Stephen Blair Mandeville a.k.a Pandemic
Contact: 0xpandemic@gmail.com

Network Wireless Security

Autor:

Stephen Blair Mandeville Armería

INDICE

1 MARCO REFERENCIAL.

1.1 Resumen.

Dicho proyecto de investigación se basa en las actuales necesidades y problemas que se presentan día con día en las redes inalámbricas (networks), dichos problemas, muy alejados de ser pequeños problemas, son en realidad grandes y desastrosos en algunos casos, ya que no importa la índole por la que suceden simple y sencillamente el más pequeño o insignificante detalle, puede significar una perdida irremediable, no solo económicamente si no a nivel información. Actualmente gracias a los avances en cuanto a tecnologías de la información, podemos proporcionar amplios conocimientos de nuevas y mejores tecnologías que garantizan una amplia protección en la trasmisión y seguridad de los datos dentro de una red de computadores. Dentro de nuestra investigación partiremos del estándar 802.11 comentando sus generalidades y características, para después centrarnos en el estudio análisis e implementación de la tecnología WPA2 como una solución a los actuales problemas arriba citados.

1.2 Planteamiento del problema.

¿Es la seguridad WPA2 una solución viable y eficaz para solucionar la vulnerabilidad de las actuales redes inalámbricas?

1.3 Justificación.

Se pretende por medio de esta investigación, informar sobre los problemas que se presentan más comúnmente en las redes inalámbricas, así como dar a conocer los puntos débiles de las mismas, con la finalidad de crear conciencia acerca de la seguridad de nuestra información, así como proponer una alternativa informática para nuestra seguridad de datos en estas redes, en este caso dicha alternativa es la tecnología WPA2.

1.4 Delimitación del tema.

Dicha investigación solo abarcará los límites informativos y demostrativos, ya que solo informaremos y vamos a proveer de información a través de una demostración sencilla acerca de la tecnología WPA2.

1.5 Hipótesis.

La seguridad WPA2 es la solución más viable para los problemas de seguridad actual en las redes.

1.6 Objetivos.

1.6.1 Objetivo general.

Demostrar la eficacia de la seguridad WPA2 en la implementación de nuevos sistemas de seguridad para redes inalámbricas.

1.6.2 Objetivos particulares.

1) Ofrecer información clara y verídica acerca de la seguridad WPA2.

2) Proponer una posible solución para el problema descrito en el planteamiento del problema

2. MARCO TEORICO

Parte I: Preliminares.

2.1. Hacking 802.11

El estándar 802.11 define un protocolo inalámbrico de nivel vínculo y es administrado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Internet wi-fi es un subconjunto del estándar 802.11, el cual es administrado por la Wi-Fi Alliance. Debido a que el estándar 802.11 es tan complejo y el proceso necesario para actualizar el estándar (que está a cargo de un comité), los principales fabricantes de equipos inalámbricos decidieron que necesitaban un pequeño comité, el grupo más ágil dedicado a mantener la interoperabilidad entre los vendedores y a su vez la comercialización de tecnología. Esto dio lugar a la creación de la Alianza Wi-Fi.

La alianza Wi-Fi asegura que todos los productos con el logotipo de *Wi-Fi Certified* pueden desempeñar un determinado conjunto de funciones. La alianza Wi-Fi define lo "correcto" . La alianza también permite a los vendedores implementar subconjuntos importantes de estándares de proyecto (las normas que aún no han sido ratificadas). Un ejemplo muy conocido de este acceso protegido Wi-Fi es (WPA) o "proyecto" en equipos 802.11.

802.11 ofrece acceso inalámbrico a las redes de cable con el uso de un punto de acceso (AP). En lo que se conoce comúnmente como ad-hoc o independiente conjunto básico de servicios (IBSS) el modo de 802.11 También se puede utilizar sin un punto de acceso

El estándar 802.11 divide todos los paquetes en tres categorías diferentes: Datos, gestión y control. Estas categorías diferentes se conocen como, tipo de paquete. Los paquetes de datos se utilizan para llevar un mayor nivel datos (como los paquetes IP).

Los paquetes de gestión son probablemente, los más interesantes para los atacantes. Los paquetes de control reciben su nombre del término "control de acceso a los medios de comunicación."

Cualquier tipo de paquete dado tiene muchos subtipos diferentes. Los paquetes llamados beacons y desautentificacion (deauth) , son ejemplos de los subtipos de paquetes de gestión, y la solicitud de envío (RTS) y borrar para enviar (CTS) son paquetes de diferentes subtipos de paquetes de control.

2.2 Direccionamiento de paquetes 802.11

A diferencia de Ethernet, la mayoría de los paquetes 802.11 tienen tres direcciones: una dirección de origen, una dirección de destino, y un servicio básico de servicios de identificación (BSSID). El campo BSSID identifica de forma exclusiva al AP y su colección de estaciones asociadas, y es a menudo la misma dirección MAC en la interfaz inalámbrica de la AP.

Sin embargo no todos los paquetes tienen tres direcciones. Debido a que el "control frames" o marcos de control (tales como acknowledgements o ACK) es tan importante que el número de bits usados se debe mantener en un mínimo. IEEE también utiliza diferentes términos para describir las direcciones en los marcos de control o "control frames". En lugar de una dirección de destino, los marcos de control tienen una dirección de transmisión.

En la siguiente ilustración se muestra un paquete de datos típico. En este paquete el BSSID y la dirección de destino son los mismos porque el paquete estaba dirigido a nuestro AP, y el AP fue la puerta de enlace predeterminada. Si el paquete estaba destinado a otra máquina en la misma red inalámbrica, la dirección de destino sería diferente a la BSSID.

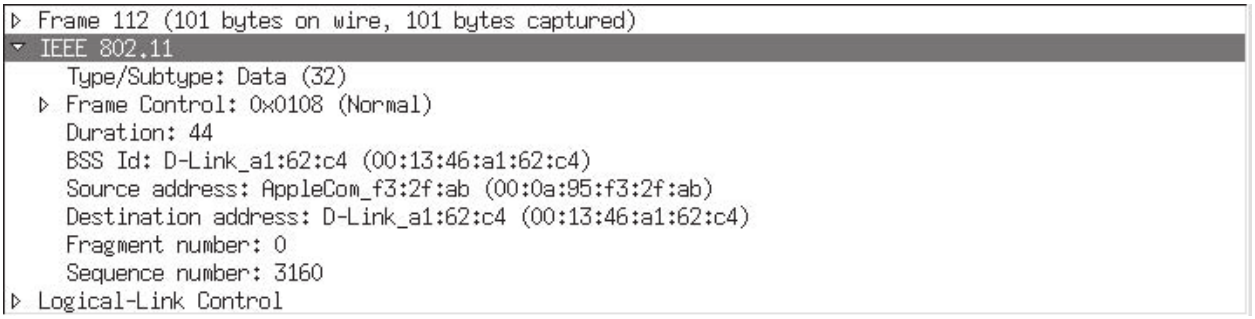

Imagen 2.1. Típicos paquetes de datos,

2.3. WEP & WPA.

Hay dos técnicas de encriptación muy diferentes que se utilizan para proteger las redes 802.11: Por cable Wired equivalent protocol (WEP) y Wi-Fi Protected Access (WPA). WEP es el más antiguo, con un nivel de extrema vulnerabilidad. WPA es mucho más moderna. Redes WEP (normalmente) se basan en un estático 40 - o key de 104 bits que se conoce en cada cliente. Esta clave se utiliza para inicializar un cifrado de flujo (RC4). Muchos ataques son interesantes contra RC4 en la forma en que se utiliza en WEP. WPA se puede configurar de dos modos muy diferentes, clave pre-compartida (PSK) (o contraseña) y el modo de empresa (Enterprise). Ambos se explican brevemente a continuación.

WPA Pre-Shared Key (WPA-PSK) funciona de manera similar a WEP, ya que exige que la parte de conexión proporcione una clave con el fin de obtener acceso a la red inalámbrica. Sin embargo ahí es donde terminan las similitudes.

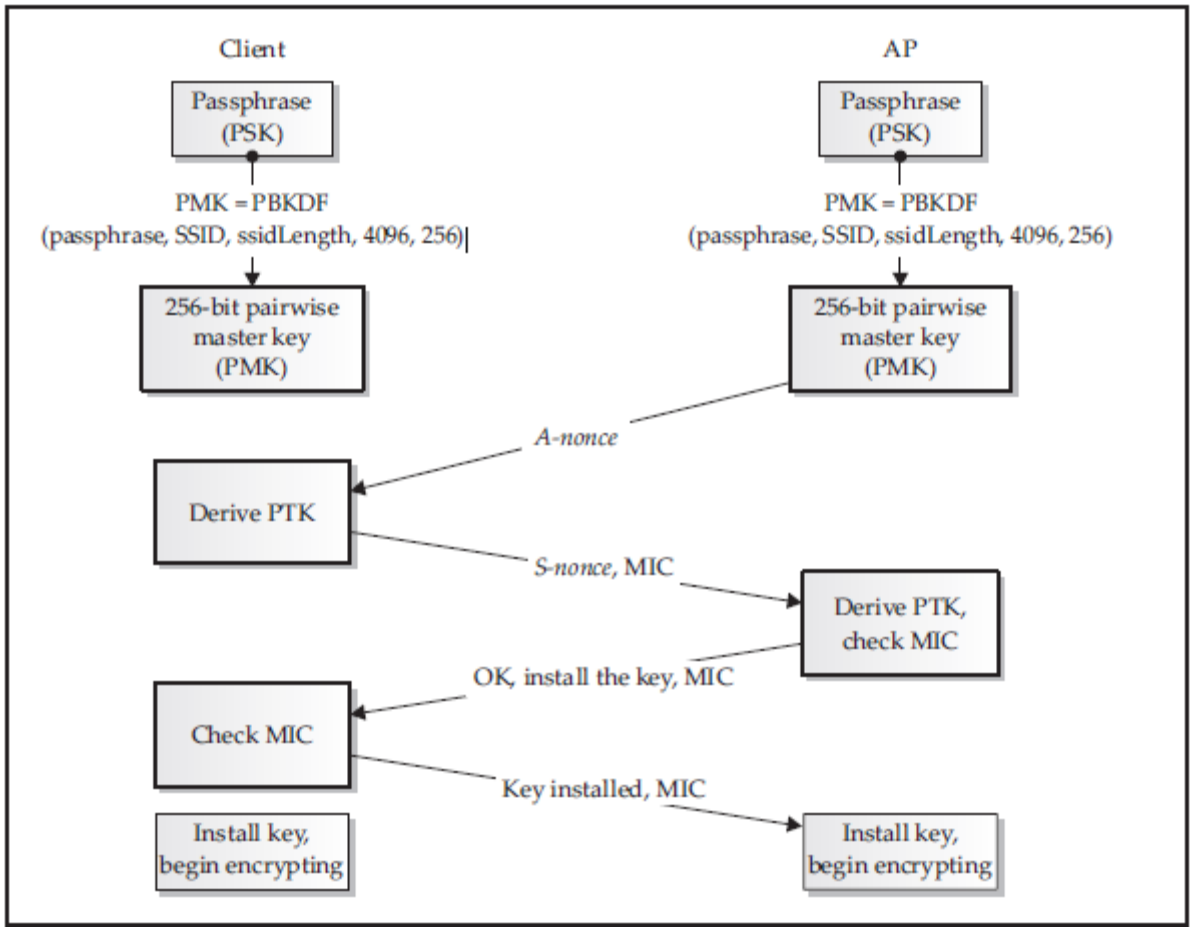

Imagen 2.2. proceso “Four-way handshake”.

La clave pre-compartida (contraseña) puede estar en cualquier lugar entre 8 y 63 caracteres ASCII imprimibles de largo. El cifrado que se utiliza con WPA se basa en una clave maestra en pares (PMK) la cual se calcula a partir de la clave pre-compartida y SSID. Una vez que el cliente tiene la PMK, y el AP se negocia una nueva clave, la clave temporal llamado por parejas transitoria (PTK). Las claves temporales se crean de forma dinámica cada vez que el cliente se conecta y se cambian periódicamente. Se trata de una función de la PMK, un número al azar (suministrado por la AP, llamado nonce), otro número al azar (suministrado por el cliente, llamado S-nonce) y las direcciones MAC del cliente y el AP. La razón por la que las claves se crean a partir de tantas variables es para asegurarse de que son únicas y no repetitivas.

El punto de acceso verifica que el cliente realmente tiene el PMK checando la integridad del mensaje de código (MIC) sobre el terreno durante el intercambio de autenticación. El MIC es un hash criptográfico del paquete que se utiliza para evitar la manipulación y para verificar que el cliente tiene la llave. Si el MIC no es correcto, eso significa que la PTK y el PMK son incorrectas porque la PTK se deriva de la PMK.

Cuando se ataca a WPA, se deben considerar dos aspectos iniciales, los cuales son: Si la red está configurada en pre-modo de clave compartida, la PMK le permite leer el tráfico de todos los otros clientes y que se autentique con éxito.

A pesar de WPA-PSK tiene casos similares como el uso de las implementaciones tradicionales de WEP, que sólo debe utilizarse en el hogar o pequeñas oficinas. Dado que la clave pre-compartida es todo lo que se necesita para conectarse a la red, si un empleado en una gran red sale de la empresa, o un dispositivo es robado, toda la red debe ser reconfigurada con una nueva clave. En su lugar, WPA Enterprise se debe utilizar en la mayoría de las organizaciones, ya que proporciona la autentificación individual, la cual permite un mayor control sobre quién puede conectarse a la red inalámbrica.

2.4. WPA Enterprise.

La autenticación en una red basada en WPA en el modo de empresa (WPA Enterprise), la PMK (Pair-wise Master Key) se crea de forma dinámica cada vez que un usuario se conecta. Esto significa que incluso si se recupera un PMK debe suplantar a un usuario único para una conexión específica.

Con WPA empresarial o WPA Enterprise, la PMK se genera en el servidor de autenticación y luego se transmite hacia el cliente. La AP y el servidor de autenticación se comunican con un protocolo llamado RADIUS. RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Server) es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP mediante módem, DSL, cablemódem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo Network Access Server (NAS) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

El servidor de autenticación y los mensajes de cambio de los clientes utilizan la AP como repetidor. El servidor en última instancia toma la decisión de aceptar o rechazar el usuario, mientras que la AP es la que facilita la conexión sobre la base de las decisiones del servidor de autentificación. Desde el punto de acceso actúa como (* repetidor RELAY), que tiene el cuidado de enviar sólo los paquetes desde el cliente que sean para fines de autenticación y no se transmiten paquetes de datos normales hasta que el cliente se ha autenticado correctamente.

Suponiendo que la autenticación es satisfactoria, el cliente y el servidor de autenticación obtienen la misma PMK. Los detalles de cómo se crea la PMK variar según el tipo de autenticación, pero lo importante es que es un número aleatorio criptográficamente fuerte, ambos lados se puede calcular. El servidor de autenticación entonces le dice a la AP que permite al usuario conectarse y también envía la PMK a la AP. Debido a que los PMK (Pair wise Master Key) se crea de forma dinámica, la AP debe recordar que PMK le corresponde a cada usuario.

Una vez que todas las partes tienen la PMK, el AP y el cliente participan en el mismo saludo de cuatro vías, este proceso confirma el cliente y el punto de acceso que tengan los PMK correctas y se puede comunicar correctamente.

2.5. EAP & 802.1X.

Probablemente se ha notado que muchos paquetes tienen EAP en ellos, EAP significa protocolo de autenticación extensible (Extensible Authentication Protocol). Básicamente EAP es un protocolo diseñado para el transporte de autenticación arbitraria, una especie de meta-autenticación de protocolo.

IEEE 802.1X es un protocolo diseñado para autenticar a los usuarios en LAN´s cableadas. 802.1X aprovecha EAP para la autenticación, y WPA utiliza 802.1X. Cuando el cliente envía los paquetes de autenticación a la AP, que utiliza EAPOL (EAP sobre LAN) un estándar especificado en la siguiente imagen.

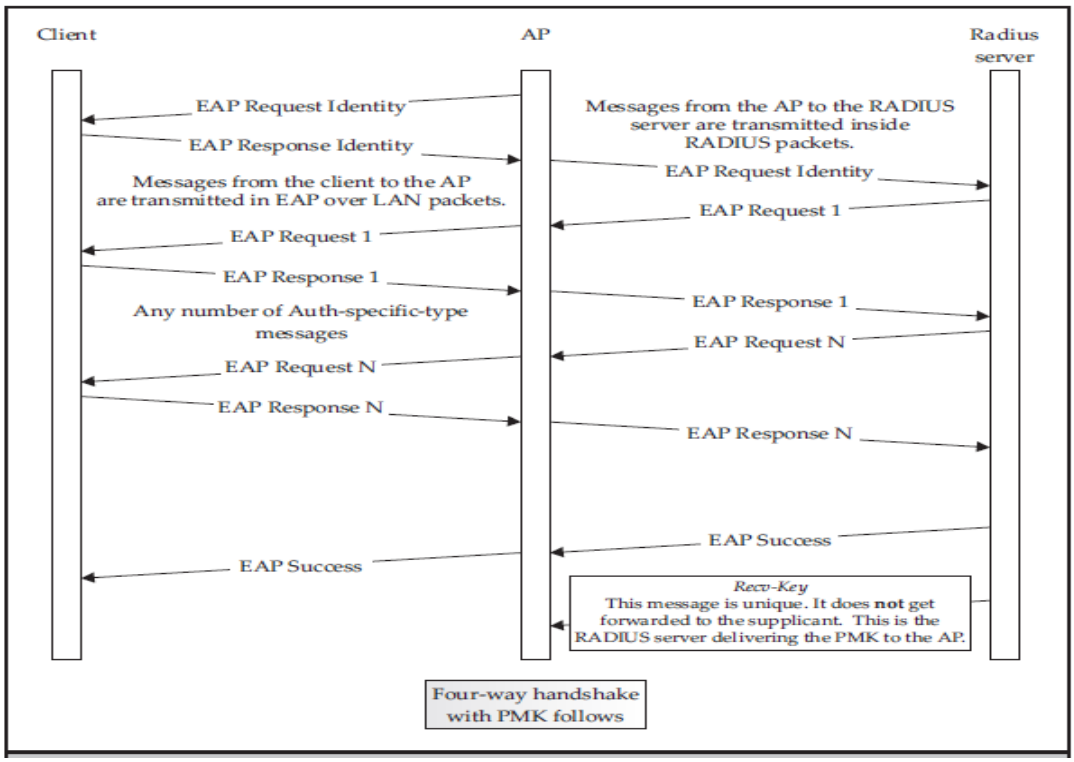

Imagen 2.3. Estándar EAPOL.

2.6. Chipsets & drivers.

2.6.1. Atheros

Esta lista de chipsets inalámbricos y controladores no pretende ser exhaustiva sino que es una lista de los chipsets más comunes con el soporte de Linux. Chipsets que no cuentan con una moderna mac80211 como conductor o son demasiado viejos para considerarse como eficaces no se muestran.

2.6.2. Atheros (AR5XXX, AR9XXX)

Los conjuntos de chips Atheros siempre han sido muy favorecidos por la comunidad hacker debido a su extensibilidad y porque se encuentran en las tarjetas de gama alta prived por Ubiquiti. También tienen el mayor apoyo para la inyección en Windows.

El kernel de linux tiene cuatro controladores únicos que dan soporte a conjuntos de chips Atheros:

madwifi: Este controlador fue el caballo de batalla por bastante tiempo, durante su reinado nunca fue lo suficientemente estable y se fusionó en el núcleo principal. Madwifi es completamente independiente.

ath5k: Este controlador es el sucesor lógico de madwifi. Es lo suficientemente estable como para ser incluido en el kernel de Linux, y al igual que todos los conductores modernos inalámbricos en Linux, que hace uso de mac80211. Ath5k proporciona soporte para muchos dispositivos que utilizan la familia de chipsets AR5XXX, sin embargo no proporciona el soporte para USB y no soporte 802.11n.

ath9k: Recientemente ofrece la mejor esperanza de un apoyo estable para los chipsets 802.11n de gran alcance en Linux. De cualquier forma el controlador original fue desarrollada por Atheros, la comunidad de código abierto ahora se mantiene.

AR8170usb: Este controlador es la única que ofrece soporte para dispositivos USB con chipset Atheros. En particular, se ofrece (Sharky) apoyo para el chipset AR9170, cual se encuentra en el SR71-USB de Ubiquiti. Aunque el chipset que soporta, este controlador en la actualidad no tiene soporte 802.11n

Imagen 2.4. Chip Atheros.

2.6.3. Broadcom (B43XX)

Broadcom tiene una parte muy importante del mercado de chips 802.11. Chipsets de Broadcom se encuentran más comúnmente integrados en muchos portátiles, a pesar de que se encuentran en tarjetas externas, los chipsets de Broadcom en la familia de B43 son compatibles con el controlador b43 mac80211 en linux.

Aunque no se recomienda comprar una tarjeta Broadcom basada explícitamente en 802.11, si desea utilizar un chipset Broadcom integrado en su computadora portátil y el conductor b43 lo reconoce, es probable que tengas algunos problemas de compatibilidad.

Imagen 2.5. Chip Broadcom

2.6.4. Intel Pro Wireless & Intel Wifi Link (Centrino)

Intel 802.11 chipsets se encuentran comúnmente integrados en los portátiles, el mayor 2100, 2200 y 2915 son compatibles con los controladores IPW en Linux. Conjuntos de chips más recientes son compatibles con el iwlwifi o el controlador de iwlagn. Todos estos factores se combinan en los últimos núcleos.

Imagen 2.6. Chipsets Intel.

Intel chipsets tienen la ventaja agradable de un sólido respaldo por parte del proveedor. Sin embargo, no se encuentran en tarjetas externas de gran alcance. Si tienes un portátil con un chipset integrado Intel, probablemente va a ser usando para propósitos de prueba, pero los hackers serios querrán al fin una solución más potente.

2.6.5. Ralink (RT2X00)

Ralink es uno de los fabricantes de chips 802.11 más pequeños. Ralink cuenta con el apoyo de un código abierto excelente. Ralink es uno de los pocos fabricantes de chipsets que tienen soporte sólido USB en Linux (el otro es el Realtek RTL8187 y con su RTL8188 chipset).

Los nuevos controladores Ralink se conocen colectivamente como rt2x00. Este controlador se mantiene en el núcleo y utiliza mac80211. Aunque el controlador in0tree rt2x00 es menos optimizado para el hacking inalámbrico, tiene la ventaja de estar disponible en cualquier distribución moderna. Por lo tanto, contando con el apoyo de los núcleos en el futuro, mientras que los existentes pueden necesitar parches para seguir trabajando con el tiempo.

Ralink tiene un buen número de conjuntos de chips. La mayoría de usuarios de Linux están interesados en las variantes o rt73usb rt5usb. Dispositivos basados en USB con un chipset rt2570 o rt73 son una buena opción para una segunda interfaz de inyección sólo en Linux. Este chipset es una de las pocas que no presentan complicaciones.

Imagen 2.7. Ralink RT2X00

2.7. Algunos datos que debe saber.

2.7.1. Potencia

Transmit (TX) de potencia, por supuesto, se refiere a qué tan lejos, su tarjeta puede transmitir y se expresa generalmente en milivatios (mW). La mayoría de las tarjetas de nivel de consumo tienen una velocidad transmisión de 30 mW (14,8 dBm).

2.7.2. Sensibilidad

Muchas personas pasan por alto la sensibilidad de una tarjeta y se centran en su potencia de transmisión. Una tarjeta que es significativamente coincidente será capaz de transmitir a grandes distancias, pero no es capaz de recibir la respuesta. Si usted puede encontrar la hoja de datos de un producto, la sensibilidad debe ser mencionada. La sensibilidad se mide en dBm (decibeles relativos a 1 mW). Cuanto más negativo sea el número, mejor serán los resultados (-90 es mejor que -86).

2.7.3. Antena apoyo

La última cosa a considerar cuando se compra una tarjeta es el soporte de la antena. Si su trabajo es mantener la seguridad o auditar una red inalámbrica, usted definitivamente necesita conseguir una o dos antenas.

En la actualidad, algunas tarjetas, ya sea con cero, uno o dos conectores de antena, necesitan por lo menos dos antenas para apoyar el "**MIMO**" que quiere decir: *Multiple-input Multiple-output*.

2.8. Antenas

El tipo de la antena determina su patrón de radiación puede ser omnidireccional, bidireccional, o unidireccional.

- *Las antenas Omnidireccionales* son buenas para cubrir áreas grandes, en la cual la radiación trata de ser pareja para todos lados es decir cubre 360°.
- *Las antenas Direccionales* son las mejores en una conexión Punto-a-Punto, asi como en los acoplamientos entre los edificios, o para los Clientes de una antena omnidireccional.

2.9. Software's para auditoria en redes inalámbricas

A continuación se hace un listado de algunos de los software más importantes y más conocidos por sus buenos resultados en el manejo de auditorías para redes de forma inalámbrica.

- A irTraf
- Aphunter
- APradar
- BSD-airtools (dstumbler)
- Classic Stumbler (mac)
- Gtkskan
- HermesAP monitor patch
- iStumbler (mac)
- KisMAC (mac)
- Kismet
- Kismet Log Viewer
- Kismet parse
- MacStumbler (mac)
- Mognet
- Perlskan
- Prismdump
- Prismstumbler
- Prismsnort
- SSIDsniff
- THC-Wardrive
- WaveStumbler
- Wellenreiter
- Wellenreiter for OPIE not mirrored
- Wi-Find
- WifiScanner
- Wispy-Tools
- Wistumbler
- Wlan-scan
- aircrack-ng suit.

2.10. Detección de redes

Los detectores de red o software de descubrimiento de red son programas informáticos que facilitan la detección de redes LAN inalámbricas con los estándares WLAN 802.11b, 802.11a 802.11g, 802.11n. Existen 2 maneras de exploración de redes, *Activa y pasiva*.

- **Exploración activa:** se realiza mediante el envío de varias solicitudes de sonda y registro de las respuestas de la sonda. La respuesta de la sonda que se reciben normalmente contiene BSSID y SSID de WLAN. Sin embargo si la transmisión de SSID ha sido desactivada, y la exploración activa es el único tipo de escaneo compatible con el software, las redes no se mostrarán.

- **Exploración pasiva:** escucha todos los datos enviados por los puntos de acceso. Una vez que un usuario legítimo se conecta con la AP, la AP finalmente envía un SSID en texto plano. El equipo que ejecuta el escáner de detección de redes se dará cuenta de este SSID por los usuarios legítimos.

2.11. Atacando 802.11

Las defensas de la red inalámbrica pueden caer en varias categorías diferentes. La primera categoría seria "totalmente ineficaz", también conocida como la seguridad por oscuridad, es trivial para irrumpir a través de cualquiera que esté realmente interesado en hacerlo.

El siguiente tipo de defensa podría ser clasificado como "molesto". En general, WEP y un diccionario basado en contraseñas WPA-PSK se ajustan a esta categoría. Teniendo en cuenta un poco de tiempo y habilidad, un atacante puede recuperar cualquier clave WEP estática.

La tercera categoría de la defensa se basa en las redes que requieren un esfuerzo genuino y cierto nivel de habilidad de penetrar en ellas. La mayoría de las redes no están bien protegidas. WPA entra en esta categoría de uso.

Muchas redes inalámbricas hoy en día operan en modo oculto, estas redes no incluyen su SSID (nombre de red) en los paquetes de envió, y no responde difundiendo peticiones de sondeo. Las personas que configuran sus redes así deben concebir su SSID como una especie de secreto. Las personas que hacen esto también pueden ser propensas a permitir el filtrado de direcciones MAC del AP.

2.12. Des autentificando Usuarios

Se puede hacer esto basándonos en los marcos de gestión en 802.11 que no estén autentificados. Si los marcos de gestión se han autenticado, el usuario sería capaz de decirle a su paquete de deauthentication los puntos de acceso. Así que todo lo que necesitamos hacer es enviar un paquete que, para el usuario, parece como si viniera de la AP. El usuario no puede notar la diferencia, y el controlador inalámbrico se volverá a conectar de inmediato. El usuario entonces transmitirá la solicitud de re-asociación con el SSID en el mismo, y el escáner le permitirá saber el nombre de la red.

Este ataque es efectivo independientemente de que tipo de seguridad de la AP está de por medio.

2.13. La derrota de filtrado de direcciones MAC

Con el fin de superar el filtrado de MAC, lo único que se tiene que hacer es conseguir un MAC de otra persona que ya este en la red, para ello es necesario ejecutar un rastreador pasivo,

acción que nos puede dar la dirección de un cliente que ya está conectado. El escenario más elegante es que espere a que un usuario se desconecte de la red por su propia cuenta.

2.14. MAC Filter medidas de prevención

Si está utilizando el filtrado de MAC, no se puede hacer nada para impedir que la gente irrumpa en su privacidad.

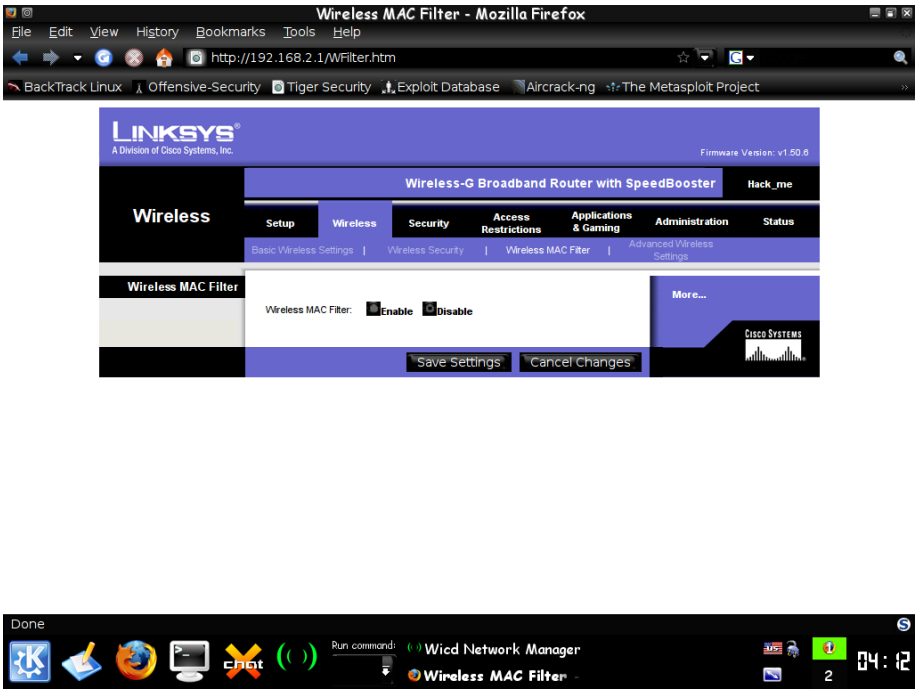

Imagen 2.8. Mac filter

2.15. La derrota del WEP

Las claves WEP vienen en dos tamaños: 40 bits (5byte) y 104 bits (13 bytes). Inicialmente, los vendedores sólo proporcionaban claves de 40 bits. Según los estándares de hoy, las claves de 40 bits son ridículamente pequeñas. Hoy en día, muchas personas utilizan claves de 104 bits. Debe tenerse en cuenta que algunos vendedores se refieren a estos como claves de 64 bits y 128 bits. Algunos vendedores incluso ofrecen claves de 256 bits. Los vendedores llegan a estos números porque WEP utiliza un vector de inicialización de 24 bits, sin embargo, la longitud de la clave es efectivamente 40 o 104 bits.

Parte II: Actividad practica llevada a cabo por el equipo.

2.16. Métodos de crackeo de red wireless con cifrado de 64/128 bits .

Este fue el equipo utilizado para la auditoria wireless.

Imagen 2.9. Equipo piloto de práctica.

Especificaciones:

- Toshiba L655 (RTL8188CE driver)-Ralink
- Linksys WUSB54GC (RT73 driver) -Ralink
- Linksys router WRT54GS ver 6.

Antes que nada tenemos que saber el tipo de chipset y driver que va mejor de acuerdo a nuestra interfaz; para este caso tuvimos que instalar el driver RTL8188CE de la tarjeta por default de la portátil *Toshiba satellite L655.*

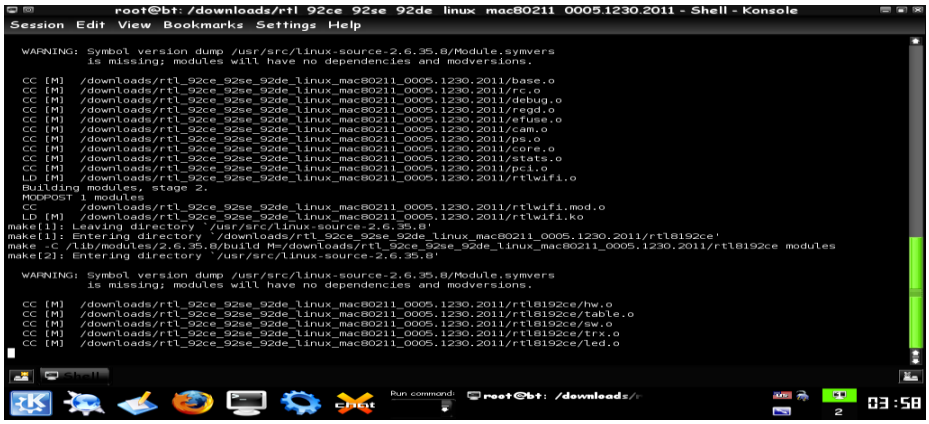

Imagen 2.10. Comienzo de la práctica.

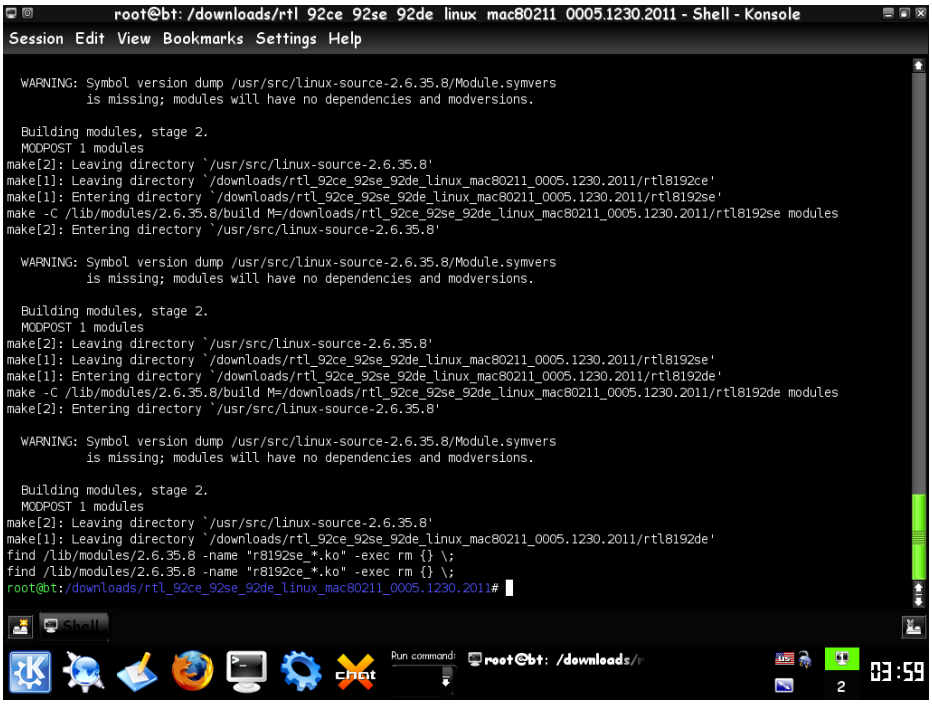

Imagen 2.11. Instalación del driver.

Una vez instalado, es necesario reiniciar el computador, para que la instalación tome efecto.

Una vez reiniciado, procedemos a conectar y configurar nuestro router, para que tenga una seguridad de 64 bits en su password. Nuestro router estará transmitiendo en frecuencia 2.4 Ghz en canal 2 en banda G, este router tiene la opción de transmitir en banda G o B o Mezclados.

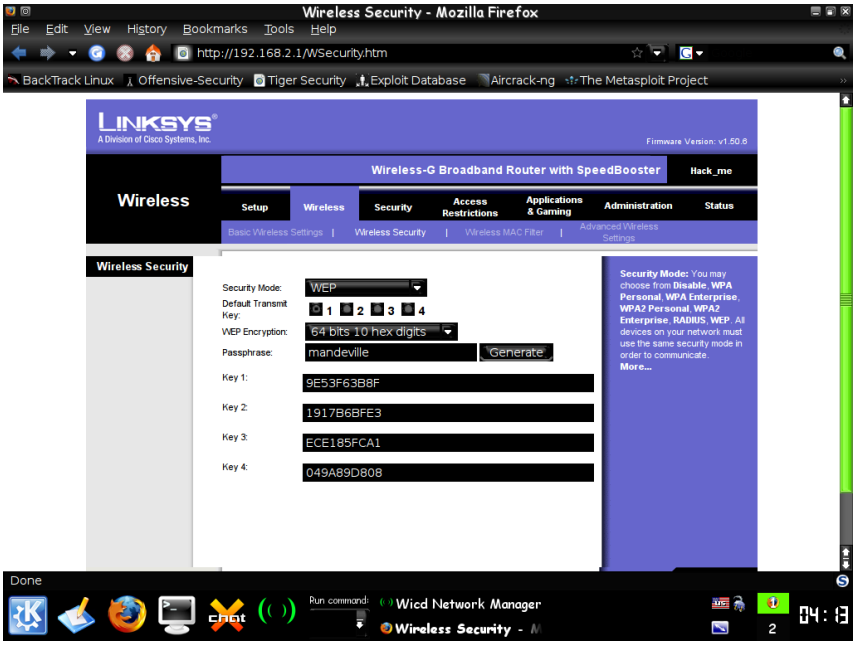

Imagen 2.12. Configuración del Router.

Nuestro AP será llamado Hack_me, para poderlo identificar rápido y fácilmente ante los Aps que lleguen a aparecer.

Seguido de esto lo que necesitamos ahora saber es en qué modo se encuentra nuestra interfaz a utilizar, existen 2 modos para las tarjetas, Managed (activo), Monitor (pasivo).

Podemos darnos cuenta con nuestro comando *iwconfig* muchas de las características de nuestra tarjeta, desde el poder de transmicion (TX) el tipo de bandas que maneja (a/b/g/n) si es que se encuentra escuchando en algún canal en especifico, si se encuentra asociado a algún punto de acceso, password de el punto de acceso asociado entre otras…

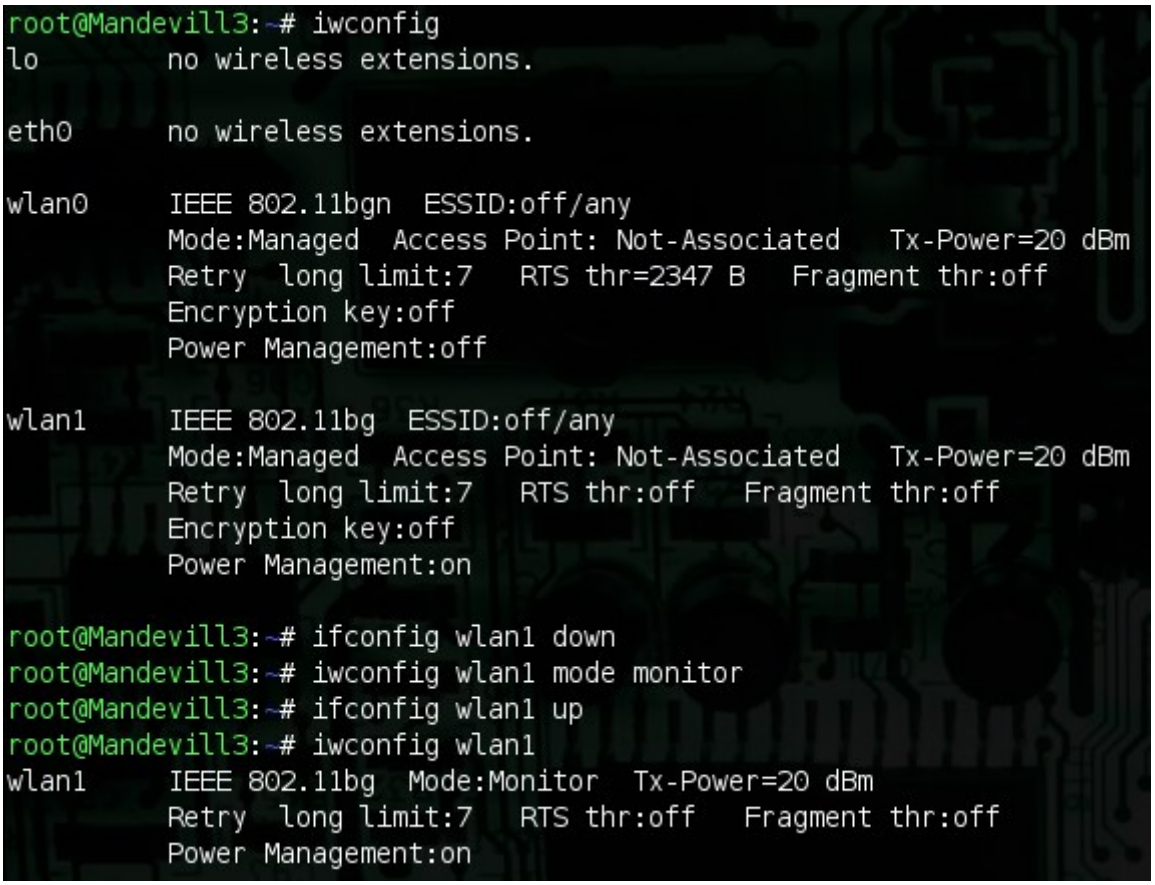

Imagen 2.13. Estado de la Interfaz.

En dicha imagen 2.13. Lo que hace el comando *ifconfig* fue dar de baja la interfaz wlan1 , seguido del comando *iwconfig wlan1 mode monitor* lo que se está haciendo aquí es poner nuestra interfaz en modo monitor ya que al inicio estaba en modo managed (activo) y asi no podremos realizar la captura de paquetes para un crackeo exitoso.

Una vez que tengamos nuestra interfaz lista para la captura de paquetes en el aire, pasamos a checar el tipo de driver que utilizaremos y si es compatible para inyección de paquetes,

utilizaremos el programa *arimon-ng* este se encuentra dentro de la suite de *aircrack-ng* que estaremos utilizando a lo largo de nuestra auditoria.

Imagen 2.14. Interfaces disponibles.

En la imagen 2.14 vemos que tenemos 2 interfaces disponibles, la primera wlan0, que no reconoce el tipo de chipset pero en realidad es Ralink, lo podemos deducir por el driver que utiliza (rtl8192ce) la segunda es nuestra USB que usaremos para la auditoria, usando el driver RT73USB (compatible para inyecciones).

Imagen 2.15. Opciones de interfaz.

En la imagen 2.15 se muestra parte del menú de *airodump-ng* dicho software se encuentra también incluido dentro de la suite de *aircrack-ng* la principal función de *airodump-ng* es capturar todo tipo de paquetes y conexiones que se lleven a cabo dentro de los estándares de 802.11 maneja todas las bandas y tiene una gran gama de configuraciones.

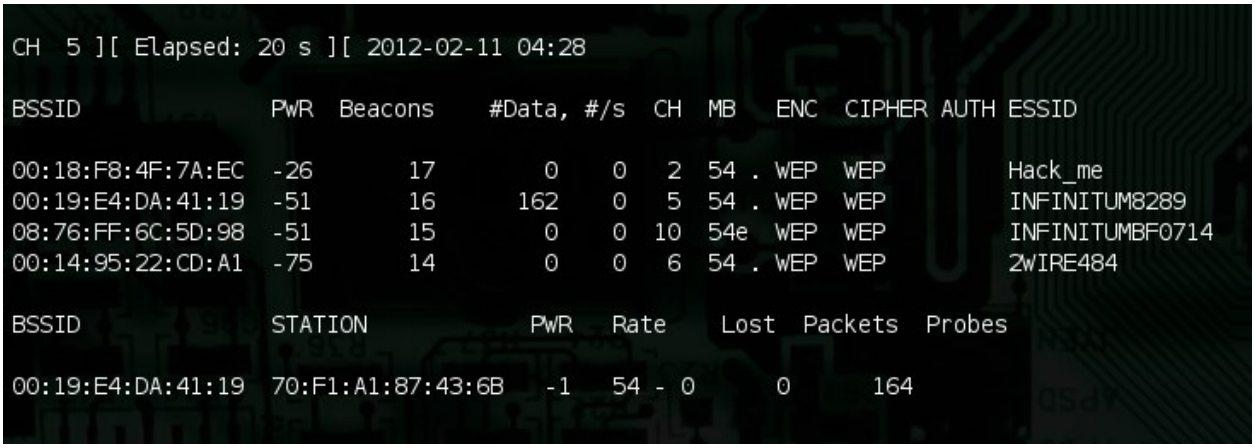

Imagen 2.16. Funcionamiento del *airodump-ng*.

En la imagen 2.16 se muestra a *airodump-ng* funcionando, hagamos un análisis a lo que estamos viendo.

• BSSID: La dirección MAC del AP (punto de acceso).

• PWR: La intensidad de señal que recibimos del AP.

• Beacons: Son tramas no validos para nuestra auditoria de la red.

• #Data: Paquetes de datos válidos, estos son los que nos interesan.

• #/S: Aquí vemos a que ritmo crecen los #Data, es útil para ver a que velocidad estamos inyectando.

• CH: El canal sobre el que opera el AP.

• MB: Velocidad del AP. -- 11 → 802.11b // 54 → 802.11g

• ENC, CIPHER, AUTH: Estos 3 campos están relacionados con la cifrado.

• ESSID: El nombre del AP.

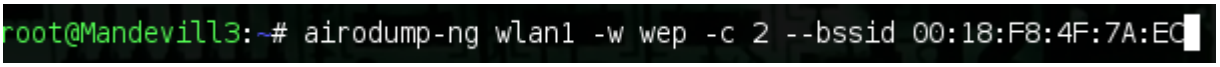

Imagen 2.17. Comando *airodump-ng.*

Seguido de la siguiente línea de comandos estaremos indicando a *airodump-ng* que utilice la interfaz *wlan1* que guarde el archivo con el nombre de *wep,* que este a la escucha únicamente en el canal *2* y solamente capture los paquetes transmitidos de nuestro punto de acceso definido por el *bssid.*

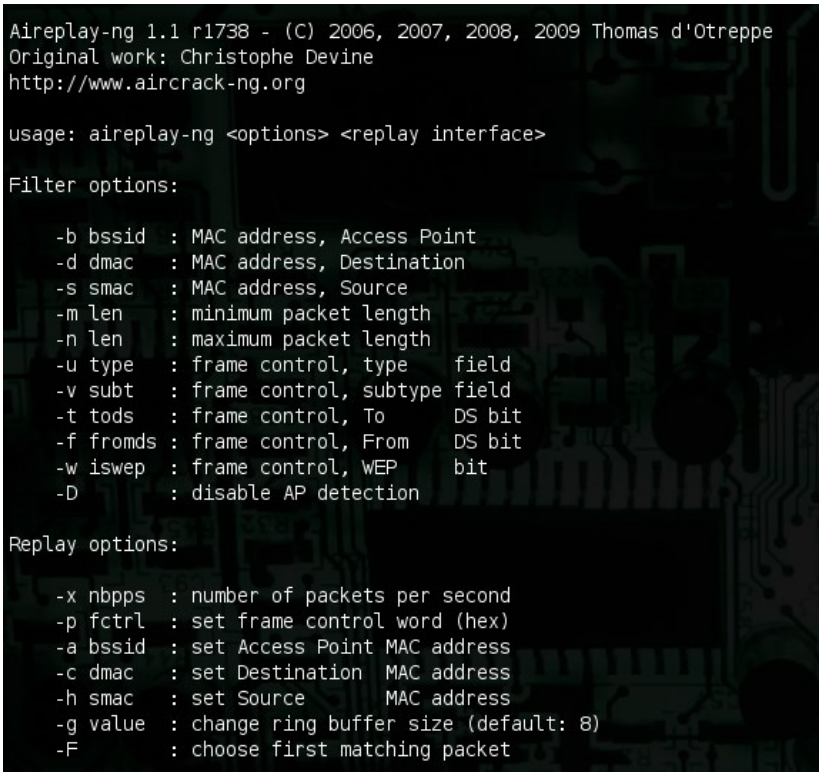

Imagen 2.18. Menú de aireplay-ng.

La imagen anterior muestra parte del menú de *aireplay-ng* incluido también dentro de la suit *aircrack-ng,* este software lo utilizaremos para realizar la mayoría de nuestra auditoria wireless.

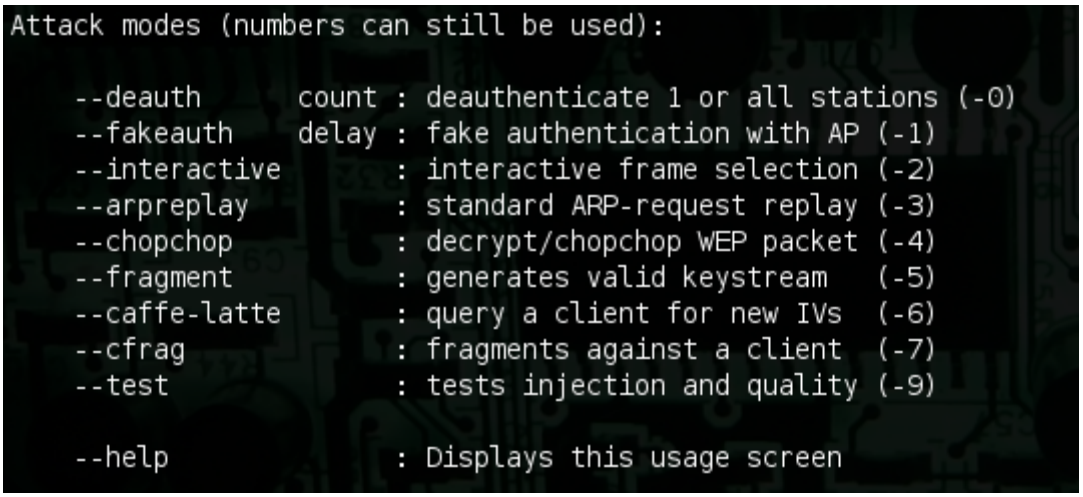

Imagen 2.19. Modos de ataque.

Con una amplia variedad de tipos de ataques, cada uno tiene su función específica y no todos tienen el mismo impacto ante nuestro objetivo, se debe de tener bien claro, qué es lo que queremos hacer y el por qué de todo lo que haremos, tener claro el significado de WEP, WPA sus funciones, en otras palabras, saber qué tipo de cifrado es el que queremos desencriptar.

Una cosa que hay que tener claro, es la dirección MAC de nuestra interfaz, ya que hay una variedad de ataques que es indispensable asignar un destinatario.

Imagen 2.20. Dirección MAC.

A continuación se muestra un ataque a una red inalámbrica con cifrado WEP, la contraseña previamente establecida y mostrada, es de 64-bits, esto significa que contiene 10 caracteres hexadecimales, los primeros pasos a realizar una vez en modo monitor nuestra interfaz, es ver si tiene autentificación OPN (abierta), en caso de que fuese así, nos permitiría inyectar tráfico para así poder generar la suficiente cantidad de IV's para desencriptar nuestra contraseña, pero ¿Cómo es que obtengo una autentificación si no la muestra OPN?

Hay varias maneras de realizar esto:

1. Esperar a que un cliente se vuelva a conectar, ya que para esto previamente explicado, contiene un paquete de autentificación con SSID dentro que a la vez si estuviera oculto el SSID este cliente lo revelaría.

2. Enviar una falsa autentificación (Fake-auth) esto nos permitirá obtener una autentificación satisfactoria entre nuestro punto de acceso.

3. Kick off an user o desconectar a un usuario de el punto de acceso para que así vuelva a re-autentificarse

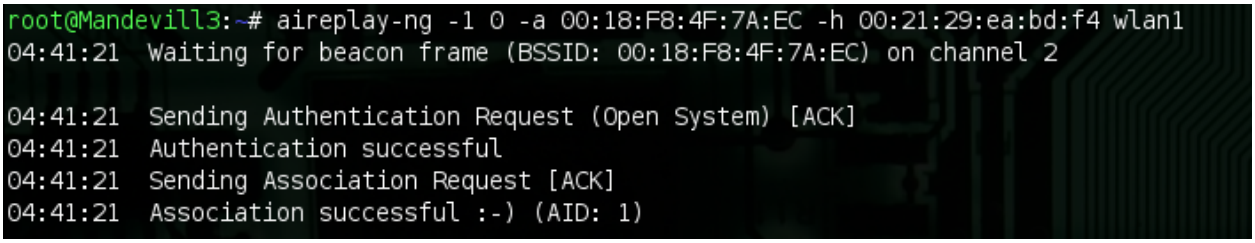

Imagen 2.21. Especificación de ataque.

Aireplay-ng -1 0 indica el tipo de ataque en este caso será de "authentificacion" y la cantidad de autentificaciones que hará, en este caso 0, puede ser 1, 5 etc.

-a indicamos la dirección MAC de nuestro punto de acceso a atacar.

-h Nuestra dirección MAC donde queremos que regresen las respuestas y paquetes.

Wlan1 El nombre de nuestra interfaz

ACK= acknowledgment viene a un acuerdo de ambos, cliente – Ap, correcto.

Una vez que nuestra asociación con el punto de acceso fue satisfactoria, comenzamos a la escucha de tráfico y toda la ***data*** que encontremos en el aire, volviendo a ***airodump-ng*** e inyectamos trafico con ***aireplay-ng*** para así obtener un aumento en la cantidad de datos necesarios para la obtención de nuestro **password**.

Imagen 2.22. Inyección de tráfico en la dirección MAC indicada.

Para la inyección de trafico tuvimos que sustituir la letra –a en *aireplay-ng* por la letra *–b* que vendría siendo igual para el BSSID, simplemente que si no la sustituimos no podrá comenzar la inyección de tráfico.

Con la función *–x 1023* podremos ajustar la cantidad de **pps** (packets per second o paquetes por segundo) enviados hacia el Ap. (máximo 1024)

Una vez realizado satisfactoriamente y podemos observar un gran incremento ante nuestros **ACK y ARP's**, podemos regresar a la ventana de *airodump-ng* donde observaremos claramente el aumento de #data , esencial para la desencriptación de nuestra **key** de 64-bits.

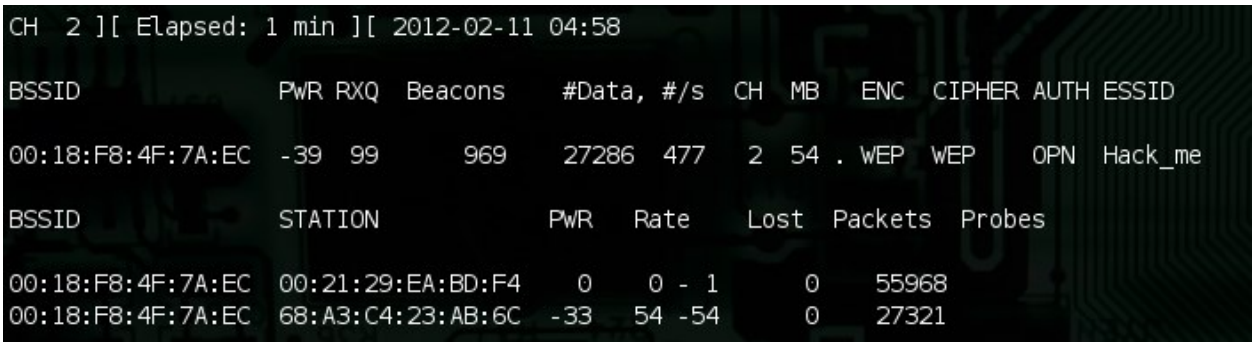

Imagen 2.23. Resultados del tráfico.

Ya obtenidos más de 20,000 **IV's** podemos continuar con el crackeo de ellos, para así llegar a la obtención satisfactoria de nuestro **password.**

- WEP 64 bits = 20,000 IV's (minimo)
- WEP 128 Bits = 100,000 (minimo)

Estos datos de captura de IV's puede variar, queda sujeto a criterio propio.

Una vez que tengamos los IV's necesarios, podemos probar con *aircrack-ng* si ya es posible obtener el password, de modo que fueran insuficientes IV's recomendamos, no detener la captura de datos en *airodump-ng* ya que de lo contrario tendríamos que volver a iniciar el proceso desde la asociación a nuestro punto de acceso.

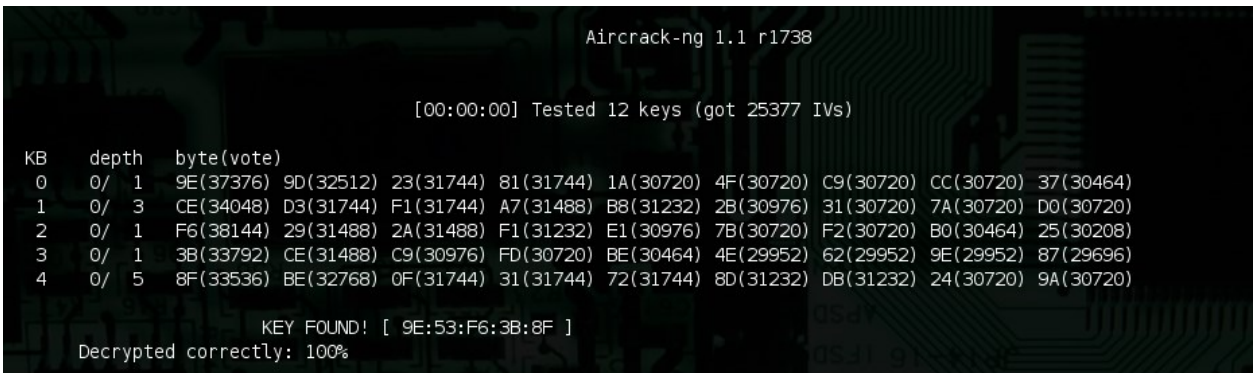

Imagen 2.24. Resultados finales.

El mismo método se aplica para wep's de 128 bits, solamente que la captura de IV's tiene que ser mayor .

2.17. La defensa frente a ataques criptográficos.

La forma más sencilla para defenderse de este ataque es utilizar WPA2.

2.18. Atacando WPA 802.11

WPA/WPA2 mejora enormemente la seguridad de las redes inalámbricas, sin embargo la protección adicional que se produce en el precio de la complejidad añadida al protocolo. En un nivel alto, los ataques de la WPA se pueden dividir en dos categorías: los ataques contra la autenticación y los ataques contra el cifrado. Los ataques de autenticación son el acceso directo más común y el rendimiento de la red inalámbrica. Cuando se ataca autenticación WPA-PSK, el atacante también tiene la capacidad para descifrar / cifrar el tráfico ya que el PMK se recupera. Ataques de cifrado son sólo contra los ataques Emergin networks. WPA proporciona la capacidad para *descifrar/ cifrar* el tráfico, pero no permiten que el atacante se una a la red como un usuario legítimo.

2.19. Romper autenticación WPA-PSK

Muchas de las implementaciones de la WPA en WPA influencian su uso hoy en día con el pre-autenticación de clave compartida, también conocido como WPA-personal. Este mecanismo de aprovechar un secreto compartido común entre todos los dispositivos de la red para la autenticación. Aunque la función de derivación de claves similares se usa con su empresa de autenticación contrapartida, este método de implementación WPA es susceptible a una serie de ataques que tomados de la seguridad global de estos despliegues inalámbricos, representan un gran riesgo.

2.20. La obtención de la saludo de cuatro vías

El **handshake** de cuatro vías permite al cliente y al punto de acceso negociar las claves utilizadas para cifrar el tráfico enviado a través del aire. Si quisiéramos obtener la clave, tenemos que el SSID, el Anonce enviado por la AP, el SNonce enviado por el cliente y el cliente de **four way handshake**.

Imagen 2.25. Four way handshake.

2.21. Los ataques activos

A veces la impaciencia saca lo mejor de nosotros y nos dicen que tenemos cosas mejores que hacer que esperar en torno a un nuevo usuario para conectarse. Aquí es donde los ataques de activos son útiles para obtener el handshake. Podemos utilizar cualquier negación del ataque del servicio 802.11 para poner un usuario fuera de línea, sin embargo el más popular es el ataque deauthentication. Nuestro primer paso es configurar nuestro sniffer pasivo. Luego, en una nueva ventana en el mismo sistema, vamos a lanzar nuestro ataque de autentificación por lo que nuestro **sniffer** captura tanto el ataque y la re- conexión del cliente.

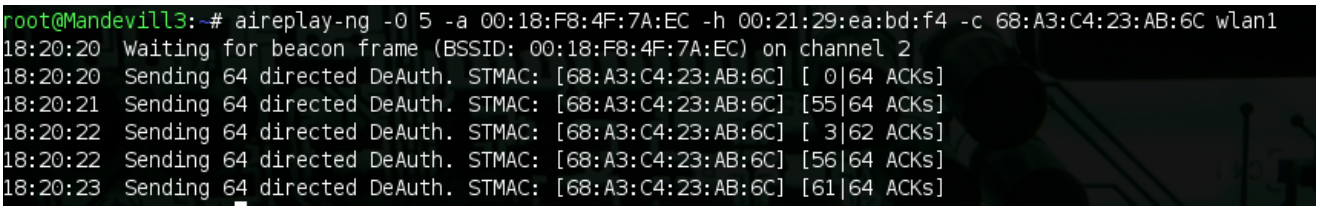

Imagen 2.26. Herramientas disponibles para autentificación.

El número de fotogramas de autentificación necesaria para forzar al cliente a volver a conectar pueden variar, a veces sólo una es necesaria, y a veces puede tardar. Una vez que el ataque termine, vamos a esperar un segundo y luego visitaremos nuestro sniffer para el handshake. Si todo va bien, podemos pasar a lanzar el ataque de forma inmediata.

2.22. Romper la clave pre-compartida

Al igual que muchos ataques de autenticación contra WPA, WPA-PSK es particularmente difícil como el conjunto de caracteres para la clave pre-compartida puede ser de entre 8 y 63 caracteres ASCII imprimibles y la contraseña elegida se aplica un algoritmo hash 4096 veces antes de usarlo en el PMK. Esto aumenta en gran medida el proceso de fuerza bruta, por lo que si la red de destino utiliza una compleja clave pre-compartida, puede que nos estanquemos durante el proceso.

2.23. Uso de aircrack-ng

Como la mayoría de las herramientas de crackeo del WPA-PSK, el Aircrack-ng requiere un archivo de captura que contenga, como mínimo dos de los cuatro cuadros que figuran en el handshake de cuatro vías. Usando Aircrack-ng es bastante sencillo:

 # aircrack-ng-w wordlist.txt hackme-01.cap

Vamos a especificar nuestro archivo de diccionario (-w wordlist.txt) y, siguiendo el ejemplo anterior, nuestro archivo de captura (hackme-01.cap).

Imagen 2.27. Aircrack-ng cuadro.

3 Marco Metodológico.

3.1 Marco metodológico apartado del trabajo que dará el giro a la investigación, es donde se expone la manera como se va a realizar el estudio, los pasos para realizarlo, su método. Según Buendía, Colás y Hernández (1997) en la metodología se distinguen dos planos fundamentales; el general y el especial. En sentido general, es posible hablar de una metodología de las ciencias aplicables a todos los campos del saber, que recoge las pautas presentes en cualquier proceder científico riguroso con vistas al aumento del conocimiento y/o a la solución de problemas.

3.2 Tipo de investigación:

3.2.1 Investigación teórica La investigación teórica es en suma, la lógica del hacer científico, y como tal, cuenta con sus propias reglas, prerrequisitos y condiciones de trabajo. La investigación teórica es un nivel de especialización de la investigación científica, que, como fundamento y guía de ésta, como su lógica, reclama de una rígida formación especializada en los más altos niveles de complejidad de la generalización y el análisis abstracto.

3.2.2 Investigación práctica tiene por finalidad la búsqueda y consolidación del saber, y la aplicación de los conocimientos para el enriquecimiento del acervo cultural y científico, así como la producción de tecnología.

3.3 Tipo de método

3.3.1 Método inductivo es un método científico que obtiene conclusiones generales a partir de premisas particulares. Se trata del método científico más usual, que se caracteriza por cuatro etapas básicas: la observación y el registro de todos los hechos, el análisis y la clasificación de los hechos, la derivación inductiva de una generalización a partir de los hechos, y la contrastación.
Esto supone que, tras una primera etapa de observación, análisis y clasificación de los hechos, se deriva una hipótesis que soluciona el problema planteado. Una forma de llevar a cabo el método inductivo es proponer, a partir de la observación repetida de objetos o acontecimientos de la misma naturaleza, una conclusión para todos los objetos o eventos de dicha naturaleza.

3.3.2 Método científico El método científico se basa en la reproducibilidad (la capacidad de repetir un determinado experimento en cualquier lugar y por cualquier persona) y la falsabilidad (toda proposición científica tiene que ser susceptible de ser falsada).
Entre los pasos necesarios que conforman el método científico, se encuentran la observación (consiste en aplicar los sentidos a un objeto o a un fenómeno, para estudiarlo tal como se presenta en realidad), la inducción (acción y efecto de extraer, a partir de determinadas observaciones, el principio particular de cada una de ellas), el

planteamiento de la hipótesis (mediante la observación), la demostración o refutación de la hipótesis, y la presentación de la tesis o teoría científica.

3.4 Metodología.

3.4.1 Manejo de cuestionarios.

Es un formulario de 10 pregunta, con varias preguntas abiertas y otras con opción múltiple. El motivo por el cual se aplicó fue para ver cual es el conocimiento que la gente tiene sobre este tema y se aplicó a un total de 100 personas.

3.4.2 Tipo de Investigación.

La investigación tiene un enfoque cualitativo y cuantitativo, lo que la hace tener un enfoque mixto.

3.4.3 Población muestra: especificaciones generales.

La población muestra que sirvió como objeto de investigación fue los estudiantes de la universidad, de las diferentes carreras que esta tiene.

3.4.4 Método.

El método es el científico, además de incluir métodos propios del enfoque mixto.

4 Bibliografía.

Cache Johnny, Hacking Exposed Wireless, 2nd edition, McGraw Hill, 2010.

Andreu Fernando, Pellejero Izaskun, Lesta Amaia; Fundamento y aplicaciones de seguridad en redes WLAN; Ed. Marcombo, 2006.

5 Anexo.

5.1. Cuestionario.

Contesta las preguntas marcando con una cruz la letra de la respuesta que creas correcta

1- ¿Qué es Wi-Fi?
a) Internet
b) Conexión de datos
c) Conexión de dispositivos inalámbricamente

2- ¿Qué es el estándar 802.11?
a) Estándar de programación
b) Estándar de conexiones inalámbricas
c) Estándar para conexiones alámbricas

3- ¿Es lo mismo crackear y hackear?
a) No b) Si

4- ¿Qué es crack?
a) Es infiltrarse en un sistema informático para saber como es
b) Es conectarse en un sistema informático para romperlo
c) Es infiltrarse en un sistema informático para modificarlo

5- ¿Qué protocolo de cifrado de datos utilizas?
a) WEP b) WPA c) WFX d) WPA2
e) Ninguno de los anteriores f) No se

6- ¿Qué es WPA?
a) Una forma de encriptación de información
b) Cifrado de clave dinámico para redes inalámbricas
c) Protocolo inalámbrico
d) No se

7- ¿Cuál es la forma de crackear seguridad WPA2?
a) Diccionarios
b) Fuerza bruta
c) GPU
d) Todas las anteriores

8- ¿Qué tan difícil crees que sea entrar a una red inalámbrica sin protección?
a) Muy fácil b) Fácil, c) Normal d) Difícil e) Muy difícil

9- ¿Crees que sea necesario proteger tu red inalámbrica en casa? ¿Por qué?
a) Si b) No _____

10- ¿Consideras que la red que utilizas es segura? ¿Por qué?
a) Si b) No _____

5.2 Análisis de cuestionario.

El cuestionario fue aplicado a un total de 100 estudiantes de diferentes carreras dentro de la universidad politécnica de San Luis Potosi, Mexico, no se analizó cuantas personas tenían el conocimiento especifico en una pregunta en particular, se analizo sin embargo, encuesta por encuesta, usando una rúbrica en la que si se contestaban al menos 6 de las 8 preguntas de conocimiento correctamente se consideraba un nivel aceptable, de 4 a 5 preguntas correctas un nivel básico, de 0 a 3 preguntas contestadas correctamente, representan un nivel bajo de conocimiento, en el siguiente grafico se muestran estas estadísticas.