MANUAL AIRCRACK-PTW ATHEROS

Los pasos se pondrán con ath0, wifi0 y ath1 como interfaces (tarjetas Atheros), sustituyendose para cada caso por la que corresponda...

1. Lo primero tener correctamente instalados los drivers para nuestra tarjeta, para poderla poner en modo monitor e inyectar trafico, esto ya depende del chipset que tenga la tarjeta, en mi caso es Atheros y el driver es MadWifi, (Aquí tenéis una buena pagina para ver que chipset usa cada tarjeta, asi como el driver, pudiendo filtrar por fabricante, chipset... Linux wireless LAN support).

2. Una vez configurada la tarjeta y funcionando, habrá que ponerla en modo monitor, normalmente:
iwconfig ath0 mode monitor
en caso de que este método no sirva (con atheros no es valido este metodo):
airmon-ng start wifi0 [canal]
Esto creara una nueva interfaz ath1 que sera la que usemos a partir de ahora (para otros Drivers/Chipsets la que corresponda). Opcionalmente podemos poner un canal.

3. Ver que redes/clientes hay al alcance, para ello usaremos airodump-ng de la siguiente manera:
airodump-ng -w archivocaptura ath1
De esta forma veremos que redes/clientes hay para todos los canales.

4. Fijamos el objetivo, y miramos su bssid o mac y el canal en el que trabaja, para capturar específicamente para esa red:
airodump-ng –channel 9 -w archivocaptura ath1
Si se quiere restringir la captura a una red determinada, porque hay varias redes en el mismo canal, y queremos que la captura sea solo de una de ellas:
airodump-ng –bssid XX:XX:XX:XX:XX:XX –channel N -w archivocaptura ath1
Siendo XX:XX:XX:XX:XX:XX la MAC del AP objetivo y N el canal en el que esta. La captura la haremos sin el –ivs, para que guarde los paquetes enteros, con vistas a poder usar aircrack-ptw que necesita que la captura se haga de esta forma.

5. Una vez que tenemos trabajando airodump-ng en un terminal, y tenemos algun cliente conectado a esa red (se ve en airodump-ng), abrimos otro terminal para la inyección de paquetes con aireplay:
aireplay-ng –arpreplay -b XX:XX:XX:XX:XX:XX - h YY:YY:YY:YY:YY:YY ath1
Siendo XX:XX:XX:XX:XX:XX la MAC del AP objetivo y YY:YY:YY:YY:YY:YY la del cliente conectado a esa red. Ahora deberíamos notar un incremento en la velocidad de captura de datos por parte de airodump-ng, en cuanto aireplay-ng capture y reinyecte paquetes ARP.

5b. Si no tenemos ningun cliente conectado, debemos utilizar el ataque fake authentication, que cuando lo utilicemos, en el airodump-ng aparecerá como si se hubiese conectado un cliente. Esta mac es la que utilizaremos en YY:YY:YY:YY:YY:YY en el punto 5:
Para asociarse con un punto de acceso, usa la falsa autenticación:
aireplay-ng -1 0 -e teddy -a 00:14:6C:7E:40:80 -h 00:09:5B:EC:EE:F2 ath0
Donde:
-1 significa falsa autenticación

•

0 tiempo de reasociación en segundos

- -e teddy es el nombre de la red wireless
- -a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso
- -h 00:09:5B:EC:EE:F2 es la dirección MAC de nuestra tarjeta
- ath0 es el nombre de la interface wireless

6. En cuanto tengamos unos cuantos paquetes capturados (80k-100k segun cada uno...) podemos poner a trabajar a aircrack-ng o usar aircrack-ptw que necesita menos datos capturados para sacar la clave.
aircrack-ng -0 -x -i 1 archivocaptura.cap
-i 1 es para decirle que el índice de clave sera 1 (1-4) que es lo normal, esto lo podemos quitar si queremos. Por defecto busca contraseñas de 128bits, si es de 64 también la sacara pero tardara algo mas). Si se quiere indicar que la clave es de 64bits, podemos poner el parametro -n 64.
Para aircrack-ptw:
aircrack-ptw archivocaptura.cap