



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





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**: Ouindi 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

 \mathbf{N} ella 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:

	less scanner -				<u>www.backtrac</u>
Kismet Sort View W	indows				
Name	BSSID T C Ch Free	Pkts	Size Bcn% Sig	Clnt Manuf Cty Seen By	DRD1812
TRENDnet	00:14:D1:5F:97:12 A 0 1 2417	1	OB	1 TrendwareI wlan0	
linksys_SES_45997	00:16:B6:1B:E4:FF A 0 6 2432	1	OB 10% -78	1 Cisco-Link wlan0	Network
Autogroup Probe	00:13:E8:92:3F:CB P N	2	0B 0	1 IntelCorpo wlan0	15
linksys	00:1A:70:D9:BC:13 A N 6 2437	2	OB 10% -86	1 Cisco-Link wlan0	
MPA41	00:1F:90:E6:E0:84 A W 11 2462			1 ActiontecE wlan0	Packet:
65103	00:1F:90:FA:F4:C8 A W 2412		OB83	1 ActiontecE wlan0	401
TFS	00:09:58:D7:9D:82 A N 2462	4	OB68	1 Netgear wlan0	
Xu Chen	00:18:01:F9:70:F0 A N 6 2437	4	OB 0% -75	1 ActiontecE US wlan0	Pkt/Sec
18421	00:18:01:FE:68:77 A 0 6 2437	4	OB/9	1 Actiontece Wianu	0
meskas	00:18:01:F5:65:E1 A 0 11 2462	51	OB 10% -/1	1 Actiontece US Wiano	F1 -1000
Elina-PC-wireless	00:24:B2:0E:E6:E2 A 0 11 2462		0B 10% -45	1 Netgear wiano	ETable
Rickles	00+15+22+52+55+44 4 0 2 2452		OP 75	1 Netgeor	00.00.5
BSSID: 00:1F:33:F3	C5:4A Crypt: TKIP WPA PSK AESCO	Manuf:	Netgear SeenBy	: wlan0	
Bada	00:16:CE:07:60:77 A W 6 2447	19	08 82	1 HonHaiPrec wlan0	
Danish Penguin	00:13:10:35:59:CB A W 9 2462			5 Cisco-Link wlan0	
GPS info (GPS not)	connected)				
GPS info (GPS not	connected)				Packets
GPS info (GPS not o	connected)				Packets
GPS info (GPS not o 5	connected)				Packets
GPS info (GPS not (connected)				Packets
GPS info (GPS not o	connected)			<u>.</u>	Packets
GPS info (GPS not 6	Connected)			_	Packets
GPS info (GPS not o	connected)			-	Packets
GPS info (GPS not (connected)			-	Packets
GPS info (GPS not (connected) bbe network "Danish Penguin". BSS	ID 00:1	3:E8:92:3F:CB.	encryption po, channel 0, 50.00 mbi	Packets
GPS info (GPS not o	connected) be network "Danish_Penguin", BSS ect to the spectools server local	ID 00:1	3:E8:92:3F:CB, (encryption no, channel 0, 60.00 mbi	Packets
GPS info (GPS not ()))))))))))))))))))	connected) obe network "Danish_Penguin", BSS ect to the spectools server local naged network "linksys SES 45997"	ID 00:1 host:30 . BSSID	3:E8:92:3F:CB, 569 00:16:B6:1B:E4	encryption no, channel 0, 60.00 mbi: :FF, encryption ves, channel 6, 54.0	Packets Data
GPS info (GPS not (0: Detected new pro 02: Could not conn 0: Detected new man 0: Detected new man 0: Detected new man	connected) obe network "Danish_Penguin", BSS act to the spectools server local laged network "linksys_ESE_45997"	ID 00:1 host:30 , BSSID :1A:70:	3:E8:92:3F:CB, 0 569 00:16:B6:1B:E4 09:BC:13, encry	encryption no, channel 0, 60.00 mbi :FF, encryption yes, channel 6, 54.00 ption no, channel 6, 54.00 mbit	Packets Data t D0 mbit wlan0

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.

L'ESTRICE.	BSSID T	C Ch Freq Pkts	Size Bcn% Sig Clnt Manuf	Cty Seen By	DRD1812
TRENDnet	00:14:D1:5F:97:12 A	0 1 2417 1	OB 1 Trendware	eI wlan0	
landscapers	00:14:BF:07:2F:84 A	N 6 2437 2	OB 1 Cisco-Lir	nk wlan0	Networks
linksys_SES_45997	00:16:B6:1B:E4:FF A	0 6 2447 2	OB 1 Cisco-Lin	nk wlan0	17
Linkeye	00:14:70-D9-PC-12 A	N 6 2412 3	OP 1 Circoli	ce us wiano	Packate
MPA41	00:1E:90:E5:E0:84 A	W 11 2462 4	OB and and 1 Actionted		1369
Autogroup Probe	00:13:E8:92:3F:C8 P	N 8	OB 1 IntelCorr	po wlan0	1565
TFS	00:09:58:D7:9D:B2 A	N 11 2462 9	OB 1 Netgear	wlan0	Pkt/Sec
	00:1F:90:FA:F4:C8 A		OB 1 Actionted	cE wlan0	10
meskas	00:18:01:F5:65:E1 A	0		wlan0	
Xu Chen	00:18:01:F9:70:F0 A	N Color	Value	# wlan0	Elapsed
TK421	00:18:01:FE:68:77 A	0 Text	white, black	wlan0	00:01.54
Elina-PC-Wireless	00:24:B2:0E:E6:E2 A	0 Text-Inactive	grey,black	wlan0	
7.J.4R0	00:1F:90:E6:04:F1 A	Window Border	blue,black	wlano	
Pickles	00:1F:33:F3:C5:4A A	0 Menu Text	hi-white,blue	WIano	
Book Property	001161CE1071601777A	Fanagaunda		WIGHU	
		Background:	X X X X X X X X X Black		
		Background: [X] X X X X X [Cancel]	X X X X X X X X X Black		
		Background: [X] X X X X X [Cancel] Clientlist AP	X X X X X X X X X Black [Save] blue,black		
		Background: [X] X X X X X [Cancel] Clientlist AP [X X X X X X X X X Black [Save] blue,black Close		
		Background: [X] X X X X X [Cancel] Clientlist AP [X X X X X X X X X Black [Save] blue,black Close	 1	
GPS info (GPS not c	connected)	Background: [X] X X X X X [Cancel] Clientlist AP [X X X X X X X X X Black [Save] blue,black Close	 1	

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

Kismet – Wirel	ess scanner -					<u>www.backt</u>	<u>rack.</u> i
~ Kismot Sort View Wi	ndows						
Name	BSSID T C Ch F	reg Pkts	Size Bon% Sig (Int Manuf Ctv	Seen By	D	RD1812
TRENDnet	00:14:D1:5F:97:12 A 0 1 2	2417 1	0B	1 TrendwareI	wlan0		
linksys SES 45997	00:16:86:18:E4:FF A 0 6 2	2447 2	0B	1 Cisco-Link	wlan0	N	etworks
QQF93		2412 3		1 ActiontecE US			7
landscapers	00:14:BF:07:2F:84 A N 6 2	2437 4	OB	1 Cisco-Link	wlan0		
linksys	00:1A:70:D9:BC:13 A N 6 2	2437 5	OB	1 Cisco-Link	wlan0		ackets
MPA41		462 5					813
Autogroup Probe	00:13:E8:92:3F:CB P N	10	0B	1 IntelCorpo	wlan0	P	kt/Sec
TFS	00:09:58:D7:9D:B2 A N 11 2	2462 13	0B	1 Netgear	wlan0	0	
meskas	00:18:01:F5:65:E1 A 0 11 2	2462 17	OB	1 ActiontecE US	wlan0		
Xu Chen	00:18:01:F9:70:F0 A N 6 2	2442 19	OB	1 ActiontecE US	wlan0	E	lapsed
TK421	00:18:01:FE:68:77 A 0 6 2	2442 23	OB	1 ActiontecE	wlan0	0	0:02.29
Elina-PC-Wireless	00:24:B2:0E:E6:E2 A 0	ifigure Cha	nnel		wlan0		
7.J4R0	00:1F:90:E6:04:F1 A W Name		Chan		wlan0		
Pickles	00:1F:33:F3:C5:4A A 0 Willing	1	9		wIano		
3868	00:16:CE107:60:77 A W				wiano		
	(Chanr Rate) Lock 1915 157,3, 3	(*) Hop 7,11,48,64,161,4	() Dwell 4,8,36,52,149,165			
		[Cancel		[Change]			
No GPS info (GPS not c	connected)						
ERROR: No update from ERROR: No update from ERROR: Could not conne ERROR: No update from ERROR: No update from	GPSD in 15 seconds or more, a GPSD in 15 seconds or more, a ct to the spectools server lo GPSD in 15 seconds or more, a GPSD in 15 seconds or more, a	attempting attempting ocalhost:30 attempting attempting	to reconnect to reconnect 569 to reconnect to reconnect			<u>₩</u> 9	lan0

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.

Kismet – Wireless scanner -		W	<u>ww.backtrack.it</u>
n <u>~ Network View</u> 16	- 1	- 4	Packet Rate
0	ai.	Î	Retry Rate
0 Group Name: Danish_Penguin # Networks: 1 BSSID: 00:13:10:35:59:CB Wanuf: Cisco-Link First Seen: May 26 20:42:39 Last Seen: May 26 20:42:39 Last Seen: May 26 20:46:24 Type: Access Point (Wanaged/Infrastructure) Channel: 9 Frequency: 2412 (1) - 4 packets, 0.13% Frequency: 2421 (6) - 7 packets, 0.31% Frequency: 2442 (7) - 7 packets, 0.31% Frequency: 2452 (9) - 2092 packets, 9.2% Frequency: 2462 (11) - 14 packets, 0.62% SSID: Danish_Penguin SSID Len: 14 Encryption: WEP (Privacy bit set) Beacon %: 90 Sig dBm -35 (max -11) Noise dBm -32 (max -54) Packets: 2262			

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

<u>in BackTrack:</u>

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

www.backtrack.it