A continuación, establecemos la tarjeta de red en modo monitor, para que pueda capturar tráfico de redes a las que no está conectada. Para ello, abrimos una terminal y utilizamos el siguiente comando: **airmon-ng start [Nombre de la interfaz de la tarjeta de red].**

FOTO MODO MONITOR



Una vez hemos puesto la tarjeta de red en modo monitor, podemos empezar a capturar todo el tráfico que sea capaz de alcanzar la tarjeta de red, y así poder ver que redes wifi están activas a nuestro alrededor. Para ello, utilizamos el comando **airodump-ng [Nombre tarjeta de red en modo monitor]**

FOTO REDES WIFI DISPONIBLES





Una vez que hemos encontrado la red que queremos atacar, abrimos otra terminal para capturar los datos del handshake. Estos datos son los que nos van a ayudar a descifrar la contraseña de la red con un ataque de fuerza bruta, que es la manera para descifrar claves WPA2. Para ello, utilizamos el siguiente comando: **airodump-ng –c [canal de la red objetivo] --bssid [Dirección MAC de la red objetivo] –w [dirección en la que alojar el archivo con los datos del handshake] [nombre de la tarjeta de red en modo monitor].**

FOTO CAPTURA HANDSHAKE



El handshake se da cuando un cliente de la red se conecta al punto de acceso de la red, en ese momento se pueden capturar muchos datos que luego van a ser relevantes para descifrar la contraseña. Podríamos esperar a que cualquier cliente de la red se conecte pero esto podría dilatarse mucho en el tiempo. Por eso, mientras estamos capturando los datos para encontrar el handshake, nosotros realizamos un ataque de desautenticacion para que uno de los clientes de la red se desautentique y se vuelva a autenticar y poder acceder a los datos del handshake. Realizamos ese ataque varias veces para capturar el máximo numero de datos posible para que se pueda después descifrar la clave. Para ello, ejecutamos el siguiente comando en una terminal en varias ocasiones: **aireplay-ng –o [Nº de veces que se desautentica] –a** **[Dirección MAC de la red objetivo] –c [Dirección MAC de un cliente de la red] [nombre de la tarjeta de red en modo monitor].**

FOTO ATAQUE DE DESAUTENTICACION





Por último, una vez hemos capturado el handshake, comparamos ese handshake con un diccionario de contraseñas o en nuestro caso lo que hacemos es que como sabemos la marca del router y sabemos que de fabrica las contraseñas de las las redes wifi son de 8 caracteres y utilizan los número 1-4 y las letra a-d, utilizamos una herramienta llamada crunch para crear cadenas de caracteres de 8 caracteres combinando dichos caracteres y a la vez compararlo con el handshake:

**Crunch 8 8 1234abcd | aircrack-ng –a [tipo de ataque, elegiremos el 2 el de fuerza bruta]** **[dirección en la que está alojado el archivo con los datos del handshake] –e [ESSID] –b [Dirección MAC de la red objetivo] –w [Ruta del diccionario, en nuestro caso no hay diccionario, pondremos -].**

FOTO ATAQUE FUERZA BRUTA

Ya tendríamos la contraseña con la que conectarnos a la red:

FOTO CONECTADO A LA RED