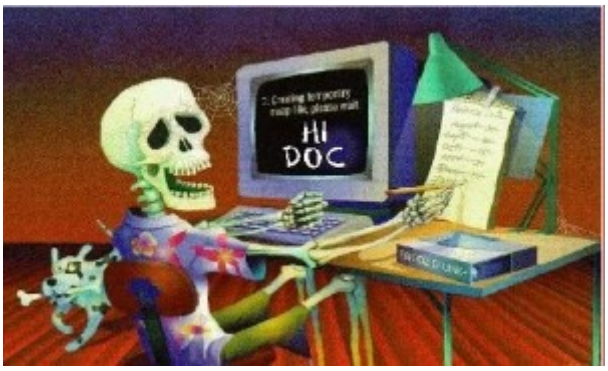
Craccare una rete Wi-fi con chiave WPA

Abbiamo già trattato le reti in un articolo precedente, vi consiglio la lettura in quanto spiega come craccare le reti wifi con protocollo WEP.
Alcune delle tecniche spiegate vi torneranno utili anche per le reti wifi con **protocollo WPA**.
Innanzitutto dobbiamo dire che il WPA fornisce due diverse modalità di autenticazione: **RADIUS e PSK**, la prima è praticamente inespugnabile, mentre una WLAN che utilizza PSK (la maggior parte) può essere attaccata tramite la cattura dell'handshake, per fare questo è necessario che almeno un client sia collegato alla rete bersaglio.
Come distro di riferimento useremo anche questa volta **Backtrack 3**.
Iniziamo a divertirci….



PRIMO PASSO: CATTURARE L'HANDSHAKE
Innanzitutto dobbiamo mettere la scheda wi-fi in modalità **Monitor mode**, quindi apriamo un terminale ed eseguiamo:
airmon-ng start eth1 11
chiaramente al posto di eth1 dobbiamo scrivere l'interfaccia della nostra scheda di rete e al posto di 11 inseriamo il canale utilizzato dall'access point bersaglio (vedi articolo precedente reti WEP).
Adesso eseguiamo **airodump-ng**, con la seguente sintassi:
airodump-ng –bssid [mac address access bersaglio] –channel [numero canale] -w wpa [interfaccia nostra scheda]
Ricordo che per avere informazioni su il MAC Address dell'access point basterà usare **Kismet** (vedi qui).
Adesso dobbiamo attendere…che un client si connetta alla rete,e nel momento in cui accadrà,nella nostra finestra dove abbiamo eseguito airodump-ng comparirà:
WPA handshake: 00:13:ce:c6:05:53

DEAUTENTICAZIONE DI UN CLIENT
L'attacco deve essere rapido e può capitare che nessun client si connetta, in questo caso è possibile forzare la deautenticazione del client cosicchè sarà costretto a riautenticarsi e noi saremo pronti per catturare i dati necessari dell'handshake.
Per far ciò apriamo un terminale (lasciando aperta quella di airodump-ng) ed esguiamo **aireplay-ng**, adesso è il momento di impiegare un **Deauthentication Attack**!
Il comando da usare sarà:
aireplay-ng -0 1 -a [BSSID] -c CLIENT eth1
Al posto di BSSID inseriremo il MAC address dell'access point bersaglio e al posto di CLIENT scriveremo l'indirizzo MAC del client. Per individuare ul client basta lanciare Kismet e seguire la guida qui.

Adesso che abbiamo i pacchetti di Handshake non ci resta che individuare la passphrase, per far ciò, il metodo più semplice è quello di fare un attacco a forza bruta.

ATTACCO A FORZA BRUTA

Iniziamo con lo scaricare una wordlist (un elenco che ci aiuterà per rubare la passphrase), per il dizionario italiano, quindi apriamo una shell e digitiamo:

wget ftp://ftp.ox.ac.uk/pub/wordlists/italian/words.italian.Z

Adesso possiamo dare questo file a **aircrack-ng** insieme al file di handshake.

Apriamo un terminale e scriviamo:

aircrack-ng -b [mac address access bersaglio] -w [percorso completo della wordlist creata prima][file contenente handshake]

Dato che questo metodo sarà molto lento, possiamo vedere di fare qualcosa per velocizzare tutto, precalcolando l'hash. Per fare questo si usa il programma **coWPAtty**. Adesso dobbiamo generare una tabella degli hash, inserendo l'SSID dell'access point (con Kismet lo troviamo) e un file dizionario (va bene quello che già abbiamo). Adesso possiamo richiamare coWPAtty.

TROVARE LA CHIAVE CON coWPAtty

Apriamo un terminale ed eseguiamo:

cd/pentest/wireless/coWPAtty:'genpmk -s [SSID] -f wordlist -d tabella_hash'.SSID

creata la tabella degli hash eseguiamo coWPAtty:

./cowpatty -d [nome tabella hash] -s [nome rete da attaccare] -r [file con i pacchetti di handshake]

Se la passphrase è composta da una parola comune ma con delle lettere variate,per esempio"casa!"…abbiamo bisogno di un tool che proverà queste permutazioni: **John the Ripper**

CRACCARE LA RETE CON JOHN THE RIPPER

apriamo un terminale e scriviamo:

john—rules –wordlist=[nome dizionario] –stdout | /pentest/wireless/cowpatty/cowpatty -f- -s [SSDI rete bersaglio] -r [file con handshake]

Prima di tutto tengo a precisare che l'uso che si fa delle conoscenze dipende dalla persona…quindi questa guida non vuole assolutamente incitare nessuno all'uso illegale di queste tecniche, quindi per i vari test che farete vi consiglio di usare la vostra rete wi-fi! In questo modo potrete verificare con quanta facilità si riesce ad avere accesso ad una rete protetta….

Adesso non vi resta che divertirvi!!

P.s. Non avete letto l'articolo "Come craccare le reti wi-fi con protocollo WEP"? vi consiglio di leggerlo subito per avere un quadro più completo

NEWS: Non perderti la Nuovissima Guida per craccare le reti wifi chiave WEP e WPA:

Guida dettagliata: craccare le reti Wifi tramite Aircrack con Interfaccia Grafica.