«Back|Track-[IT]

www.backtrack.it

(c) 2009 keeley
lord.dingo@gmail.com

Kismet

***

Questo pdf contiene due sezioni, una dedicata alla configurazione ed impiego generale di Kismet, mentre la seconda descriverà l' utilizzo dello scanner.

Kismet nasce con l'intento di individuare le reti wireless, difatti è il tool preferito dai Wardrivers, in quanto permette di raccogliere i dati con locazione geografica, sfruttando un ricevitore gps.

Questa guida si focalizzerà principalmente sulla nuova versione **new-core-2009**.

***

Kismet, è uno strumento composto da un client / server presente in **BackTrack** ed installabile anche su altre piattaforme come **GNU/Linux** / **Windows**.

La sua fama è anche dovuta alla sua versatilità, difatti può essere utilizzato come sniffer o intrusion detection system, senza contare l'utilizzo di plugin esterni.

Le sue caratteristiche principali possono essere riassunte:

- **Rilevamento reti wireless in modo attivo/passivo**
- **Rilevamento reti wireless nascoste**
- **Channel hop**
- **Identificazione del produttore del dispositivo rilevato**
- **Rilevamento blocco IP**
- **Mappatura access point geo-localizzata attraverso l'utilizzo di un dispositivo GPS**
- **Individuazione Clients connessi sul AP**

***

Come prima operazione da effettuare è la configurazione del server **Kismet**:

Quindi andiamo ad editare il file **/usr/etc/kismet.conf**

Per i neofiti > **kate /usr/etc/kismet.conf**

Iniziamo subito con la configurazione:

alla voce *ncsource*, andrà la nostra interfaccia, ad esempio wlan0, se non si è certi lanciare il comando iwconfig da terminale ed accettarsi dell'interfacce disponibili.

ncsource=wlan0

***

:# Extra: data la versatilità di kismet, è possibile utilizzare multi interfacce, e creare profili diversi per ogni interfaccia.

Es : interfaccia integrata wifi abgn, interfaccia esterna alfa g.

ncsource=wlan0:channellist=IEEE80211n

channellist=IEEE80211n:120,112 ….

ncsource=wlan1:channellist=IEEE80211g

channellist=IEEE80211g:1,2 ….

E' inoltre possibile avviare un'altra interfaccia una volta avviato il client, o semplicemente avviare la seconda interfaccia, senza specificarla nel kismet.conf, in quanto se specificata, al momento dell'avvio del server l'interfaccia DEVE essere presente, pena errore del server.

la voce *channelvelocity* indica il tempo di passaggio tra un canale e l'altro, di default è 5, ma io consiglio di impostare 7, specialmente per i wardrivers, che utilizzano mezzi di locomozione.

channelvelocity=7

veniamo ora alla configurazione dei canali disponibili attraverso la voce *channellist,* consiglio di configurare la *channellist=IEEE80211b*: con i canali di base, in quanto viene presa come default in caso di inserimento di nuove interfacce come nel caso della Extra di sopra, salvo diversa specifica in caso di caricamento dell'interfaccia.

channellist=IEEE80211b:1:3,6:3,11:3,2,7,8,4,9,5,10,12,13

N.B.*=questi sono i canali standard del wireless g*

:#Extra : per una lista completa dei canali supportati dalla vostra interfaccia, da terminale digitate il comando *iwlist " nome interfaccia" channel*

iwlist wlan0 channel

N.B.*= backtrack4 di default è settato sul regulatory USA, per cui i canali 12,13 non sono abilitati, per abilitarli, da console digitare*

iw reg set IT

I numeri 1:3,6:3,11:3, il :3 sta ad indicare il tempo dedicato alla ricerca di segnali provenienti da quel canale, in quanto la maggior parte degli apparati sono impostati di default sui canali 1,6,11.

Nello specifico è da intendersi in caso che il channel velocity, sopra impostato sia 10 come 10/3 del tempo di rimanere su quel canale.

Commentare le variabili ***ouifile=/etc/manuf*** *e* ***ouifile=/usr/share/wireshark/wireshark/manuf*** in quanto il file giusto è nella terza opzione, ovvero ***ouifile=/usr/share/wireshark/manuf***

Se abbiamo la possibilità di connettere un ricevitore GPS settiamo la variabile ***gps=true***, altrimenti su false.

Una fra le opzioni interessanti, è la possibilità di utilizzare i suoni, in particolare il server può riprodurre dei suoni per degli eventi particolari, se si ha questa necessità impostare *sound=true,* i tipi di eventi sono elencati sotto questa la suddetta variabile.

Inoltre c'è una opzione molto comoda per i wardrivers, ovvero la possibilità che il server legga e riproduca tramite audio il nome della rete più altre impostazioni configurabili. Per abilitare questa opzione bisogna abilitare ***speech=true*** , tuttavia bisogna prima installare il pacchetto ***festival***, per i neofiti > ***apt-get install festival*** .

Inoltre si può scegliere il tipo di riproduzione, molta comoda è la modalità parlata ovvero *speech_type=speech* , ma qualcuno potrebbe preferire lo speeling Nato o Spell, questo sta all'utente decidere.

Le variabili *speech_encrypted* e *speech_unencrypted* servono proprio a configurare l'evento riprodotto in caso si verifichi la condizione; di default viene riprodotto il messaggio di una nuova rete rilevata il suo ssid, il canale nella quale opera ed il tipo protetto *(wep,wpa,wpa2)* o non *(open).*

La variabile *metric* va impostata su *true*, e serve a far capire al server di utilizzare la notazione metrica-decimale, ovvero quella europea.

metric=true

Veniamo ora ai tipi di file che vengono salvati di default, la variabile *logtypes=pcapdump,gpsxml,netxml,nettxt,alert* ma per "semplicità" possiamo fare a meno di alcuni tipi di file, ma veniamo del dettaglio a cosa salvano:

pcapdump *= fa un salvataggio di tutti i pacchetti che sono stati sniffati, se non abbiamo bisogno di questo tipo di file possiamo disattivarlo.*

gpsxml **=** *è il salvataggio dei dati provenienti dal ricevitore GPS, disattivarlo in caso non si abbia intenzione di creare mappe.*

netxml **=** *salva i dati delle reti rilevate in formato xml, è comodo tenerlo attivo*

nettxt **=** *è simile a netxml ma invece di essere in formato xml è in formato testo, poco rilevante, in quanto la maggior parte dei tool utlizza il file xml.*

alert **=** *è un elenco degli eventi rilevati, sene parlava sopra nella variabile sound*

Nella maggior parte dei casi, salvo diverse esigenze:

logtypes=gpsxml,netxml

Se la variabile *pcapdump* è abilitata è utile configurare anche le voci:

noiselog=true se si vuole registrare nei log i disturbi

corruptlog=true se si vuole registrare nei log i pacchetti corrotti / ritrasmessi

beaconlog=true se si ha esigenza di registrare i beacon inviati dagli AP

Veniamo ora alla questione log, la variabile *logdefault* imposta il nome da dare al file dei log ed anche alla cartella di destinazione, di default è *Kismet,*ovvero verranno salvati sul desktop utente.

Se si vuole evitare ciò basta far puntare ad una cartella specifica come ad esempio:

logdefault=/home/log/kismet/Kismet

la variabile *logtemplate* invece decide il nome completo del file, di default imposta un nome del tipo istanza numero – data corrente – numero incrementale in caso di multi log, si consiglia di lasciarlo così, salvo diverse esigenze.

***

Avvio, ora possiamo lanciare da terminale il comando *kismet,* e controllare che tutto funzioni regolarmente.

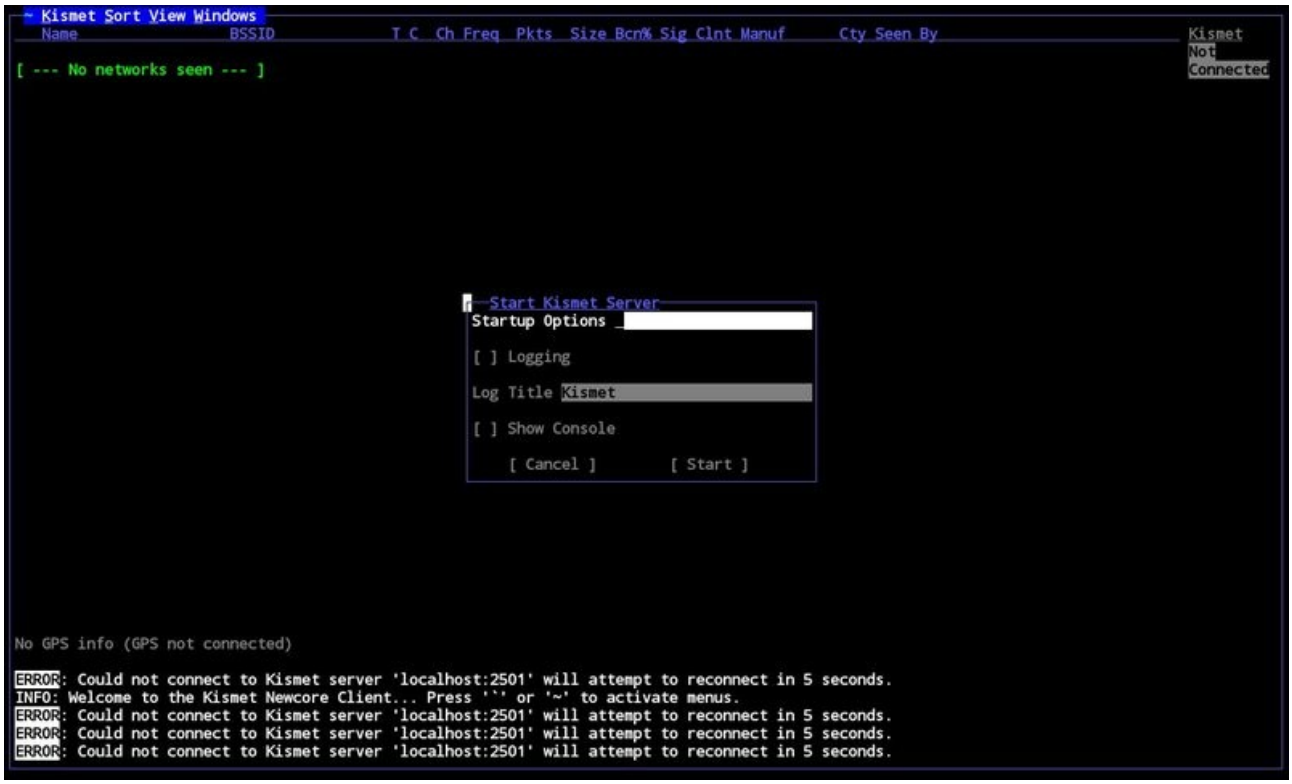
N.B. l'interfaccia di rete che verrà utilizzata in kismet, va impostata in monitor mode, per i neofiti,

ifconfig wlan0 down

iwconfig wlan0 mode monitor

ifconfig wlan0 up

l'interfaccia risultate dovrebbe essere questa, nella quale ci viene richiesto se inserire qualche parametro per l'avvio del server, in questo caso tramite l'ausilio del tasto *TAB* andiamo direttamente su *Start*

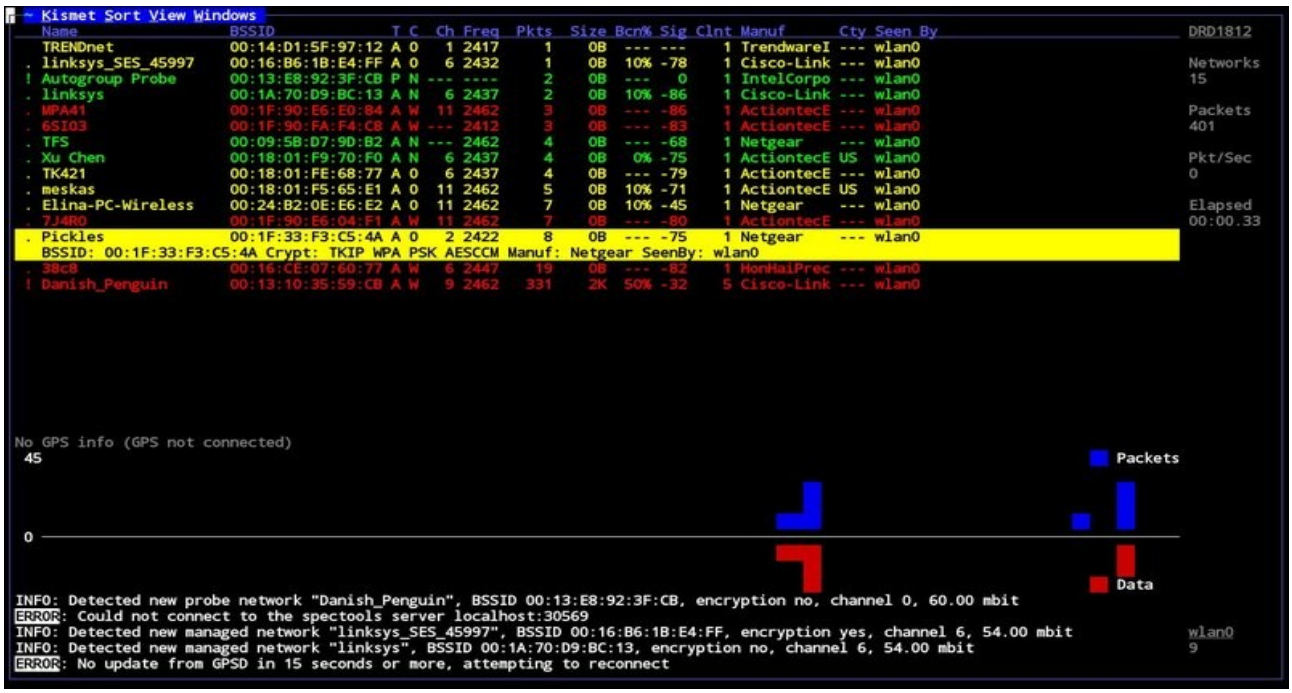


***

Successivamente si verrà spostati nella console dei log del server, controllare che non ci siano errori, poi proseguire con l'aiuto del tasto TAB su Close.

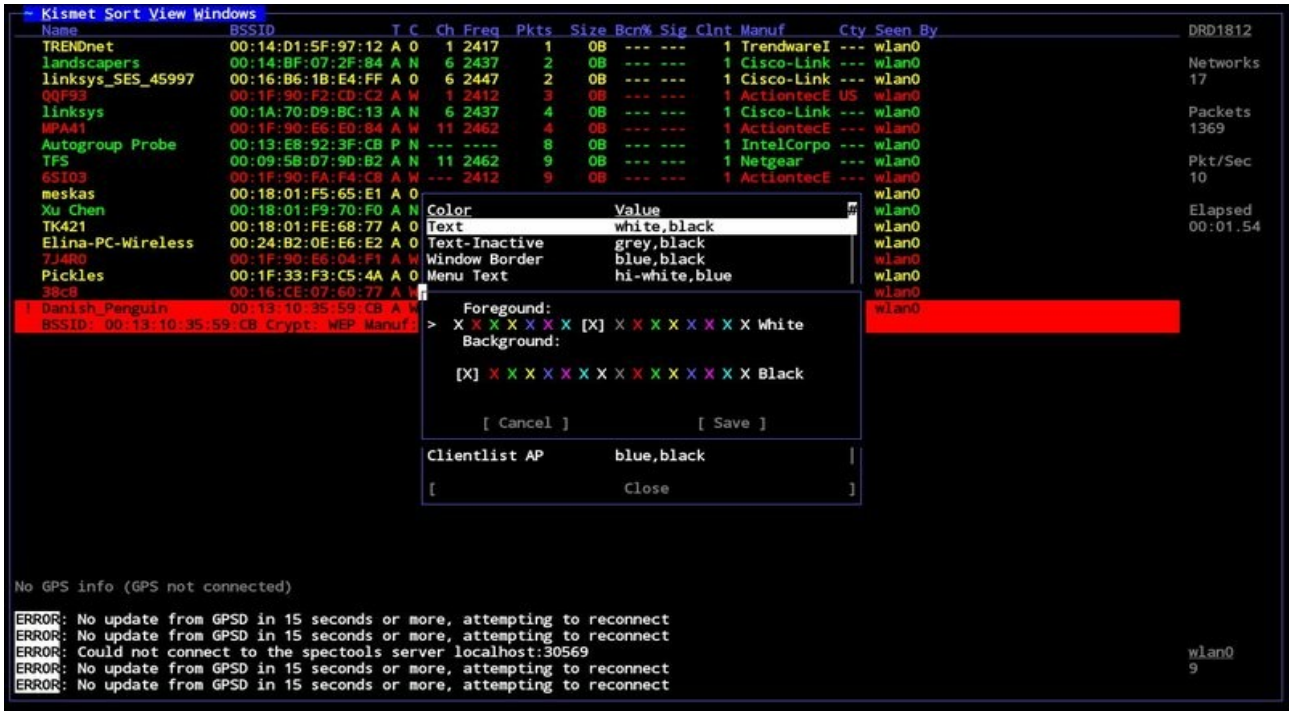
***

L'interfaccia è molto intuitiva, si può navigare fra la barra dei menu utilizzando il tasto Alt+F e successivamente le freccette. Consiglio di impostare *Sort* su *channel* o altro parametro che non sia *Auto-fit* in quanto, permette agilmente di ottenere informazioni sulle reti connesse, utilizzando le freccette. La finestra risultante è simile a questa:

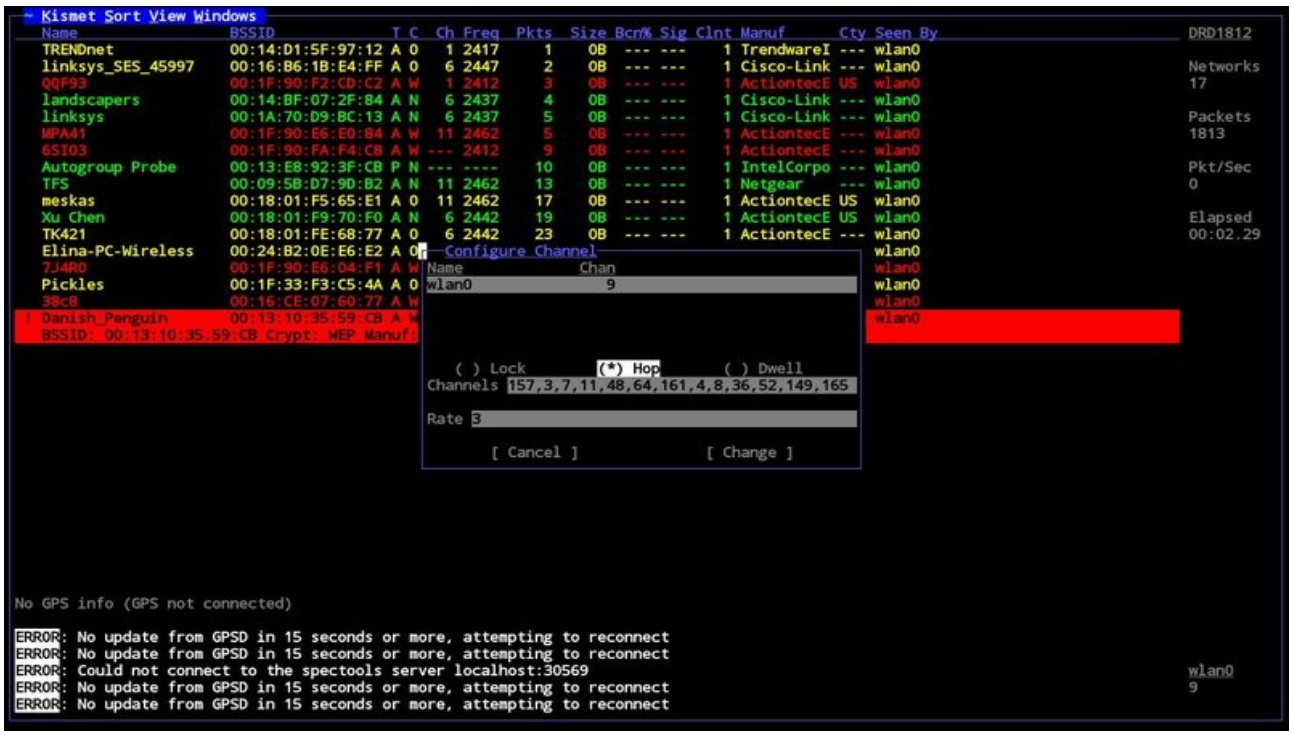


Le colonne possono essere personalizzate, per far comparire informazioni extra come ad esempio il numero di client connessi sul AP, o la potenza del segnale o tante altre informazioni, semplicemente andando nel menu ***Kismet*** > ***Preferences*** > ***Network Columns***.

Così come le altre impostazioni riguardanti i colori.



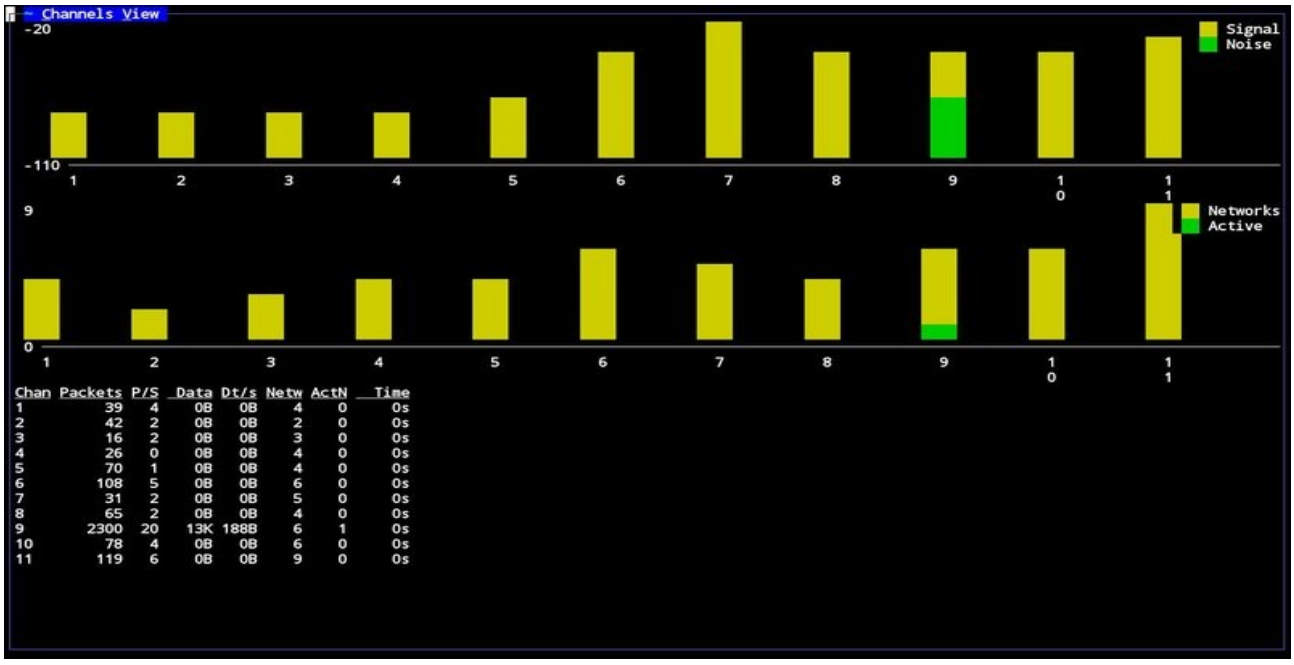
Inoltre sempre dal menu Kismet è possibile cambiare dinamicamente i canali monitorati, o puntare su un canale specifico (*lock*), andando in ***Kismet*** > ***Configure Channel.***

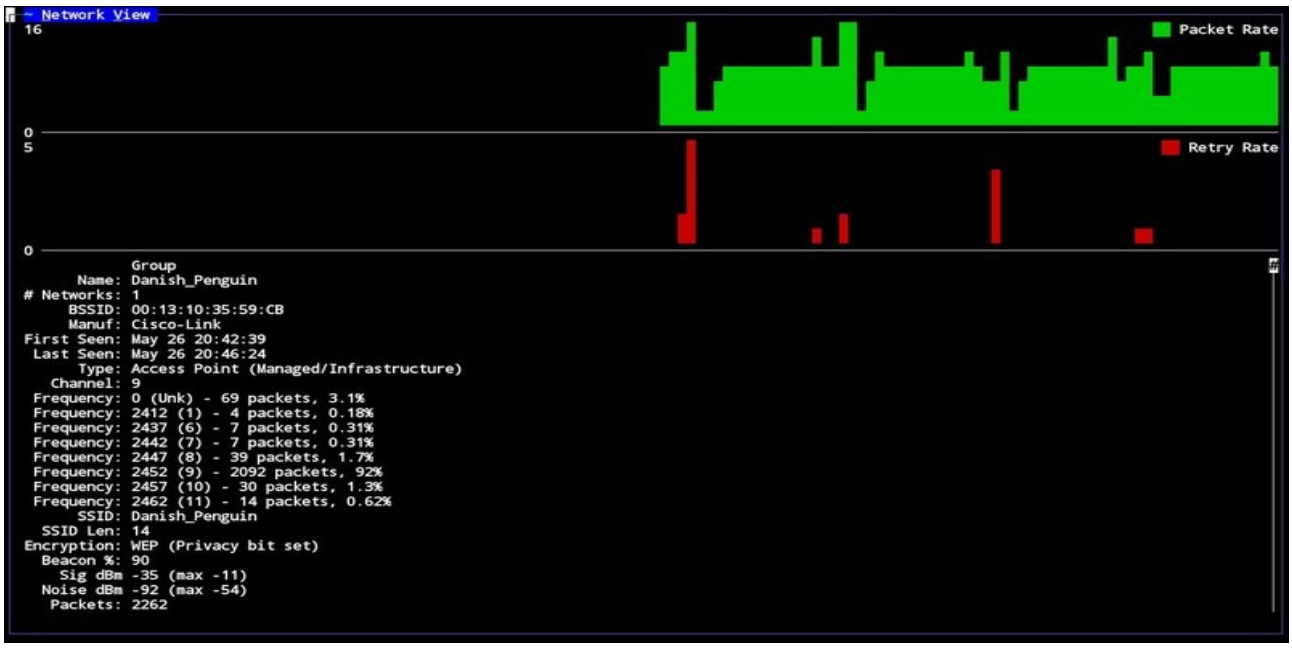


Data la versatilità di Kismet è possibile come è stato fatto notare prima in fase di configurazione di aggiungere un'altra interfaccia di rete in modo dinamico: ***Kismet*** > ***Add Source*** > ***intf = nome interfaccia*** *(es wlan1)* , di default vengono caricate le impostazioni ***IEEE80211b,*** ma se specificato diversamente in ***Opts*** si possono caricare profili specifici.

Ricordo che le interfacce devono essere già impostate in modalità monitor per essere caricate correttamente in Kismet.

Le opzioni di visualizzazione nell'interfaccia sono molte, pertanto invito l'utilizzatore a prenderne confidenza semplicemente imparando ad utilizzare i vari menu View e Windows.





Brevemente elencherò delle notazioni nell'interfaccia di kismet:

- *Name* : Sta ad indicare il nome della rete rilevata, (Probe Request, non è una rete, ma dei clients che stanno cercando una rete per collegarsi)
- ! : Indica attività sull'host puntato
- *T :* Indica il tipo di rete, ad esempio A = access point, H = ad-hoc
- *C:* Indica il tipo di protezione, O = other (wpa,wpa2), Y = wep, N = open

Tuttavia, Kismet non è soltanto questo, difatti in questo guida non si è presa in considerazione la creazione di mappe tramite Google Earth ed i dati raccolti da kismet, o all'utilizzazione di plugin esterni, o all'utilizzo di altra interfaccia grafica come ad esempio Qkismet.

Kismet homepage

---

in BackTrack:

BackTrack->Radio Network Analysis->80211->Cracking-> Kismet

www.backtrack.it

***

Questo documento è da ritenersi esclusivamente per scopi informativi / didattici, l' autore del testo e coloro che lo ospitano sul proprio spazio non sono responsabili delle azioni commesse da terze parti.

***

(c)2009 ***keeley*** *for* ***backtrack.it*** *published under* **GNU/GPL-v3**