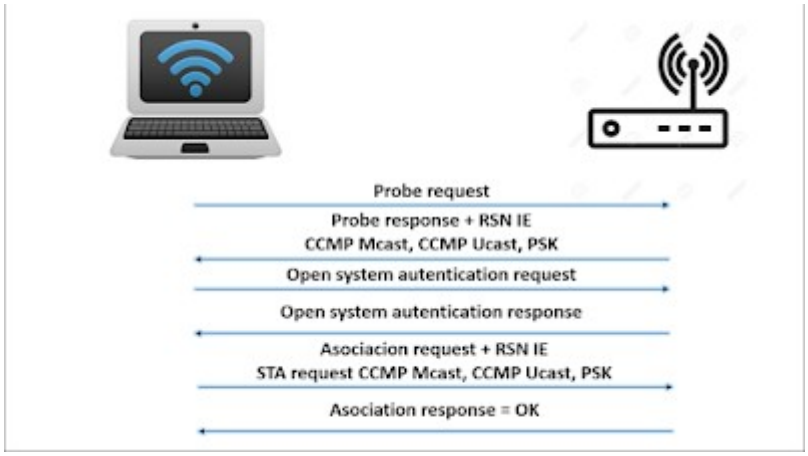
10 Palabras de seguridad de la información!

Handshake
El handshake es, a grosso modo, una negociación entre cliente y router para preestablecer la conexión. Digamos que cuando capturamos el handshake, no capturamos la clave, sino una serie de parámetros, que entre ellos va la contraseña WiFi pero cifrada.

Handshake
En una conexión inalámbrica es el proceso de negociación entre el cliente y el Punto de Acceso (AP), cuando el AP está emitiendo Beacon Frames (que no está oculto), la negociación se lleva a cabo en 2 fases: la primera de autenticación ya sea abierta o con clave compartida y una segunda de asociación.
En el caso de que el AP no este emitiendo Beacon Frames (cuando la red esta oculta) existe una fase de prueba inicial donde le cliente envía el SSID de la red a la que quiere conectarse esperando que el AP responda y así iniciar las fases de autenticación y asociación.

Este proceso para una conexión Wpa2-PSK puede verse en la siguiente imagen:



Esto quiere decir que en el handshake va incluida la contraseña (cifrada).

A la hora de capturar un handshake existen 2 formas de hacerlo:

1) Esperar capturando paquetes a que un cliente se conecte a la red normalmente.
2) Des-autenticar un cliente conectado actualmente esperando a que se conecte nuevamente y en ese momento capturar el handshake.

Abiertas
Redes sin seguridad, toda la información se envía sin cifrar, si alguien con sniffer captura el tráfico podrá ver la información sin problema.

WEP
Fue la primera medida de cifrado que se le dio a las redes Wifi, pero hace mucho tiempo que ha perdido seguridad y no es recomendable usarlas actualmente.

WPA
La evolución del anterior, su protocolo de seguridad es muy superior al WEP, es un estándar con un muy robusto nivel de seguridad.

WPA2
Algo parecido al anterior, pero incluye algunas mejoras, igualmente cuenta con muy buen nivel de seguridad.
E igualmente, ya que usaremos aircrack en este caso, hay que tener algunos conceptos claros:

Canal
Es la frecuencia en la que se emite la red.

BSSID
Es la dirección MAC del punto de acceso que emite el wifi.

ESSID
Es el nombre asignado a la red wifi.

Airmon-ng
Nos permite poner nuestra tarjeta de red en modo monitor.

Airodump-ng
Nos permite analizar las redes que están a nuestro alcance.

Aircrack-ng
Nos permite el crackeo en base a fuerza bruta.

WlanX
Suele ser la interfaz wifi de nuestra computadora el x suele cambiar según tu dispoditivo , para ver ello en linux se utiliza el comnado iwconfig

PWR
Es una forma de determinar la potencia con la que recibimos la red o bien la distancia que tenemos a la red, mientras menos sea el valor de PWR más cerca estaremos de la red o bien la recibiremos con más potencia.

Beacons
Cantidad de paquetes que emite el PA.
#Data
Paquetes de datos que ha mandado.

CH
El canal por el que se emite la red.

MB
Cantidad de MegaBytes que se puede enviar.

ENC
Tipo de encriptación que se está utilizando.

CIPHER
Tipo de cifrado que se está utilizando.

AUTH
La autorización.

¿Que es un Deauth Attacks?
ataque de desauntentificación en cristiano, para entender que es, primero tenemos que entender el estandar que regula el modo de conexión de las redes wifi el IEEE 802.11.

Si estudiamos el estandar IEEE 802.11 vemos que el paquete de desauntentificación es un paquete legítimo que utiliza el Punto de Acceso en su funcionamiento normal. Este paquete lo que hace es que le dice al cliente que se desconecte del Punto de Acceso.

¿Y el Punto de Acceso para que utliza este paquete? os voy a poner un par de ejemplos para que sea fácilmente entendible, cuando un cliente esta gestionando la clave con el Punto de Acceso y este no tiene la clave correcta, el Punto de Acceso coge y le dice al cliente que la clave proporcionada es erronea y "desconectate", otro ejemplo, cuando tenemos en el router conectados a la vez el máximo de clientes soportados o que tiene configurados, al nuevo cliente que se intenta conectar le manda el paquete "deauth" para que no establezca conexión.

Una vez entendido el funcionamiento del paquete "deauth", procedemos a ver en que consiste el "Deauth Attack"

Este ataque consiste en hacerse pasar por el Punto de Acceso y mandar a un cliente o a todos los clientes paquetes de desauntentificación con el objetivo de que el cliente o clientes no se conecten con el AP ("Access Point").

El propósito de este ataque puede ser diverso, hacer un ataque de denegación de servicio, la realización del Evil Twin Attack (trataremos este ataque en un artículo específico), forzar la desconexión de un cliente para que en una posterior reconexión conseguir el handshake, etc

Las aplicaciones más conocidas que realizan estos ataques son aireplay de la suit aircrack y mdk3

Archivos con extensión .IVS

Los Archivos de Vector de inicialización utilizado por Aircrack-ng, así como otras aplicaciones para la red inalámbrica WEP cracking clave son llamados archivos IVS. Estos se clasifican como archivos de datos que contienen vectores de inicialización que son útiles para la generación de los datos cifrados en la red

Archivos con extención .CAP

El archivo CAP es un archivo de captura de paquetes, generado por el programa de rastreo de paquetes. Estos archivos también se denominan

archivo de rastreo o archivo de huesos y son utilizados por numerosos programas de detección de paquetes.

Se puede acceder a los archivos de extensión CAP que son archivos de captura de paquetes usando el programa gratuito Wireshark o Microsoft Network Monitor