

Guida dettagliata: Craccare rete WiFi tramite Aircrack con interfaccia grafica

Argomento scottante...

Torno a trattare l'utilizzo di alcune tecniche per **craccare le reti wifi** protette sia con **chiave WEP** che con **chiave WPA**.



Se non l'hai ancora fatto ti consiglio di leggerti le mie **due guide** precedenti:

[Craccare una Wifi con chiave WEP](#)

[Craccare una Wifi con chiave WPA](#)

Ti starai chiedendo: questa guida cosa ha di nuovo rispetto alle altre due? Semplice...potrai **craccare una rete wifi senza smanettare con il terminale**.

Infatti da oggi potrai sfruttare **Aircrack con interfaccia grafica**. L'interfaccia è stata sviluppata da [BUC \(Basta un Click\)](#) e ti permette di eseguire tutte le operazioni per craccare la rete wifi senza utilizzare il terminale.

Pronto? Iniziamo subito con l'**installazione del software**...

Per utilizzare questo applicativo devi aver installato sul tuo pc **Aircrack**. Se hai ubuntu ti basta aprire un terminale e digitare:

```
sudo apt-get install aircrack-ng
```

Adesso devi installare **BUC**, ti consiglio di leggere e seguire [questa guida](#). Se non vuoi utilizzare il terminale puoi anche cliccare con il tasto destro sul pacchetto scaricato e installarlo tramite **GDebi**, l'installatore di pacchetti.

Adesso vai nella pagina [Download](#) di BUC e scarica il programma **Aircrack.zip**. Puoi scaricarlo anche direttamente da [questo link](#).

Decomprimi il file compresso che hai appena scaricato, così facendo avrai un file di nome **aircrack.mc**.

Vai sul menù in alto a sinistra “**Applicazioni**” → “**Altro**” → “**BUC**”, ti verrà chiesto di inserire il file che hai appena decompresso. Selezionalo e clicca su **Load**.

Ci sei? Bene...adesso dovrai impostare il tuo nuovo applicativo per **craccare le reti wifi**.

Impostazioni Iniziali

Dovresti avere davanti **Aircrack con interfaccia grafica**. Dirigiti nella prima scheda: **Impostazioni**. Hai davanti **4 Step da impostare**.



Step1: devi scegliere una cartella nella quale Aircrack salverà i dati generati allo scopo di **decriptare la password della rete wifi**. Nella riga sotto devi inserire il **nome della periferica wifi**. Se non lo sai apri un terminale (Applicazioni → Accessori → Terminale) e digita **iwconfig**. Nella terza riga devi inserire il **MAC Address della periferica wifi**, anche in questo caso puoi ricavarlo dando da terminale il seguente comando: **ifconfig** (guarda il valore alla voce **HWaddr**)

Step2: Se vuoi utilizzare Aircrack devi impostare la tua scheda wifi per lavorare in **Monitor Mode**. In questa fase dovrai appuntarti delle informazioni importanti: **ssid**, **bssid** e **il canale**. Per fare questo basta cliccare sul pulsante “**Attiva airodump-ng**”. Ti si aprirà un terminale con all’interno tutti i dati di cui hai bisogno. Prendi carta e penna e appuntati **BSSID** (è il MAC Address dell’access point vittima), **CH** (il canale) e **ESSID** (nome access point).

Step3: Devi semplicemete inserire i dati che hai appena appuntato.

Step4: in questa schermata ti viene notificato se hai inserito i dati in maniera corretta. Una volta terminata tutta la procedura ricorda di utilizzare questo pulsante per **disattivare il Monitor Mode**.

Iniziamo a divertirci!!

Craccare Rete Wifi con chiave WEP e client collegato

Questa guida ti permette di **craccare una rete wifi con chiave wep** con almeno un client connesso.

Per controllare se c'è almeno un client connesso ti basta guardare se ci sono delle righe sotto la **colonna BSSID**.



Sfoggia la **scheda WEP** e clicca sul tasto **“Airodump-ng-recuperare IVs-”**. Si aprirà un terminale, presta particolare attenzione alla colonna **#Data**, qui potrai controllare la quantità di pacchetti IVs catturati.

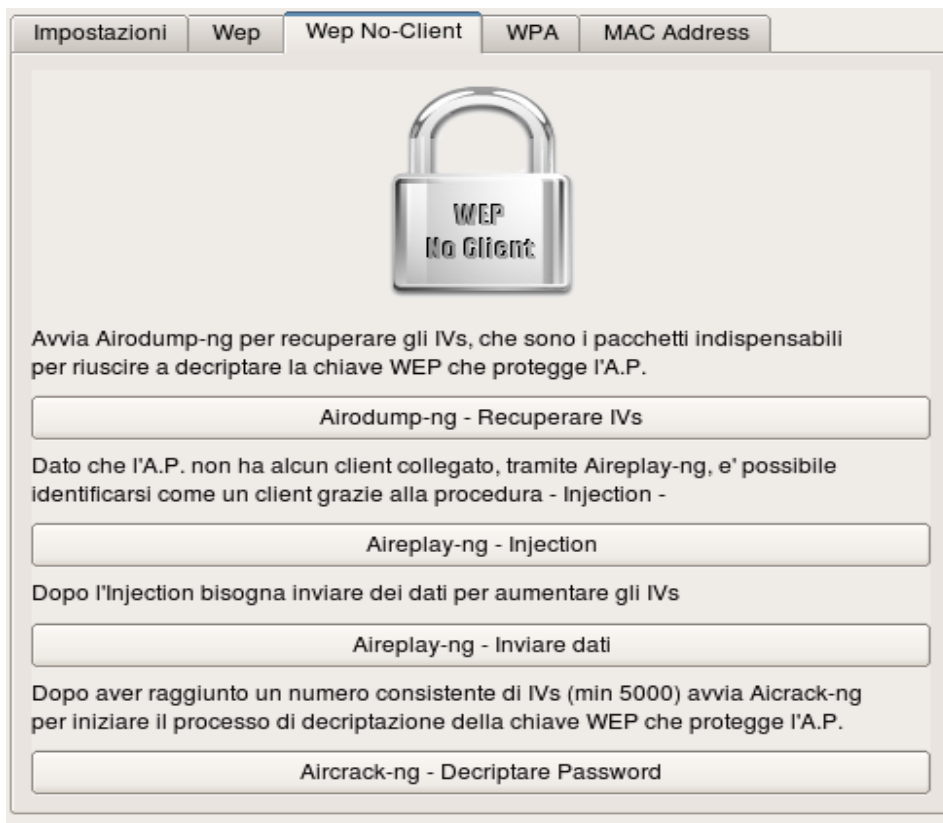
Adesso non ti resta che attendere e lasciare lavorare Aircrack.

Devi catturare una elevata quantità di pacchetti, almeno **7000** (per esperienza personale). Quando avrai raggiunto questa soglia di pacchetti puoi cliccare sul tasto **“Aircrack-ng – Decriptare Password-”**.

Alla fine di questo processo avrai la tua password di rete. Nel caso in cui i pacchetti fossero pochi dovrai catturarne altri e riprovare.

Craccare Rete Wifi con chiave WEP senza client collegato

Vediamo adesso come craccare una rete wifi con chiave wep nel caso in cui **nessun client è collegato** all'access point.



Vai nella **scheda Wep No-client**. Clicca su **“Airodump-ng – Recuperare IVs”**. Si aprirà un terminale simile al precedente, ma in questo caso non saremo in grado di catturare nessun pacchetto grazie al client collegato (in quanto non c’è).

Per risolvere questo problema clicca sul tasto **“Aireplay-ng – Injection-”** . tramite questa operazione il programma cercherà di autenticarsi all’access point e nel caso tutto vada a buon fine vedrai comparire il **tuò MAC Address nella colonna BSSID**.

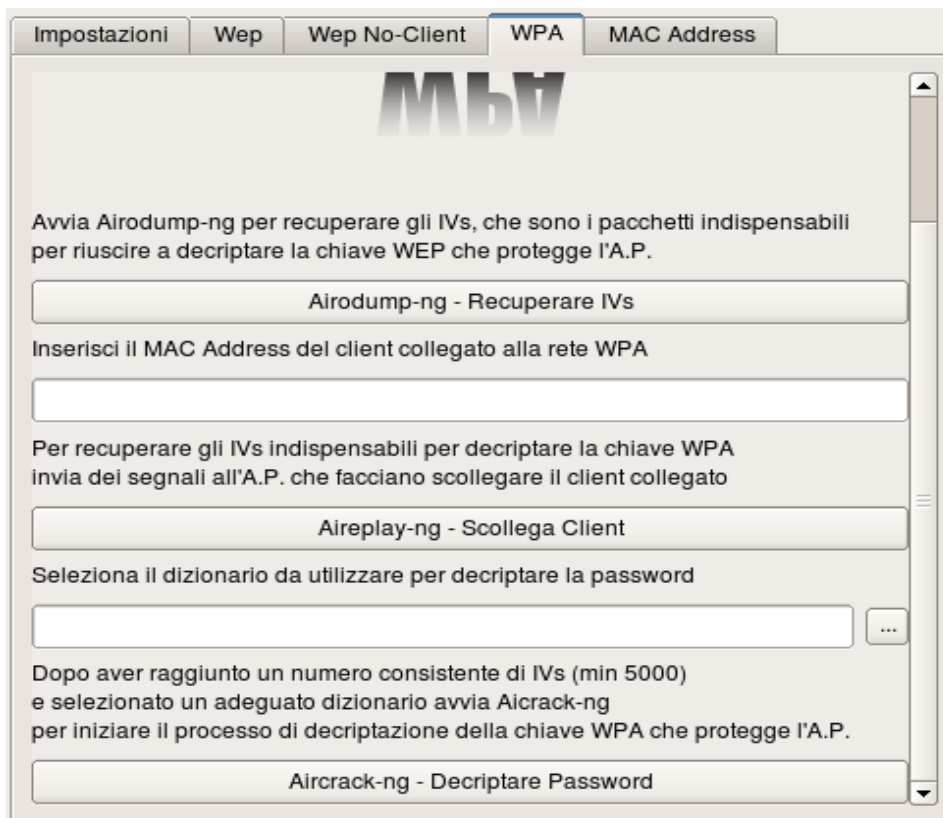
Attenzione: Non tutte le schede wifi supportano questa pratica, quindi potrebbe non andare a buon fine. E’ possibile risolvere installando driver diversi adatti a questo scopo.

Se tutto è andato a buon fine puoi cliccare sul tasto **“Aireplay-ng – Inviare Dati”** . In questo modo inizieremo ad inviare pacchetti all’access point.

Nota che i pacchetti catturati aumenteranno notevolmente (colonna **#Data**). Una volta catturata una buona quantità di pacchetti, consiglio almeno **7000**, puoi cliccare sul tasto **“Aircrack-ng – Decriptare Password”**. Attendi qualche istante e preparati a leggere la password della rete wifi.

Craccare Rete Wifi con chiave WPA

In questa sezione ti spiego come **craccare una rete wifi con chiave WPA** con almeno un client collegato all’access point “vittima”.



Posizionati nella **scheda WPA**.

Clicca sul pulsante **“Airodump-ng – Recuperare IVs”**. Si aprirà un terminale come al solito dal quale potrai vedere i pacchetti che vengono catturati dalla colonna **#Data**.

Se noti che la cattura dei pacchetti è **molto lenta** devi inserire nello spazio bianco il **MAC Address del client collegato** all’access point e cliccare sul tasto **“Aireplay-ng – Scollega Client”**.

In questo modo **disconnetterai il client collegato** e non appena il client tenterà di ricollegarsi tu sarai pronto a carpire porzioni della chiave da decriptare.

Adesso devi attendere che il software catturi un numero sufficiente di pacchetti, almento **7000** (consiglio personale).

Una volta raggiunta questa soglia dovrai **selezionare il vocabolario** per decriptare la password.

Un vocabolario puoi trovarlo nella cartella **usr/share/dict**, una volta selezionato clicca sul pulsante **“Aircrack-ng – Decriptare Password”**. Attendi che il processo di decriptamento sia terminato e controlla se è stato possibile recuperare la password o meno.

Sei arrivato al termine...spero di esserti stato utile.

Ti ricordo che questa guida è stata scritta solo a **scopo informativo** e non mi assumo nessuna responsabilità sull’utilizzo che ne farai. Craccare reti wifi altrui o di cui non si ha autorizzazione è un **reato**.

Ho scritto questa guida perchè credo che sia giusto che ognuno abbia il diritto di sapere e conoscere.

Cosa ne pensi? Hai dei suggerimenti da darmi? Ti sono stato di aiuto? Lascia un Commento.

Per i più Smanettoni, e per gli amanti del terminale:

[Craccare una Wifi con chiave WEP](#)

[Craccare una Wifi con chiave WPA](#)

