Hacking delle reti wireless

Autore: *Roberto Saia*
Tratto dal libro: *Sicurezza wireless e mobile*

Le reti wireless si stanno diffondendo tra gli utenti sempre di più e spesso senza un minimo di sicurezza. Ma sapete come può venire attaccata la vostra rete? Scopritelo in questo articolo, può essere utile conoscere le operazioni messe in atto da un aggressore al fine di operare illecitamente all'interno di una rete di tipo wireless.

I pericoli delle reti wireless

A differenza di quanto avviene nell'ambito delle reti cablate tradizionali, le tecniche di hacking delle reti wireless possono contare su un nuovo elemento che complica notevolmente il tutto, un qualcosa che, paradossalmente, rende più agevole il compito degli aggressori ingigantendo le difficoltà di chi opera legittimamente per garantirsi la propria sicurezza.
Il nuovo elemento è rappresentato dalla possibilità per l'aggressore di agire in modo totalmente anonimo, in quanto, non avendo la necessità di connettersi fisicamente alla rete presa di mira, egli può svolgere le sue operazioni tenendosi a debita distanza. Questa è la ragione per la quale, in concomitanza quasi perfetta con la diffusione delle tecnologie di tipo wireless, è nata una nuova modalità di hacking denominata **wardriving**.
Lo scopo di chi opera il wardriving è quello di guadagnarsi una connessione abusiva a una rete privata o pubblica, come per esempio, Internet, attraverso lo sfruttamento abusivo di una rete senza fili.
Gli strumenti principali adoperati da coloro che mettono in pratica il wardriving sono essenzialmente tre: un computer portatile munito di adattatore di rete wireless, un veicolo per gli spostamenti e un apposito software.
Non è infrequente, inoltre, l'utilizzo di un sistema satellitare di rilevamento tipo GPS, in abbinamento al software utilizzato (molti ne contemplano l'uso), al fine di ottenere la mappatura (quella che in gergo viene definita **wireless mapping**) dei punti di accesso rilevati.
Tempo addietro, invece degli attuali sistemi GPS, i wardriver adoperavano dei gessetti colorati con i quali marcavano, utilizzando un apposito simbolismo, i muri degli edifici
o i marciapiedi al fine di indicare il tipo di punto di accesso rilevato. Nata oltreoceano, questo tipo di tecnica oggi inizia a diffondersi anche nel nostro Paese e, infatti, non è difficile reperire in Internet delle mappe dettagliate dei punti di accesso identificati in questo modo, relativi ad alcune grandi metropoli italiane. La possibilità che un aggressore sia in grado di rilevare e utilizzare senza sforzi uno di questi punti d'accesso è, ovviamente, subordinata alla totale assenza di meccanismi di protezione o, quantomeno, all'inadeguata configurazione di questi ultimi.

Le tecniche e gli strumenti

Anche in questo particolare settore del networking sono presenti tecniche e strumenti creati allo scopo di violare i sistemi di protezione eventualmente presenti e penetrare abusivamente all'interno di una rete.
Molti di questi metodi/strumenti sono gli stessi che vengono abitualmente adoperati per compiere analoghe operazioni sulle reti tradizionali di tipo cablato. Altri, invece, sono stati realizzati appositamente per operare in questo ambito specifico.
Riguardo al processo di **hacking**, gli addetti ai lavori effettuano una differenziazione basata sul tipo di informazioni iniziali che sono in possesso del potenziale aggressore nel momento in cui questo decide di compiere un attacco: si parla di **full knowledge** quando egli dispone già dei dati relativi, almeno, al canale di ricetrasmissione adoperato dall'access point e agli indirizzi fisici MAC di quest'ultimo e della macchina client; in caso contrario, cioè in assenza di ogni informazione iniziale, si parla di **zero knowledge**.
In assenza totale o parziale di informazioni, l'aggressore è costretto ad adoperare appositi software in grado di fornirgli i dati mancanti. Tra i tanti prodotti oggi disponibili, quelli che offrono i migliori risultati

e, proprio per questa ragione, risultano tra i più adoperati, sono i software che compongono la suite denominata **aircrack-ng**, descritti nella *tabella 1*.

Programma	Compito svolto
Airmon-ng	Pone l'adattatore di rete wireless in modalità monitor
Airodump-ng	Cattura dei pacchetti in transito (sniffer)
Aireplay-ng	Immissione in rete di pacchetti appositamente assemblati (packet injection)
Aircrack-ng	Decodifica delle chiavi crittografiche statiche di tipo WEP/WPAPSK (cracker)
Airdecap-ng	Decodifica dei file catturati contenenti il traffico WEP/WPA
Packetforge-ng	Permette di creare pacchetti arbitrari (UDP, ICMP ecc.) criptati
Airtun-ng	Il compito principale è quello di creare un'interfaccia di rete virtuale in grado di ricevere una copia del traffico wireless criptato

Tabella 1: composizione della suite aircrack-ng

Occorre sottolineare che questi software, originalmente concepiti per le piattaforme Linux, operano correttamente solo con alcuni tipi di adattatori di rete wireless, quindi è indispensabile assicurarsi preventivamente che l'hardware utilizzato sia compatibile con essi.
Una volta accertato, attraverso la consultazione del manuale o tramite una ricerca su Internet, quale tipo di chipset utilizza l'adattatore di rete wireless in nostro possesso, è possibile verificarne la compatibilità con aircrack-ng tramite le informazioni presenti sul sito del produttore: al momento della stesura di questo articolo esse erano disponibili nell'area denominata **Other Documentation**, sotto la voce **Compatibility**, **Drivers**, **Which Card to Purchase**. Un esempio di quanto detto è riportato, sinteticamente, nella *tabella 2*, tratta, appunto, dal sito in questione.

Chipset utilizzato	Airodump per Windows	Airodump per Linux	Aireplay per Linux
AIRONET	SI	SI	NO
ATHEROS	Dipende dall'interfaccia	SI, solo PCI e CardBus	SI, con apposito aggiornamento
ATMEL, MARVEL	NO	NO	NO
BROADCOM	Solo modelli datati	SI, a partire dal 2.6.14	NO
CENTRINO B	NO	SI	parzialmente NO
CENTRINO B/G	NO	SI, a partire dal firmware 1.0.6	NO
HERMESI	SI	SI	NO
PRISM2/3	NO	SI, a partire dal firmware 1.5.6	
PRISMGT	SI	Dipende dall'interfaccia	Dipende dall'interfaccia
RALINK	NO	SI	SI
RTL8180	SI	SI	SI, con apposito aggiornamento
TI (ACX100/ACX111)	NO	Non testato	NO
ZYDAS 1201	NO	NO	NO

Tabella 2: compatibilità degli adattatori di rete wireless

Essendo Linux l'ambiente nativo di questa suite, i successivi esempi di utilizzo saranno fatti riferendosi a questo sistema operativo. In ogni caso, l'eventuale trasposizione di quanto detto in ambiente Microsoft Windows (pur con alcune limitazioni) non comporta particolari difficoltà: le implementazioni Windows della suite, al momento, non permettono l'utilizzo del software aireplay-ng per il **packet injection** in ambiente 802.11 e, proprio per questa ragione, coloro che desiderano utilizzare appieno le funzionalità di questo software sono costretti a orientarsi verso alternative di tipo commerciale.
Esiste, comunque, una soluzione di ripiego anche per coloro che non intendono acquistare un prodotto commerciale e, allo stesso tempo, non hanno alcuna intenzione di far migrare i loro sistemi verso piattaforme **Unix like**.
Il rimedio è rappresentato dalle distribuzioni Linux di tipo **live CD/DVD** (distribuzioni che si avviano direttamente da CD/DVD e non richiedono alcuna installazione come, per esempio, quella denominata Backtrack), che sono orientate alla verifica della sicurezza dei sistemi e, proprio per questa ragione, contengono tutto il software necessario per questo utilizzo.

Fonti: Aircrack-ng: http://www.aircrack-ng.org; Backtrack http://www.remote-exploit.org.

Articolazione di un attacco

Prima di addentrarci nel dettaglio delle operazioni che caratterizzano l'hacking delle reti wireless, proviamo a delineare in modo sintetico quale sia la cronologia di un tipico attacco di questo genere: l'obiettivo è quello di descrivere sia la sequenza temporale sia il tipo di operazioni effettuate.
Occorre premettere che il successo in questo genere di azioni non è assolutamente garantito, in quanto esso dipende sia dall'abilità dell'aggressore sia dal livello di vulnerabilità della rete: un uso errato o inefficace degli strumenti software e/o un livello di protezione particolarmente avanzato nella rete oggetto dell'attacco renderanno certamente vani gli sforzi dell'aggressore.
Nella tabella 3 non è menzionata la fase preliminare comprendente tutte le operazioni di installazione e di verifica dei software che costituiscono la suite aircrack-ng. Le informazioni riportate, estremamente sintetiche, verranno analizzate e approfondite successivamente.

Fase	Software adoperato	Obiettivo da conseguire
1	Airmon-ng	Predisposizione dell'adattatore di rete wireless nella modalità definita monitor
2	Airodump-ng	Cattura del traffico di rete, in particolare di quello relativo agli IV (Initialization Vector)
3	Aireplay-ng	Operazione opzionale da eseguire qualora, attraverso la fase 2, non si siano raccolti sufficienti IV per la successiva fase di decodifica
4	Aircrack-ng	Analisi del file di cattura generato nella fase 1 da airodumpng al fine di individuare la chiave adoperata
5	Strumenti di sistema	Qualora nonostante l'individuazione della chiave non si riesca ad accedere alla rete, è possibile tentare alcune operazioni come la modifica dell'indirizzo IP o MAC; nel caso di segnale debole, si può anche provare a cambiare la posizione della macchina adoperata
6	Strumenti di sistemi	Una volta in possesso delle informazioni è possibile connettersi alla rete attraverso gli strumenti standard offerti dal sistema operativo; se nell'access point è stata inibita la diffusione dell'SSID (Service Set Identifier), è possibile ricavarlo con Aircrack-ng

Tabella 3: articolazione di un attacco

Fase 1 - Utilizzo di airmon-ng

Questo comando, in pratica, è uno script che pone l'adattatore di rete wireless nella modalità monitor, che permette di accedere a tutto il traffico di rete indipendentemente dal fatto che sia diretto o meno verso la nostra macchina.
L'utilizzo preventivo del comando airmon-ng, senza alcun parametro, permette di visualizzare interfaccia, chipset e driver dell'adattatore di rete installato e correttamente riconosciuto dal sistema operativo:

```
> airmon-ng

Interface  Chipset  Driver
eth1       HermesI  orinoco
```

Un successivo utilizzo con il parametro **start** porrà l'adattatore nella modalità monitor:

```
> airmon-ng start eth1

Interface  Chipset  Driver
eth1       HermesI  orinoco (monitor mode enabled)
```

Volendo, è possibile specificare il canale sul quale far operare l'adattatore di rete, attraverso l'aggiunta del numero di canale al termine della riga di comando:

```
> airmon-ng start eth1 5
Interface  Chipset  Driver
eth1       HermesI  orinoco (monitor mode enabled)
```

L'indicazione **monitor mode enabled** al fianco del tipo di driver segnala il successo dell'operazione: a questo punto si è pronti per la fase successiva.

Fase 2 - Utilizzo di airodump-ng

Il software airodump-ng si occupa di catturare i pacchetti relativi al traffico di rete 802.11; i file da esso creati saranno indispensabili per la successiva fase di decodifica delle chiavi WEP mediante l'utilizzo degli IV (Initialization Vector) intercettati.
Ogni pacchetto catturato possiede un proprio IV della lunghezza di tre byte: dopo aver intercettato un numero adeguato di pacchetti, è possibile tentare la decodifica della chiave WEP utilizzata nella rete attraverso l'esecuzione con aircrack-ng di una serie di attacchi statistici KoreK (una serie di attacchi molto efficienti sviluppati da un personaggio soprannominato **KoreK**). Nel successivo esempio è stato scelto **myfile** come prefisso per i file di cattura generati (che avranno, comunque, estensione .ivs), mentre il nome dell'adattatore di rete è quello identificato in precedenza tramite il comando airmon-ng:

```
> airodump-ng –w myfile eth1
```

Airodump creerà due file dal nome myfile.cap (traffico intercettato) e myfile.txt (dati di tipo statistico).
Come impostazione predefinita airodump-ng opera su tutti i canali da 1 a 11, commutando automaticamente in modo da coprire l'intera gamma dei 2,4 GHz: questa impostazione predefinita può essere liberamente modificata dall'utente.
Nella *tabella 4* è possibile osservare le opzioni relative all'utilizzo di airodump-ng.

Opzione	Descrizione
--ivs	Durante l'operazione di cattura del traffico si limita a salvare solo gli IV (Initialization Vector)
--gpsd	Abilita l'utilizzo di un sistema GPS per la registrazione delle coordinate degli access point
--write <nome>	Abilita la registrazione delle informazioni di tipo beacon
--beacons	Abilita la registrazione delle informazioni di tipo beacon
--encrypt <suite>	Filtra gli access point in base al tipo di cifratura utilizzata
--netmask <netmask>	Filtra gli access point in base alla maschera di rete
--bssid <bssid>	Filtra gli access point in base al BSSID
-a	Filtra le macchine client non associate
--channel <channels>	Intercetta solo il traffico relativo al canale indicato
--band <abg>	Specifica la banda dove operare in modo automatico (hop mode)
Cswitch <method>	Modalità con la quale effettuare il cambio di canale automatico (hop mode): 0 = FIFO (predefinita); 1 = round robin; 2 = hop on last

Tabella 4: opzioni relative a airodump-ng

Per una maggiore comodità di utilizzo, è possibile scrivere le opzioni utilizzando la prima lettera del nome preceduta da un solo trattino (short form). Per esempio, al posto di --write è possibile adoperare -w.
Durante il suo utilizzo, airodump-ng visualizza un elenco sia dei dispositivi access point rilevati sia delle macchine client da questi servite (associate e non associate). L'interruzione dell'attività di cattura dei pacchetti avviene mediante l'utilizzo della combinazione di tasti **Ctrl+C**.
Il risultato finale, al termine della fase di cattura, sarà qualcosa di simile:

```
BSSID                PWR  Beacons   #Data  CH  MB  ENC  ESSID
08-00-17-18-12-83     12         11      99  11  22  WEP  Amee

BSSID              STATION            PWR   Packets  ESSID
08-00-17-18-12-83  00:15:11:20:14:2C   23       512  Amee
```

Cerchiamo adesso di descrivere il significato dei campi che compongono l'output del comando.
La prima area (quella in alto) è dedicata alle informazioni relative ai dispositivi access point rilevati, ed è strutturata come descritto nella *tabella 5*.

Campo	Contenuto
BSSID	Indirizzo MAC dell'access point
PWR	Livello del segnale: un numero alto indica la vicinanza all'access point; un valore uguale a -1 indica il mancato supporto di questa funzionalità da parte del driver in uso
Beacons	Numero degli annunci (beacon) inviati dall'access point: esso ne invia circa una decina al secondo
#Data	Numero dei pacchetti catturati inclusi quelli di tipo broadcast: nel caso sia in uso il sistema di protezione WEP, viene rilevato il numero degli IV diversi
CH	Numero del canale, rilevato tramite la lettura dei beacon ricevuti

Campo	Contenuto
MB	Velocità massima che l'access point è in grado di supportare (11 = 802.11b, 22 = 802.11b+, maggiore di 22 = 802.11g)
ENC	Algoritmo di cifratura utilizzato (OPN = in chiaro, WEP? = WEP o WPA, WEP = WEP statico/dinamico, WPA = utilizzo di TKIP o CCMP)
ESSID	Indica il SSID dell'access point. Nel caso l'emissione di questo sia stata disabilitata, il programma tenta di recuperarlo dalle risposte alle richieste di associazione

Tabella 5: output del comando airodump-ng (prima parte)

Nella parte in basso, invece, sono riportate le informazioni relative ai client della rete in esame, vedi *tabella 6*.

Campo	Contenuto
BSSID	Indirizzo fisico MAC dell'access point al quale la macchina è associata
STATION	L'indirizzo fisico MAC address della macchina associata
PWR	Livello del segnale (valgono gli stessi criteri già visti in precedenza)
Packets	Numero dei pacchetti catturati
ESSID	Indica il SSID dell'access point al quale la macchina è associata

Tabella 6: output del comando airodump-ng (seconda parte)

Una volta che sono stati visualizzati tutti gli access point a distanza di rilevamento, è possibile restringere l'operato di airodump-ng verso un solo canale specifico, attraverso l'opzione **channel**. Presupponendo che il canale da selezionare sia il numero 5, scriveremo:

```
> airodump-ng –w myfile –c 5 eth1
```

Riepilogando, il canale adoperato è soltanto il numero 5, l'interfaccia di rete wireless selezionata è **eth1** e, infine, i nomi dei file generati saranno myfile-01.cap/myfile-01.txt, myfile-02.cap/myfile-02.txt e così via (ricordiamo che i file creati da airodump-ng sono due: uno contenente i dati veri e propri, con estensione **.cap**, e uno di tipo statistico, con estensione **.txt**).
Otterremo quindi qualcosa di simile a quanto visto in precedenza, ma con il campo d'azione ristretto a un solo canale:

```
BSSID              PWR  Beacons  #Data  CH  MB  ENC  ESSID
08-00-17-18-12-83   12       11     99   5  22  WEP  Amee

BSSID              STATION           PWR Packets ESSID
08-00-17-18-12-83  00:15:11:20:14:2C  23     512 Amee
```

Dato che il successo della successiva operazione di decodifica del traffico catturato dipende dal numero di IV intercettati e che ciò è fortemente legato al modo in cui la rete sta operando, per evitare lunghe attese (anche di giorni) è talvolta necessario, come vedremo nella prossima fase, mettere in opera degli stratagemmi in grado di forzare l'emissione in rete di questi IV.

Nota
Nell'ambito delle operazioni di wardriving, qualora adoperato insieme a un dispositivo GPS, airodump-ng è in grado di registrare in modo automatico le coordinate relative agli access point intercettati.

Fase 3 - Utilizzo di aireplay-ng

Attraverso l'utilizzo di aireplay-ng si possono inviare in rete dei pacchetti opportunamente realizzati, effettuando quello che in gergo tecnico viene indicato con il termine di **packet injection**.
Abbiamo inizialmente premesso che l'esecuzione di questa fase è subordinata al risultato della fase 2, cioè la fase di raccolta dei dati svolta tramite airodump-ng: quando gli IV raccolti non sono sufficienti per la decodifica della chiave in uso, oppure quando i tempi occorrenti per questa raccolta sono troppo elevati, è possibile tentare di accelerare l'emissione di IV attraverso l'invio in rete (tramite aireplay-ng) di un certo tipo di traffico. Il compito principale di questo software, infatti, è proprio l'invio di pacchetti opportunamente forgiati per agevolare le operazioni di decodifica delle chiavi WEP e WPA-PSK.
Vedremo come sia possibile compiere questa operazione attraverso vari metodi come, per esempio, la deautenticazione forzata di una macchina client in precedenza regolarmente associata o la cattura delle informazioni relative al processo di handshake.

Nota
Per poter effettuare correttamente operazioni di packet injection, molti adattatori di rete wireless necessitano l'applicazione di un'apposita patch; al momento della stesura di questo articolo, il software supportava solo i chipset Prism2, PrismGT (FullMAC), RTL8180, Atheros, RTL8187, ACX1xx, Ralink e Zydas, mentre, non supportava il packet injection su Hermes, Centrino, Marvell, Aironet e Broadcom.

Come già accennato all'inizio, non è possibile effettuare questo genere di operazione sui sistemi della famiglia Microsoft Windows e, inoltre, anche per effettuare solo le operazioni di cattura, occorre installare appositi driver modificati, in quanto quelli standard forniti dai produttori non supportano questa funzione: è possibile trovare questi particolari driver sul sito della **wild packets** all'indirizzo: http://www.wildpackets.com; sempre al momento della stesura di questa parte del articolo, nessun adattatore di rete di tipo USB risultava supportato.
Dalle informazioni che è possibile rilevare sui forum dedicati a queste problematiche, emerge che i chipset che offrono il miglior livello di compatibilità e affidabilità sono l'**Atheros** e il **Ralink**. Pertanto, qualora non si sia già in possesso di un adattatore di rete wireless compatibile, si consiglia di tenere conto di questa indicazione.
Successivamente, verranno illustrati i sei attacchi, numerati da 0 a 5 nella documentazione ufficiale, che è possibile effettuare con aireplay-ng: in realtà, il numero complessivo degli attacchi disponibili è sette, in quanto esiste un cosiddetto **attacco 9** che ha lo scopo di verificare la funzionalità di **packet injection** sulla macchina da adoperare per l'attacco.

Attacco di tipo Deauthentication
Classificato come **attacco numero zero**, il suo scopo è quello di togliere l'associazione esistente a uno o più client precedentemente associati a un access point.
Le ragioni che giustificano un attacco del genere sono diverse, come per esempio:

- l'ottenimento dell'identificatore EDDID del dispositivo access point qualora il broadcast di questo sia stato appositamente inibito (cloaked);
- l'intercettazione del traffico relativo alla procedura di handshake WPA/WPA2 (processo iniziale di dialogo) attraverso la forzatura a un nuovo processo di autenticazione delle macchine già regolarmente autenticate;
- la generazione di traffico del tipo **ARP Request** (in pratica, esso simula uno svuotamento della cache ARP di un client Windows durante la fase di disconnessione dalla rete).

Nota
ARP è l'acronimo di Address Resolution Protocol, protocollo di risoluzione degli indirizzi operante nel livello Internet; esso risolve la corrispondenza tra indirizzi IP e indirizzi fisici MAC all'interno delle reti locali.

L'esecuzione di un attacco di questo genere è subordinata alla presenza di uno o più client wireless correttamente associati all'access point (operazione realizzabile anche artificialmente mediante un attacco **fake authentication**).
Nell'esempio successivo è possibile osservare un tipico utilizzo di questo metodo:

```
> aireplay-ng -0 10 -a [MAC-ACCESS-POINT] -c [MAC-CLIENT] eth1
```

Il primo parametro `(-0)` indica il tipo di attacco (deauthentication), mentre il secondo `(10)` stabilisce il numero di volte che occorre deautenticare la macchina client (impostando questo parametro a zero, il processo continuerà senza mai arrestarsi). Successivamente, deve essere indicato l'indirizzo MAC dell'access point `(-a)` e del client da associare `(-c)` e, per ultimo, il nome dell'interfaccia di rete wireless.
Il risultato che si dovrebbe ottenere è il seguente:

```
08:05:18 Sending DeAuth to station -- STMAC: [MAC-CLIENT]
```

Esso indica l'avvenuto invio all'access point dei pacchetti che forzeranno la deautenticazione del client identificato dall'indirizzo MAC MAC-CLIENT.

Nota
Riferimenti: RFC 826 (Ethernet Address Resolution Protocol: or converting network protocol addresses to 48 bit Ethernet address for transmission on Ethernet hardware).

Attacco di tipo Fake Authentication
Classificato come **attacco numero uno**, permette l'esecuzione di due diversi tipi di autenticazioni WEP, quella denominata **open system** e quella denominata **shared key**.
Esso permette, inoltre, l'associazione della macchina in uso all'access point, consentendo in questo modo l'effettuazione di alcuni tipi di attacco (come, per esempio, quello deauthentication descritto in precedenza) quando non sono presenti in rete altri client associati.
In alcuni casi, a seconda del dispositivo di accesso presente in rete, potrebbe essere necessario reiterare questa finta associazione allo scadere di un certo intervallo temporale.
Questo problema può essere risolto tramite l'utilizzo di una particolare opzione che fissa l'intervallo di tempo dopo il quale deve essere avviato un nuovo processo di associazione:

```
> aireplay -1 20 -e 'SSID' -a [MAC_ACCESS_POINT] -h [MAC_DA_ASSOCIARE]eth1
```

Nell'esempio precedente il primo parametro (-1) indica il tipo di attacco (fake authentication), mentre il secondo stabilisce dopo quanti secondi occorre avviare un nuovo processo di riassociazione (20). Successivamente, occorre indicare il nome della rete wireless (-e), l'indirizzo MAC dell'access point (-a) e del client da associare (-h) e, infine, il nome dell'interfaccia di rete da adoperare.
L'indirizzo MAC del client da associare è quello della macchina che sta effettuando l'attacco e può essere modificato nel modo seguente:

```
> ifconfig eth1 down
> ifconfig eth1 hw ether [MAC_DA_ASSOCIARE]
> ifconfig eth1 up
```

Il risultato, in caso di esito positivo, sarà qualcosa di simile:

```
10:18:02 Sending Authentication Request
10:18:02 Authentication successful
10:18:02 Sending Association Request
10:18:03 Association successful :-)
```

Piuttosto che utilizzare un indirizzo MAC inventato è preferibile adoperarne uno realmente esistente sulla rete in esame, per poi provvedere alla sostituzione non appena se ne presenti la possibilità.

Nota
Questa finta autenticazione, a differenza di una regolare, non genera alcun traffico di tipo ARP.

Attacco di tipo interactive packet replay
Classificato come **attacco numero due**, consente di selezionare quali pacchetti inviare in risposta. Questo può essere fatto in due differenti modi o, per meglio dire, da due differenti fonti: è possibile utilizzare il traffico reale proveniente dall'adattatore di rete wireless, oppure utilizzare un apposito file di tipo **pcap**.
Quest'ultimo è un file realizzato nel formato standard **Packet CAPtured** adoperato da molti software di sniffing sia commerciali sia **open source**, come per esempio **tcpdump**.
Essi, attraverso l'utilizzo di una particolare libreria denominata libcap, sono in grado di catturare il traffico di rete operando in modalità promiscua; il traffico catturato può essere salvato all'interno di un file di tipo **pcap** e questo rende possibile il differimento nel tempo di alcune operazioni.
Riassumendo, lo scopo di questo attacco è quello di riciclare un certo tipo di traffico, catturato o disponibile attraverso un file **pcap**, al fine di raggiungere un determinato obiettivo.
Non si possono riutilizzare tutti i tipi di pacchetti, ma solo quelli che possiedono alcune specifiche caratteristiche tali da indurre l'access point a produrre nuovi IV.
Un primo esempio circa l'uso di questo comando si svolge nell'ambito di una rete wireless dove esiste un client regolarmente associato a un access point, un client di cui conosciamo l'indirizzo fisico MAC:

```
> aireplay-ng -2 -b [MAC_AP] -d FF:FF:FF:FF:FF:FF -t 1 eth1
```

Il primo parametro (-2) indica il tipo di attacco (interactive packet replay), il secondo (b) limita la cattura ai soli pacchetti provenienti dall'access point avente l'indirizzo MAC indicato, il terzo (-d) stabilisce quali sono i pacchetti da catturare (in questo caso l'indirizzo MAC `FF:FF:FF:FF:FF:FF` indica i pacchetti di tipo broadcast) e infine è indicata l'interfaccia di rete.
A questo punto verrà chiesta all'utente una conferma circa l'utilizzo dei pacchetti catturati e, in seguito a questa, essi verranno immessi in rete e, contemporaneamente, verrà creato un file con estensione cap contenente il traffico in questione: il successivo utilizzo di airodump-ng permetterà la cattura delle risposte a questi pacchetti.
Una variante del sistema appena visto permette di giungere allo stesso risultato:

```
aireplay-ng -2 -b [MAC_AP] -t 1 -c FF:FF:FF:FF:FF:FF -p 0841 eth1
```

Le varianti, in questo caso, sono il parametro -t, che limita l'operazione ai soli pacchetti aventi il flag to **distribution system** attivo, e il parametro p, dove il numero 0841 imposta il **frame control field** (esso è formato dall'unione di undici sottocampi) in accordo con quello utilizzato dai client wireless.
Il numero degli IV al secondo ottenibile con questo metodo dipende dalle dimensioni dei pacchetti selezionati: minori sono le dimensioni di questi, maggiore è la frequenza di generazione degli IV.

Fonti: tcpdump e libpcap library, http://www.tcpdump.org.

Attacco di tipo ARP request replay
Classificato come **attacco numero tre**, rappresenta uno degli attacchi più efficaci per la generazione di nuovi IV.
Esso intercetta il traffico di tipo ARP e, successivamente, lo rinvia verso l'access point allo scopo di costringere quest'ultimo a replicare attraverso l'invio di un nuovo IV; la reiterazione continua di questo processo procura una generazione massiccia di nuovi IV.

Nota
Al fine di effettuare dei test, è possibile generare pacchetti di tipo ARP semplicemente effettuando un ping verso un indirizzo inesistente della nostra rete.

Nel prossimo esempio è possibile osservare la sintassi relativa a questo tipo di attacco:

```
aireplay-ng -3 -b [MAC_AP] -h [MAC_CLIENT] eth1
```

Il primo parametro (-3) indica il tipo di attacco (ARP request replay), mentre il secondo (-b) ed il terzo (-h) sono, rispettivamente, l'indirizzo MAC dell'access point e quello di un client associato (anche attraverso una **fake authentication**). L'ultimo parametro, come al solito, indica l'interfaccia di rete.

Attacco di tipo KoreK chopchop
Classificato come **attacco numero quattro**, sebbene si riveli inefficace con la maggior parte degli access point, può essere eseguito per tentare di decifrare un pacchetto di dati codificato tramite una chiave WEP statica o dinamica. Esso non è in grado di individuare la chiave usata per la crittografia dei dati, ma permette esclusivamente la visione in chiaro dei dati stessi.
Come accennato in precedenza, esso basa il suo funzionamento su una vecchia vulnerabilità non più presente nei recenti access point.
Per poter operare questo attacco, ovviamente, occorre entrare in possesso di almeno un pacchetto di dati codificato tramite WEP.
L'utilizzo tipico di questo attacco è il seguente:

```
> aireplay-ng -4 -h [MAC_CLIENT] -b [AP_CLIENT] eth1
```

Il primo parametro (-4) indica il tipo di attacco (KoreK chopchop), mentre il secondo (-h) e il terzo (-b) sono rispettivamente l'indirizzo MAC di un client associato (anche attraverso una fake authentication) e l'indirizzo MAC dell'access point. L'ultimo para-metro è l'interfaccia di rete.
Dopo la solita conferma circa l'utilizzo dei pacchetti, in caso di successo dell'operazione verrà mostrata una lunga serie di dati terminante con le seguenti righe:

```
The AP appears to drop packets shorter than 35 bytes.
Enabling standard workaround: ARP header re-creation.

Saving plaintext in replay.cap
Saving keystream in replay.xor

Completed in 37s (1.18 bytes/s)
```

Il file con estensione **xor** potrà essere adoperato con il software packetforge-ng, mentre il file in chiaro, avente estensione **.cap**, potrà essere letto attraverso diversi software come, per esempio, tcpdump.

Attacco di tipo fragmentation
Quest'ultima modalità, classificata come attacco numero cinque, riesce a identificare il cosiddetto PRGA (Pseudo Random Generation Algorithm), senza però identificare la chiave WEP in uso: il PRGA potrà poi essere utilizzato per la generazione di pacchetti attraverso packetforge-ng.
In questo caso il presupposto indispensabile è la presenza di un pacchetto inviato dal dispositivo access point.
Il suo utilizzo è il seguente:

```
aireplay-ng -5 -b [MAC_AP] -h [MAC_SOURCE] eth1
```

Il primo parametro (-5) indica il tipo di attacco (fragmentation), mentre il secondo (-b) e il terzo (c) sono rispettivamente l'indirizzo MAC dell'access point e quello da scrivere nel campo source dei pacchetti inviati; l'ultimo parametro è sempre l'interfaccia di rete. In questo comando è possibile avvalersi di diverse opzioni di filtraggio e replica, riassunte nelle *tabelle 7 e 8*.

Opzioni di filtro	Descrizione
b bssid	Indirizzo MAC dell'access point
-d dmac	Indirizzo MAC di destinazione
-s smac	Indirizzo MAC di origine
-m len	Lunghezza minima dei pacchetti
-n len	Lunghezza massima dei pacchetti
-u type	Tipo di campo Frame Control
-v subt	Tipo di sottocampo Frame Control
-t tods	Frame Control, To DS bit
f fromds	Frame Control, From DS bit
-w iswep	Frame Control, WEP bit

Tabella 7: aireplay - opzioni di filtro

Opzioni di replica	Descrizione
-k IP	Indirizzo IP di destinazione dei frammenti (quello predefinito è 255.255.255.255)
-l IP	ndirizzo IP di origine dei frammenti (quello predefinito è 255.255.255.255)

Tabella 8: aireplay - opzioni di replica

Nel caso l'operazione abbia successo si otterrà un file contenente le informazioni PRGA, informazioni che sarà possibile adoperare negli attacchi eseguiti tramite il software packetforge-ng.

Attacco di tipo injection test
Classificato come **attacco numero nove**, esso è utilizzato esclusivamente per l'effettuazione di test inerenti alle funzionalità di **packet injection**.
Il test principale verifica sia la capacità di invio dei pacchetti sia la corretta ricezione delle relative risposte e, sulla base dei dati ottenuti, fornisce una stima circa la bontà della connessione.
I test possono anche essere effettuati utilizzando uno specifico access point: in questo caso, occorrerà indicare nome e indirizzo fisico MAC del dispositivo desiderato; questo tipo di operazione è utile nel caso esista un solo access point con propagazione del SSID disabilitata.
Nell'esempio successivo verrà eseguito uno di questi test di base al fine di verificare l'effettiva capacità del nostro adattatore di rete di effettuare **packet injection**:

```
> aireplay-ng -9 eth1
```

Il primo parametro (-9) seleziona la modalità di test e il secondo (eth1) l'adattatore di rete da verificare.
Una volta eseguito il comando, otterremo un risultato del genere:

```
10:00:31 eth1 channel: 9
10:00:31 Trying broadcast probe requests...
10:00:31 Injection is working!
10:00:32 Found 3 APs
10:00:32 Trying directed probe requests...
10:00:32 00:01:5f:5a:C1:2b - channel: 5 - 'NET1'
10:00:38 0/30: 0%
10:00:38 00:02:5f:a8:35:a2 - channel: 6 - 'NET2'
10:00:34 0/30: 0%
10:00:34 00:03:2C:6a:4b:c1 - channel: 6 - 'NET3'
10:00:35 Ping (min/avg/max): 1.733ms/2.121ms/4.112ms
10:00:35 27/30: 90%
```

Analizziamo nel dettaglio le informazioni riportate in questo output:

- le prime righe indicano l'interfaccia di rete adoperata e il canale in uso;
- il messaggio **Injection is working!** segnala la capacità dell'adattatore di effettuare **packet injection**;
- l'indicazione **Found 3 APs** segnala la presenza di tre access point attivi;
- le righe successive riporteranno, per ognuno di questi dispositivi, l'indirizzo fisico MAC, il canale adoperato e il nome.

Possiamo osservare che l'access point denominato **NET3** è l'unico con il quale è stato possibile comunicare: è possibile accorgersi di questo dalla riga relativa all'esito dell'operazione di ping che riporta i valori minimi, medi e massimi rilevati (1,733 ms, 2,121 ms e 4,112 ms).

Fase 4 - Utilizzo di Aircrack-ng

Aircrack-ng è un software utilizzato per la decodifica delle chiavi crittografiche statiche di tipo WEP e WPA/WPA2-PSK.
Sulla base del traffico catturato da airodump-ng, esso è in grado di tentare l'individuazione della chiave WEP adoperata attraverso differenti approcci:

- il primo di questi, denominato PTW (acronimo composto dalle iniziali dei nomi **Pyshkin**, **Tews** e **Weinmann**), ha la caratteristica di richiedere l'intercettazione di un esiguo numero di pacchetti;
- il secondo, denominato **FMS/KoreK**, cerca di raggiungere il risultato attraverso la combinazione di metodi basati sulla statistica con altri basati su tentativi reiterati (brute force);
- il terzo approccio contempla l'uso di un file dizionario per la decifrazione della chiave WEP (quest'ultimo è l'unico approccio possibile per quel che concerne le chiavi WPA/WPA2 di tipo **pre-shared**).

Prima di iniziare a vedere qualche esempio d'uso di aircrack-ng, soffermiamoci un attimo per illustrare, nella *tabella 9*, tutte le possibili opzioni di questo potente software.

Opzione	Descrizione
a amode	Modalità di attacco (1 = WEP statico, 2 = WPA-PSK)
-e essid	ndirizzo IP di origine dei frammenti (quello predefinito è 255.255.255.255)
-b bssid	Questa opzione è indispensabile per decodificare WPA-PSK quando l'ESSID è nascosto; il suo uso abilita l'utilizzo di tutti gli IV provenienti da reti aventi lo stesso ESSID
-p nbcpu	Nel caso di macchine multiprocessore, imposta il numero di CPU da utilizzare
-q none	Opera in modalità silenziosa, mostrando l'output solo quando identifica la chiave (o fallisce)
-c none	Nell'operazione di decodifica WEP utilizza solo chiavi alfanumeriche con caratteri compresi tra i valori esadecimali 0x20 e 0x7F
-t none	Nell'operazione di decodifica WEP utilizza solo caratteri esadecimali codificati in binario
-d start	Nell'operazione di decodifica WEP imposta in esadecimale l'inizio della chiave WEP a fini di debug (ricerca errori)
-m maddr	Nell'operazione di decodifica WEP utilizza l'indirizzo fisico MAC per filtrare i pacchetti dati WEP, oppure permette di utilizzare -m ff:ff:ff:ff: ff:ff per utilizzare tutti gli IV a prescindere dalla rete
-n nbits	Nell'operazione di decodifica WEP permette di specificare la lunghezza della chiave; il valore predefinito è 128 (64 = WEP a 40 bit, 128 = WEP a 104 bit ecc.)
-i index	Nell'operazione di decodifica WEP utilizza solo gli IV che possiedono per la chiave l'indice specificato da 1 a 4 (per impostazione predefinita, il comando non tiene conto di questo indice)
-f fudge	Nell'operazione di decodifica WEP utilizza 2 come valore predefinito per il WEP a 104 bit e 5 per il WEP a 40 bit; valori più alti aumentano le possibilità di successo, ma anche il tempo di esecuzione
-k korek	Nell'operazione di decodifica WEP sono disponibili 17 attacchi statistici di KoreK; se uno di questi crea molti falsi positivi, nonostante l'uso di molti IV, è possibile adoperare da -k 1 a -k 17 per escluderlo
-x none	Nell'operazione di decodifica WEP utilizza la decodifica basata su brute force solo per gli ultimi due byte della chiave
-y none	Nell'operazione di decodifica WEP permette l'utilizzo di un tipo di attacco bruteforce particolare quando l'operazione è precedentemente fallita nonostante l'uso di oltre un milione di IV
-w words	Nell'operazione di decodifica WEP indica il percorso del file dizionario da utilizzare

Tabella 9: opzioni relative a aircrack-ng

La sintassi generica da utilizzare è la seguente:

```
> aircrack-ng [opzioni] <file catturato>
```

Pur esistendo statistiche abbastanza confortanti circa la possibilità di identificare una chiave di tipo WEP, queste non forniscono alcuna certezza che essa possa sempre essere decodificata o, quantomeno, che questa decodifica possa essere compiuta nei tempi medi staticamente individuati.

Nota
L'opzione k di aircrack-ng prende il nome KoreK da colui che ha implementato la serie di 17 attacchi statistici.

In merito al numero degli IV necessari per questa decodifica, sulla base dei dati oggi disponibili, è possibile dedurre le informazioni riportate in *tabella 10*.

Lunghezza della chiave in bit	nitialization Vector (IV) necessari per la decodifica
40	Da 250.000 a 300.000
104	Da 1.000.000 a 2.000.000

Tabella 10: Initialization Vector necessari per la decodifica

Dato che l'unica informazione che non è possibile dedurre dall'intercettazione del traffico è proprio la lunghezza della chiave, è consigliabile presupporre inizialmente l'uso di una chiave da 40 bit. Quindi, una volta raccolti circa 250.000 IV, adoperare **aircrack** per tentare di estrarre la chiave adoperata (opzione –n 64); nel caso l'operazione non dovesse andare a buon fine, si ripeterà l'operazione con un milione (e poi, eventualmente, con due milioni) di IV utilizzando aircrack per la decodifica di chiavi a 104 bit (senza l'opzione –n 64).
Nel prossimo esempio è possibile osservare le operazioni da compiere per cercare di decodificare un file precedentemente creato da airodump-ng, denominato **mywepnet.ivs**, relativo al traffico di una rete protetta tramite WEP:

```
> aircrack-ng mywepnet.ivs
```

La prima schermata di output che otterremo sarà la seguente:

```
Opening mywepnet.ivs
Read 462022 packets.

#  BSSID              ESSID  Encryption

1  00:01:02:a1:b2:c3           WEP (567022 IVs)

Choosing first network as target.
```

Dato che il traffico sul file è riferito a una sola rete, la selezione verrà effettuata in modo automatico dal programma (Choosing first network as target); in caso contrario, occorrerà specificare manualmente la rete sulla quale operare.

La *figura 1* mostra la schermata che si ottiene quando una chiave WEP viene identificata con successo. Al fine di velocizzare le operazioni e operare in modo più comodo, è possibile utilizzare due console di comandi distinte: una per l'esecuzione del comando airodump-ng e una per l'esecuzione di aircrack-ng. Questo modo di operare consentirà un agevole aggiornamento di aircrack-ng ogniqualvolta siano disponibili nuovi IV, senza la necessità di dover, volta per volta, specificare i file con estensione .cap o .ivs ai quali fare riferimento.

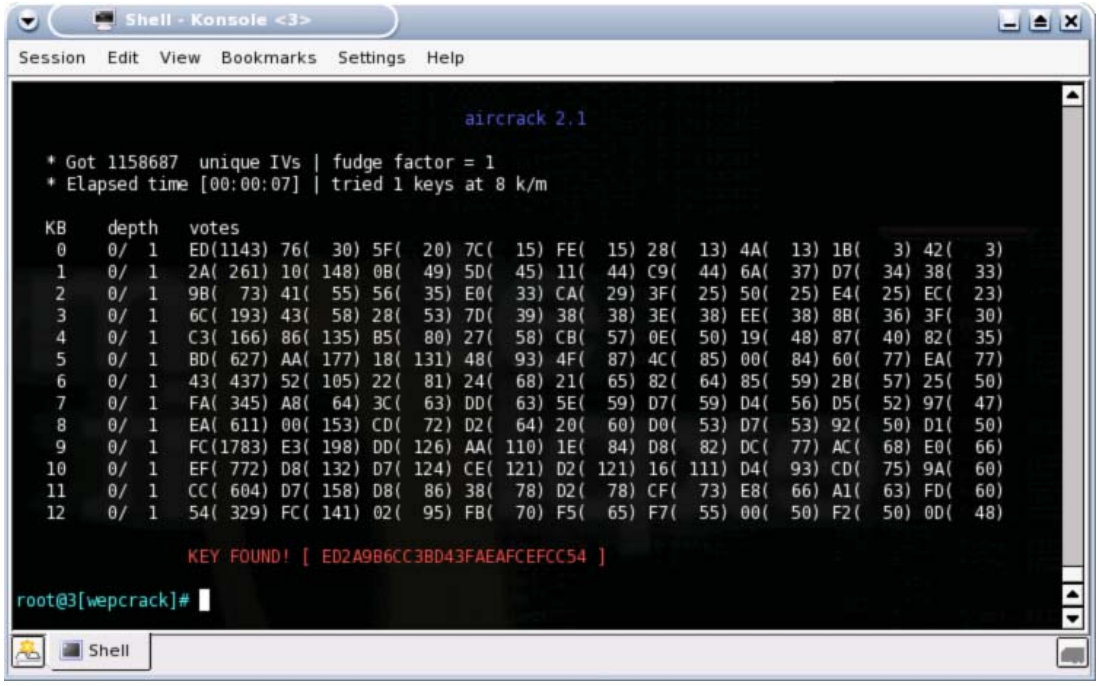

Figura 1: identificazione di una chiave WEP

Nota
Attraverso il parametro -p è possibile far operare aircrack in modalità multiprocessore, in modo da sfruttare le potenzialità delle CPU multi-core.

Fase 5 - Spoofing dell'indirizzo

Qualora, nonostante l'individuazione di una chiave valida, non si riesca in alcun modo ad accedere alla rete, è possibile che sull'access point di questa sia stato abilitato il filtro MAC (che consente l'acceso alla rete solo alle macchine che possiedono un determinato indirizzo fisico), oppure che siano state attivate regole di firewalling per limitare l'accesso a un determinato numero di indirizzi IP.
La soluzione in questi casi è una sola: attendere che una delle macchine identificate tramite airodump. ng sia inattiva e, quindi, impersonarla effettuando quello che viene definito spoofing.
Gli strumenti per effettuare questa operazione sono già disponibili nel sistema operativo ma, nel caso non lo fossero (almeno per quel che concerne la modifica dell'indirizzo MAC), è possibile utilizzare uno dei tanti software gratuiti disponibili su Internet.
Nel caso dei sistemi Microsoft Windows, per modificare l'indirizzo IP è sufficiente operare sulla finestra di configurazione della connessione di rete wireless, mentre per l'indirizzo MAC occorre operare nelle opzioni avanzate relative all'adattatore di rete utilizzato: vi si accede attraverso un apposito pulsante posto nella parte alta della stessa finestra di opzioni citata in precedenza.
Per i sistemi Linux (presupponendo che eth1 sia l'interfaccia di rete wireless) è possibile impostare l'indirizzo IP attraverso il seguente comando:

> ifconfig eth1 192.168.0.1 netmask 255.255.255.0

Per quanto concerne la configurazione dell'indirizzo fisico MAC (presupponendo che esso sia a1:b2:c3:d4:e5:f6), il comando da eseguire è:

> ifconfig eth1 down hw ether a1:b2:c3:d4:e5:f6
> ifconfig eth1 up

Invece di operare dalla linea di comando (che in questo ambiente rappresenta il mezzo più efficiente), se lo si desidera è possibile avvalersi degli appositi tool grafici di configurazione disponibili sul sistema.

Fase 6 - Accesso alla rete

Una volta identificata e testata la chiave di crittografia utilizzata nell'ambito della rete da violare, è possibile accedevi in modo molto semplice: in ambiente Microsoft Windows, utilizzando le funzionalità per le reti senza fili denominate **Zero Configuration** (servizio di Microsoft Windows che permette la configurazione automatica degli adattatori di rete wireless), è sufficiente scegliere la rete e indicare al chiave da adoperare; sulle piattaforme Linux, invece, il metodo più semplice consiste nell'eseguire queste istruzioni da una console di comandi:

```
> iwconfig eth1 mode managed key [KEY]
> dhcpcd eth1
```

Il comando **iwconfig**, simile a ifconfig, viene adoperato per impostare i parametri relativi agli adattatori di rete wireless o, semplicemente, per mostrare questi parametri
o altri dati di tipo statistico: in questo caso è adoperato per utilizzare la chiave identificata in precedenza (KEY) con l'adattatore di rete wireless (eth1) posto in modalità **Infrastructure** (modo managed); il successivo comando **dhcpcd eth1** forza l'acquisizione dei parametri relativi alla rete tramite il protocollo DHCP.
Un successivo utilizzo del comando **ifconfig eth1** mostrerà l'avvenuta configurazione dell'adattatore di rete e i parametri a esso associati: l'utilizzo di un qualsiasi servizio di rete verificherà in modo definitivo la funzionalità della connessione conquistata. Nel caso occorra specificare un indirizzo IP ben preciso, magari perché sull'access point non è attivo un server DHCP, oppure, perché è indispensabile assumere l'indirizzo IP di una precisa macchina della rete (spoofing), invece del comando dhcpcd eth1 possiamo utilizzare ifconfig con la sintassi già vista in precedenza:

```
ifconfig eth1 192.168.0.1 netmask 255.255.255.0
```

Questo configurerà la macchina con l'indirizzo IP e la Subnet Mask specificati.

Verifica della chiave con Airdecap-ng

Per verificare l'effettiva identificazione di una chiave valida non è sufficiente effettuare una connessione, in quanto occorre assicurarsi che la chiave sia effettivamente capace di decodificare il traffico della rete in esame: per effettuare questo controllo è possibile ricorrere al comando airdecap, sottoponendogli in ingresso un file codificato catturato in precedenza.
La sintassi per il corretto utilizzo di airdecap può essere visualizzata da riga di comando con il seguente risultato:

```
usage: airdecap [options] <pcap file>
-l : don't remove the 802.11 header
-b bssid : access point MAC address filter
-k pmk : WPA Pairwise Master Key in hex
-e essid : target network ascii identifier
-p pass : target network WPA passphrase
-w key : target network WEP key in hex
```

Per esempio, utilizzando una chiave WEP precedentemente identificata (22b3e117011 319cc25a67e1919), è possibile testarne l'efficacia verificando la sua capacità di decodificare correttamente il file wep-captured.cap:

```
> airdecap -w 22b3e117011319cc25a67e1919 wep-captured.cap
```

Utilizzo di Packetforge-ng

Questo software permette di inviare in rete dei pacchetti cifrati opportunamente realizzati: è possibile generare pacchetti di tipo diverso come, per esempio, quelli UDP, ICMP, ARP ecc.
Uno degli scopi per cui questo software è comunemente adoperato è la generazione di un certo genere di traffico ARP (ARP request).
La realizzazione di traffico cifrato è subordinata al possesso di un file PRGA (Pseudo Random Generation Algorithm), in quanto solo in questo modo è possibile criptare i pacchetti in uscita. Abbiamo visto in precedenza che questo file può essere ottenuto, per esempio, mediante un attacco di tipo **fragmentation** o KoreK chopchop con aireplay-ng.
Nelle *tabelle da 11 a 13* sono indicate le opzioni che è possibile adoperare per la creazione dei pacchetti, per il tipo di dati in ingresso e per la selezione del traffico da generare.

Opzioni	Descrizione
-p <fctrl>	Specifica, in formato esadecimale, il Frame Control Word
-a <bssid>	Specifica l'indirizzo MAC dell'access point
-c <dmac>	Specifica l'indirizzo MAC di destinazione
-h <smac>	Specifica l'indirizzo MAC di origine
-j	Attiva il bit FromDS
-o	Disabilita il bit ToDS
-e	Disabilita la codifica WEP
-k<ip[:port]>	Specifica l'indirizzo IP e la porta di destinazione
-l <ip[:port]>	Specifica l'indirizzo IP e la porta di origine
-t ttl	Configura il parametro time to live
-w <file>	Specifica il file pcap sul quale indirizzare il traffico

Tabella 11: opzioni di creazione relative a packetforge-ng

Opzioni	Descrizione
-r <file>	Specifica il file contenente il traffico
-y <file>	Specifica il file PRGA da leggere

Tabella 12: opzioni di dati relative ad packetforge-ng

Tipo di traffico	Descrizione
–arp	Genera pacchetti di tipo ARP (-0)
–udp	Genera pacchetti di tipo UDP (-1)
–icmp	Genera pacchetti di tipo ICMP (-2)
–null	Genera pacchetti di tipo NULL (-3)
–custom	Genera pacchetti di tipo arbitrario (-9)

Tabella 13: opzioni di traffico relative ad packetforge-ng

Un tipico esempio dell'utilizzo di questo software al fine di creare uno specifico traffico di tipo ARP **request** è il seguente (si presuppone il possesso di un file PRGA denominato a.xor):

```
packetforge-ng -0 -a [M1] -h [M2] -k 10.0.0.2 -l 10.0.0.1 -y a.xor -w out
```

Il primo parametro `(0)` seleziona il traffico di tipo ARP; il secondo `(M1)` e il terzo `(M2)` sono, rispettivamente, l'indirizzo MAC dell'access point e l'indirizzo MAC di provenienza dei pacchetti (scelto arbitrariamente); il quarto parametro `(10.0.0.2)` rappresenta l'indirizzo di destinazione corrispondente all'interrogazione ARP iniziale **Who has this IP**, mentre, il quinto parametro `(10.0.0.1)` è l'indirizzo di origine corrispondente alla risposta ARP **Tell this IP**; gli ultimi due parametri indicano il file contenente i dati PRGA (a.xor) e quello di output (out).

Utilizzo di Airtun-ng

Questo software, operante esclusivamente sulle piattaforme Linux, permette di creare sulla macchina un'interfaccia virtuale alla quale verrà indirizzato tutto il traffico wireless. Le opzioni, indispensabili e facoltative, relative a questo software, sono riportate nelle *tabelle 14 e 15*.

Opzioni	Descrizione
-x nbpps	Massimo numero di pacchetti per secondo (opzionale)
-a bssid	Imposta l'indirizzo MAC dell'access point (obbligatorio)
-i iface	Effettua la cattura dei pacchetti dall'interfaccia specificata (opzionale)
-y file	Legge i dati PRGA dal file indicato (opzionale)
-w wepkey	Chiave WEP da usare per la codifica dei pacchetti (opzionale)
-t tods	Destinazione dei pacchetti 1 = AP, 0 = client (opzionale, default = 0)
-r file	Legge i pacchetti dal file pcap indicato (opzionale)

Tabella 14: opzioni generiche relative ad airtun-ng

Per quanto concerne le opzioni -i e -y, almeno una di queste deve essere adoperata.

Opzioni	Descrizione
- -repeat	Attiva la modalità ripetizione (è anche possibile adoperare –f)
- -bssid <mac>	Identificativo BSSID da ripetere (è anche possibile adoperare –d)
- -netmask <mask>	Netmask per il filtro BSSID (è anche possibile adoperare –m)

Tabella 15: opzioni di risposta relative ad airtun-ng

La sintassi generica con la quale usare airtun-ng è la seguente:

```
> airtun-ng <opzioni> <interfaccia di risposta>
```

Gli utilizzi possibili dell'interfaccia virtuale realizzata da airtun-ng sono sostanzialmente due: controllo e creazione di traffico arbitrario.

Nota
Se non si utilizza l'opzione -t, come impostazione predefinita, airtun-ng invierà i pacchetti verso i soli client wireless; se si desidera dirigere il traffico verso un access point o una rete di tipo wired, occorrerà adoperare l'opzione -t 1.

Il controllo è tipicamente indirizzato ai dispositivi di tipo WIDS (Wireless Intrusion Detection System), utilizzati per il rilevamento delle operazioni illecite sulla rete.
L'operazione appena descritta può essere effettuata nel seguente modo:

```
> airtun-ng -a [MAC-AP] -w [KEY] eth1
```

Il primo parametro (MAC-AP) è l'indirizzo MAC del dispositivo access point da monitorare, mentre il secondo (KEY) è la chiave di crittografia utilizzata e il terzo (eth1) indica l'interfaccia di rete wireless che sta operando in modalità **monitor**.
Il risultato che si otterrà, in caso di successo dell'operazione, è il seguente:

```
created tap interface at0
WEP encryption specified. Sending and receiving frames through eth1.
FromDS bit set in all frames.
```

Esso ci informa circa la creazione di un'interfaccia virtuale denominata at0, interfaccia sulla quale sarà presente una copia del traffico dell'interfaccia (reale) eth1.
A questo punto, è possibile operare con questa nuova interfaccia nel modo consueto e scrivere, quindi:

```
> ifconfig at0 up
```

L'interfaccia è adesso liberamente utilizzabile da tutti i programmi, compresi appunto gli IDS. Il secondo possibile utilizzo è, invece, quello relativo all'immissione in rete di pacchetti arbitrari. Esso si realizza specificando, nel precedente comando, un indirizzo IP:

```
> ifconfig at0 192.168.0.10 netmask 255.255.255.0 up
```

Questo permette di utilizzare qualsiasi software per interagire con la rete wireless. Sul sito del produttore sono comunque illustrati altri possibili utilizzi di airtun-ng.

Mappare la rete su Google Earth con KNSGEM

Da qualche tempo è disponibile sul mercato un software, denominato **KNSGEM**, in grado di utilizzare i file di log prodotti da software come **NetStumbler** o **Kismet** (descritti in seguito) per produrre mappe a colori relative alle aree di copertura wireless individuate durante le operazioni di **wardriving**.
Il software **KNSGEM**, definito nel sito ufficiale come una sorta di convertitore in grado di mappare in **Google Earth** le reti wireless individuate tramite l'utilizzo dei software per lo sniffing, si rivela utile, oltre che nelle attività di **wardriving**, anche in quei casi dove occorre verificare la reale copertura della nostra rete rispetto al territorio, oppure, per evidenziare quali sono le aree non raggiunte dal segnale (zone d'ombra) o, ancora, per identificare le zone di intersezione tra la nostra rete e altre reti operanti con lo stesso canale; sono davvero molti gli usi possibili di questo software, sia in ambito di attacco sia, ancora più importante, in ambito di difesa e configurazione.

Figura 2: mappatura delle reti in Google Earth

Nella precedente *figura 2* è possibile osservare il risultato finale della mappatura effettuata su **Google Earth** tramite l'ausilio di questo software: le aree dove sono state individuate reti wireless attive sono marcate con colori diversi a seconda se queste siano o meno protette: (colore rosso = rete insicura, colore verde = rete sicura); la selezione con il mouse di una di queste aree permetterà di accedere a un'ulteriore finestra di dettaglio.

Nota
Google Earth è un software in grado di generare immagini virtuali della superficie terrestre, immagini basate su rilievi satellitari e successivamente arricchite da strade, edifici, luoghi di interesse e tantissimi altri dettagli. Esso è distribuito gratuitamente da Google, sebbene esistano versioni a pagamento che presentano particolari caratteristiche avanzate; attualmente Google Earth supporta le piattaforme Linux, Mac OS X e Microsoft Windows.

L'installazione del software in ambiente Microsoft Windows non presenta alcuna difficoltà, in quanto esso è distribuito tramite un file eseguibile che, se non si alterano le impostazioni predefinite, installa il programma all'interno della cartella **C:\knsgem**: durante il processo di installazione verrà richiesto il percorso relativo al **Borland Database Engine** (necessario per il funzionamento del software); anche in questo caso, è sufficiente confermare il percorso predefinito. Dopo aver installato KNSGEM è necessario installare anche il software **Google Earth**, prelevabile all'indirizzo: http://earth.google. com/download-earth.html.
Una volta terminate le procedure di installazione, prima di eseguire KNSGEM è indispensabile copiare all'interno della cartella principale del programma C:\Knsgem (se non sono state modificate le impostazioni predefinite) i file generati da **NetStumbler** (aventi estensione **.ns1**) o da **Kismet** (con estensioni **.csv**, **.xml** e **.gps**).
Una volta eseguito, KNSGEM presenterà a video, vedi *figura 3*, una finestra di dialogo relativa alle fasi di elaborazione dei file in ingresso (**.ns1** o **.csv**, **.xml** e **.gps**) e, successivamente, porrà il risultato in un'apposita cartella (**C:\knsgem\KML**): sarà adesso sufficiente eseguire il file **Knsgem_Master.kml** per avviare **Google Earth** e visualizzare al suo interno i risultati.

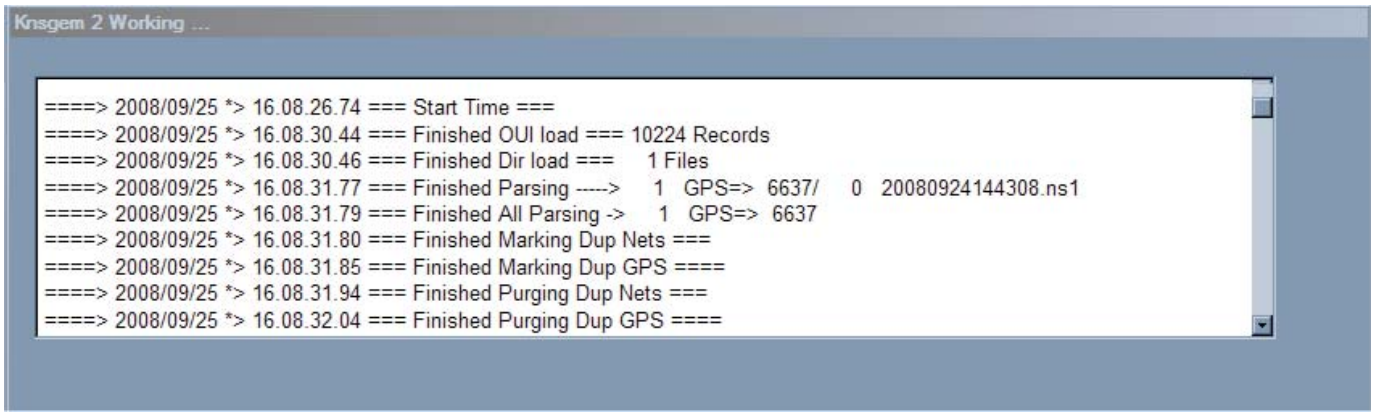

Figura 3: procedura di importazione all'avvio di un file di tipo .ns1

Il software non dispone di un'interfaccia grafica di configurazione, quindi le possibili opzioni devono necessariamente essere configurate tramite la modifica di un file denominato **knsgem.cfg**.
Le configurazioni che è possibile compiere riguardano principalmente:

- i colori di riempimento e dei bordi delle aree evidenziate e delle indicazioni relative al canale e al tipo di protezione (per queste ultime due indicazioni è possibile scambiare i colori);
- le etichette dei SSID o dei BSSID;
- alcuni aggiustamenti relativi al tracciamento;
- il raggio massimo, il tipo di icone e le regolazioni relative al tempo GMT.

Fonti: sito ufficiale KNSGEM, http://www.rjpi.com/knsgem.htm;
sito ufficiale Google Earth, http://earth.google.it.

Rivelatori portatili di reti wireless

Molto usati sia nell'ambito delle operazioni di troubleshooting sia per coadiuvare le operazioni di hacking, sono i dispositivi di rilevazione delle reti wireless, denominati solitamente **Wi-Fi finder**: questi piccoli apparati sono in grado di identificare la presenza di una rete wireless (e non solo) senza la necessità di dover utilizzare un elaboratore.
Mediante il loro utilizzo gli amministratori/utenti sono in grado di stimare la portata degli access point attivi sulla loro rete e allo stesso tempo possono identificare eventuali sovrapposizioni di access point estranei.
Con un Wi-Fi finder un malintenzionato è in grado di mappare grossolanamente un'area che, in caso di riscontro positivo, verrà successivamente passata al setaccio attraverso i canonici strumenti di hacking.
In figura 4 è mostrato uno dei tanti rilevatori reperibili in commercio. Di dimensioni tanto contenute da poter essere usato come un normale portachiavi, esso è in grado di rilevare rapidamente la presenza di una rete Wi-Fi e non solo; infatti, l'intervallo di frequenza nel quale opera (similmente ad altri analoghi rivelatori) è quello compreso tra 1 MHz e 6 GHz, riuscendo in questo modo a rilevare anche altre apparecchiature operanti nel suo raggio di azione come, per esempio, le telecamere di sorveglianza connesse in modalità wireless e diversi tipi di microspie.
A seconda delle funzionalità offerte, il prezzo di questo genere di dispositivi oscilla tra qualche decina di euro e un centinaio di euro.

Figura 4: rivelatore portatile di reti Wi-Fi

Conclusioni

In questo articolo vi abbiamo mostrato i possibili attacchi che è possibile effettuare su una rete wireless allo scopo di mostrarvi i rischi che si corrono se non si effettuano delle corrette configurazioni.
Se volete rimanere sempre aggiornati sui nuovi articoli in uscita, abbonatevi gratuitamente alla nostra newsletter all'indirizzo http://www.comefarea.it/newsletter/ o, se utilizzate Windows Live Messenger, abbonatevi ai nostri Windows Live Alerts all'indirizzo http://www.comefarea.it/abbonamenti.php.

Il libro

Sicurezza wireless e mobile
Soluzioni basate sulle comunicazioni senza filo sono oggi sempre più spesso adottate da coloro che desiderano creare o espandere una rete informatica e, inoltre, rappresentano una scelta obbligata nell'ambito della telefonia mobile, ambiente recentemente rivoluzionato dall'introduzione di dispositivi di ultima generazione definiti smartphone, degli ibridi dalle incredibili potenzialità in grado di coniugare le caratteristiche degli elaboratori con quelle dei telefoni cellulari. Questo scenario è all'insegna del "mobile computing" un fenomeno destinato a crescere ulteriormente nell'immediato futuro, per cui è indispensabile acquisire per tempo competenze adeguate per la sua gestione e per fronteggiare le nuove minacce. Pur dedicando ampio spazio alla scelta e alla configurazione dei dispositivi, il libro si concentrerà maggiormente sugli aspetti più cruciali per gli utenti finali, aspetti come la configurazione pratica delle periferiche, il contrasto alle operazioni di hacking e l'identificazione di coloro che operano abusivamente sulla rete. In conclusione verranno anche affrontati alcuni temi trasversali a queste tecnologie come, ad esempio, quelli relativi alla cosiddetta guerra elettronica.

Come acquistare il libro
Se desiderate acquistare questo libro potete farlo direttamente online sul sito di FAG all'indirizzo:
http://www.fag.it/scheda.aspx?ID=29652

La recensione
Per conoscere e approfondire gli argomenti trattati in questo articolo è disponibile la recensione del libro da cui e tratto. Visita la pagina Sicurezza Wireless e mobile all'indirizzo:
http://www.comefarea.it/recensioni/sicurezzawirelessmobile/

L'autore
Autore di vasto materiale su temi informatici, svolge attività di docenza e consulenza collaborando con diverse aziende ed enti del settore IT. Professionalmente impegnato da tempo nel campo dell'amministrazione delle reti informatiche, si occupa oggi prevalentemente dei problemi inerenti alla loro sicurezza.