]HackingTeam[| TSF

Descrizione della metodologia relativa ad una attività di risk assessment in ambito reti wireless

Milano

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
1.0	26 Febbraio 2009	Emissione
//	//	//
//	//	//
//	//	//

INFORMAZIONI		
Data di Emissione	26 Febbraio 2009	
Versione	1.0	
Tipologia Documento	Documento tecnico	
Numero di Protocollo	//	
Numero Pagine	9	
Numero Allegati	0	
Descrizione Allegati	1	//
	2	//
Redatto da	Danilo Cordoni Costantino Imbrauglio	
Approvato da	Roberto Banfi	

INDICE

INDICE DELLE FIGURE

1 Metodologia di verifica

In questa sezione illustriamo la metodologia impiegata per la verifica del livello di sicurezza della rete wireless.

La metodologia prevede le seguenti fasi:

- Fase di riconoscimento e verifica delle configurazioni degli apparati
- Fase di attacco

1.1 Fase di riconoscimento

In questa fase si procede a identificare le reti wireless attive e raggiungibili. Inoltre, una volta identificati gli apparati (access point) oggetto dell'attività di verifica, si procede ad analizzarne la configurazione.

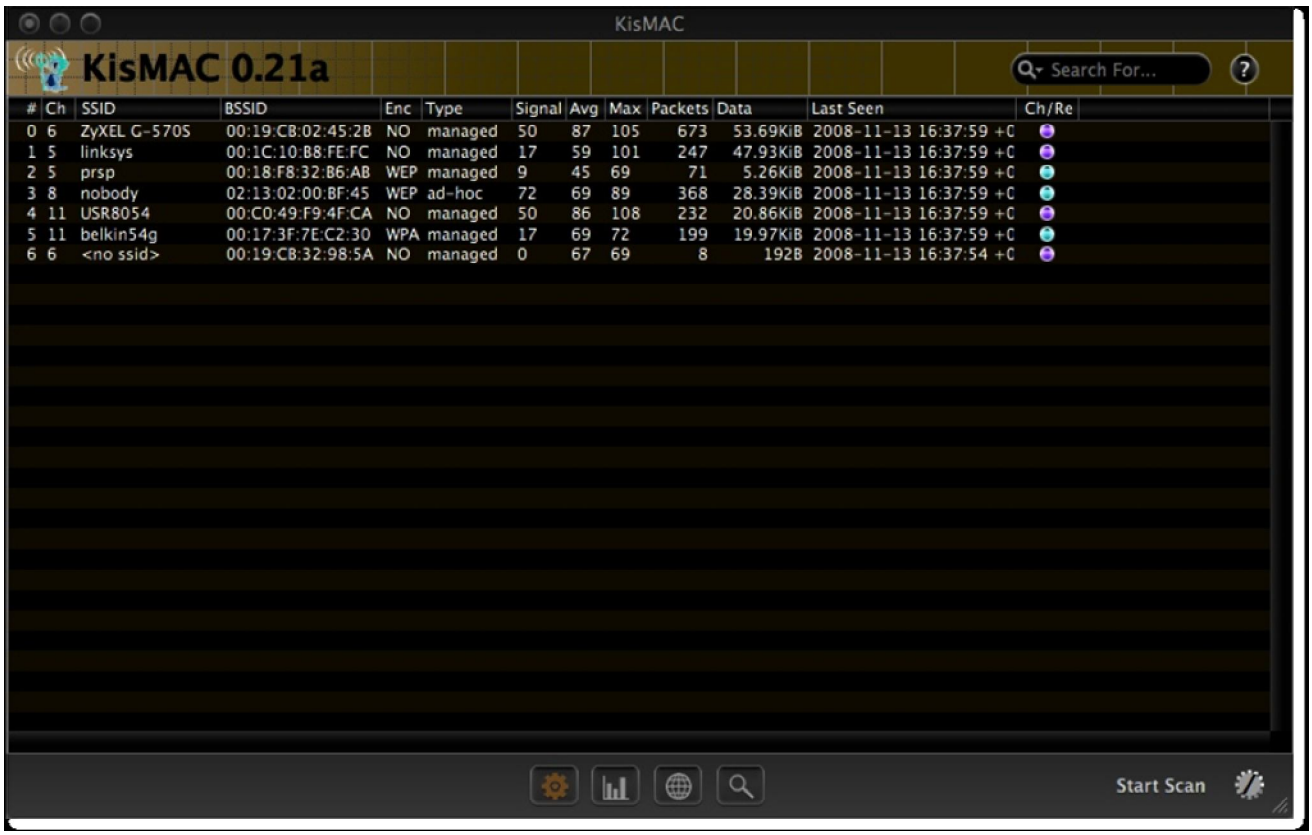

Figura 1 - Identificazione delle reti wireless attive e raggiungibili

Una volta identificata la rete wireless da verificare è possibile ottenere informazioni di dettaglio sulla medesima.

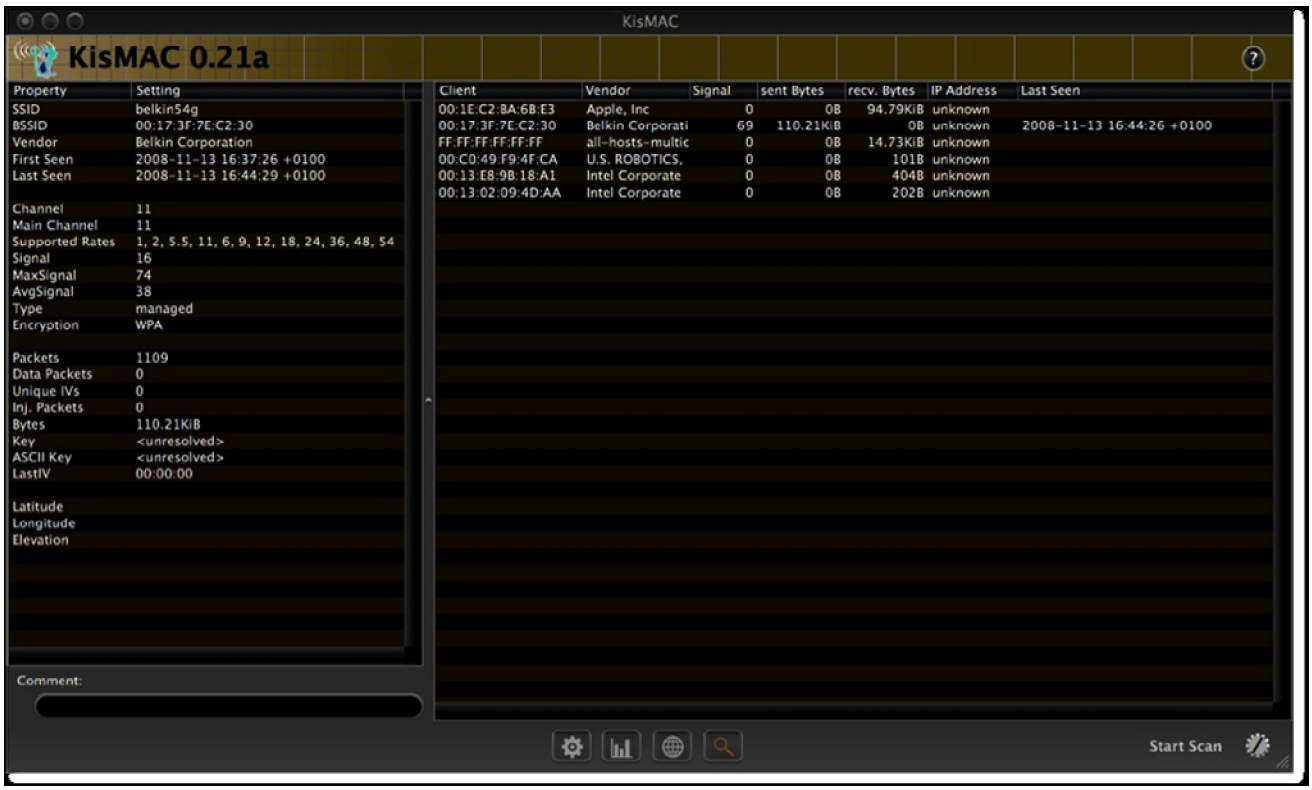

Figura 2 - Informazioni di dettaglio sulla rete wireless da verificare

Tra le informazioni di dettaglio, particolare interesse rivestono le seguenti:

- SSID (nome della rete eventualmente anunciato dall'access point)
- Open/Closed network (ovvero SSID annunciato o meno)
- Main channel (canale principale su cui opera l'access point)
- Encryption (meccanismo di sicurezza a protezione della rete wireless. Es.: WEP o WPA)
- Injection Vector (Vettori di Iniezione legati al processo di autenticazione WEP)
- MAC address dell'access point
- MAC address dei client attualmente collegati alla rete wireless

1.2 Fase di attacco

L'attività di attacco è riassumibile nelle seguenti fasi:

- Tentativi di intercettazione del traffico
- Tentativi di intrusione verso gli apparati wireless
- Tentativi di attacchi "forza bruta" o basati su dizionari verso gli access point
- Introduzione di device wireless rogue
- Attacchi Client-to-Client
- Denial of Service
- Tentativi di sfruttare malconfigurazioni
- Furto d'identità

1.2.1 Intercettazione

La fase di intercettazione differisce a seconda che la rete sia protetta con WEP piuttosto che con WPA/WPA2. In entrambi i casi però è necessario intercettare i pacchetti legati al processo di autenticazione di un client sulla rete wireless. Tali pacchetti contengono infatti le informazioni necessarie al recupero della chiave di accesso.

N.B. In assenza di sessioni di autenticazione dei client verso la rete wireless non è possibile operare alcun tipo di attacco e dunque non è possibile recuperare la chiave di accesso.

Se un insieme di client è già collegato alla rete wireless, sono possibili due approcci per intercettare i pacchetti legati a una sessione di autenticazione.

- Approccio passivo – Consiste nell'attendere passivamente la ri-autenticazione di un client (o l'autenticazione di un nuovo client) sulla rete wireless.
- Approccio attivo – Consiste nel forzare lo sganciamento del client dalla rete wireless e dunque causare volutamente un nuovo processo di autenticazione del client medesimo.

Il primo approccio non richiede interventi attivi e dunque non comporta il rischio di essere scoperti e identificati. D'altra parte può succedere di dover attendere a lungo prima che si verifichi un nuovo processo di autenticazione

Il secondo approccio permette di generare artificialmente e in pochi secondi un processo di autenticazione, ma richiede un intervento attivo che può essere rilevato.

Una volta raccolti i pacchetti relativi ai processi di autenticazione è possibile procedere con la vera e propria fase di *cracking* delle chiavi di accesso.

1.2.2 Cracking

Anche questa fase differisce profondamente a seconda che la rete wireless implementi WEP piuttosto che WPA/WPA2.

Nel primo caso, disponendo di un sufficiente numero di *vettori di iniezione* sarà possibile estrarre la chiave WEP in pochi secondi.

Nel secondo caso invece, si procederà con attacchi a forza bruta o basati su dizionari (i dizionari sono raccolte di parole-chiave che vengono provate reiteratamente nella speranza di individuare una coincidenza con quella impiegata per proteggere la rete wireless).

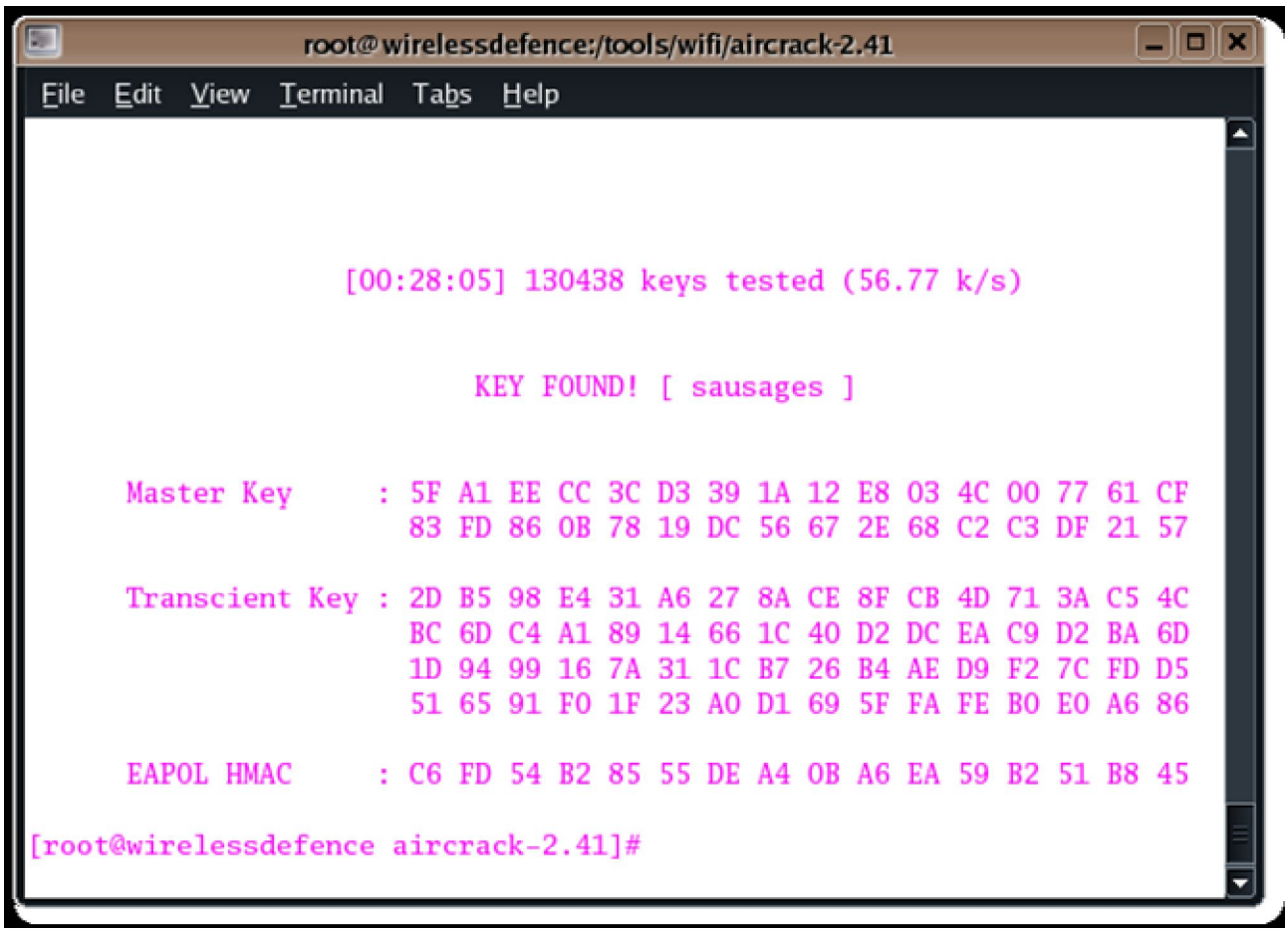

Figure 3 - Esempio di attacco basato su dizionario

N.B. La disponibilità di buoni dizionari (possibilmente creati ad hoc per il contesto in cui si sta operando) può aumentare le probabilità di decifrazione della chiave. Di converso l'adozione di una buona chiave di cifratura riduce enormemente tale possibilità. La scelta di una buona password è in genere legata all'adozione di una opportuna password policy.

1.2.3 Introduzione abusiva di device wireless rogue

Questa tipologia di attacchi consiste nell'introdurre nella rete wireless un dispositivo wireless allo scopo di compromettere la sicurezza della rete stessa e, possibilmente, per creare reti wireless abusive. Sono possibili due scenari:

- Rogue client: il malintezionato, attraverso un sistema fasullo (ad esempio un laptop), prova a connettersi ad un access point abusivamente;
- Rogue access point: il malintenzionato installa un access point configurato volutamente in modo altamente insicuro per permettere l'accesso alle risorse della rete target.

Entrambi gli scenari possono permettere l'accesso non autorizzato alla rete wireless e, nei casi peggiori, anche alle risorse della rete cablata.

1.2.4 Attacchi Client-to-Client

Una rete wireless può essere configurata in modo da permettere ai client di comunicare direttamente fra loro, senza dunque la necessità di passare attraverso un access point. Questa tipologia di reti wireless viene chiamata **Ad-Hoc.** Questa modalità di comunicazione wireless permette ad un client di effettuare attachi verso gli altri client wireless allo scopo di ottenere il controllo del sistema operativo o per causare malfunzionamenti al suo interno.

1.2.5 Attacchi Denial of Service

Questa tipologia di attacchi viene praticata allo scopo di rendere inutilizzabile la rete wireless e quindi di rendere inaccessibili le risorse delle rete. Tipicamente questo attacco consiste nell'immettere un numero di pacchetti di de-autenticazione e di de-associazione elevatissimo nella rete wireless in modo da "innondare" (fllooding) i client wireless legittimi negando loro così la possibilità di accedere alla rete locale.

Un altro attacco DoS wireless consiste nell'immettere nella rete un elevatissima quantità di dati in modo da saturare la larghezza di banda della rete wireless stessa. In questo modo la rete wireless vittima viene forzata a rifiutare tutti i pacchetti. Questo attacco, può inoltre ripercuotersi

negativamente sulle perfomance delle risorse hardware agganciate all'access point vittima dell'attacco.

1.2.6 Malconfigurazioni

Un access point non confiugurato correttamente può permettere ad un malintenzionato di compromettere la sicurezza della corrispondente rete wireless. Un access point di solito non prevede di default un meccanismo di autenticazione dei client. Inoltre, il controllo centralizzato delle configurazione può risultare arduo ed oneroso, di conseguenza spesso vengono mantenute inalterate le configurazioni base (out of the box) per garantire una elevata funzionalità del sistema (a discapito della sua sicurezza).

1.2.7 Furto d'identità

Il furto di identità in una rete wireless avviene quando un malintenzionato assegna alla propria macchina un indirizzo di rete (di solito il MAC Address) valido e appartenente ad un client wireless autorizzato all'accesso delle risorse della rete target. In questo modo si può tentare di accedere alle risorse ed ai servizi in modo autorizzato. Un altro attacco di questo tipo consiste nell'impersonare un access point (esistente o credibile) in modo che i client gli mandino la richiesta di autenticazione. In questo modo è possibile sottrarre loro le credenziali.

2 Deliverable

In questa sezione si elencano gli output che verranno rilasciati al termine dell'attività sopra descritte:

- Executive summary: sintesi non tecnica dell'attività svolta e dei risultati ottenuti,
- Metodologia: descrizione del *modus operandi* degli step effettivamente seguiti e dei tools utilizzati per l'attività,
- Security Evaluation e risultati: esposizione dettagliata dei risultati ottenuti (supportata dalle relative evidenze) e valutazione delle vulnerabilità riscontrate (analisi delle minacce e dell'impatto),
- Contromisure: breve descrizione delle possibile contromisure applicabili per rimuovere le vulnerabilità trovate,
- Reportistica: log e report relativi agli output forniti dagli strumenti utilizzati.