#1

UNDERCODE

TALLER DE SEGURIDAD WIRELESS

TEMAS

INTRODUCCIÓN
RESUMEN DE 802.11
FUNDAMENTOS
SEGURIDAD EN EL PROTOCOLO 802.11
DISTRIBUCIONES
Y MUCHO MAS..!

TUTOR

ARYENAL.BT

1. Introducción

Desde ya unos años, las tecnologías y las amenazas a las que se enfrentan las comunicaciones han crecido en gran número como en sofisticación. Unido al rápido incremento de su implantación, el riesgo al que se enfrentan este tipo de tecnologías se han agravado. No obstante, dicho peligro se ve superado por las ventajas y la comodidad que ofrecen las tecnologías inalámbricas, que han sido un factor importante en la propagación de estos dispositivos en hogares, oficinas y empresas por todo el mundo.

2. Resumen de 802.11

El estándar 802.11 define un protocolo inalámbrico de capa de enlace administrado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, Institute of Electrical and Electronics Engineers). Muchos piensan en WI-FI cuando se menciona el 802.11, pero no es exactamente lo mismo. Wi-Fi es un Sub-Conjunto del estándar 802.11 administrado por la Alianza Wi-Fi. Como el estándar 802.11 es tan complejo y el proceso requerido para su constante actualización involucra a tantas personas (un comité es el encargado de dicha tarea), casi todos los fabricantes de equipos inalámbricos decidieron que necesitaban un grupo más pequeño y dedicado a mantener la interoperabilidad entre los distribuidores y a promover esa tecnología con el marketing adecuado. Así se creó la Alianza WI-FI.

Este Sub-Conjunto se asegura de que todos los productos certificados con el logo Wi-Fi pueden funcionar juntos para un determinado grupo de acciones. De este modo si existe alguna ambigüedad en el estándar 802.11, la Alianza Wi-Fi define lo correcto. También permite a los distribuidores aplicar importantes Sub-Conjuntos de borradores de estándares (aquellos que no han sido todavía rectificados). El ejemplo más conocido de esta situación es el Acceso Wi-Fi protegido (WPA Wi-Fi Protected Access) o el equipamiento del prototipo 802.11n.

3. Fundamentos

Se sabe que el protocolo 802.11 proporciona un acceso inalámbrico a redes cableadas utilizando un punto de acceso (AP, Access Point). En el modo conocido como ad-doc o conjunto de servicio básico independiente (IBSS, Independent Basic Service Set); también se puede usar sin un AP. Como, normalmente, quienes están preocupados por la seguridad inalámbrica no hablan de redes ad-doc y debido a que los detalles del protocolo 802.11 cambian extraordinariamente cuando se encuentran en dicho modo.

El estándar 802.11 divide todos los paquetes diferentes: **datos, administración y control**, las cuales son conocidas como tipo de paquete.

- ✓ Los de **datos** se utilizan para transportar información de nivel superior, como los paquetes de IP
- ✓ Los de **administración** probablemente sean los más interesantes para los atacantes, ya que manejan la administración de la red.

- ✓ Los de **control** deben su nombre al término “control de acceso al medio” y se emplean para gestionar el acceso al medio compartido.

Cualquier tipo de paquete tiene muchos Sub-Tipos distintos. Por ejemplo, los de señalización (beacon) y los de desautenticacion (deauthentication) son dos ejemplo de Sub-Tipos de paquetes de administración; y los de solicitar para enviar (RTS, Request to Send) y Borrar para enviar (CTS, Clear to Send) son Sub-Tipos de paquetes de control.

4. Direccionamiento de los Paquetes 802.11

Al contrario que Ethernet, la mayoría de los paquetes 802.11 tienen tres direcciones:

1.- Origen

2.- Destino

3.- Identificador del conjunto de servicio básico (**BSSID**), el campo BSSID identifica de forma única el AP y su grupo de estaciones asociadas; normalmente posee la misma dirección MAC que la Interfaz Inalámbrica del AP.

Las tres direcciones indican a los paquetes quien los envía, hacia donde deben ir y que AP van a utilizar.

5. Seguridad en el protocolo 802.11

Posiblemente tendrán conocimiento que existen técnicas de cifrado muy diferentes que se utilizan para proteger las redes 802.11: la privacidad equivalente al cableado (WEP, Wired Equivalency Protocol), Acceso Wi-Fi protegido (WPA, Wi-Fi Protected Access) y el Acceso Protegido Wi-Fi 2 (WPA2, Wi-Fi Protected Access 2).

- ✓ **WEP (Privacidad Equivalente a Cableado):** es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.

- ✓ **WPA (Acceso Wi-Fi protegido):** es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo, Wired Equivalent Privacy (WEP).1 Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida

intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por The Wi-Fi Alliance («La alianza Wi-Fi»).

- ✓ **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.

6. Fundamentos del Descubrimiento

Antes de poder atacar una red inalámbrica, primero tenemos que encontrarla. Asique que para ello existen diversas herramientas disponibles pero todas ellas se pueden clasificar dentro de dos categorías principales:

Escaneo Activo: estas herramientas trabajan enviando paquetes de solicitudes de rastreo, en espera de una respuesta.

Contramedidas del Escaneo Activo: evadir un escáner activo es relativamente fácil pero tiene un inconveniente importante que se explicara enseguida. Como los escáneres activos solo procesan dos tipos de paquetes (respuesta de rastreo y de señalización), el AP tiene que ejecutar dos técnicas diferentes para ocultarse de forma efectiva.

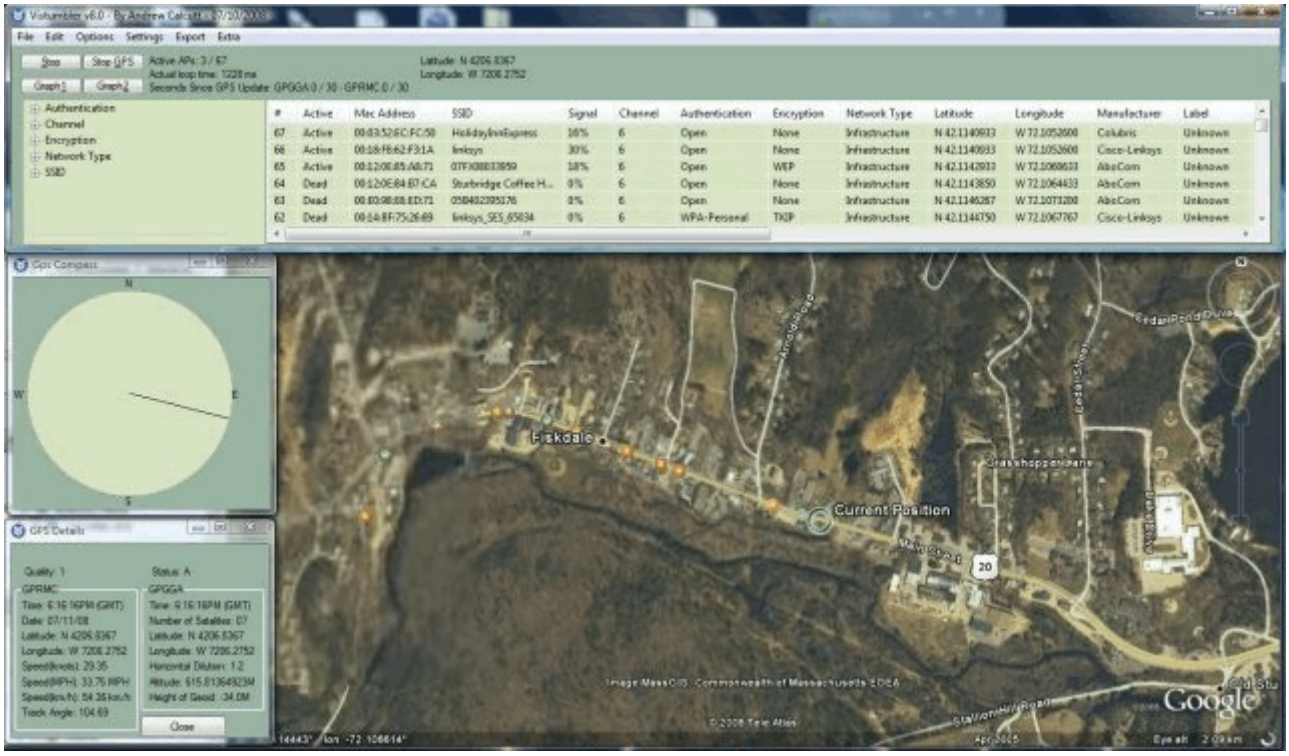
La primera técnica consiste en no responder a las solicitudes de rastreo que se le hayas enviado al SSID de transmisión. Si el AP ve una solicitud de rastreo dirigida a él y no contiene su SSID, responde. Siendo este caso, entonces el usuario ya conoce el nombre de la red y solo está buscando su conexión. Cuando la solicitud se envía al SSID de transmisión, el AP lo ignora. Podemos decir entonces que cuando se configura un AP para no responder solicitudes de rastreo de transmisión, también se censura su SSID.

Escaneo Pasivo: Son herramientas que están diseñadas para escanear las ondas de cualquier paquete en un determinado canal y paralelamente analizan dichos paquetes para determinar qué clientes se comunican con qué punto de acceso.

Contramedidas del Escaneo Pasivo: evadir un escáner pasivo es totalmente diferente al de evitar uno activo. Si está transmitiendo algo en un canal, un escáner pasivo lo visualizara, sin embargo para minimizar la exposición, se pueden tomar algunas opciones: si el AP lo admite y no tiene ningún cliente en 802.11 b/g heredado, deshabilite el modo mixto del AP y siga estrictamente 802.11n, esto hará que todos los paquetes de datos que transmite el AP utilicen dicha codificación.

La otra opción es la de colocar la red en la banda 802.11 de 5 GHz ¿**POQUE**?, pues porque muchos controladores no se preocupan en escanear este rango por que la mayoría de redes trabajan en 802.11 de 2.4 GHz y los atacantes solo quieren comprar un conjunto de antenas. Las tarjetas que admiten 5 GHz son más caras.

Nota: **evidentemente ninguna de estas precauciones evitaran o trataran de ser una barrera inquebrantable para alguien que se encuentre a unos treinta metros de su AP y que este muy interesado en localizar su red oculta la descubra.**



7. Distribuciones enfocadas a la Seguridad Inalámbrica

Una distribución y/o Live CD (hoy en días varios dedicados y equipados con herramientas o arsenales enfocados directamente a la seguridad informática) son de gran ayuda ya que podemos disponer rápidamente de herramientas muy poderosas y dispuestas a auditar un campo específico.

BackTrack: **(http://www.backtrack-linux.org) es** un arsenal penetración de Linux basada en las pruebas que los profesionales auxiliares de seguridad en la capacidad de realizar evaluaciones en un entorno puramente indígena dedicado a la piratería.

Wi-FiSlax: **(http://www.Wi-Fislax.com)** basado en el sistema operativo Linux, puede ser ejecutado sin necesidad de instalación directamente desde el CDROM o también desde el disco duro como LiveHD, además de poderse instalar en memorias USB o en disco duro. Wi-Fislax es un linux live cd diseñado por www.seguridadWireless.net y está adaptado para el Wireless.

AirUbuntu: **(http://sourceforge.net/projects/airubuntu/)** está basado en Ubuntu con las herramientas básicas para el crackeo de redes Wi-Fi, además contiene manuales en los que podemos identificar un manejo más preciso de las herramientas que tiene.

Nota: **No se han mencionado todas las distribuciones, pero si las más útiles que podrían utilizarse en el momento para auditar Tecnologías Inalámbricas y sobre todo tres de los mejores Live CD's, con los que paralelamente en el transcurso de este curso iremos familiarizándonos.**

8. Resumen:

En este capítulo hemos conocido un poco del protocolo 802.11, como está integrado un paquete de datos, que es un escaneo activo y pasivo al igual que sus contramedidas y distribuciones enfocadas y dedicadas para auditar tecnologías inalámbricas.