#2

UNDERCODE

TALLER DE SEGURIDAD WIRELESS

CLAVES WEP

```
                    Aircrack-ng 1.1

[00:00:06] 2796 keys tested (434.78 k/s)

                  KEY FOUND! [ 12345678 ]

Master Key     : CE 02 16 C5 28 B2 45 70 39 EC 8C A0 8A 5C 51 92
                 E9 D1 41 F0 32 AB 18 37 FA A9 89 D8 56 FD 69 D0

Transient Key  : FE CF D0 E4 96 99 61 9E EE 1F 29 71 8E 2E 3B 01
                 65 A9 B2 8D 40 EE 8A DE 66 A1 A3 1E C2 F5 FB 10
                 01 65 B8 6F 83 78 0C 9D F6 3E 2F 2D F8 0D 75 2A
                 EE F4 67 4B 95 AE 3E F4 B9 0C 17 9A 66 00 0D 94

EAPOL HMAC     : 7A 83 E3 2A FB 72 23 DF 71 97 F5 26 A9 1C 0C 4E
```

TEMAS

Conceptos

- **WLAN** – Wireless local área network, esta será nuestra red inalámbrica la cual tendremos como objetivo a lo largo del taller
- **WEP** – Seguridad equivalente a cableado (Wired equivalent Protection)
- **WPA** – Acceso protegido inalámbrico(Wireles Protected Accees)
- **OPN** – Tipo de autentificación (OPEN)
- **SKA** – Tipo de autentificación wep (Shared Key acess)
- **TKP** – Tipo de encriptación WPA
- **ESSID** – Nombre de punto de acceso
- **BSSID** – Dirección MAC de punto de acceso
- **AP** – Punto de acceso (WLAN)
- **NIC** – Network Interface Card (Tarjeta de interfaz de red)
- **WPS** - Wi-Fi Protected Setup
- **IV's** - Un vector de inicialización (IV) es un número arbitrario que puede ser utilizado junto con una clave secreta para el cifrado de datos.
- **STATION** – Dirección MAC de cliente asociado a un punto de acceso.

Existen 3 tipos de frames dentro de una WLAN:

1. **Managment Frames**: También conocidos como paquetes de gestión estos son responsables de mantener la comunicación que está presente entre el punto de acceso y el cliente asociado a él, este frame contiene las siguientes subclases:

    a. Autentificación
    b. Des autentificación
    c. Solicitud de asociación
    d. Respuesta de asociación
    e. Solicitud de re-asociacion
    f. Respuesta de re-asociacion
    g. Des asociación
    h. Beacon
    i. Prueba de solicitud
    j. Prueba de respuesta

2. **Control frames**: O llámese también como paquetes de control, estos son responsables de un intercambio adecuado de información (Data) entre el punto de acceso y los clientes asociados mediante **wireless**, dicho frame contiene la siguientes subclases:

a. Request to Send (RTS)
b. Clear to send (CTS)
c. Acknowledgment(ACK)

3. Data frames: Los paquetes con información estos son los más importantes cuando uno está tratando de descifrar la contraseña encriptada por algún tipo de seguridad en particular llámese **WEP**, principalmente, ya que dichos paquetes contienen toda la información que se envía a través de nuestra red inalámbrica.

Ya que sabemos los distintos tipos de frames que maneja nuestra **WLAN** un conocimiento solido en cuanto a la potencia y la sensibilidad es fundamental.

Potencia

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

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)**.

Más adelante aprenderemos la lectura de los datos que nos muestra **airodump-ng** permitiéndonos una comprensión más digerible en cuanto a la potencia de transmisión y así poder identificar que tan cerca y tan lejos nos encontramos de el punto de acceso que tratamos de auditar.

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.

Tipos de autentificación:

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.

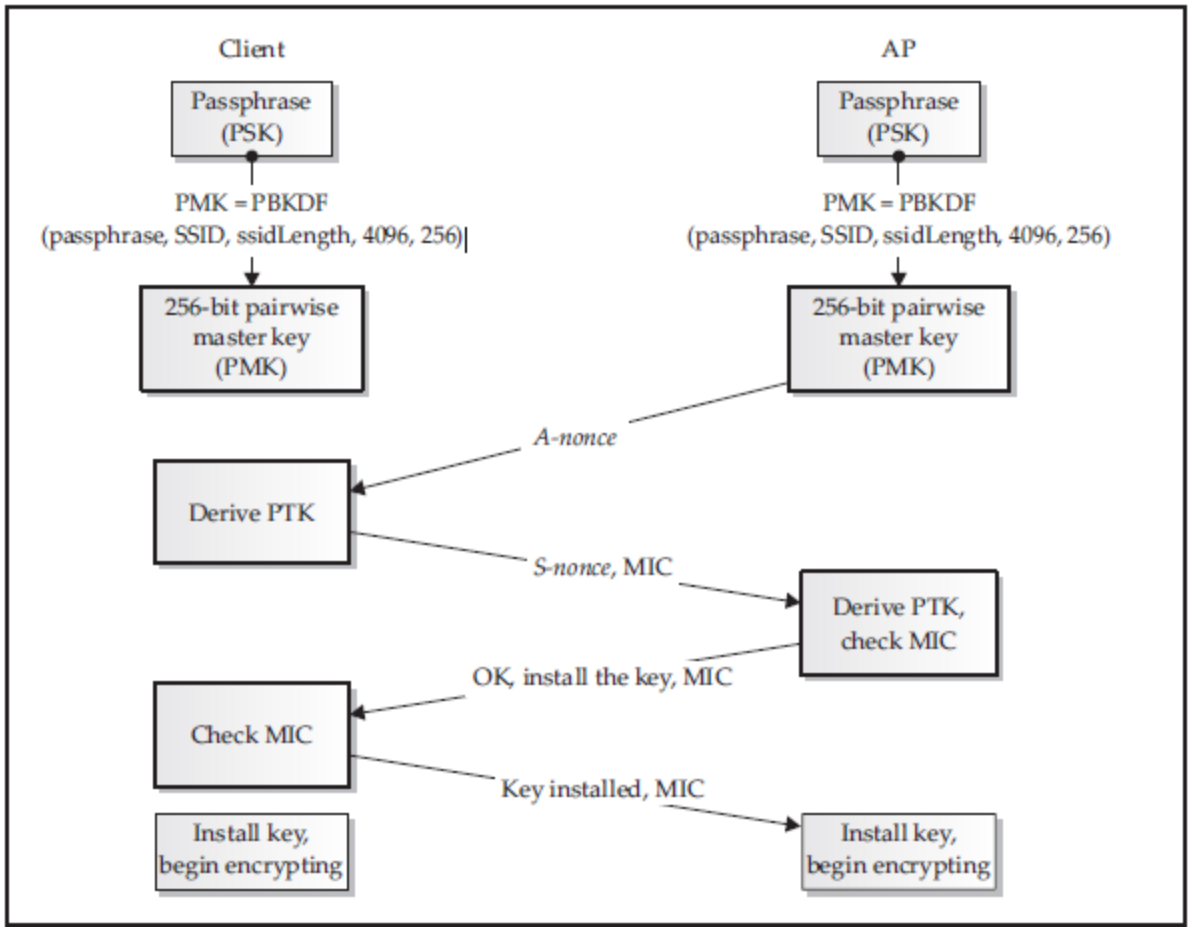


Imagen 2.2. proceso “Four-way handshake”.

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, cable módem, 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.

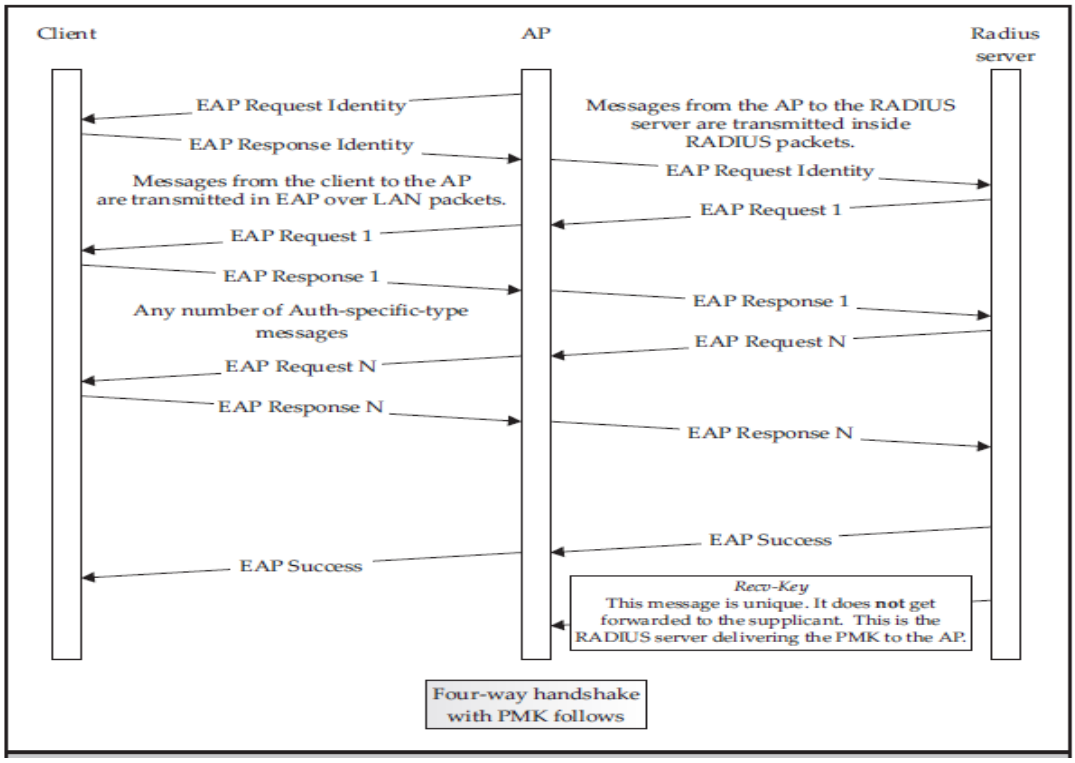


Imagen 2.3. Estándar EAPOL.

WPS

WPS (Wi-Fi Protected Setup) creado en 2007, promovido por la Wi-Fi Alliance para facilitar la creación de redes WLAN, WPS no es un mecanismo de seguridad por sí, se trata de la definición de diversos mecanismos para facilitar la configuración de una red WLAN segura con WPA2

Arquitectura:

WPS define una arquitectura con tres elementos con roles diferentes:

- **Registrar:** dispositivo con la autoridad de generar o revocar las credenciales en la red. Tanto un AP como cualquier otra estación o PC de la red pueden tener este rol. Puede haber más de un Registrar en una red.
- **Enrollee:** dispositivo que solicita el acceso a la red WLAN.
- **Authenticator:** AP funcionando de proxy entre el Registrar y el Enrolle.

Formación de implementación de seguridad:

Las principales 4 configuraciones de **WPS** son las siguientes

1. **PIN** (Personal Identification Number)
2. **PBC** (Push Button Configuration)
3. **NFC** (Near Field Communications)
4. **USB** (Universal Serial Bus):

Cabe mencionar que la que es prácticamente obligada hoy en día es solamente es el uso del PIN.

PIN: Esta contiene una clave de pocos dígitos que permitirá tanto al registrar como al enrolle poder llevar un intercambio de credenciales de manera satisfactoria, ambas partes deben de conocer este PIN.

PBC: la generación y el intercambio de credenciales son desencadenados a partir que el usuario presiona un botón (físico o virtual) en el AP (o en otro elemento Registrar) y otro en el dispositivo en otras palabras se lleva a cabo una sincronización de parte de ambos dispositivos.

NFC: intercambio de credenciales a través de comunicación NFC. La tecnología NFC, basada en RFID permite la comunicación sin hilos entre dispositivos próximos (0 - 20 cm). Entonces, el dispositivo Enrolle se tiene que situar al lado del Registrar para desencadenar la autenticación. De esta manera, cualquier usuario que tenga acceso físico al Registrar, puede obtener credenciales válidas.

USB: Prácticamente este método físico, de transferencia de credenciales, se transfieren mediante un dispositivo de memoria flash desde el Registrar al Enrolle.

Dicha configuración se presenta un flujo de seguridad principalmente en el momento de la implementación de el PIN ya que este puede llegar a ser crackeado por medio de fuerza bruta y usualmente utiliza pocos dígitos, el tiempo de crackeo no es tan prologando, permitiendo así una paciente y satisfactoria espera para su posterior obtención de **numero PIN** usado por el AP.

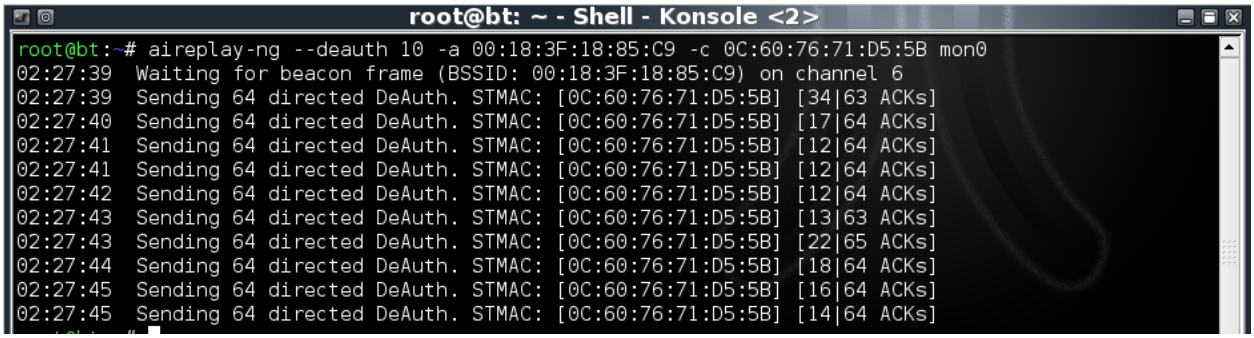
Rompiendo la seguridad

ESSID Oculto

Por default la mayoría de los puntos de acceso transmiten su **ESSID** mediante los paquetes denominados beacon's , esto permite a los clientes y toda persona que desee poder identificar el punto de acceso de manera sencilla, mostrando el nombre del punto de acceso al público.

Una de las desventajas es el método de ocultación de **ESSID** , este no nos proporciona una seguridad solida ya que la obtención del nombre de la red , puede ser obtenida de manera sencilla, simplemente al estar a la escucha de manera pasiva esperando a que algún cliente se asocie a dicho punto de acceso o bien enviando un paquete de des autentificación hacia el cliente asociado , desconectándolo de esta red y así forzándolo a una re conexión, permitiéndonos capturar los paquetes donde se encuentra el nombre de nuestra red.

El envió de paquetes de des autentificación se puede llevar a cabo utilizando el software de **aireplay-ng** que viene dentro de la suite de **aircrack-ng**



Descripción de las opciones:

Aireplay-ng : llamado al programa aireplay-ng

--deauth : Opción de envío de paquetes de des autentificación seguido por el numero "5" , cantidad de paquetes de des autentificación a enviar

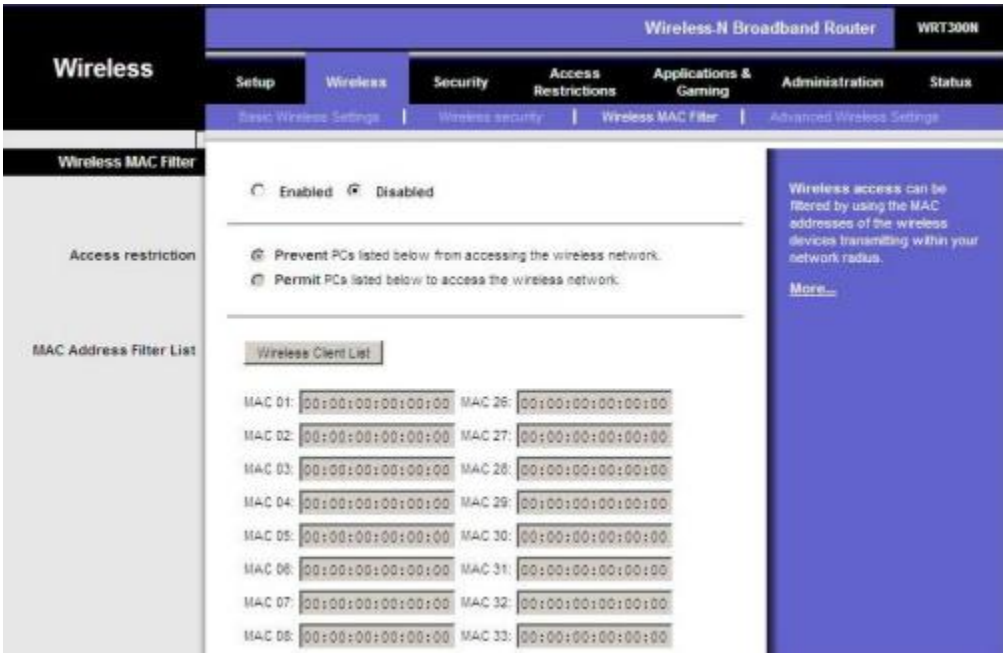
-a: Nos permite colocar la dirección MAC que deseamos des autentificar de el punto de acceso, forzándolo a una re conexión a nuestra AP.

-c: Indica el cliente al que queremos que se desasocie del punto de acceso.

De esta manera obtendremos satisfactoriamente el nombre de la red, siempre y cuando tengamos a la escucha **airodump** o cualquier otro sniffer de wireless de manera pasiva.

Filtrado MAC

Otra implementación dentro de muchas redes inalámbricas, además de poder colocar el ESSID de manera oculta, se utiliza el filtrado MAC, este filtro lo que nos permite es tener una lista de direcciones MAC que están autorizadas a la asociación con el punto de acceso para su posterior conexión, de esta manera aun que tengan la contraseña de el punto de acceso no es suficiente ya que no se podrá llegar a entablar una conexión de manera satisfactoria y completamente funcional.



No existe un sistema 100% seguro ya que por mucho o por poco siempre existen flujos en la seguridad, para llevar a cabo este tipo de bypass al filtrado de **MAC** se realiza de siguiente manera:

1-Identificar la **MAC** de algún cliente que se encuentre asociado de manera satisfactoria al punto de acceso que tenemos en la mira.

2-Utilizando el software "**macchanger**", clonaremos su dirección **MAC** remplazándola por la nuestra

De esta forma obtendremos derrotar el filtrado MAC, permitiéndonos una asociación con la dirección MAC de algún cliente registrado de manera satisfactoria.

Haciendo énfasis este tipo de seguridad aplicada a una red es una de las más débiles y más fáciles de explotar su debilidad por el reconocimiento de direcciones MAC que se asocian al punto de acceso.

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.

Para el siguiente paso práctico realizaremos una auditoria a una red inalámbrica para poner en práctica lo ya aprendido, este punto de acceso contiene la siguiente configuración:

- **ESSID oculto**
- **Filtrado MAC activado**
- **WEP – 64 Bits**

De esta manera el equipo con el que se montara el laboratorio virtual será el siguiente:

- **NIC (Network Interface card) con chipset Atheros.**
- **Backtrack 5 R3**
- **Dell Laptop**
- **Access Point HG530**

A la hora de utilizar **airmon-ng** nos permite “dividir” nuestra interfaz en 2 , creando una segunda en modo monitor y otra en modo managed, permitiéndonos poder realizar la conexión con una y estar monitoreando el trafico que se encuentra presente en el aire con la otra.

Getting our hands dirty

Para llevar a cabo la auditoria se debe de llevar una secuencia ordenada para la resolución de nuestro problema, se propone el siguiente algoritmo, que es recomendable se siga en los siguientes pasos:

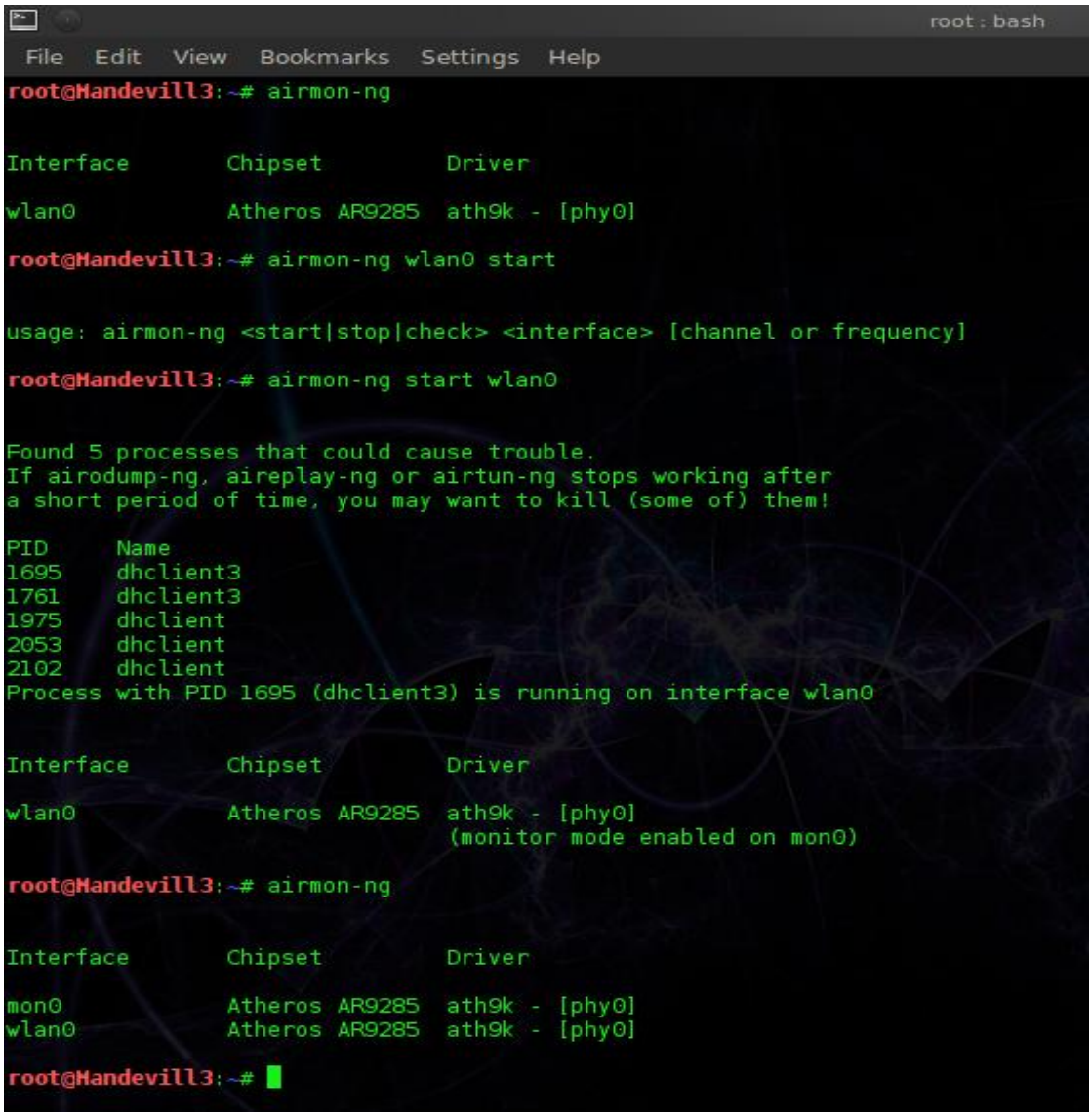
1. Iniciar nuestra interfaz en modo monitor
2. Estar a la escucha de paquetes en el aire , siempre guardando un registro de ellos
3. Si se encuentra nuestra ESSID oculta, des autentificar al cliente o esperar su conexión para obtener el **ESSID**
4. Enviar paquetes de falsa autentificación hacia el punto de acceso, para poder visualizar el tipo de autentificación que se tiene por configuración en el punto de acceso.
5. Si se presenta filtrado **mac**, clonar la dirección **mac** de algún cliente que ya se encuentre asociado, remplazando nuestra dirección **mac** de la **NIC** , por la de este.
6. Si no se presenta un flujo de tráfico aceptable para la captura de estos paquetes, se debe de inyectar tráfico para incrementar la cantidad de paquetes de tipo data.

7. Ya capturada una cantidad decente de paquetes de datos , se procederá al crackeo o descifrado de estos paquetes
8. Y así obtener la contraseña.

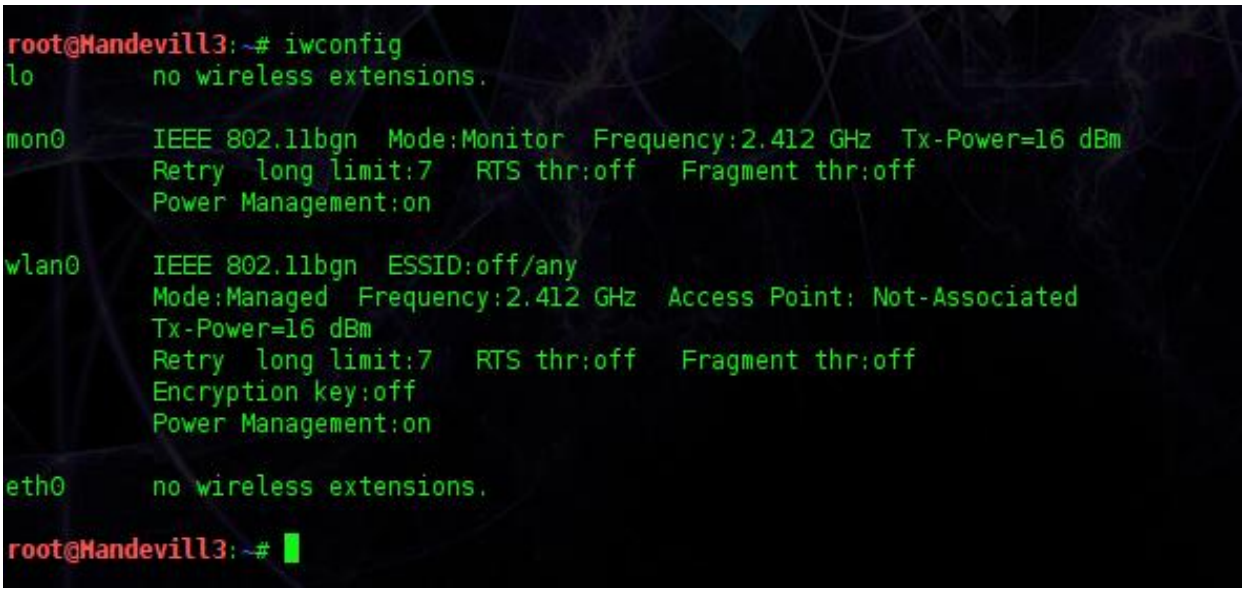
Estos pasos pueden variar de red en red, depende de la configuración con la que se esté empleando en el punto de acceso y nuestros objetivos.

Colocando en modo monitor nuestra interfaz

Debemos de colocar nuestra interfaz en modo monitor, lo que haremos será utilizar **airmon-ng** ya que este nos permite crear una segunda interfaz , con la misma **MAC**, pero una en modo monitor y la otra en modo managed.



En la imagen se muestra como nuestra interfaz **wlan0** se creó una segunda en modo monitor llamada **mon0**, esta será la que utilizaremos para la auditoria.



Podemos comprobar con el comando **iwconfig**, de que nuestras 2 interfaces están funcionando correctamente como modo monitor y como modo managed, este paso es muy importante ya que si no colocamos en modo monitor nuestra interface no podremos realizar una auditoría adecuada y no nos permitirá poder capturar los paquetes que necesitamos para el crackeo de nuestra red inalámbrica.

Iniciando airodump-ng

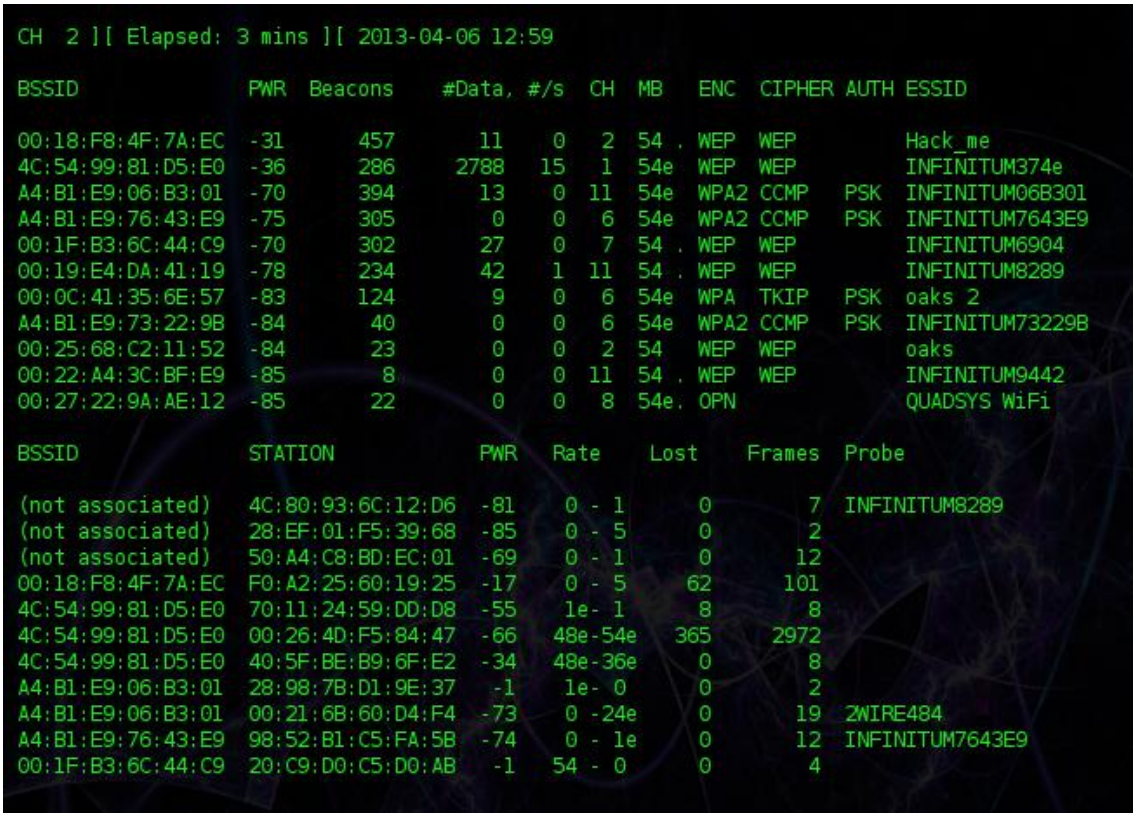
Ahora utilizaremos el programa **airodump-ng** para poder capturar los paquetes y ver las redes disponibles tanto así como su información de nombre, MAC y todo cliente que se encuentre asociado a los puntos de acceso mostrados.

Airodump-ng presenta la siguiente sintaxis para poder colocarla a la escucha:

Airodump-ng interfaz –opciones

Ejemplo:

Airodump-ng mon0 –w prueba --bssid 00:00:00:00:00:00 –c 2



```
CH  2 ][ Elapsed: 3 mins ][ 2013-04-06 12:59

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:18:F8:4F:7A:EC  -31      457       11    0   2  54 . WEP  WEP         Hack_me
4C:54:99:81:D5:E0  -36      286     2788   15   1  54e  WEP  WEP         INFINITUM374e
A4:B1:E9:06:B3:01  -70      394       13    0  11  54e  WPA2 CCMP   PSK  INFINITUM06B301
A4:B1:E9:76:43:E9  -75      305        0    0   6  54e  WPA2 CCMP   PSK  INFINITUM7643E9
00:1F:B3:6C:44:C9  -70      302       27    0   7  54 . WEP  WEP         INFINITUM6904
00:19:E4:DA:41:19  -78      234       42    1  11  54 . WEP  WEP         INFINITUM8289
00:0C:41:35:6E:57  -83      124        9    0   6  54e  WPA  TKIP   PSK  oaks 2
A4:B1:E9:73:22:9B  -84       40        0    0   6  54e  WPA2 CCMP   PSK  INFINITUM73229B
00:25:68:C2:11:52  -84       23        0    0   2  54   WEP  WEP         oaks
00:22:A4:3C:BF:E9  -85        8        0    0  11  54 . WEP  WEP         INFINITUM9442
00:27:22:9A:AE:12  -85       22        0    0   8  54e. OPN              QUADSYS WiFi

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   4C:80:93:6C:12:D6  -81    0 - 1      0         7  INFINITUM8289
(not associated)   28:EF:01:F5:39:68  -85    0 - 5      0         2
(not associated)   50:A4:C8:BD:EC:01  -69    0 - 1      0        12
00:18:F8:4F:7A:EC  F0:A2:25:60:19:25  -17    0 - 5     62       101
4C:54:99:81:D5:E0  70:11:24:59:DD:D8  -55   1e- 1      8         8
4C:54:99:81:D5:E0  00:26:4D:F5:84:47  -66   48e-54e    365      2972
4C:54:99:81:D5:E0  40:5F:BE:B9:6F:E2  -34   48e-36e      0         8
A4:B1:E9:06:B3:01  28:98:7B:D1:9E:37   -1   1e- 0      0         2
A4:B1:E9:06:B3:01  00:21:6B:60:D4:F4  -73    0 -24e     0        19  ZWIRE484
A4:B1:E9:76:43:E9  98:52:B1:C5:FA:5B  -74    0 - 1e     0        12  INFINITUM7643E9
00:1F:B3:6C:44:C9  20:C9:D0:C5:D0:AB   -1   54 - 0      0         4
```

Descripción de la información que muestra airodump

En la imagen 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 el cifrado.
- **ESSID:** El nombre del AP.

Envió de paquete deauth

Para poder obtener un ESSID oculto, tenemos las siguientes opciones:

- Esperar a que algún cliente se asocie al punto de acceso
- Enviar un paquete de des autentificación a un cliente forzando su re conexión con el punto de acceso

Para poder enviar paquetes de des autentificación a un usuario podemos utilizar **aireplay**, este tipo de procedimiento puede ocasionar un **D.O.S** (denial of service o denegación de servicio) a el cliente que estamos des autentificando ya que si enviamos infinitas cantidades de paquetes de des autentificación este le será imposible reconectarse a su red siempre y cuando el cliente este recibiendo paquete tras paquete de des autentificación.

La sintaxis utilizada por **aireplay-ng** es muy similar que la de **airodump-ng** y las demás ya que ambas se encuentran dentro de la suite de **aircrack-ng**

Aireplay-ng –tipo de ataque –MAC del AP –nuestra MAC interfaz

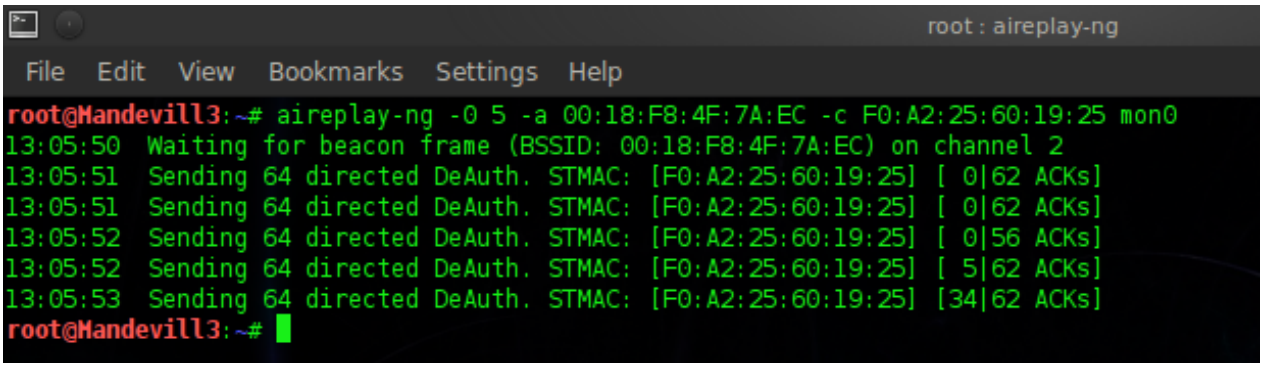
Ejemplo:

Aireplay-ng –deauth 5 –a 00:00:00:00:00:00 –h 11:11:11:11:11:11 mon0

*Su sintaxis y sus opciones pueden cambiar dependiendo el tipo de ataque a realizar, para poder visualizar todos los tipos de ataques y sus respectivas configuraciones solo es necesario colocar "**aireplay-ng**" y así nos desplegara en pantalla todas sus opciones y configuraciones posibles*

Una vez que ya tengamos a nuestro cliente desconectado de su red y hecho su re conexión nos mostrara el **ESSID** oculto si es que tenia **ESSID** oculto y en muchas veces nos permitirá ver el tipo de autentificación que utiliza el AP.

Ya teniendo este paso hecho podemos autentificarnos al AP para poder posteriormente comenzar a inyectar tráfico si es que no se presenta un flujo de datos dentro de la red relativamente alto, de manera contraria no es necesario inyectar tráfico, pero en la mayoría de los casos este paso es esencial.

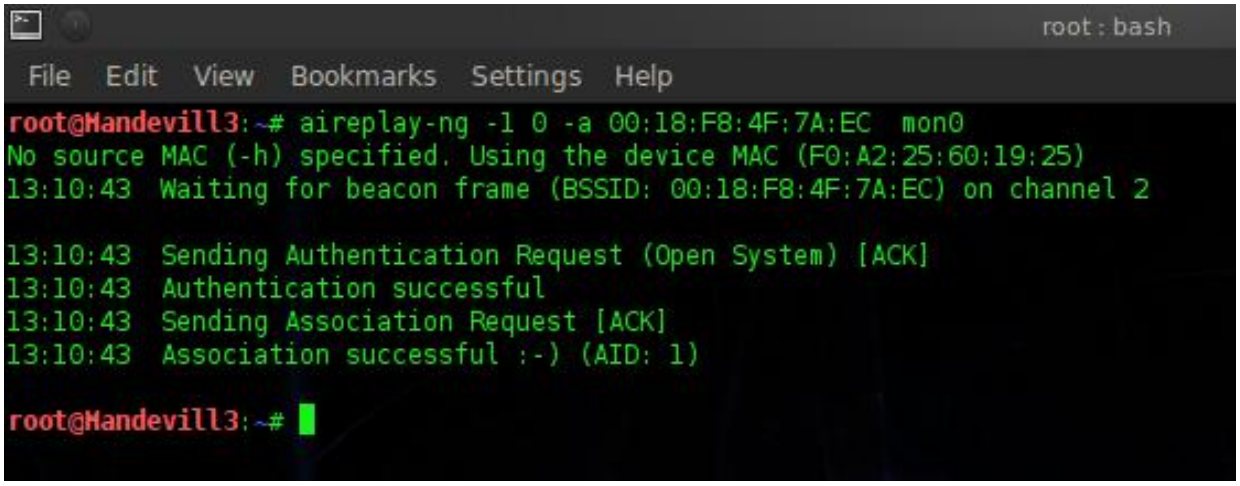


Inyección de fake auth aireplay

Enviando el paquete de asociación, en el paso anterior des autentificamos a nuestro cliente que se encuentra asociado a la AP, muchas veces ya no es necesario este paso si y solo si, des autentificamos a un usuario, pero es mejor asegurarnos que nos asociamos con el punto de acceso para así poder inyectar trafico de manera satisfactoria.

Comando en **aireplay-ng**:

Aireplay-ng -1 0 –a MAC de el AP mon0



Si vemos algo como en la imagen, hemos conseguimos la asociación al punto de acceso de manera satisfactoria, en muchos casos esto puede fallar, lo que podemos hacer es tratar de acercarnos mas al punto de acceso o podemos probar subiéndole el **rate** a nuestra tarjeta con el siguiente comando:

Iwconfig rate 1M interfaz

Esto nos permitirá tener un mayor alcance y así poder lograr la asociación de manera correcta.

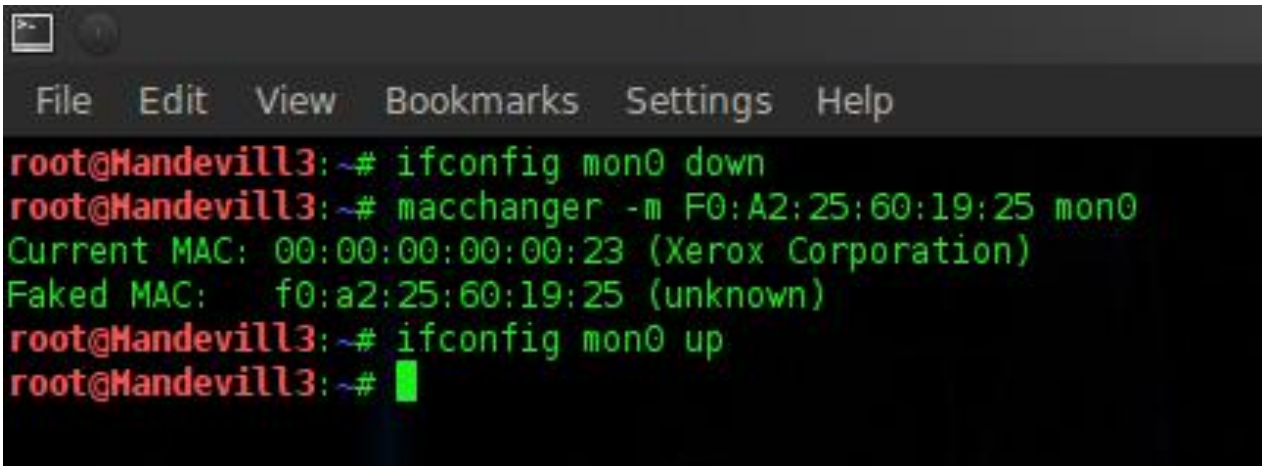
macchanger

Puede presentarse el caso que a la hora que tratamos de autentificarnos con el punto de acceso nos rechaza nuestra dirección **MAC**, esto se presenta cuando los puntos de acceso tienen en su configuración activada el filtrado MAC, este fusiona de la siguiente manera:

Al activar el filtrado MAC en un punto de acceso nos permite configurarlo de 2 maneras, mediante una lista en la que agregaremos direcciones MAC, se puede permitir el acceso y la asociación al AP o se puede a esta lista rechazar la asociación al AP.

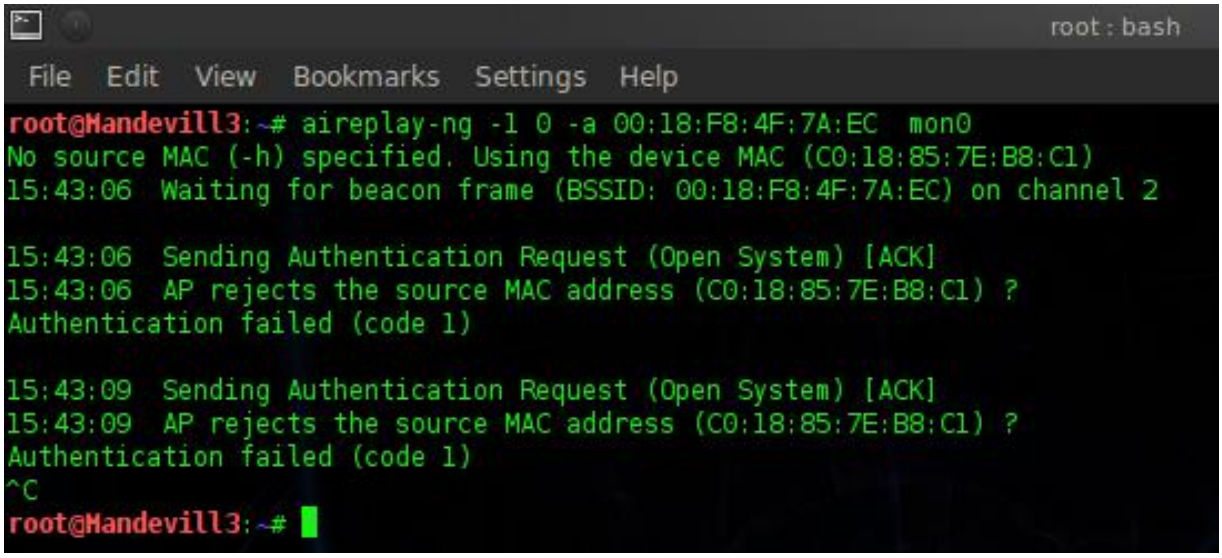
En caso de que se nos presente el filtrado MAC activo al momento de realizar una auditoría, se verá reflejado al momento de que tratemos de enviar los paquetes de falsa autentificación, imprimiéndonos en pantalla que nuestra MAC ha sido rechazada por el punto de acceso, denegándonos cualquier asociación a esta.

Esto lo podemos evadir de la siguiente manera:



Como se muestra en la imagen, clonamos la dirección MAC del cliente asociado al punto de acceso y la remplazamos por la nuestra, ahora así podremos autentificarnos y realizar los pasos anteriores (Falsa autentificación, asociarnos con el punto de acceso) de manera correcta.

Se puede apreciar en la siguiente imagen, de que manera nos bloquea la dirección MAC de nuestra NIC debido al filtrado activo de MAC presente en el punto de acceso.

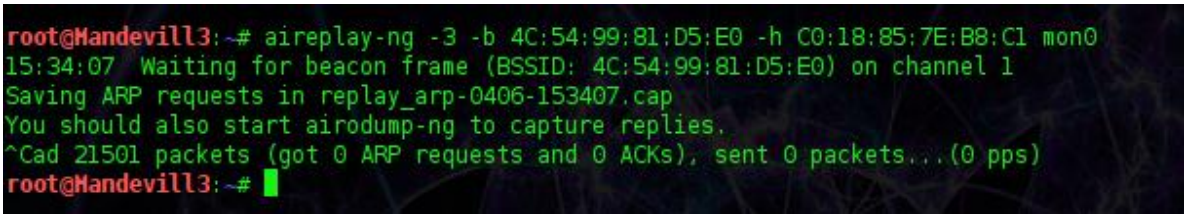


Si no se nos presenta algo similar, podemos continuar sin necesidad de hacer el **spoof** en nuestra dirección mac.

Inyección de tráfico en la red

Cuando una red presenta un flujo de tráfico en ella, se verá representado en **#Data** en **airodump-ng**, estos serán los paquetes que contendrán los datos necesarios para la des encriptación de nuestra clave WEP, en rara ocasión se presenta que exista un flujo muy grande dentro de la red, que nos permita ver como incrementan de manera rápida los números en #Data, de no serlo, existe una solución.

Nosotros podemos inyectar el trafico y acelerar el incremento de paquetes necesarios para el crackeo, esto se puede realizar con **aireplay-ng** usando la opción 3, que inyectara trafico obteniendo un gran tráfico en solicitudes **ARP** generando a gran velocidad una gran cantidad de **IV's**



Después de comenzar a inyectar trafico nuestro incremento en los paquetes **#Data** deberán de incrementarse de manera rápida, podemos configurar la cantidad de paquetes que queremos inyectar con la **opción –x** en **aireplay**, la máxima cantidad de paquetes que podemos inyectar es de 1024.

Nuestro **airodump** deberá de verse algo similar a la siguiente imagen:

Vemos que **#Data** se encuentra superior a los 20,000 paquetes, no existe realmente un numero predeterminado para poder crackear una encriptación **WEP**, pero usualmente se recomienda que este arriba de los 20,000 IV's para una clave con encriptación de 64 bits, y arriba de unos 100,000 para una encriptación de 128 bits.

Aircrack-ng

Tras esperar unos minutos de captura, nuestro **airodump-ng** a la hora de grabar la captura generara un archivo **.cap**, este lo utilizaremos en conjunto con la herramienta de **aircrack-ng** para poder desencriptar los paquetes capturados.

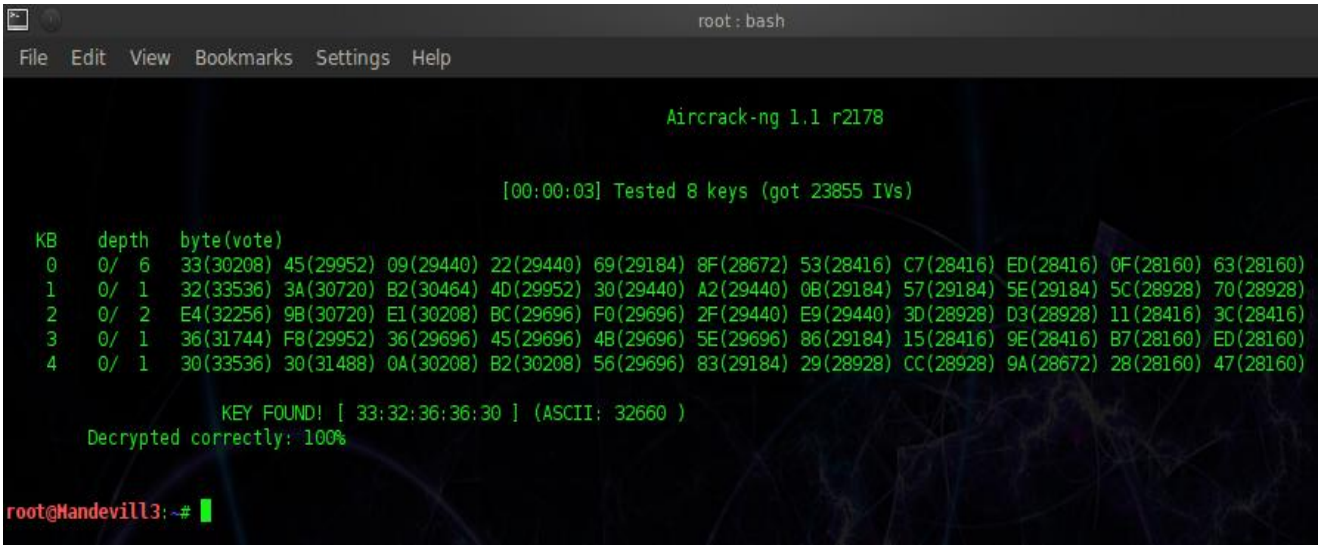
La sintaxis para **aircrack-ng** es la siguiente:

Aircrack-ng archivo

Ejemplo:

Aircrack-ng wep.cap

Muchas veces se pueden agregar más opciones y la sintaxis puede cambiar dependiendo del tipo de encriptación que se está empleando en el punto de acceso.



¡LISTO! Nos muestra que fue desencriptada de manera correcta, imprimiendo en pantalla la contraseña de el punto de acceso, dependiendo de la complejidad y la cantidad de paquetes capturados, definirá el tiempo en que **aircrack** pueda crackearlo, usualmente **aircrack-ng** puede con cualquier **WEP** que se le presente.

Solo queda conectarnos a la red utilizando cualquier gestor de redes inalámbricas, una vez conectados se nos puede llegar a presentar el problema de que no nos da una IP ya que no presenta su configuración un servidor DHCP y utiliza IP estáticas, este tema lo dejaremos para la siguiente entrega.