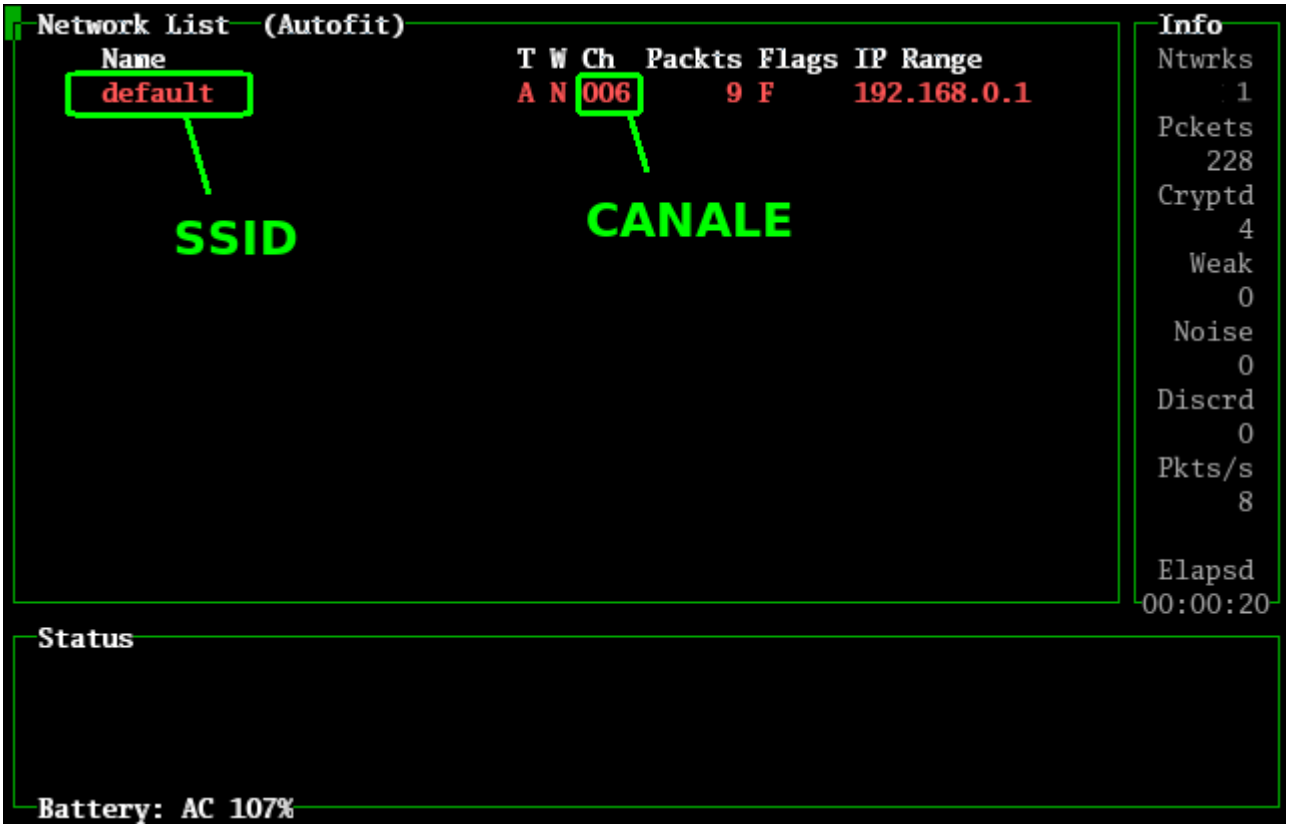
WARDRIVING E WEP CRACKING
evilsocket
http://evilsocket.altervista.org/

Ciao a tutti, scrivo questo articolo per spiegare la tecnica del wep-cracking, ovvero crackare la chiave wep di un determinato access-point wireless al fine di ottenere una connessione alla sua rete ed eventualmente al web .

Gli strumenti necessari (almeno quelli che uso io, ce ne saranno degli altri, boh XD) sono i seguenti :

a) 1 pc con una scheda wireless ... doh ! :D
b) Kismet, il fantastico monitor di rete, scaricabile da http://www.kismetwireless.net/
c) la suite di programmi "aircrak-ng" scaricabile da http://aircrack-ng.org/

Ok, iniziamo ... prima di tutto dobbiamo ottenere la lista dei punti di accesso raggiungibile ... le informazioni necessarie sono il SSID nel access point (il nome) ed il canale sul quale opera .
Lanciamo Kismet, lasciamolo in esecuzione e dopo un po dovremmo vedere una cosa del genere



Dove vedete indicato un access point chiamato "default" che opera sul canale 6 .

Fatto questo, procediamo a catturare alcuni pacchetti da quel canale, al fine di iniziare il cracking della chiave, quindi lanciamo

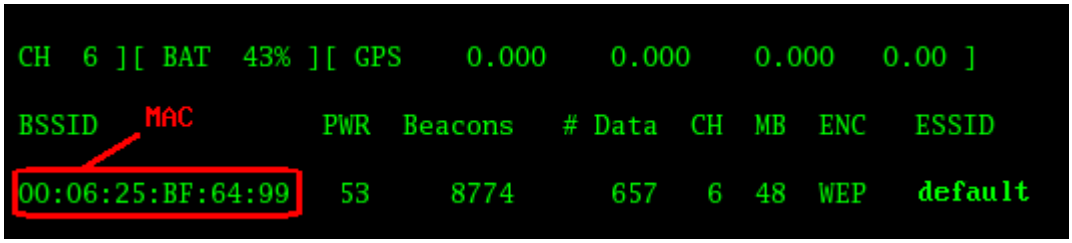
airodump-ng -w file_di_capture -c 6 wlan0

dove

-w file_di_capture : indica che i pacchetti catturati verranno salvati nel file "file_di_capture.cap .

-c 6 : indica di "sniffare" pacchetti solo sul canale 6, ovvero quello dell access point che abbiamo scelto .
wlan0 : il nome della scheda wireless, nel mio caso wlan0 .

Lasciate che airodump catturi un po di pacchetti, prestando attenzione al MAC address dell access point rilevato come nella figura



E' di fondamentale importanza che il programma catturi QUANTI PIU' PACCHETTI possibile, poichè in questo modo avrete + speranze di catturare anche il traffico generato dall autenticazione tra un pc della rete e l'access point, con relativa chiave wep .
Ci sarebbe anche un modo per "forzare" una delle macchine della rete a riloggarsi verso l'access point ri-inviando la chiave, ma con un po di fortuna e pazienza non dovrebbe essere necessario .

Quando pensate di avere abbastanza pacchetti per iniziare l'attacco fermate airodump (premendo CTRL+C da console/cmd.exe) .

A questo punto ci troviamo il nostro bel file_di_capture.cap da crackare, quindi procediamo con aircrack-ng :

aircrack-ng -f 4 -m 00:06:25:BF:64:99 -n 64 file_di_capture.cap

dove

-f 4 : è il numero di volte che bisogna lanciare l'attacco "Fudgefactor", impostatelo a 4 (qui vi dovete fidare di me almeno che non volete che vi faccia una lezione di crypto-analisi :)).
-m 00:06:25:BF:64:99 : è il mac address del punto di accesso, come airodump ci aveva mostrato .
-n 64 : indica i bit della chiave, possono essere 64, 128, ecc .
file_di_capture.cap : il file che contiene i pacchetti catturati .

Ora lasciatelo elaborare e nell arco di qualche decina di minuti, avrete la vostra bella chiave WEP da usare per autenticarvi nella rete :) .

evilsocket