Crack di una rete WPA

Nell crack di una rete wpa/wpa2 è più semplice e veloce la fase di sniffing mentre la fase del cracking è un po' una lotteria poichè per ora si tratta di bruteforce attack con dizionari..
Il vantaggio è che una volta catturato l'handhake occorrente al crack è possibile operare il crack offline,lo svantaggio è che la parola non è di senso compiuto o contenuta nei nostri dizionari il crack risulta per ora impossibile.

Che cos'è il wpa handhake?

Possiamo definirlo come una specie di "saluto" (hand-shake,..) tra due computer prima di iniziare la comunicazione,in questa fase essi "concordano" la velocità di trasmissione,i protocolli...e la criptazione.Si sente sempreparlare nelle guide di four way handshake, in poche parole si tratta di una semplice comunicazione request/acknowledgement.

```
A chiede a B     -->ciao sono una scheda wifi
B risponde ad A, -->eila' io sono un access point son protetto da wpa,trasmetto a 54M in modalità b.
A chiede a B     -->ma io trasmetto a 11M,ti va bene la mia WPA,PSK ed il mio MAC?
A risponde a B   -->ok è giusta, connettiti pure
```

Dobbiamo catturare questa comunicazione per operare il crack wpa, ovviamente con la suite aircrack..No client no crack..
Sarà lasciato sottointeso l'uso di strumenti linux-live come backtrack e kismet

Analisi della rete

Avviamo kismet e cerchiamo tutti questi dati:

la rete obiettivo della nostra analisi, è fondamentale che la sua protezione sia del tipo wpa/wpa2 con PSK (Pre Shared Key),

* il suo canale,il suo MAC adress
* la velocità di trasmissione (rate, ad esempio 11 M, 22M,54M...)
* la modalità di trasmissione (802.3b o g)

Ora è necessario cercare dei client connessi, possiamo ancora farlo con kismet (premendo c).
Certo anche se non ci sono client connessi è sempre possibile continuare il tutorial ma bisognerà comunque attendere che qualche buonanima si connetta..
Ora che abbiamo annotato tutto ciò che ci serve possiamo impostare la cattura..

settaggi fondamentali

Dopo aver spento kismet (che sembra a me sembra un po' interferire con la cattura), impostiamo il monitor mode sul canale della rete,
supponiamo sia il canale 11:

```
airmon-ng stop wlan0
airmon-ng start wlan0 11
```

ora impostiamo il rate e la modalità di trasmissione con i seguenti comandi,(personalmente credevo non fosse importante ma i fatti mi hanno smentito..):

```
iwconfig wlan0 rate 22M  # supponendo il rate sia 22M
iwpriv wlan0 mode 2      # modalità b (0 sta per auto 1 per g..etc)
```

Ora ricordiamo che se la cattura non andra' a buon fine è buona norma riprovare abbassando il rate al minimo:

```
iwconfig wlan0 rate 1M
```

catturare dell'handshake

mettiamo in ascolto airodump sul canale giusto ,(bssid è il mac dell'access point obiettivo, scriviamo i risultati nel file "testhandshake")
airodump-ng --bssid 00:1D:8B:XX:XX:XX --channel 11 -w testhandshake wlan0

Ora dobbiamo aspettare che qualche client si connetta con la password corretta affinchè ci sia un handshake corretto... Oppure possiamo deautenticare un client già connesso per farlo riconnettere,per farlo inviamo uno o più pacchetti di deautenticazione conaireplay:

aireplay-ng -0 1 -a 00:1D:8B:XX:XX:XX -c 0E:1B:DA:XX:XX:XX wlan0

-0 sta per modalità --deauth ed il numero che segue è il numero di pacchetti di de-autenticazione (proviamo anche 5,9,10, ma non troppi,altrimenti l'AP non ci ascolta)

Il primo MAC è quello della stazione, mentre il secondo è quello del client da disconnettere.

A questo punto con un po' di pazienza e tentativi (modificando anche il rate a 1M) nella finestra di airodump dovrebbe apparirci in alto a destra la scritta:
WPA HANDSHAKE !
Ora in molti dicono di verificare l'handshake conwiresharkcon filtro eapol, ma io ho notato che se airodump lo dice c'è da fidarsi,e poi lo controlla anche aircrack.
(NOTA: a chi dice che ci devono essere tutti e quatto i reply handshake scopiazzando le guide senza esperienza personale, provate solo con tre e funziona lo stesso il crack...)

Crack del wpa

E' veramente dura se si tratta di access point con una password casuale di 24 caratteri...
Ma fortunatamente in molti usano parole di uso comune che sono spesso contenute in molti dizionari.

Quindi a questo punto è fondamentale reperire molti dizionari della lingua giusta per ilbruteforcingcon aircrack, ne esistono moltissimi sulla rete.
Ma un po' di social engineering non guasta, se la rete si chiama CapitanoKirk procuratevi un dizionario con tutti i personaggi di star trek no?

Per il crack potete operare offline (anche su windows con aircrack windows) digitando:

aircrack-ng -w dizionario.txt -b 00:19:5B:XX:XX:XX testhandshake.cap

dove ovviamente dizionario.txt è la vostra wordlist ed il MAC è quello dell APoint.
Nota: sul bruteforcing wpa dedicheremo un articolo a parte dove analizzeremo anche le cosiddette rainbow tables (genpmk,cowpatty...etc)
Qui riporto una efficace worlist italiana di date e parole.(15.5 MB,compressa 5MB)

Generazione di wordlist mirate

Neisuccessivi articoli ci occuperemo della generazione di wordlist efficaci tramite script di shell.
Un primo esempio di generazione di wordlist di numeri lo trovate qui.

UPDATE:Non perdere i nuovi articoli sulla generazione di wordlist e sulle tabelle di hash precomputate!
HOT UPDATE:RELAZIONE sull'attacco al wpa di Erik Tews (NEW!)
La tesi e la successiva esposizione pubblica hanno già suscitato un gran polverone(vd metodo Michael), è reperibile a questo indirizzo http://eprint.iacr.org/2007/471.pdf e apre nuove frontiere e metodi per il crack wpa.