Sicurezza reti wireless: come scoprire una chiave WEP

Introduzione

Esistono centinaia, forse migliaia di articoli su Internet che descrivono le numerose vulnerabilità di WEP, Wired Equivalent Privacy, ovvero il protocollo utilizzato nelle reti wireless per "garantire" la sicurezza della comunicazione, ma quanti in realtà sanno sfruttare tali vulnerabilità?

Per un utente comune in realtà potrebbe rivelarsi una pratica ardua a causa delle numerose schede di rete in commercio, dei comandi che bisogna impartire e del fatto che i software adatti a tale scopo girano principalmente sotto linux. In questo articolo cercheremo di spiegare passo passo l'approccio usato per rompere una chiave WEP. Quello che si cercherà di fare è concentrarsi sulla procedura usata senza tenere conto dei problemi inerenti l'hardware e ai bug presenti nei software che ricordiamo sono tutti freeware. L'intero attacco viene fatto senza dare risalto a un particolare software o hardware, l'importante è avere a disposizione dei portatili e delle schede di rete.

Non hai bisogno di essere un esperto di reti per portare a termine le indicazioni di questo articolo, ma deve esserti familiare la terminologia di rete e i principi base. Dovresti sapere come effettuare un ping, aprire il prompt dei comandi di Windows, inserire linee di comando e saper maneggiare le principali schermate di Windows riguardo le reti.

La pratica di forzare una rete protetta con WEP è chiamata WEP Cracking. Quello che ci proponiamo di fare è la decifrazione di una **wepkey** a 40 o 104 bit.

Per ricavare la wepkey sfrutteremo le debolezze di RC4 e ci serviremo delle falle presenti in tutto il protocollo WEP per procurarci i dati necessari; al nostro scopo metteremo quindi in atto vari attacchi come deauth-attack, replay-attack, spoofing.

L'attacco verrà descritto tenendo conto che tutta l'operazione sia svolta a scopi didattici, ed è quindi possibile accedere all'hardware da attaccare. Ad ogni modo, quando necessario, verranno illustrati i passaggi da effettuare nel caso si voglia simulare un attacco reale, senza quindi poter accedere o conoscere nulla della rete da attaccare.

Attori

Vediamo quali sono gli attori coinvolti durante l'attacco.

Attaccati:

- **Access Point (AP)** : è l'access point di cui vogliamo conoscere la chiave per riuscire ad entrare nella rete.
- **Target Client (TC)** : è un client collegato all'access point.

Attaccanti:

- **Sniffing Client (SC)** : è uno dei pc dell'attaccante. Questo si occuperà di sniffare quanto più traffico possibile. Questo traffico verrà registrato sull'hard disk (non tutto il contenuto dei pacchetti ma solo alcune informazioni come i IV). Svolge un ruolo passivo.
- **Attacking Client (AC)** : è un client che si occuperà di "stimolare" il giusto traffico nella rete, vedremo dopo che cosa si intende. Svolge un ruolo attivo.

In realtà il WEP Cracking può essere effettuato con un solo computer, ma questa suddivisione permette di essere più chiari nell'esposizione.

Di cosa abbiamo bisogno

Vediamo ora l'hardware e il software di cui abbiamo bisogno.

Hardware:

Wireless Access Point: questo è l'obiettivo dell'attacco e può essere di qualunque marca e modello, basta che stia trasmettendo pacchetti cifrati con WEP a 40 o 104 bit. Nel nostro caso è stato usato un Netgear WGT624 v2.

Target Client : è il computer che sta dialogando con l'access point. Anche in questo caso non è importante la marca o il modello di scheda Wireless utilizzata, inoltre non è importante il sistema operativo utilizzato per effettuare la comunicazione. Nel nostro caso è stato usato un portatile Dell con wireless intergato.

Sniffing Client : è il computer che si occuperà di sniffare il traffico della rete. In questo caso il computer dovrà montare Linux (poiché i relativi software open source utilizzati sono nativi di Linux) e la scheda Wireless utilizzata dovrà supportare la modalità Monitor, ovvero la modalità utilizzata per captare i pacchetti, nonché la capacità di fare packet injection. A questo scopo consigliamo di usare schede wireless basate sul chipset PRISM 2 che è supportato da tutti i programmi usati.

Attacking Client: è il computer che si occuperà di "stimolare" la rete a produrre traffico utile per la decodifica della chiave. La stimolazione, come vedremo, verrà effettuata con attacchi di tipo Packet Injection, la scheda Wireless dovrà quindi supportare tale modalità o non potrà inviare pacchetti verso la rete quando si trova in Monitor Mode. In generale vanno bene tutte le schede che si basano sui Chipset PRISM 2, PrismGT (FullMAC), Atheros, RTL8180 e Ralink.

Software:

La procedura di WEP Cracking richiede diversi pacchetti software. Questi per fortuna sono tutti open source, funzionano sotto Linux e in alcuni casi esistono delle versioni per Windows. Per gli utenti Windows è possibile inoltre, in alcuni casi, utilizzare un emulatore di ambiente Linux chimato Cygwin (**http://www.cygwin.com**).

Risulta molto interessante la soluzione proposta da remote-exploit.org (**http://new.remote-exploit.org/index.php/Main_Page**). In questo sito è possibile trovare una versione di Linux di tipo LIVE (ovvero che parte da cd senza installare nulla) chiamata Auditor Security Collection LIVE CD che contiene tutti i programmi necessari già preinstallati (e molto altro). Durante il boot questa distribuzione di Linux è in grado di trovare e configurare molte schede Wireless. Una volta scaricata l'ultima versione si dovrà masterizzare l'immagine su cd, usando programmi come Nero o CDBurnerXP (free), e avviare la macchina usando il cd come disco di boot.

Avrai bisogno di un cd per ogni computer. Il resto della guida procede dando per scontato che si stà utilizzando tale distribuzione nelle proprie macchine.

In ogni caso la lista dettagliata dei software necessari è la seguente:

- **Pacchetto "aircrack"** , comprende:
  - Airdump – Uno sniffer
  - Aireplay - Un software per il packet injection
  - Aircrack – Cracker per chiavi statiche WEP e WPA-PSK
  - Airdecap – Decifra file catturati
- **Pacchetto "Wireless Tool"** scaricabile dal sito http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html . Questo è un pacchetto che contiene una serie di programmi di gestione delle reti wireless comprende:
  - iwconfig – Per manipolare i parametri wireless di base della propria scheda
  - iwlist – Esegue uno scanning per determinare frequenze, bit-rate, chiavi, ecc
  - iwspy – Per verificare la qualità del collegamento
  - iwpriv – Permette di manipolare le Wireless Extension specifiche del driver
  - ifrename - Permette di rinominare le interfacce

- **Kismet** - Disponibile alla pagina http://www.kismetwireless.net/ è un software in grado di funzionare come sniffer e Intrusion Detection System per reti Wireless. Kismet funziona con tutte le schede wireless che supportino la modalità raw monitorig (rfmon) ed è in grado di sniffare reti 802.11b\a\g.

Preparativi

É importante preparare il proprio "laboratorio" per la pratica che andremo a eseguire, infatti bisogna prevenire possibili effetti collaterali che potrebbero danneggiare gli altri Access Point a noi vicini. Nella seconda parte ad esempio verrà descritto un modo per scollegare i client dal proprio Access Point e non vogliamo che ciò vada a danneggiare il lavoro di qualcuno. Se ci si trova in un complesso di uffici, un palazzo o altri posti con molte reti wireless sarebbe prudente aspettare la notte quando le reti sono poco usate. Fate pratica in maniera sicura e responsabile!

Il primo passo è collegare e configurare la rete wireless che vogliamo violare
Se l'operazione di WEP Cracking è fatta a scopi didattici, ovvero è possibile accedere ad AP e TC bisogna verificare che:

1. L'access point sia acceso e sia stata abilitata la codifica WEP con chiave a 64 bit. (Inizialmente è consigliabile utilizzare una chiave a 64 bit per poi passare ad una da 128 bit).

2. Il TC sia acceso e connesso all'AP. In questo caso, se possibile, è consigliabile far comunicare il Target Client con l'Access Point sotto Windows XP poiché tutte le procedure di configurazione sono molto semplificate rispetto a Linux. Verificare quindi, cliccando 2 volte sull'icona di stato in basso a destra che il PC sia connesso.

3. Avviare entrambi i computer SC e AC utilizzando la distribuzione Auditor Linux come disco di boot. (Per il boot da cd bisogna accedere al bios ed indicare il lettore cd\dvd come prima unità di avvio). Naturalmente al momento dell'accensione le schede wireless devono essere preventivamente inserite ed accese.

4. Una volta avviato il sistema operativo per verificare che le schede di rete siano state riconosciute e configurate è possibile usare il comando **iwconfig**, un programma che fa parte del dei "wireless tools".

Dopo aver digitato il comando dovrebbe apparire una risposta del tipo:

Figura 3.3- Con il comando iwconfig è possibile conoscere tutte le informazioni sulla nostra interfaccia Wireless

Se invece non vengono rilevate le schede allora bisogna procurarsi il driver adatto e installarlo, quindi riprovare.

Attacco “zero knowledge”

Finora abbiamo descritto i passaggi tenendo conto che l’attacco che vogliamo eseguire sia a scopi didattici, è quindi sia possibile accedere alle macchine da attaccare. Nella realtà se si vuole penetrare in una rete Wireless non è possibile accedere all’hardware, quindi alcune delle informazioni necessarie su questi vanno ricercate con metodi alternativi.

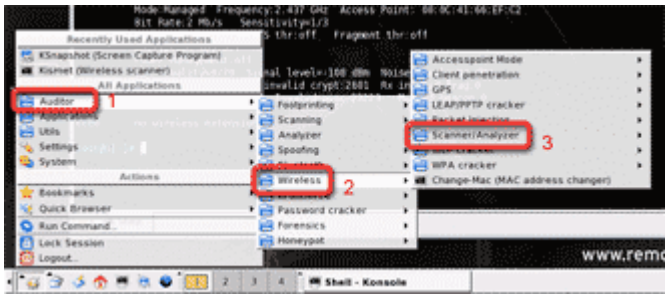
Quando si vuole effettuare una attacco di questo tipo, senza conoscere niente a priori della rete, si parla di attacco **“Zero Knowledge”**, mentre se l’attaccante già conosce le informazioni necessarie si parla di attacco **“Full Knowledge”**. Assumendo di voler procedere ad un attacco del primo tipo vediamo di cosa abbiamo bisogno e quindi come ottenerlo.

Sono necessari:

- MAC Address dell’Access Point
- MAC Address del Target Client
- Channel - Canale di comunicazione dell’AP

Per reperire queste informazioni è sufficiente utilizzare Kismet, uno scanner di reti wireless che permette di trovare le reti presenti nel punto dove ci troviamo. Kismet è anche uno sniffer in grado di catturate traffico ma ci sono tool come airodump (una parte di Aircrack) che lavorano meglio dal punto di vista del WEP Cracking. Kismet ci sarà utile per verificare che le schede di rete stiano lavorando bene e per ricavare alcune informazioni interessanti sulla rete wireless.

Per avviare Kismet basta ciccare su Programs, Auditor, Wireless, quindi su Scanner\Anayzer e infine su Kismet.



Nella prima schermata vengono visualizzate tutte le reti Wireless trovate, il canale di comunicazione, il numero di pacchetti, i canali analizzati, etc.

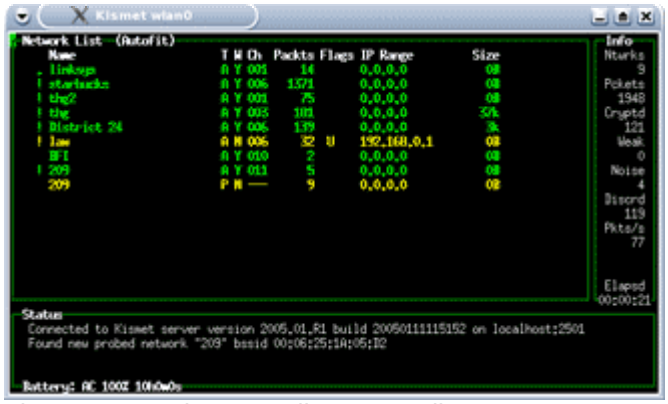


Figura 3.4 – Schermata di apertura di Kesmet

A questo punto digitate **"s"** per accedere alla schermata per l'ordinamento delle reti, quindi digitate **"c"** per ordinarle per canale.

Ora è possibile scorrere le reti con le frecce direzionali, quindi posizionarsi sulla rete che si vuole crackare e premere Invio.
Si aprirà una schermata dove è possibile trovare delle informazioni interessanti come BSSID\MAC (il MAC dell'AP) e Channel, che corrispondono a una buona parte delle informazioni che erano necessarie.

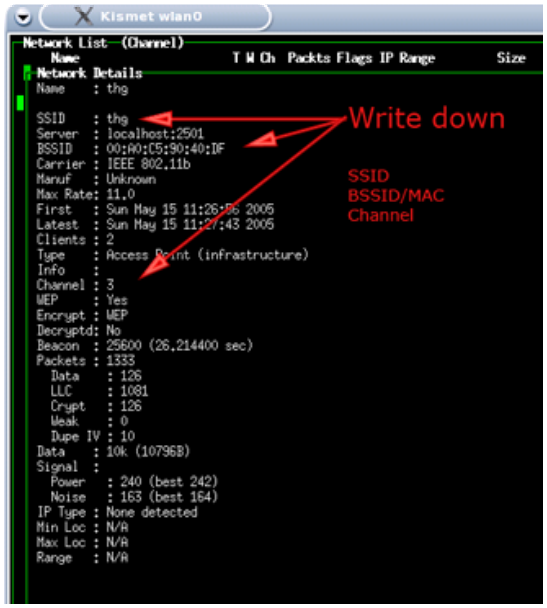


Figura 3.5 – Informazioni che è possibile ricavare sull'AP grazie a Kismet

Nota: In alcune reti è possibile disabilitare la trasmissione in broadcast del SSID per aumentare la sicurezza della rete. Mentre questo è vero per altri software, Kismet riesce facilmente a trovare reti con SSID disabilitato seguendo la comunicazione tra l'access point e i suoi client.

Come ultima informazione abbiamo ancora bisogno dell'indirizzo MAC del Target Client. Questo si ricava facilmente sempre con Kismet, infatti dal menù principale basta posizionarsi sulla rete che ci interessa e premere **shift-C**. In questa nuova schermata viene visualizzata la lista degli indirizzi MAC dei client associati alla rete, ovvero quello del TC.

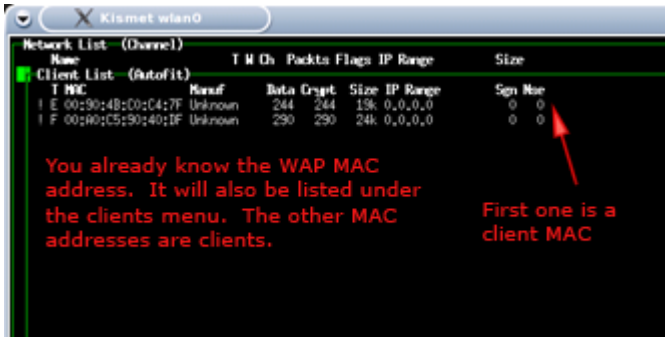


Figura 3.6 – Client associati ad un AP

Inizia l'attacco

Arrivati a questo punto ci troviamo nella seguente situazione:

- Le schede Wireless di TC, SC, AC sono accese e funzionati
- L'AP sta comunicando con il suo client
- I software "aircrack" e "wireless tool" sono installati
- Le informazioni necessarie sono state appuntate

Possiamo iniziare l'attacco.

Cosa si vuole fare:

L'idea base è catturare quanto più traffico cifrato possibile attraverso lo sniffer **airodump**. Ogni pacchetto dati WEP ha associato il suo Vettore di Inizializzazione (IV): quando sono stati catturati abbastanza pacchetti, eseguiremo aircrack sul file di cattura che procederà ad una serie di attacchi statistici con lo scopo di recuperare la chiave WEP.

Il numero di IV richiesti dipende dalla lunghezza della chiave WEP e dalla fortuna. Di solito, una chiave WEP da 40 bit si può crackare con 200.000 IV, e una chiave WEP da 104 bit con 500.000 IV ma esistono casi in cui possono essere necessari anche 2 milioni di IV.

In generale **non c'è modo di sapere quanto è lunga una chiave WEP**: questa informazione è segreta e non viene diffusa, nè nelle frame di gestione nè in quelle dati; quindi, airodump non può indicare la lunghezza della chiave.

Per risolvere il problema l'unica cosa da fare è eseguire aircrack due volte: quando si hanno 200.000 IV, lanciamo aircrack con l'opzione "-n 64" (la sintassi verrà introdotta in seguito) per crackare la chiave a 40 bit. Quindi se non trovi la chiave, rilancia aircrack (senza l'opzione -n) per crackare la chiave a 104 bit.

Come lo si vuole fare

Ecco in grandi linee come eseguiremo l'attacco:

- Avvieremo lo sniffer **airodump** sul SC.
- Avvieremo **aireplay** sull'AC per stimolare la rete a produrre velocemente IV.
- Quando avremo un numero sufficiente di pacchetti catturati avviamo **aircrack** che, lavorando sui file di cattura generati da airodump, tenta di recuperare la chiave WEP.

Avviare lo sniffer

Nello Sniffing Client apriamo una shell e digitiamo i seguenti comandi

N	Comando
1	**iwconfig wlan0 mode monitor**
2	**iwconfig wlan0 channel 11**
3	**mkdir cap**
4	**cd cap**
5	**airodump wlan0 cap 11**

Con il commando 1 stiamo **abilitando** la modalità monitor della scheda wireless. Sostituire "wlan0" con il nome della propria interfaccia se necessario. (Il nome dell'interfaccia è visualizzato con il comando iwconfig senza parametri)

Il comando 2 serve a posizionare la scheda sul canale di trasmissione dell'AP. Sostituire 11 con il canale ricavato nel paragrafo 3.4.1

Con il comando 5 si avvia lo sniffer utilizzando l'interfaccia wlan0 ascoltando il canale 11 e il file di cattura avrà il prefisso "cap".

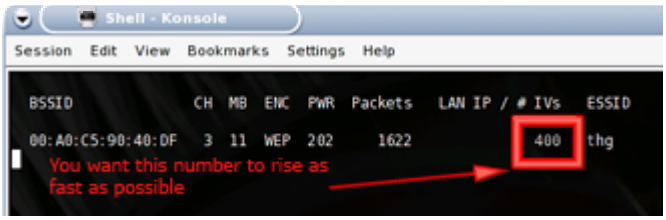


Figura 3.7 – Airodump al lavoro

Nota: Se il programma viene fermato (con ctrl-c si esce) e poi riavviato con gli stessi parametri verrà creato un nuovo file cap1, cap2, che potrà essere fuso con i precedenti.

Durante lo sniffing della rete il nostro obbiettivo è catturare quanti più IVs possibile. La velocità con cui vengono letti i IVs cambia a seconda dell'uso che si sta facendo della rete. I pacchetti "beacons" invece non sono utili per crackare WEP in quanto non sono cifrati.

Indicativamente, come già accennato, avremo bisogno da 50.000 a 200.000 IVs per decifrare una chiave da 64 bit (40 + 24 dell'IV) e da 200.000 a 700.000 per decifrare una chiave da 128 bit (104 + 24 dell'IV).

Arrivati a questo punto ci saremo resi conto che **non è affatto facile accumulare IVs** con un utilizzo normale della rete, anche se i client della rete stanno eseguendo dei download molto lunghi. Senza ulteriori accorgimenti sono necessarie molte ore se non giorni per accumulare un numero sufficiente di IVs per eseguire aircrack con successo. Fortunatamente esistono molti tool progettati appositamente per velocizzare la ricezione di IVs.

Inviare i giusti stimoli

É giunto il momento di utilizzare l'Attacking Client. Con questo PC in pratica andremo a "stimolare" la rete a produrre più velocemente i IVs.

La tecnica utilizzata è quella di forzare la de-autenticazione del Target Client nella rete. Infatti, appena questo se ne accorgerà non farà altro che provare a ri-autenticarsi e durante la ri-autenticazione verranno generati molti IVs. Questo processo viene comunemente chiamato **deauth-attack** e viene implementato da aireplay. Vediamo quali sono gli attacchi che aireplay è in grado di eseguire.

aireplay

Se il driver della scheda Wireless ha la patch corretta, aireplay può iniettare pacchetti raw 802.11 in Monitor mode ed effettuare quindi 5 attacchi diversi di tipo Packet Injection. Di questi 5 noi utilizzeremo il numero 0 e 2.

Attacco 0 – Deautentication

Questo attacco è utile soprattutto per recuperare un ESSID nascosto (non annunciato) e per catturare gli handshakes WPA forzando i client a ri-autenticarsi. Può anche essere usato, come faremo, per generare richieste ARP come fanno i client Windows a volte quando vuotano la ARP cache in fase di disconnessione. Ovviamente, questo attacco è inutile se non ci sono client associati.

Attacco 1 – Autenticazione falsa

Questo attacco serve solo quando hai bisogno di un MAC address associato per gli attacchi 2, 3, 4 (ovvero opzione -h) e in questo momento non ci sono altri client associati. In genere è meglio usare il MAC address di un client vero negli attacchi 2, 3 e 4. L'attacco con falsa autenticazione NON genera ARP requests. Ricorda inoltre, gli attacchi successivi funzioneranno meglio se modifichi il MAC address della scheda, cosi che spedisca ACKs correttamente.

Attacco 2 – Replay interattivo di pacchetti

Questo attacco permette di scegliere un pacchetto specifico per il replay; a volte dà risultati migliori dell'attacco 3 (ARP reinjection automatica).

Attacco 3 – ARP-request reinjection

Serve per eseguire l'attacco ARP-request replay ed è il più efficace nel generare nuovi IVs. Hai solo bisogno del MAC address di un client associato, o di un MAC falso dall'attacco "attacco 1". Può darsi che sia necessario aspettare un paio di minuti, o anche di più, fino a vedere una ARP request; questo attacco non funziona se non c'è traffico.

Ricordiamo che il protocollo **ARP** (**Address Resolution Protocol**) fornisce la "mappatura" tra l'indirizzo IP a 32bit (4byte) di un calcolatore e il suo MAC address, l'indirizzo fisico a 48bit (6 byte).
ARP è un protocollo di servizio, utilizzato in una rete di calcolatori che usa il protocollo di rete IP sopra una rete di livello datalink che supporta il servizio di broadcast.
Per inviare un pacchetto IP a un calcolatore della stessa sottoreteè necessario incapsularlo in un pacchetto di livello datalink, che dovrà avere come indirizzo destinazione il mac address del calcolatore a cui lo si vuole inviare. ARP viene utilizzato per ottenere questo indirizzo.
Se il pacchetto deve essere inviato a un calcolatore di un'altra sottorete, ARP viene utilizzato per scoprire il mac address del gateway.
In ogni calcolatore, il protocollo ARP tiene traccia delle risposte ottenute in una apposita cache, per evitare di utilizzare ARP prima di inviare ciascun pacchetto. Le voci della cache ARP vengono cancellate dopo un certo tempo di inutilizzo.

Attacco 4 - KoreK's "chopchop" (CRC prediction)

Questo attacco, quando funziona, può decifrare un pacchetto dati WEP senza conoscere la chiave. Può anche funzionare con uno WEP dinamico. Questo attacco non recupera la chiave WEP, ma *semplicemente recupera il plaintext.* Tuttavia, la maggior parte degli access point non è vulnerabile. Questo attacco richiede almeno un pacchetto dati WEP.

Deauth-Attacck

Per procedere con la forzatura della de-autenticazione del TC digitare i seguenti comandi:

iwconfig wlan0 mode monitor
aireplay -0 5 –a <MAC del AP> -c <MAC del TC> wlan0

Il primo comando serve per far passare la scheda in monitor mode.
Il secondo comando invia 5 segnali di de-autenticazione.

Dopo aver ricevuto questo segnale il Target Client tenta di ri-associarsi all'AP inviando una gran quantità di dati. In pochi secondi sarà possibile vedere con airodump, che è ancora in esecuzione, un incremento di 100-200 IVs.

Questo incremento, pur essendo interessante, non permette un avanzamento apprezzabile della quantità di IVs richiesta.

Come ottenere tanti IVs in pochi minuti

Esistono ulteriori strumenti che interferiscono più seriamente con il normale funzionamento della rete wireless e permettono di collezionare tutti gli IVs che occorrono in pochissimo tempo. Questo tipo di attacco è chiamato **replay attack**.

In questo attacco viene catturato un pacchetto generato dal Target Client e viene replicato più e più volte. Inoltre, utilizzando la tecnica dello **spoofing**, (l'invio di pacchetti facendo credere all'host di destinazione che il pacchetto provenga da un'altra sorgente) la rete crederà che il pacchetto provenga da un client valido.

Quello di cui abbiamo bisogno è catturare un pacchetto che sia stato generato dal deauth attack e avviare il replay attack usando proprio quel pacchetto. Un perfetto candidato per la cattura sono gli **Address Resolution Protocol** (ARP), i pacchetti che sono inviati durante la fase di ri-autenticazione, poiché sono molto piccoli (68 Byte) e hanno un formato semplice.

Passiamo a vedere la procedura da eseguire.

Per prima cosa riavviamo le AC e SC in modo da avere le macchine pulite.
Ora nella AC dobbiamo avviare aireplay nella modalità 2 ovvero "Replay interattivo di pacchetti" in modo che appena abbia sniffato un pacchetto ARP inizi a replicarlo.

Per eseguire questa operazione dobbiamo digitare:

aireplay -2 -b <MAC dell'AP> -d <MAC di destinazione dei pacchetti> -m 68 -n 68 -p 0841 -h <MAC dell'TC> wlan0

Osservazioni:

- **-d** è l'indirizzo di destinazione dei pacchetti che vengono replicati, mettiamo un indirizzo falso tipo FF:FF:FF:FF:FF:FF

- **-m e –n** indicano rispettivamente la lunghezza minima e massima dei pacchetti. Se lo impostiamo a 68 probabilmente capteremo i pacchetti ARP
- **-h** è l'indirizzo che verrà scritto sui pacchetti inviati. Dobbiamo mettere il MAC del TC se vogliamo fare spoofing.

A questo punto avviamo aireplay nel SC in modo che venga forzata la de-autenticazione dei client (aireplay in modalità 0) così da generare pacchetti ARP necessari all' AC.

Per fare ciò dobbiamo digitare i seguenti comandi

iwconfig wlan0 mode monitor
aireplay -0 5 –a <MAC del AP> -c <MAC del TC> wlan0

Alcune note:

- In alternativa al commando 1 è possibile usare **airmon.sh start wlan0** che è uno script contenuto in aircrack.
- Se omettiamo il parametri –c il comando di de-autenticazione verrà inviato in broadcast a tutti i client.

Ora dovremo ricorrere a tutta la nostra abilità manuale e coordinatoria perché non appena il AC avrà captato un pacchetto ARP dobbiamo velocemente nell'ordine:

In AC -> Indicare ad aireplay di iniziare la replicazione (ovvero premere 'y') come è possibile vedere nella figura precedente.

In SC -> Chiudere aireplay per terminare il deauth-attack (ctrl-c)

In SC -> Avviare airodump per iniziare lo sniffing dei pacchetti

Dopo che abbiamo avviato airodump potremo vedere che il contatore di IVs **aumenta alla velocità di circa 200 IV\sec**

Scacco matto

Dopo che avremo catturato un numero sufficiente di IVs, mentre airodump continua a sniffare, avviamo aircrack che procederà alla decodifica della chiave. Il comando che dobbiamo digitare è:

aircrack –f 2 –m <MAC dell'AP> -n <dim della chiave> cap*.cap

Dove:

- **-n** indica la dimensione della chiave che dobbiamo cercare in bit ovvero 64 o 128. Come già accennato in precedenza questo è l'unico parametro che non è possibile conoscere in alcun modo. Per questo motivo al limite sarà necessario avviare aircrack due volte:
  - una quando avremo collezionato circa 200.000 IVs con il parametro –n 64
  - una quando avremo collezionato circa 500.000 IVs con il parametro –n 128
- **-f** è il fattore che stabilisce il rapporto tra velocità e probabilità di successo. Valori bassi hanno meno probabilità di successo ma sono più veloci.

Se durante l'esecuzione di aircrack terminiamo il programma con ctrl-c oppure il programma termina senza successo, quando verrà riavviato procederà alla decodifica del file utilizzando solo le informazioni che airodump ha aggiunto nel frattempo.

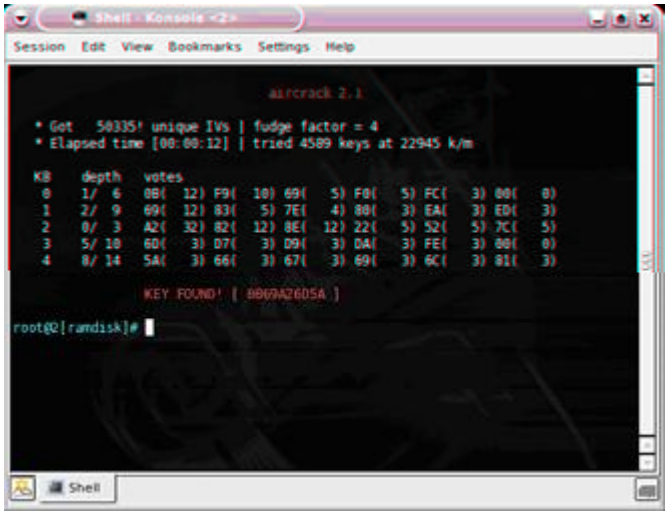


Figura 3.8 – Aircrack al lavoro. Ha trovato una chiave

Prestazioni

Aircrack come avremo notato non ha bisogno di accedere alla rete wireless. Questo software lavora sul file di cattura *.cap quindi in teoria può essere eseguito su un server collegato in rete e che, presumibilmente, dispone di un processore molto più veloce del portatile utilizzato per lo sniffing. Ad esempio è possibile sfruttare i nuovi processori **dual core** aggiungendo ad aricrack l'opzione –p e sfruttando così la potenza dei core paralleli.

Potrebbe essere utile quindi copiare i file *.cap su una penna USB per essere trasportati sul server.
Per fare questo basta digitare i seguenti comandi:

mkdir /mnt/usb
mount –t vfat /dev/uba1 /mnt/usb
cp cap/cap*.cap /mnt/usb
umount /mnt/usb

Se tutto va bene il tempo necessario a rompere una chiave da 64 bit è circa 5 minuti nei casi più fortunati. Alcune volte sono sufficienti 25.000 IVs altre volte ne servono 200.000. Stesso discorso vale per le chiavi a 128 bit, il numero di IVs necessari va da 200.000 a 700.000 Da notare infine che l'uso di un attacco attivo con Packet Injection per aumentare la velocità di accumulo del IVs incrementa di molto le probabilità di essere rilevati.