba en el primer punto, es necesario que los usuarios de la red sepan cómo hacer un buen uso de las Redes Inalámbricas Wi-Fi. Con usuarios bien formados se podrán algunos de los ataques, que se describirán en el próximo apartado, como el Wi-Phishing y los problemas con Hotspots y Puntos de Acceso Hostiles.

La experiencia demuestra que gracias a una formación básica de los empleados en cuanto a la seguridad de sus sistemas se pueden reducir notablemente los riesgos que acechan a las Redes Wi-Fi. El proceso de formación de los empleados puede ser realizado en la misma empresa o enviando a los empleados que se desea formar a cursos externos.

Lo importante es que dentro de la política de seguridad se asegure que los usuarios de la red disponen de los conocimientos necesarios para poder hacer un buen uso de la misma. Con esta rentable inversión se puede mejorar la seguridad incluso más que con el uso de herramientas tecnológicas.

2.9. Vulnerabilidades en las Redes Wi-Fi

Ningún tipo de red es totalmente intocable, incluso las redes con cable sufren de distintos tipos de vulnerabilidades. Las redes inalámbricas son aún más vulnerables que las redes con cables, debido a la propagación de la señal en todas direcciones.

Ataques más comunes en redes inalámbricas

Wardriving y warchalking.

En los comienzos de Wi-Fi se generó una práctica en los países anglo-sajones que consistía en marcar unos símbolos con tiza donde se detectaban redes con esta tecnología, con la finalidad de que otros pudieran hacer uso de las mismas gratuitamente. A esta práctica se la conoce como Warchalking.

Dentro del Warchalking existe un lenguaje de símbolos para poder describir las características de la red existente, diferenciando entre redes abiertas o cerradas, el ESSID o nombre de la red, la tecnología utilizada, el ancho de banda, el tipo de cifrado, etc., como vemos en la imagen.

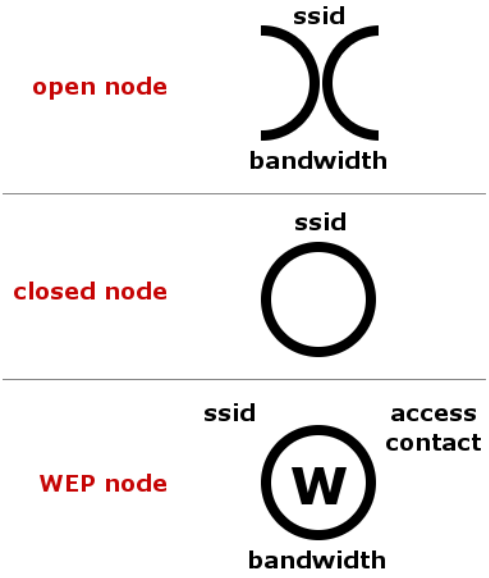


Figura 2.9: Simbolos Warchalking

Access Point Spoofing.

Access Point Spoofing o .ªsociación Maliciosa": en este caso el atacante se hace pasar por un access point y el cliente piensa estar conectándose a una red WLAN verdadera. Ataque común en redes ad-hoc.

ARP Poisoning.

ARP Poisoning o "Envenenamiento ARP", ataque al protocolo ARP (Address Resolution Protocol) como el caso de ataque denominado "Man in the Midle" o "hombre en medio". Una computadora invasora X envía un paquete de ARP reply para Y diciendo que la dirección IP de la computadora Z apunta hacia la dirección MAC de la computadora X, y de la misma forma envía un paquete de ARP reply para la computadora Z diciendo que la dirección IP de la computadora Y apunta hacia la dirección MAC de X.

Como el protocolo ARP no guarda los estados, las computadoras Y y Z asumen que enviaron un paquete de ARP request solicitando esta información, y asumen los paquetes como verdaderos. A partir de este punto, todos los paquetes enviados y recibidos entre las computadoras Y y Z pasan por X (hombre en medio).

DoS-Ataques de Denegación de Servicio

Denial of Service o "Negativa de Servicio", también conocido por D.O.S. Consiste en negar algún tipo de recurso o servicio. Puede ser utilizado para ïnundar"la red con pedidos de disociación, imposibilitando así el acceso de los usuarios, pues los componentes de la red se asocian y desasocian una y otra vez. Al rechazar algún servicio, también puede dar origen a interferencias por equipamientos de Bluetooth, hornos de microondas y teléfonos inalámbricos, debido a que estos equipamientos trabajan en la misma franja de frecuencia que las redes inalámbricas.

MITM-Man In The Middle

El atacante con este método consigue ubicarse entre el AP y el dispositivo Wi- Fi cliente, de esta manera consigue controlar la comunicación entre el cliente y el AP. Realizando este tipo de ataque el hacker podrá modificar o alterar la información que se está transmitiendo a través suyo, con el fin de engañar al receptor, transmitir la información sin ningún cambio, de manera que nadie se de cuenta de su presencia y pueda conocer el contenido de la conversación, o bloquear la transmisión de manera que la información nunca llegue al receptor.

Para llevar a cabo este ataque, en primer lugar, se deberá localizar la red objetivo y conseguir información sobre la misma, tanto del Punto de Acceso como de los clientes. Además se necesitará un Punto de Acceso Wi-Fi que suplantará al AP original y una estación con una Tarjeta de Red Wi-Fi que suplantará al cliente objetivo. Existe software que emula Puntos de Acceso en un PC, lo que resultaría suficiente para realizar el ataque si se dispone de un tarjeta de red.
Una vez está todo dispuesto, el atacante deberá conseguir que el cliente objetivo se asocie a su Punto de Acceso pensando que es el auténtico y, además, asociarse al AP original con el cliente falso. Una vez conseguido esto, el atacante podrá participar en las actividades de la Red Wi-Fi pues ante el Punto de Acceso será un cliente legítimo.

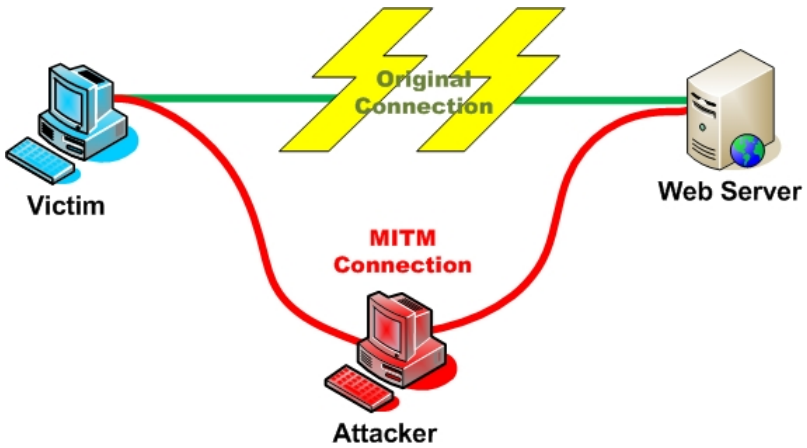


Figura 2.10: Ataque Man in the middle

Session Hijacking

El ataque de "Secuestro de Sesión", esta basado en desautenticar a un usuario que está asociado a la red y reemplazarlo.

El modo de operación, como en todos los ataques, comienza detectando y seleccionado la red objetivo y monitorizándola para obtener información como ESSID, direcciones MAC, etc. A continuación se realiza un ataque de Denegación de Servicio contra el cliente seleccionado para ser suplantado, consiguiendo así que sea desautenticado.

Con la información que había obtenido, el atacante procede a conectarse a la red en reemplazo del usuario expulsado, suplantándolo. El usuario legítimo intentará conectarse, pero el AP no se lo permitirá, pues ya existirá un cliente con sus características conectado. Evidentemente este ataque se realizará cuando el Punto de Acceso utiliza mecanismos o listas de autenticación.

Una vez conectado, el atacante debe actuar rápidamente para evitar sospechas, pues el cliente al notar que no se puede conectar a la red notará que algo no va bien, pudiendo dejar un backdoor en el sistema de seguridad de la red para poder volver a acceder posteriormente. Una vez hecho esto el atacante se deberá retirar permitiendo al cliente volver a conectarse.

Si el tiempo que el atacante quiere dejar desconectado al usuario auténtico de la red no es suficiente para completar posteriores ataques, que requieren que esté asociado a la red, podrá repetir el proceso de suplantación sobre otros clientes evitando así sospechas.

Al ser un ataque que habitualmente dura muy poco tiempo, resulta muy complicado para el administrador de la red detectar el ataque, sobretodo si no se cuenta con herramientas específicas como los ya comentados Switches WLAN.

2.10. Herramientas de auditorias Wi-Fi

Suite del Aircrack-ng.

Realmente no solo es un programa, sino un conjunto completo, muy fáciles de utilizar. Es una de las mejores herramientas para analizar el nivel de seguridad de nuestras instalaciones wireless ya que suele ser el arma mas utilizada por la mayoría de personas que quieren reducir nuestro ancho de banda. Los principales son:

1.- Airodump-ng: Programa que permite capturar paquetes de datos.

2.- Aircrack.ng: Permite averiguar y recuperar claves con cifrado WEP.

3.- Wzcook-ng: Permite averiguar y recuperar claves con cifrado WEP almacenada en una estación cliente en windows.

4.- Airdecap-ng.

Winairodump.

Basado en el airodump pero con entorno completamente gráfico. El cual que permite capturar paquetes de datos, así como ciertas informaciones y errores al intentar trabajar en modo monitor en windows si la configuración no esta bien realizada.

Network Stumbler.

NetStumbler es una sencilla herramienta que te permite detectar redes de área local sin cables (Wireless Local Área Network). Puedes usarlo para comprobar la integridad y correcto funcionamiento de tu WLAN, localizar zonas donde no haya cobertura, detectar otras redes que puedan estar interfiriendo con la tuya o incluso puntos de acceso no autorizados.

Snort.

Un sistema de detección de intrusiones (IDS) libre para las masas. Snort es una sistema de detección de intrusiones de red de poco peso (para el sistema), capaz de realizar análisis de tráfico en tiempo real y registro de paquetes en redes con IP. Puede realizar análisis de protocolos, búsqueda/identificación de contenido y puede ser utilizado para detectar una gran varidad de ataques y pruebas, como por ej. buffer overflows, escaneos indetectables de puertos “stealth port scans”, ataques a CGI, pruebas de SMB “SMB Probes”, intentos de reconocimientos de sistema operativos “OS fingerprinting” y mucho más. Snort utilizar un lenguaje flexible basado en reglas para describir el tráfico que debería recolectar o dejar pasar, y un motor de detección modular.

TCPDump/WinDump.

El sniffer clásico para monitoreo de redes y adquisición de información. Tcpdump es un conocido y querido analizador de paquetes de red basado en texto. Puede ser utilizado para mostrar los encabezados de los paquetes en una interfaz de red "network interface" que concuerden con cierta expresión de búsqueda. Podemos utilizar esta herramienta para rastrear problemas en la red o para monitorear actividades de la misma. Hay una versión port para Windows llamada WinDump. TCPDump es también la fuente de las bibliotecas de captura de paquetes Libpcap y WinPcap que son utilizadas por Nmap y muchas otras utilidades.

Wifiway.

Es una distribucíon GNU/Linux pensada y diseñada para la auditoría de seguridad de las redes WiFi, Bluetooth y RFID. Se publican imágenes iso con funcionalidades de LiveCD y LiveUSB Incluye una larga lista de herramientas de seguridad y auditoría inalámbrica listas para ser utilizadas, especializadas en la auditoría Wireless, además de añadir una serie de útiles lanzadores. Aunque está influida por inicio de varios desarrollos, algunos muy populares como es el caso de WiFiSlax, se debe destacar que Wifiway no está basada en otras distribuciones sino que se realizó usando Linux From Scratch

BackTrack.

Es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.
Es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Capítulo 3

CommView para wifi

3.1. Antecedentes

Desde el punto de vista de seguridad wireless nos han hecho creer que las redes inalámbricas son ciertamente seguras a partir del cifrado WEP, todos sabemos que esto no es así, pero se basaban que en la excusa de que no todo el mundo tiene capacidad para asumir los nuevos retos en linux, y que la inseguridad con Windows era limitada ya que había pocas tarjetas cuyo chipset entraban en modo monitor en Windows, previo paso necesario para capturar trafico y poder así analizarlo mediante técnicas que no vamos a explicar. Estas tarjetas era pocas y las que podían se consideraban unas reliquias, y solo se podía con los drivers específicos que todos conocemos. Aun la cosa en Windows se complico cuando los fabricantes sacaron al mercado revolucionarios chipset super g para las atheros. Estas tarjetas si entraban en modo monitor en Windows pero la captura de trafico era cero patatero.

Hace ya tiempo ya sacaron un programa comercial, donde podéis optar por una versión de evaluación para probar, donde se incluyen nuevos drivers que permiten capturar trafico de forma correcta y mas cosas.

Digo hace tiempo porque en la Biblia de seguridad ya se menciona desde entonces, pero su uso fue limitado, ya que no era posible la inyección en Windows, quizás si lo era, pero nadie obtuvo resultados dignos de documentar en castellano, pues bien este objetivo ya ha sido logrado, y por lo tanto previo paso a explicar la inyección de trafico en Windows es necesario saber como funciona este nuevo programa para la captura de trafico de forma normal.

3.2. Objetivo

Entender como funciona este programa comercial en Windows para poder capturar trafico y demostrar la vulnerabilidad de las redes en Windows, y una variante mas, a las ya muchas existente, para poder hacerlo exclusivamente en un entorno Windows. Trataremos exclusivamente el tema de captura de trafico pero en el manual de inyección podéis observar que la inyección es valida tanto para WEP como para WPA. Las WPA si son seguras en función de la contraseña usada, al ser necesario usar diccionarios externos difíciles de encontrar.

3.3. ¿Que programa es y donde lo localizo?

El programa es cuestión es el CommView for Wifi.

Figura 3.1: CommView for Wifi

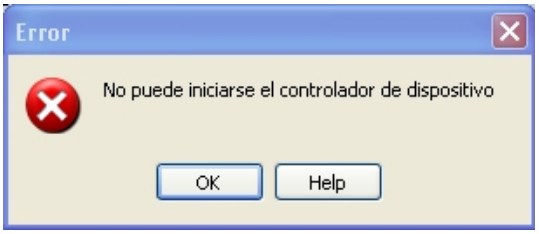
Se puede encontrar todo tipo de explicación y características del mismo en su Web principal: `http://www.tamos.com/`

Pero han sido muy generosos al ofrecer una versión de evaluación, tiene algunas capacidades limitadas, pero es valido para explicar su funcionamiento y citar sus mejores posibilidades.

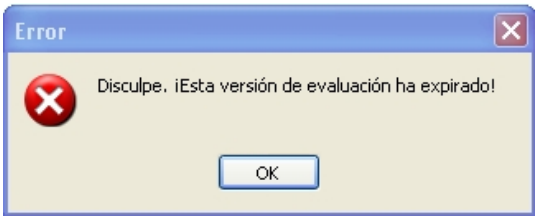
La versión de evaluación podéis descargarla de aquí:
http://www.tamos.com/download/main/

3.4. ¿Como empezar a trabajar con este programa?

Como hemos dicho lo descargamos, los descomprimimos, y ejecutamos el setup.exe. Y esta será la pantalla de bienvenida.



Aquí ya nos entra el miedo y pensamos que nuestra tarjeta no va a funcionar,pulsamos “OK” y listo.



Si hace días que hemos usado este programa, pues nos avisara que la versión de evaluación ha expirado. Pero en vuestro caso, como lo acabáis de bajar no os dará ningún problema, y esta será la pantalla principal.

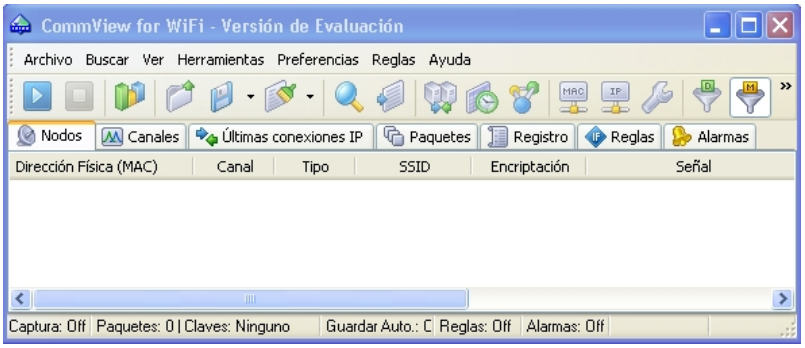


Figura 3.2: Pantalla principal del CommView para Wifi

3.5. Configuración de explorador

Pestaña Explorar

Los componentes mas importantes son:

Capturar:

no necesita mucha explicación y se entiende por si mismo. Se inicia la captura del trafico wireless existente.

Canal:

donde le podemos indicar en que canal debe de realizar la captura.

La captura solo puede realizarse en un canal especifico, al igual que todas las futuras acciones que se puedan realizar , dicho canal es fijado en la lista habilitado para ello.

Banda 802.11b/g:

en función del estándar permitido por nuestra tarjeta en este caso el modo compartido habitual de b/g para frecuencias de 2.4GHz. Pero pudiera haber sido también el estándar 802.11a para frecuencias de 5KHz.

Iniciar Exploración:

Inicia un rastreo de todas la redes inalámbricas del entrono. Esta información aparecerá en la ventana de la izquierda. Es algo similar a cualquier rastreador de redes wireless. Pero si seleccionamos cualquier punto de acceso, en la ventana de la derecha nos dará una información exhaustiva del tipo de red o nodo wireless con la que estamos tratando.

El modo de trabajo de la exploración es diferente al modo de trabajo de la captura. Su diferencia mas notable es la siguiente:

En modo de captura solo se puede trabajar en un canal fijado en la lista que hemos comentado anteriormente.

En modo de exploración podemos trabajar en los canales que queramos. Estas formas y algunas mas de trabajo podemos definirlas en esta misma ventana “Explorador” pero en otra pestaña diferente “Opciones”.

Pestaña Opciones

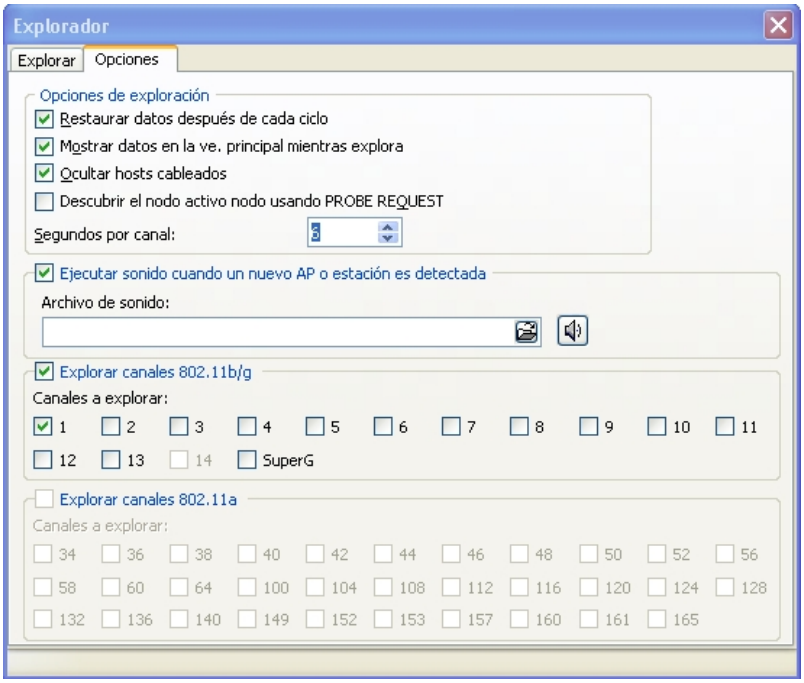


Figura 3.3: Pestaña Opciones

Los componentes mas importantes son:

Opciones de exploración

Esta configuración solo afecta cuando iniciamos una exploración. Recordad que la exploración de redes no tiene nada que ver con la captura de paquetes (trafico) de esas misma redes.

Restaurar datos después de cada ciclo:

La exploración efectúa un recorrido por los diferentes canales que hayamos seleccionado, si habilitamos esta casilla cuando finalice el rastreo borrara los nodos localizados cuando vuelva a realizar otro escáner, por lo tanto es mejor tenerla no seleccionada para poder observar siempre los nodos localizados.

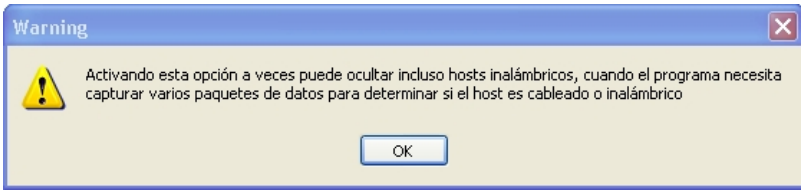
En ambas formas la exploración no acaba hasta que no le forzamos a ello.

Mostrar datos en la ventana principal mientras explora:

Si habilitamos esta casilla, la información que aparece en la ventana de exploración también será visible en la pantalla principal del programa en "Nodos". Siempre es mejor tenerla no seleccionada, ya que la creación de .Alias.es mucho mas fácil, luego veremos lo que son .Alias".

Ocultar host cableados:

Si solo queremos obtener información de estaciones que solo sean inalámbricas deberemos de habilitar esta casilla, pero si lo hacemos corremos ciertos riesgos, la misma aplicación nos informa:



Así que la dejaremos no seleccionada.

Descubrir el nodo activo nodo usando PROBE REQUEST:

Si esta habilitada realizara envíos de sondas para detectar la existencia de nodos con essid ocultos. Esta es la forma habitual de trabajo del NetStumbler. Esta emisión de sondas hace detectable la posición de la tarjeta que corre bajo la aplicación. Por lo tanto la dejaremos como no seleccionada.

Os aconsejo dejar configurada las opciones de exploracion de la siguiente manera:

Segundos por canal:

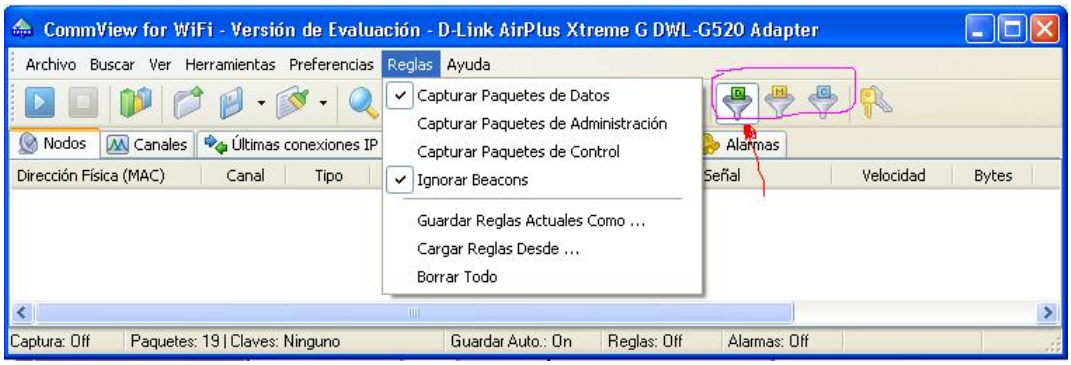
Limitamos el tiempo que la tarjeta tiene para rastrear las redes dentro de un canal que se haya elegido, en este caso recordad que no solo es necesario que se uno solo como ocurria en la caotura, sino que pueden ser varios o todos.

Ejecutar sonido cuando un nuevo AP o estacion es detectada:

Sin comentarios, y lo mismo para el fichero de sonido.

Configuración de captura:

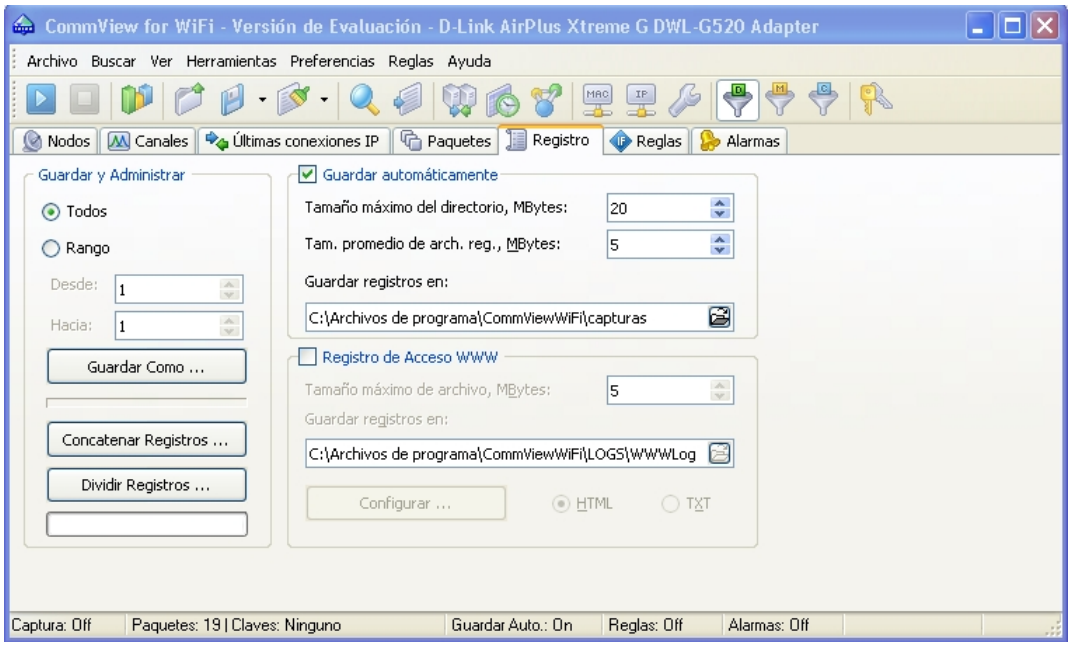
Este programa como hemos dicho permite la captura de muchas cosas, pero como solo nos interesa en estos momentos el trafico de paquetes de datos, previo acción al análisis de la seguridad wireless, pues debemos de indicarlo de esa manera. Es decir usamos un filtro del programa y mas al ser una versión de evaluación.



Siempre para este tipo de capturas, debemos de marcar la casilla “Capturar Paquetes de Datos” e “Ignorar Beacons”, o bien lo hacéis mediante la barra de menú, o bien mediante los iconos destinados para este uso.

Tratamiento de ficheros (registro):

Observamos de nuevo la pantalla principal, en ellas podemos determinar 7 pestañas, pues para el trato de ficheros, nos iremos hasta la pestaña "Registro" y automáticamente la información de la pantalla principal cambia.



Selecciono la casilla "Guardar automáticamente", y podéis ver en la barra de estado de programa en todo momento que así lo indica. Si el tamaño de la suma de todas las capturas es superior al tamaño fijado al directorio, durante el proceso de guardado automático, se sobrescribirán los datos sobre los iniciales de estos mismos ficheros. Por lo tanto una vez realizadas las capturas es mejor portarlas a otro directorio, y acostumbrarnos a dejar vació el directorio de las capturas para el modo de guardar de forma automática.

Como valores, cada uno determinara la capacidad de rendimiento de su equipo. Para empezar y probar podéis usar los que se ven en la captura de pantalla anterior, es decir 20MB para el directorio y 5M de tamaño medio para cada archivo de captura.

Una vez iniciado el proceso de captura, no hay que realizar ningún control, es mas, hay una opción de la aplicación que permite programar capturas, por lo tanto debemos de tener el sistema configurado de forma adecuada, es decir que se graben los datos de forma automática, pero este tipo de ficheros hace bajar el rendimiento del equipo y mas con microprocesadores mas antiguos y con limitación de memoria RAM, por lo tanto, no dejamos que se grabe todo en un fichero sino en varios, dicha acción la asignamos con el campo definido como "Tamaño de promedio".

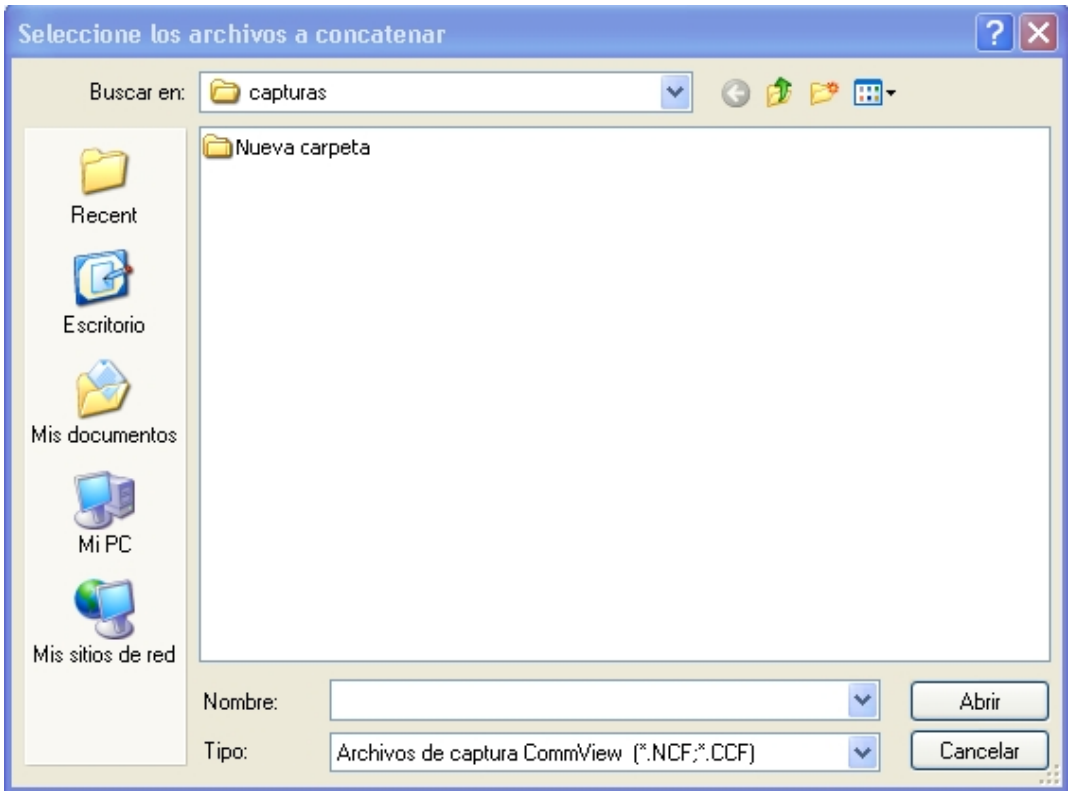
Después de horas de captura (no en la versión de evaluación), podemos volver y ver como esta ese directorio, se habrán generado pues, diferentes tipos de ficheros con los datos obtenidos. Pero recordad que al ser una versión de evaluación tenemos restringida la captura de datos y el tiempo de captura. Aun así esta versión nos permite observar como debe de funcionar el programa con una licencia valida.

Siempre que podamos, realizaremos varias capturas seguidas con diferentes intervalos dentro de la versión de evaluación. Así al final de día, podemos tener en esa ruta de directorios, una serie de ficheros de datos, siempre que el tamaño no sea mayor al determinado en "Tamaño máximo del directorio"si eso fuera así, la misma aplicación para autocorregir y ajustarse al tamaño máximo especificado en "Tamaño máximo del directorio"borraría los datos de los ficheros para poner los nuevos, y así cíclicamente, por lo tanto recodar de dejar siempre libre el directorio de trabajo.

¿Podemos capturar ya?, no todavía no, primero la concatenación de archivos, que es algo diferente a como estamos acostumbrado a tratar, aunque en base es lo mismo.

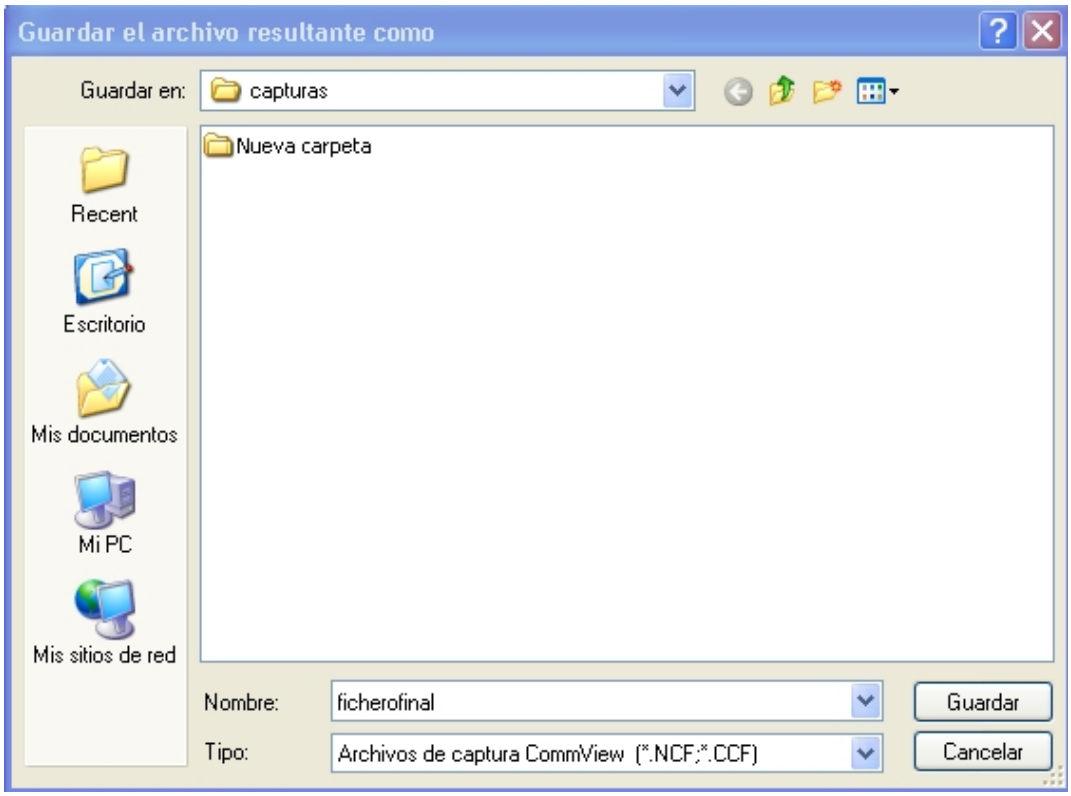
Concatenación de archivos (registros):

Este proceso debe de realizarse siempre, después de haber realizados las capturas. En esta misma pantalla podemos observar un botón denominado "Concatenar registros". Registro es equivalente a ficheros de captura. Pinchamos sobre el y:



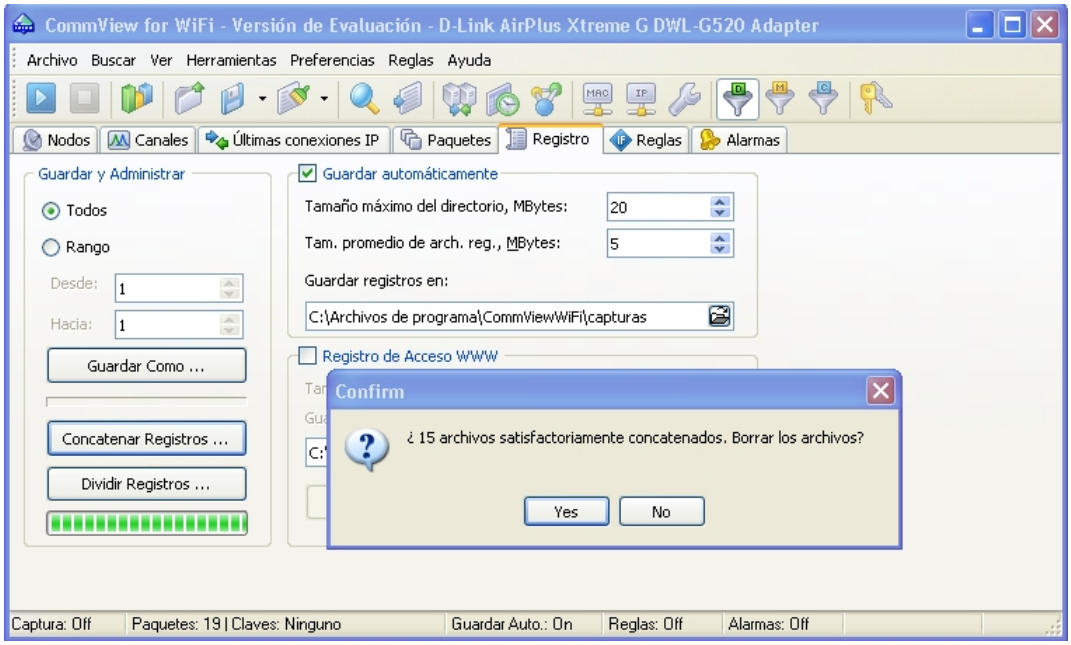
Se abre la típica ventana de Windows para control de archivos, podemos seleccionar todos los que queramos, pero no aconsejo mas de 5, para un mejor rendimiento del sistema.

Si vuestro equipo lo permite, podéis tener todas las capturas en un mismo archivo, pero de igual forma cuando expliquemos el proceso de cambio de formato, podemos pasarlos uno por uno. Según que casos puede ser hasta mucho mas rápido. Solo que si el numero de capturas son elevadas y estas son pequeñas, si es un poco estresante, transformar de fichero en fichero, esta manera de proceder os corresponde a vosotros elegirla, yo personalmente prefiero agruparlos (concatenarlos) y mantener cierto orden en mi ordenador.



Nos pedirá donde queremos que grabe el archivo resultante y su nombre. Es decir para entenderlo, lo que hacemos es sumar todas las capturas y generar una sola. Una vez elegido el destino y el nombre de archivo para agrupar todas las capturas tomadas o aquellas que queramos, pulsamos sobre el botón “Guardar”

Seguidamente se inicia el proceso de concatenación de archivos (registros) y al finalizar nos preguntara lo siguiente:



Podemos observar la duración del proceso y el tiempo restante mediante una barra de seguimiento, la que esta verde.

Una vez concatenados podemos borrar los ficheros base (los de las capturas una por una), yo siempre los borro, por que si no es un lió con tanto fichero, pero optar por la opción que queráis.

Pues bien, ya tenemos el fichero concatenado con todas nuestras capturas. Solo tenéis que usar el explorador de Windows para comprobar que el resultado ha sido bueno y el fichero esta donde tiene que estar y con un tamaño considerable en función del numero de capturas parciales que se hayan hecho. Indistintamente de que cada captura se haya realizado en canales diferentes, pero también es cierto que es mejor agruparlas por nodos.

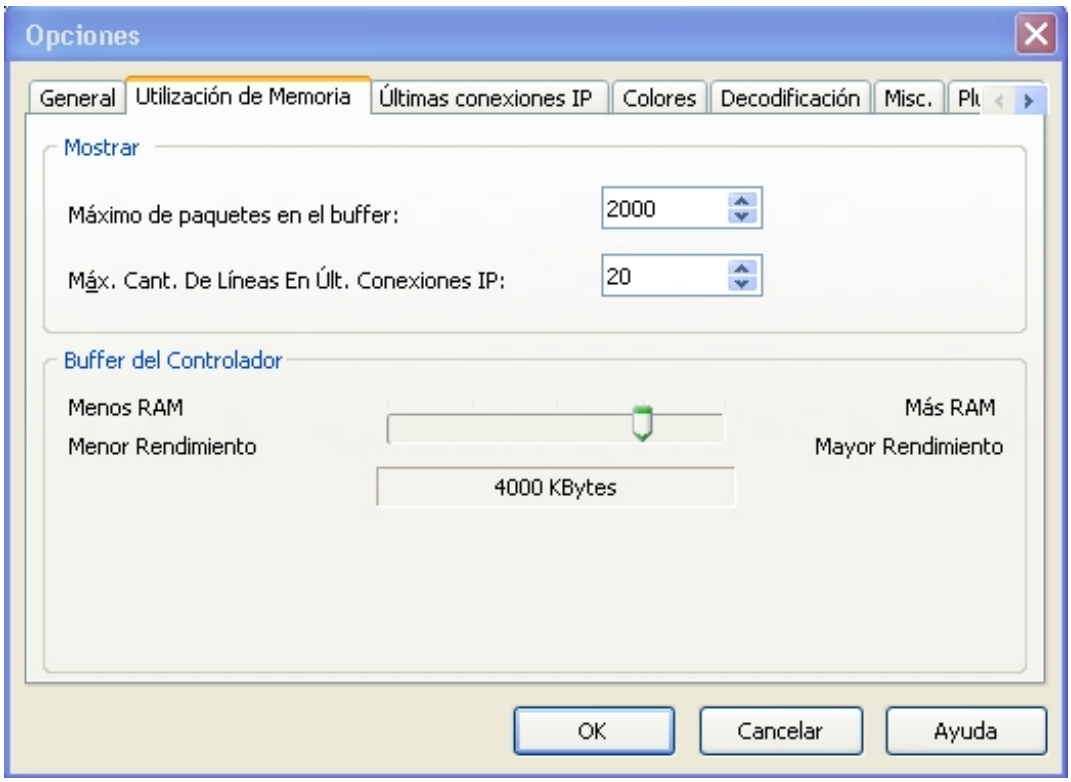
Este proceso deber de realizarse con las capturas ya tomadas, pero si es la primera vez que usáis este programa, leer con mucho interés lo que he explicado aunque lo haya repetido dos veces.

Buffer de captura:

Mediante los menús de la aplicación, podemos configurar una serie de cosas importantes, muy fáciles de entender y de usar. En este manual os estoy explicando lo mas básico y importante.

Para acceder a ello, pinchamos en el menú definido como "Preferencias" y luego sobre la lista que aparece (submenús) seleccionamos el de "Opciones"

Y obtendremos como resultado la siguiente ventana:



Los datos no se graban de forma automática constantemente en los ficheros, primero se cargan en un buffer de datos y posteriormente se graban en el archivo. Tal como esta de serie ya puede funciona, pero tenerlo en cuanto en virtud de la memoria RAM de vuestros equipos. El numero de datos en el buffer podemos determinarlo en esta ventana así como el rendimiento del mismo.

¿Por que se trabaja con buffer de datos y no se graba directamente en los registros (ficheros)?:

Muy fácil, el proceso de lectura y escritura en memoria RAM es mucho mas rápido que el acceso a cualquier otro sistema de almacenamiento de datos (si bien es temporal y los datos pueden perderse por el corte del fluido eléctrico), si continuamente accedemos al disco duro para grabar datos, se perderían muchos paquetes de datos, un SO como Windows es multitarea, pero a nivel de comunicación wireless este proceso es mucho mas rápido que los procesos que corren en los equipos informáticos. Por lo tanto, al ser grabados en RAM la perdida es casi nula. Cuando se llega al nivel máximo de buffer (definido en la casilla de numero máximo de paquetes del buffer) entonces se procede al borrado del buffer y a la descarga en el fichero del disco duro, pero el borrado no es total sino progresivo. Esta es la gran ventaja d linux que teóricamente ocupa menos recursos del sistema.

Esta aplicación es bastante completa y permite incluso obtener la información (lectura) de las posibles inyecciones que tu mismo hagas con la tarjeta que esta en modo monitor (capturando trafico).

Suponer que enviamos una desautentificación de cliente (ataque 0 = reasociación de nodo) con el generador de paquetes (esto lo veremos mejor en el capitulo de inyección) pues bien, el paquete enviado también es captado por la misma tarjeta que lo mando y la respuesta inmediata del punto de acceso, así podemos ver como trabajan las conexiones wireless en todo su proceso. Mediante a accesos a ficheros constantemente no podría verse.

Capturando trafico:

Como ya si tenéis mi permiso para poder pulsar el botón “Play”, hacerlo, y veréis todo lo que pasa. Podemos tener conocimiento de todo lo que pasa en cada momento, este programa como ya he dicho esta provisto de varias pestañas, y en función de la seleccionada, la información mostrada será uno u otra en cada momento.

puntos de acceso. Modo managed. Dentro de la columna “Tipo” los define como “AP”

estaciones clientes de ordenadores: es decir PCs con tarjetas wireless asociadas y autenficadas a los puntos de acceso: Modo infraestructura. Dentro de la columna “Tipo” las define como “STA”

estaciones simples de ordenadores no asociados a ningún punto de acceso. Modo adhoc. Dentro de la columna “Tipo” las define como “ADHOC”.

Veamos un ejemplo:

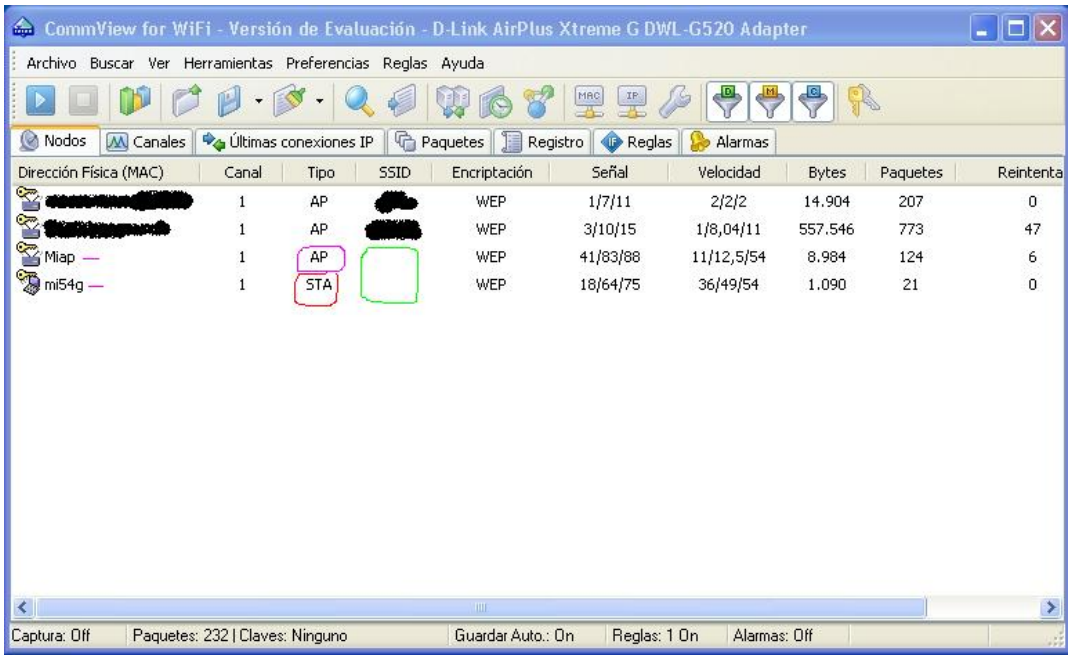
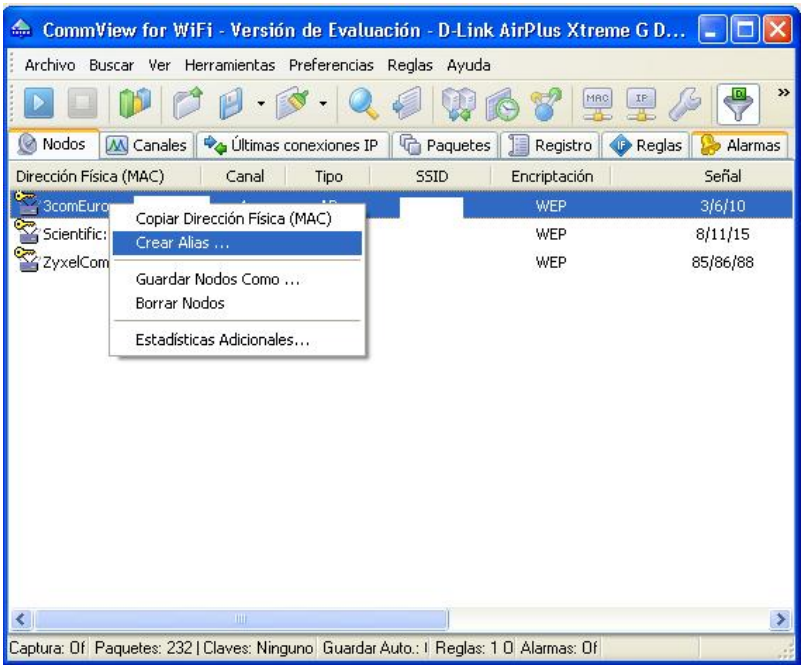


Figura 3.4: Capturando tráfico [8]

En esta captura podemos contemplar que no aparecen direcciones MAC como estamos acostumbrados a tratar, y las que si aparecen estas tachadas, de sobras ya sabéis que no me gusta publicar las direcciones MAC de otros nodos. No aparecen las direcciones MAC debido a que es posible editar el nombre de las direcciones MAC. Lo que el programa denomina como .ªlias"(eso aparte de lo que yo he tachado).

Si seleccionáis un punto de acceso o estación, y pulsáis el botón secundario del ratón, os saldrá un menú contextual.

Entre otras cosas permite crear "Alias", los alias son etiquetas que se dan a las direcciones MAC, las cuales estas ultimas están en hexadecimal. Así se recuerdan mejor. También es interesante ver como media palabra de la dirección MAC, es decir las 3 primeras no salen en hexadecimal sino que sale el nombre del fabricante, todo esto es configurable y editable a través de menús. Y lo veremos al final cuando volvamos a hablar de la opción del menú "Preferencias" y su submenú "Opciones". Cuando se hablo del buffer de datos y de los colores ya hicimos referencia al mismo. Tenemos la opción de crear "Alias" esto es muy útil ya que evitamos trabajar con valores hexadecimales.



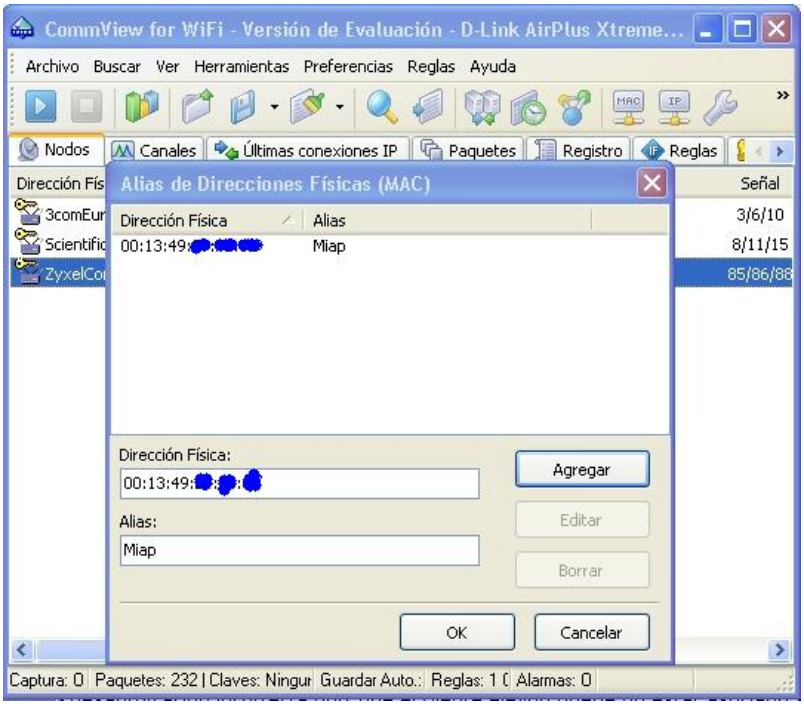


Figura 3.5: Capturando tráfico [8]

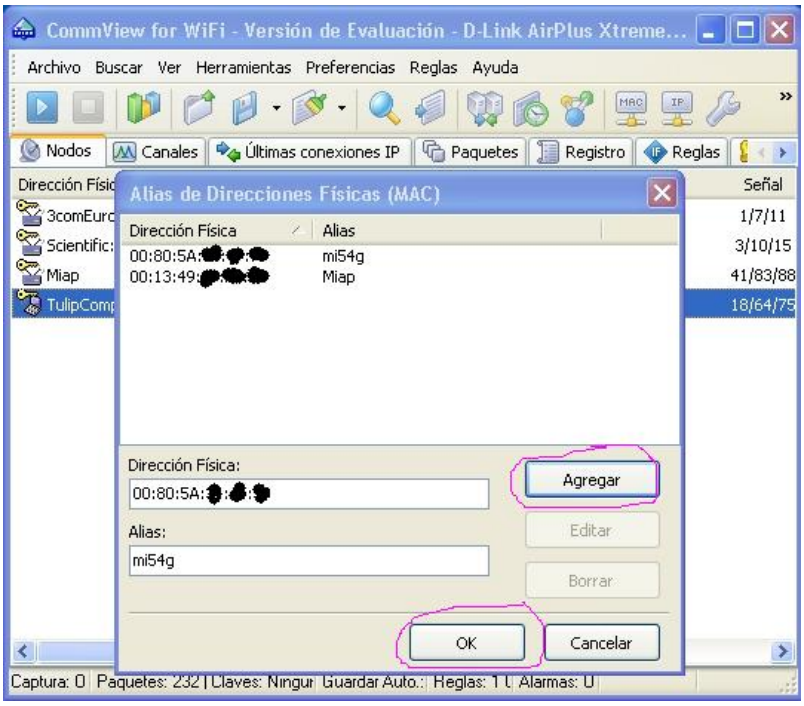


Figura 3.6: Capturando tráfico [8]

Y como hemos visto anteriormente ya aparecerán los “Nodos” con sus “Alias”.

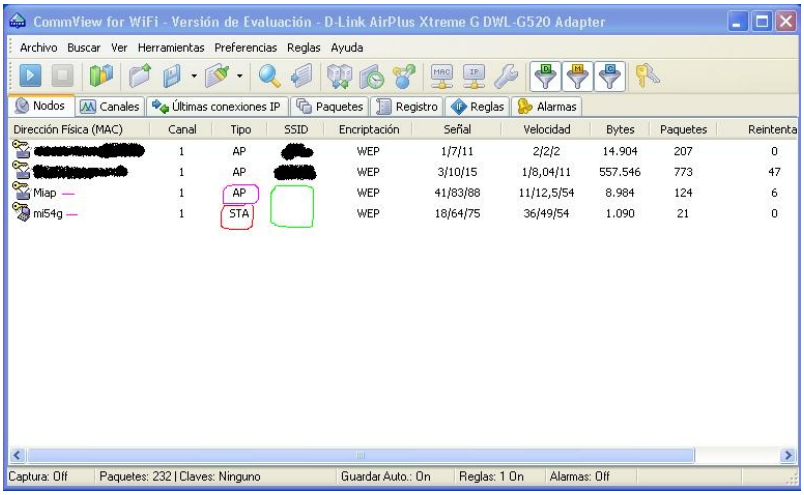
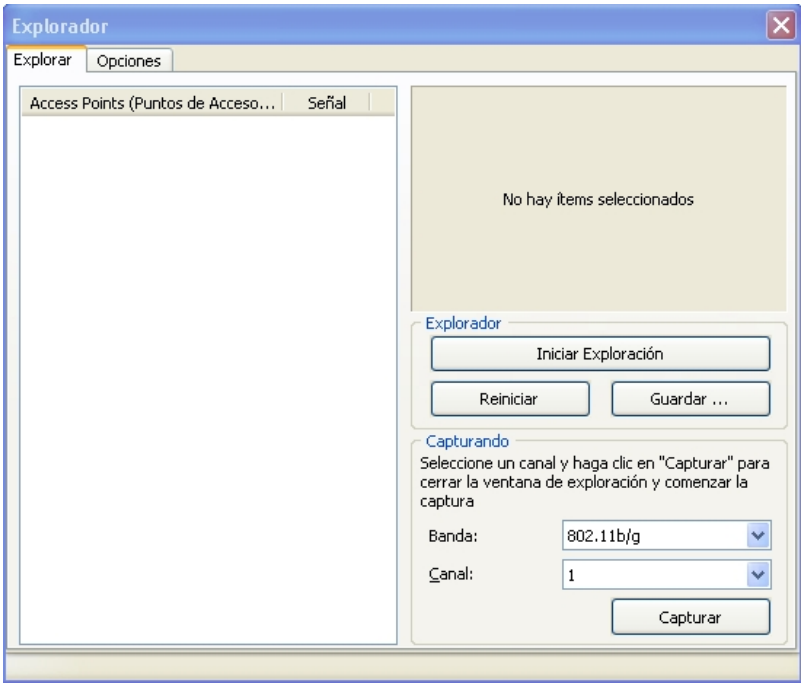


Figura 3.7: Capturando tráfico [8]

Para que aparezcan las redes inalámbricas en la pantalla de “Nodos” antes de iniciar la captura recordad de usar el botón “Iniciar Exploración” y tener seleccionada la casilla “Mostrar datos en la ventana principal mientras se explora”.



Canales: podemos ver lo que esta pasando en cada canal. Datos recibidos, es mera estadística y tampoco sirve para mucho mas.

Ultima conexión IP: no hace falta decirlo, muestra todas las IP de las redes abiertas, similar al Kismet en linux.

En Alertas de momento no es necesario tocar nada, para controles mas avanzados si será necesario.

En Reglas podemos limitar la captura de trafico para un nodo en concreto, y también para ciertos bloques de datos con ciertas particularidades. Esto ultimo lo veremos en el manual de inyección de trafico en windows.

Pero aquí podemos especificar como seria la regla para limitar la captura solo a un nodo especifico.

Lo vemos:

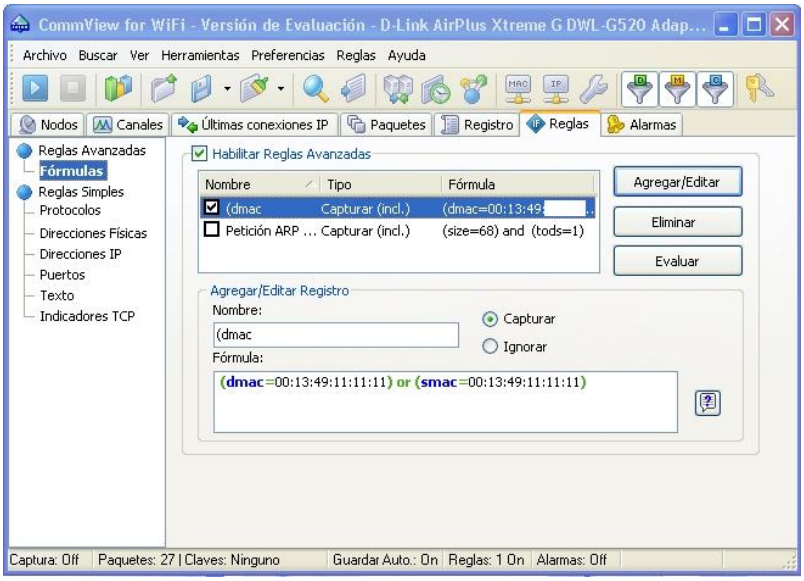


Figura 3.8: Capturando tráfico [8]

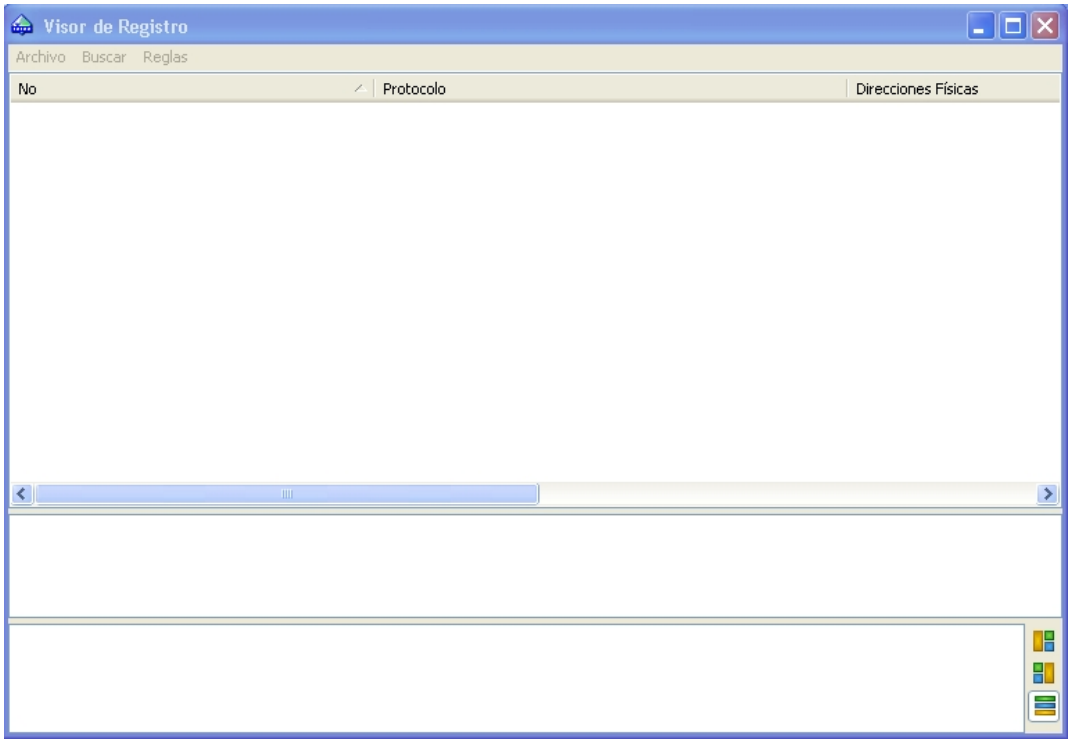
Los valores de dirección MAC pueden ser copiados con el ratón directamente en la ventana "Nodos" o en la ventana "Paquetes", ya existe la especificación "Guardar dirección MAC", luego en las reglas simplemente usáis las teclas de pegar, "Control + V".

Exportación de Ficheros:

Este es una de las partes mas importantes y que quizás entendemos un poco menos. Una vez realizadas las capturas y disponibles en ficheros con extensión NCF, y además con los archivos (registros) de diferentes capturas ya concatenados en uno solo. Tenemos que convertirlos a otros formatos, para poder iniciar una recuperación valida y correcta de claves WEP, y de esa forma comprobar lo frágil que es nuestra conexión wireless con dicho sistema de encriptación.

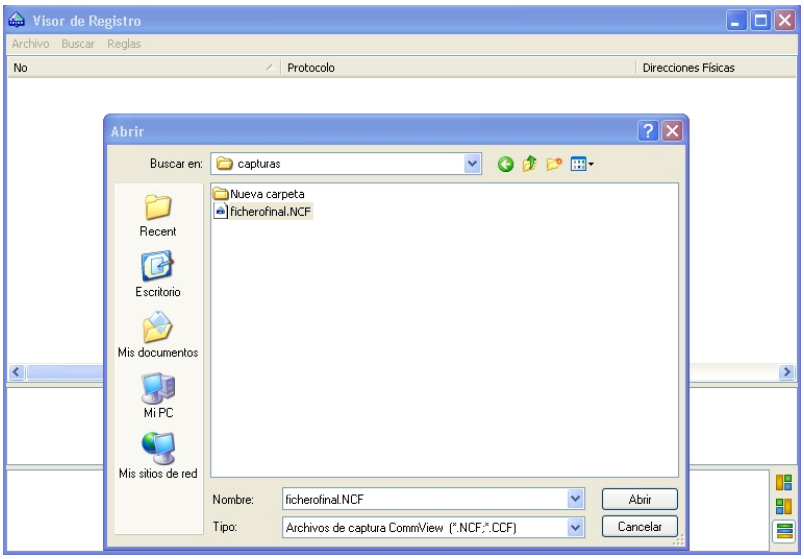
Para eso podemos disponer del método de teclado abreviado, es decir mediante la pulsación en el mismo de "Control+L" o bien mediante el menú correspondiente. En este caso "Archivo" y de la lista emergente pulsamos sobre " Visor de Registro"

Sea de una forma o de otra, se nos mostrara el "Visor de Registro", el cual podemos verlo a continuación:



Seleccionamos en el Menú “Archivo” y de la lista disponible, pinchamos sobre “Archivos de Commview”.

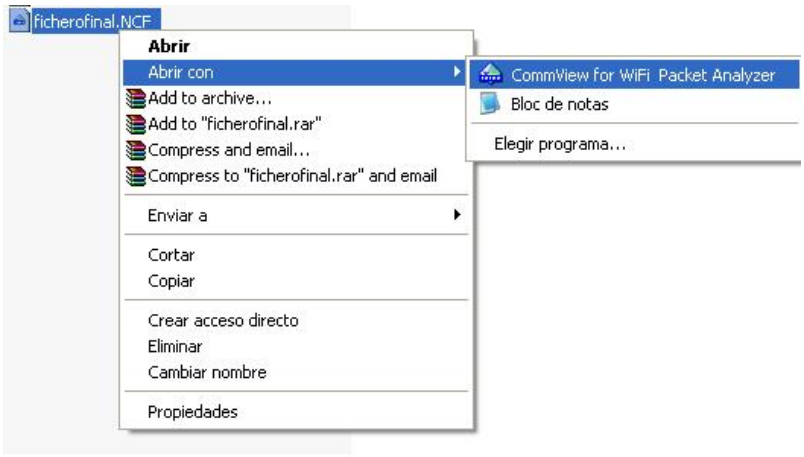
En ese caso se nos abrirá un explorador muy habitual en procesos Windows y marcamos el fichero que anteriormente habíamos concatenado.



Tras un cierto tiempo, cargara en el “Visor de Registro” todos los paquetes que haya capturados en ese fichero, sean buenos o malos, por eso podemos creer que tenemos un cierto numero de IV validos y, aplicaciones posteriores nos indicara lo contrario o incluso puede darnos error al abrir los mismos.

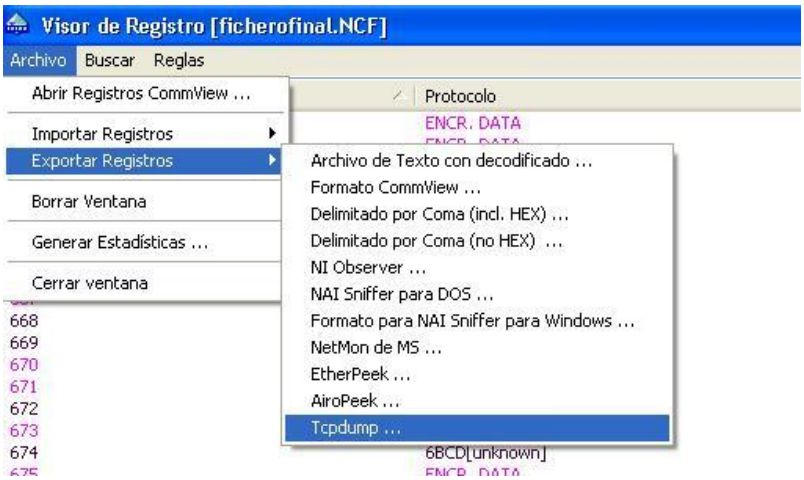
También podéis cargar varios ficheros a la vez, pero si estos, estaban ya concatenados anteriormente y quizás su contenido pudiera ser muy grande, mejor no lo hagáis o el rendimiento del sistema bajara bruscamente. Recordar que si son paquetes de datos buenos, es decir IVs que es lo que nos interesa, pues, el color predominante tiene que ser nuestro color preferido. Posteriormente explicaremos la forma de evitar que se graben en las capturas datos no validos, incorrectos o con errores.

También podéis abrirlos de la siguiente forma, usáis el explorador norma de Windows, seleccionáis el o lo ficheros y pulsáis el botón secundario del ratón en ese caso, sobre el menú contestas saliente, pincháis sobre:

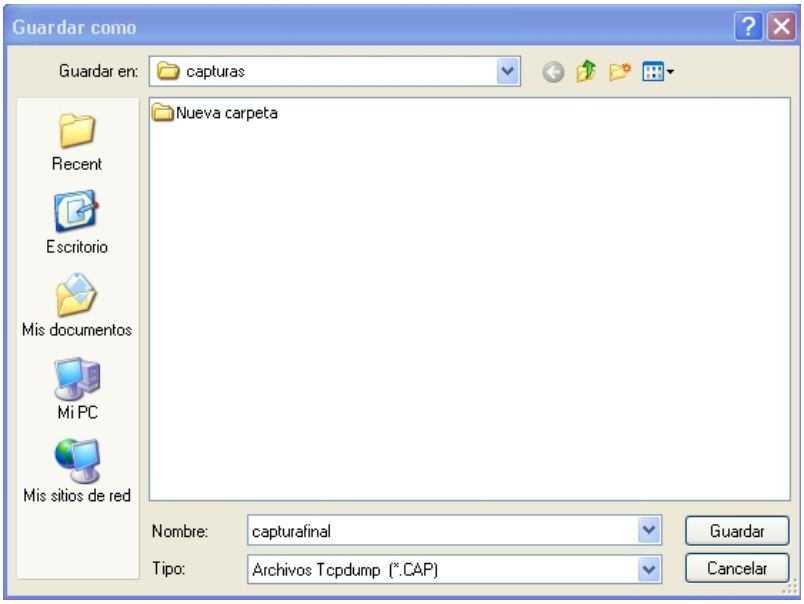


Sea de una forma o de otra tendréis que tener cargados todos los paquetes en vuestro "Visor de Registro", previo paso a la conversión.

Como los datos están correctamente ya cargados en dicho "visor", ha llegado el momento de convertirlos de formato. En este caso, elegimos por ejemplo el formato "Tcpdump", por ser el ultimo de la lista.



Nos volverá salir un explorador para indicar donde guarda el fichero resultante:



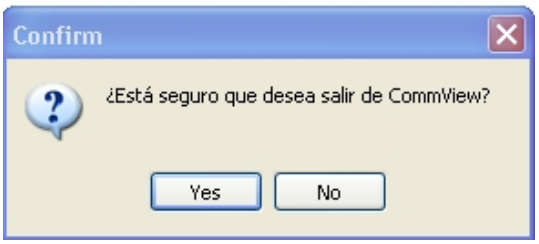
Elegimos el nombre y la ruta del mismo, y lo guardamos.

Nota: No se deben de indicar las extensiones de los ficheros, por ejemplo, si en este caso, escribimos "capturafinal.cap", el fichero resultante quizás seria "capturafinal.cap.CAP" y lo mismo para los formatos de captura (NCF).

Llegados a este punto, ya podemos cerrar el programa y el "Visor de Registro".

Como no sale ningún aviso de que el proceso de conversión se ha realizado de forma correcta, supongo si saldrá si hay algún error, comprobar con vuestro explorador habitual que el fichero convertido este donde tiene que estar, sino es así repetir el proceso.

Una vez comprobado ya podemos cerrar el programa, y si esta configurado para tal forma nos confirmara el cierre de la sesión.



Capítulo 4

Inyeccion de trafico con commonView

4.1. Antecedentes

Todos sabemos que significa el termino de inyección de trafico en las redes inalámbricas, sino es así, has hecho mal en empezar a entenderlo leyendo este manual. Aunque comentare a nivel de recordatorio en cada apartado unos conceptos mínimos a modo de resumen. La inyección de trafico, sus razones y sus motivos están mas que explicado en la Biblia de seguridad, pero nunca se pudo hacer en Windows de forma correcta, solo en linux.
Pero este hecho ha cambiado drásticamente, y supone un cambio bastante a tener en cuenta en la auditoria wireless.
Últimamente han salido muchos live CD que recopilan multitud de herramientas para la auditoria, pues bien los desarrolladores de software para entornos Windows (un gigante que camina con pasos muy pesados) han visto la necesidad de desarrollar nuevas herramientas para tales propósitos, aun así el entorno Linux es mejor sistema para la auditoria wireless, pero nunca nos debemos a cerrar a nada.

Todavía no se ha conseguido la eficacia del sistema linux y difícilmente se conseguirá debido a la multitud de programadores libres que trabajan en GNU/Linux, pero podemos decir que los primeros pasos se han dado satisfactoriamente, y en este manual, único en lenguaje castellano podremos aprender la inyección de trafico en Windows.

4.2. Tipos de inyeccion en linux

Ataque 0: desautentificación de clientes

Este ataque es probablemente el más útil para recuperar un ESSID oculto (no difundido) y para capturar "saludos" WPA forzando a los clientes a reautentificarse.
También puede ser usado para generar peticiones ARP en tanto que los clientes Windows a veces vacían su cache de ARP cuando son desconectados. Desde luego, este ataque es totalmente inservible si no hay clientes asociados. Normalmente es más efectivo fijar como blanco una estación específica. Aunque podemos realizar una denegación de servicio masiva con una tarjeta.

Ataque 1: Falsa autentificación

Este ataque es particularmente útil cuando no hay clientes asociados: creamos la dirección MAC de un cliente falso, la cual quedará registrada en la tabla de asociación del AP. Esta dirección será usada para los ataques 3 (reinyección de peticiones ARP) y 4 (desencriptación WEP "chopchop"). Es mejor preparar la tarjeta de ataque con la misma MAC que el cliente falso de esta forma el controlador puede envíar ACKs de forma mas adecuada.

Ataque 3: Reinyección de trafico

Es el clásico ataque de reinyección de petición ARP es el mas efectivo para generar nuevos IVs, y funciona de forma muy eficaz. Puede que tengas que esperar un par de minutos, o incluso más, hasta que aparezca una petición ARP; este ataque fallará si no hay tráfico.

Ataque 4: El "chopchop" de KoreK (predicción de CRC)

Este ataque, cuando es exitoso, puede desencriptar un paquete de datos WEP sin conocer la clave. Incluso puede funcionar con WEP dinámica. Este ataque no recupera la clave WEP en sí misma, sino que revela meramente el texto plano.
De cualquier modo, la mayoría de los puntos de acceso no son en absoluto vulnerables. Algunos pueden en principio parecer vulnerables pero en realidad tiran los paquetes menores de 60 bytes. Este ataque necesita al menos un paquete de datos WEP.

4.3. Tipos de inyección en Windows con el CommView 5.2

Desautentificación de clientes

Es el denominado ataque 0 o desauntetificación de clientes, valido para redes wireless tanto con seguridad WEP como WPA. La recuperación de clave WPA requiere el uso de ficheros o diccionarios auxiliares.

Se puede incluso realizar una petición de denegación masiva, deshabilitando a todos los clientes o una en particular, y dejar fuera de servicio el nodo wireless al completo el tiempo que se quiera

Reinyección de trafico en windows

Es puramente la reinyección de trafico o reinyección de petición de ARP, y su finalidad es aumentar la velocidad de la captura de datos para no sufrir el agotamiento mental de horas largas de captura.

En Windows y mediante esta aplicación no tiene sentido hablar de ataques 2 y 3 ya que se indexan conjuntamente. Es un concepto totalmente nuevo donde se pueden unificar ambas formas de hacerlo, recordad que en el ataque 3 era la propia aplicación que interpretaba si la petición de ARP encriptado era correcto o no, lo intuía, en Windows es algo similar pero tu decides que paquete se debe de mandar, y esto es mas parecido al ataque 2.

Si la red a analizar ya tiene un cliente y el trafico es elevado, con la simple captura en modo monitor, será mas que suficiente, pero este proceso de reinyección puede ser tan efectivo, que pueden tomarse datos suficientes en 10 minutos para una red de poco trafico o incluso muchos menos tiempo si la misma tiene un trafico considerable.

La reinyección de trafico puede realizarse de varias formas, o bien observamos el trafico en la pantalla de paquetes, hasta observar cuales son las peticiones de ARP encriptados, (yo ya me lo conozco de memoria), o podemos efectuar un ataque 0, y esperar a la petición de ARP y aplicando una serie de reglas de filtrado.

Mediante el CommView podemos conseguir un nivel de trafico mas alto enviando paquetes de ARP cifrados, el punto de Acceso responderá con paquetes de respuesta ARP, generando así tráfico adicional.

4.4. Inyectando trafico con CommView

¿Cómo efectuar un Ataque 0 ?

En primer lugar ponemos la aplicación a capturar datos, botón “Play”. Mediante la barra de menús del programa nos dirigimos hasta “Reasociación de nodo”.

Figura 4.1: Herramientas [8]

Esta incluido en “Herramientas” y de la lista seleccionamos “Reasociación de modo”. La pantalla que mostrara la aplicación será la siguiente:

Si hemos dedicado un poco de tiempo a crear alias a partir de los datos obtenidos en la ventana de “Nodos”, en la lista que hay debajo de la etiqueta: “Enviar una solicitud de desautorización desde esta AP”, tendremos definidas todos los que hemos creado, pero siempre que en ese momentos estemos en proceso de captura y sean detectadas por la aplicación, es decir, estemos por así decirlo online.
Vemos el canal actual, que esta seleccionado y capturando. Definimos el numero de paquetes a enviar y el intervalo entre cada paquete. Decir que, un solo envió de paquetes puede ser mas que suficiente.

También podemos definir si queremos realizar una denegación de servicios masiva a todos los clientes mediante selección de “Enviar a todos los clientes” o bien fijar la casilla “Enviar a clientes seleccionados”.

Para realizar una desauntetificación completa, agresiva y total, podemos marcar “Enviar a todos los clientes”, definir el numero de paquetes a enviar y aumentar el intervalo en milisegundos. **Como comprobamos que es efectivo este ataque, muy simple, tenéis varias formas, vamos a verlas:**
Veamos el icono de conexión wireless de nuestro ordenador, o sea en la barra de estado del windows. Antes de efectuar la desauntetificación:

Todo esta correcto, efectuamos el ataque 0 y:

Como el ataque es muy breve enseguida tendremos de nuevo:

Ya que windows se recupera de forma automática

Obtención del handshake sobre encriptación WPA-PSK

En primer lugar citar que si estamos ante un nodo con encriptación WPA, necesitamos filtrar solo los contenidos de los paquetes e ignorar las balizas (beacons).

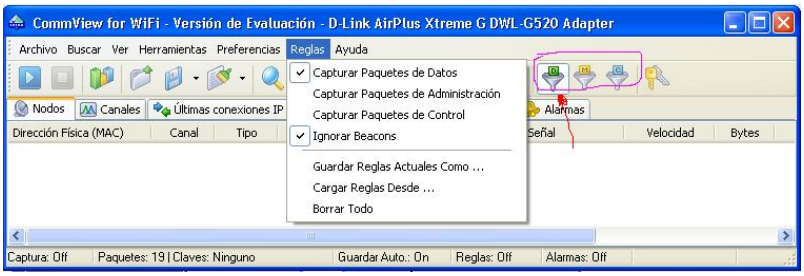


Figura 4.2: Obtención del handshake [8]

Y también es interesante filtrar mediante "Reglas avanzadas" el trafico de solo el nodo a analizar para la recuperación de claves WPA. El filtro pare ese nodo y todos los que queráis podéis realizarlos "Regla avanzadas"

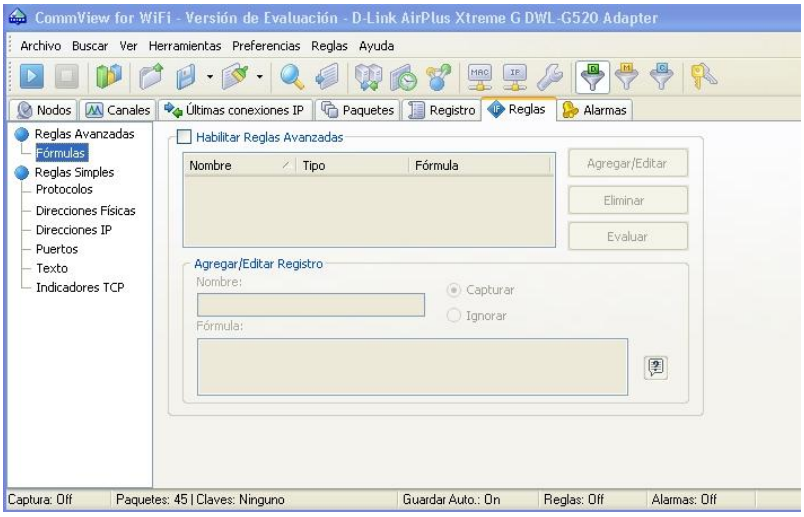
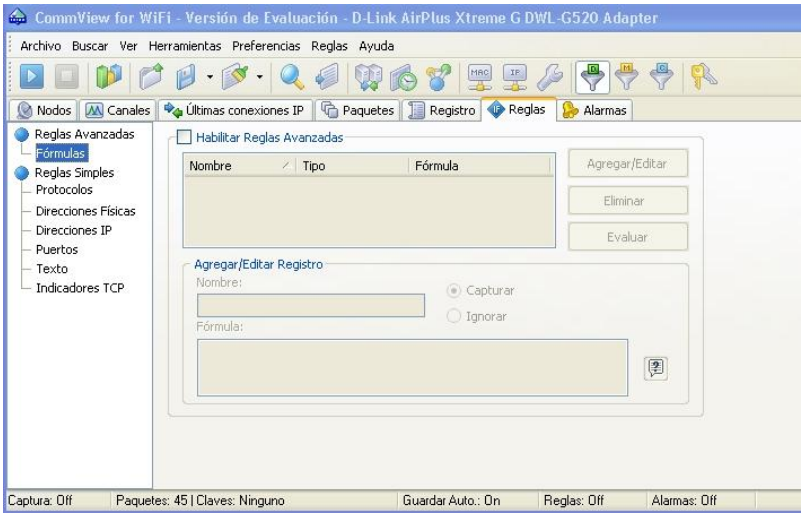


Figura 4.3: Reglas avanzadas



Descubrir el ESSID oculto de una conexión wireless (nodo)

En primer lugar filtramos al igual que anteriormente, el trafico de ese nodo.

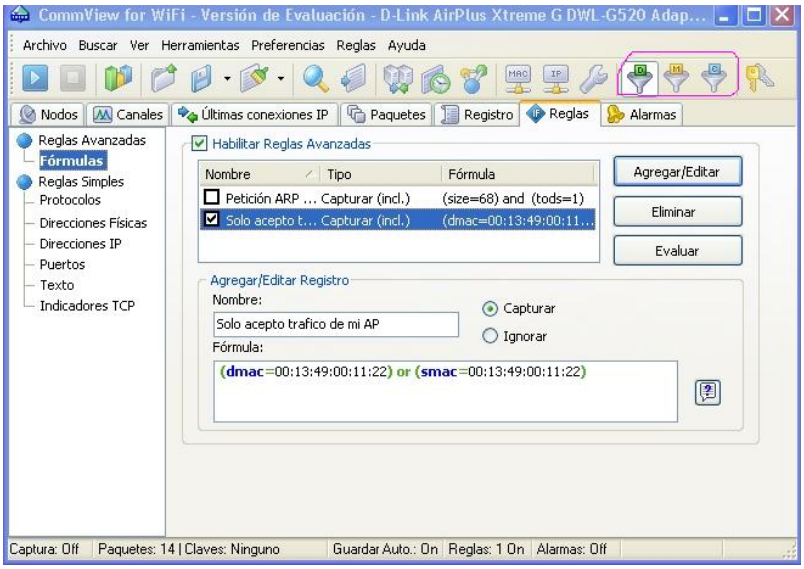


Figura 4.4: Descubrir ESSID [8]

En segundo lugar, aceptamos en este caso, todos los tipos de paquetes excepto los paquetes de datos.

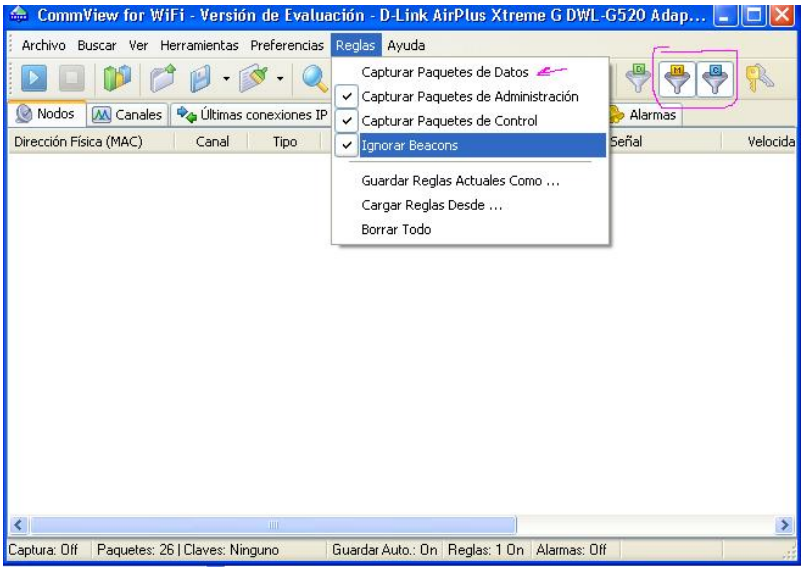


Figura 4.5: Descubrir ESSID [8]

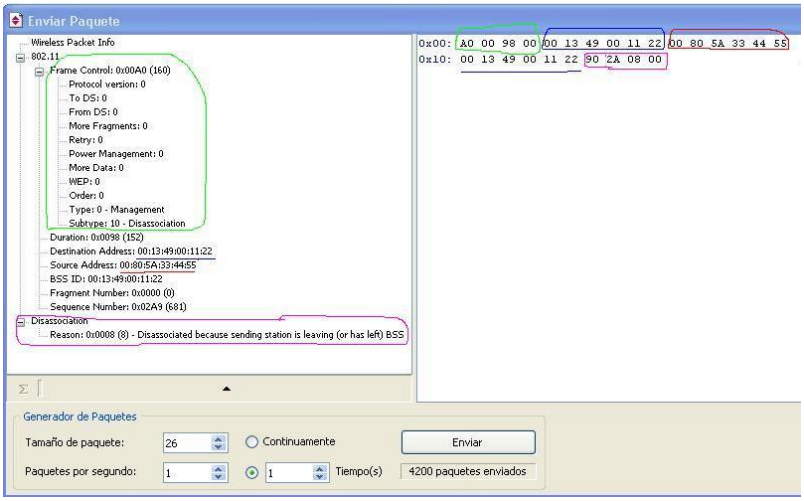


Figura 4.6: Descubrir ESSID [8]

Capítulo 5

Conclusiones

En este proyecto “Seguridad Wireless:Auditoria con CommView para Wi-Fi”,se ha podido ver los diversos problemas de seguridad que afectan a las redes wi-fi.

La motivación de dicho Proyecto es conseguir dar una vision sobre el nivel de seguridad de las reses wi-fi bajo el Sistema perativo Windows,las vulnerabilidades de las misma asi como metodos para mantener una red sin intrusos.

Para conseguir ese grado de conocimiento son necesarias unas nociones teóricas, expuestas a lo largo del Proyecto, describiendo la tecnología Wi-Fi, su modo de funcionamiento y todos los mecanismos necesarios para el buen funcionamiento de dicha tecnologia. Comprendiendo la base de la tecnología, resulta muchos más sencillo comprender donde se encuentran las vulnerabilidades de seguridad y que mecanismos de protección utilizar según la situación.

Para poder saber hasta donde llega el alcance de las vulnerabilidades y optimizar los sistemas de seguridad, es necesario conocer los ataques, incluso poder ponerlos en práctica, es por eso que se describen los principales ataques existentes sobre redes Wi-Fi actualmente.

Cualquier sistema operativo sirve para aprender de la inseguridad y mejorar la seguridad. No obstante, a la hora de realizar tareas de auditoría sobre redes Wi-Fi, se recomienda el uso de distribuciones basadas en Linux, puesto que la mayoría de herramientas están diseñadas para su uso en ese tipo de sistemas operativos.

Dicho esto tambien es verdad que actualmente la mayoria de heramientas para la uditoria,se estan haciendo versiones que puedan soportar el sistema operativo Windows,prueba de ello es el programa Commview.

De alguna forma se pretende introducir al lector al mundo de las auditorias con la herramienta Commview para wi-fi,como hacer la inyeccion de paquetes y tener nociones basicas a cerca de esta herramienta,para poder mantener las red wi-fi de una forma mas segura ,conociendo todos los por menores de la misma.

Capítulo 6

Glosario

AP-Access Point punto de acceso, estación base de una red Wi-Fi que conecta clientes inalámbricos entre sí y a redes de cable.

ARP-Address Resolution Protocol protocolo para traducir las direcciones IP a direcciones MAC. BSSID-Basic Service Set Identifier, Dirección MAC del punto de acceso.

CCMP-Counter-Mode / Cipher Block Chaining Message Authentication Code Protocol protocolo de encriptación utilizado en WPA2, basado en la suite de cifrado de bloques AES.

CRC-Cyclic Redundancy Check pseudo-algoritmo de integridad usado en el protocolo WEP (débil).

EAP-Extensible Authentication Protocol entorno para varios métodos de autenticación.

EAPOL-EAP Over LAN protocolo usado en redes inalámbricas para transportar EAP.

GEK-Group Encryption Key clave para la encriptación de datos en tráfico multicast (también usada para la integridad en CCMP).

GIK-Group Integrity Key clave para la encriptación de datos en tráfico multicast (usada in TKIP).

GMK-Group Master Key clave principal de la jerarquía de group key.

ARP-Address Resolution Protocol GTK-Group Transient Key, clave derivada de la GMK.

ICV-Integrity Check Value campo de datos unido a los datos de texto para la integridad (basado en el algoritmo débil CRC32).

IV. Initialization Vector, vector de inicialización, datos combinados en la clave de encriptación para producir un flujo de claves único.

KCK-Key Confirmation Key. clave de integridad que protege los mensajes handshake.

KEK-Key Encryption Key. clave de confidencialidad que protege los mensajes handshake.

MIC-Message Integrity Code. campo de datos unido a los datos de texto para la integridad (basdo en el algoritmo Michael).

MK-Master Key. clave principal conocida por el suplicante y el autenticador tras el proceso de autenticación 802.1x.

MPDU-Mac Protocol Data Unit. paquete de datos antes de la fragmentación.

MSDU-Mac Service Data Unit. paquete de datos después de la fragmentación.

PAE-Port Access Entity. puerto lógico 802.1x.

PMK-Pairwise Master Key. clave principal de la jerarquía de pares de claves.

PSK-Pre-Shared Key. clave derivada de una frase de acceso que sustituye a la PMK normalmente enviada por un servidor de autenticación.

PTK-Pairwise Transient Key. clave derivada de la PMK.

RSN-Robust Security Network. mecanismo de seguridad de 802.11i (TKIP, CCMP etc.).

RSNA-Robust Security Network Association. asociación de seguridad usada en una RSN.

RSN IE-Robust Security Network Information Element. campos que contienen información RSN incluida en Probe Response y Association Request.

SSID-Service Set Identifier. Identificador de la red (el mismo que ESSID).

STA-Station. Estación, cliente wireless.

TK-Temporary Key. Clave para la encriptación de datos en tráfico unicast (usada también para la comprobación de la integridad de datos en CCMP).

TKIP-Temporal Key Integrity Protocol. Protocolo de encriptación usado en WPA basado en el algoritmo RC4 (como en WEP).

TMK-Temporary MIC Key. Clave para la integridad de datos en tráfico unicast (usada en TKIP).

TSC-TKIP Sequence Counter. Contador de repetición usado en TKIP (al igual que Extended IV).

TSN-Transitional Security Network. Sistemas de seguridad pre-802.11i (WEP etc.).

WEP-Wired Equivalent Privacy. Protocolo de encriptación ,por defecto para redes 802.11.

WPA-Wireless Protected Access. Implementación de una versión temprana del estándar 802.11i, basada en el protocolo de encriptación TKIP.

Bibliografía

[1] IEEE Computer Society "IEEE 802.11: Wireless LAN Medium Access Control and Physical Layer Specifications", Aug. 1999.

[2] Tanenbaum, Andrew S.: Computer Networks, 4th Ed. Prentice-Hall, 2003.

[3] Halsall, Fred.: Rredes de computadores e Internes, 5ª Ed. Addison-Wesley, 2006.

[4] Stallings, William: Comunicaciones y Redes de Computadores, 7ª Ed. Prentice Hall, 2000.

[5] TCP/IP. Arquitectura, protocolos e implementación, 2ª Ed. Mc-Graw Hill.

[6] http://es.wikipedia.org/wiki/WIFI

[7] http://es.wikipedia.org/wiki/IEEE_802.11

[8] http://www.seguridadwireless.net/

[9] http://www.laperlaonline.com.ar/site/modules.php?name=Content&pa=showpage&pid=2

[10] http://www.virusprot.com/cursos/Redes-Inal%E1mbricas-Curso-gratis0.htm

[11] http://www.mailxmail.com/curso-redes-inalambricas-wi-fi-futuro-comunicacion