WPA

RESUME

Je vais étudier dans ce projet WPA (WPA et WPA2, en particulier la version personal la plus utilisée, mais aussi la version enterprise utilisant un serveur d'authentification de type radius donc plus compliquée) son fonctionnement (protocole de cryptage, authentification) puis ses faiblesses et ensuite quels sont les moyens utilisés pour le craquer, et je finirais par un test de craquage sur ma propre box qui ne dispose que du WPA-PSK.

SOMMAIRE

I Présentation du WPA (Wi-Fi Protected Access) 2
1. Origine du WPA 2
1. Wi-Fi Alliance (WPA) 2
2. 802.11i (WPA2) 2
2. Présentation 2
1. Types 2
1. WPA personal : clés partagées (PSK) 3
1. Schéma et explication de connexion, d'authentification 3
2. Explication des différentes clés utilisées 3
2. WPA enterprise : architecture 802.1x (RADIUS avec EAP) 5
1. Schéma et explication de connexion, authentification 5
2 .Types EAP 6
2. Cryptages 7
1. WPA : TKIP 7
1. Présentation 7
2. Nouveautés par rapport au WEP (clé RC4) 7
2. WPA2 : TKIP et AES (CCMP) 7
1. Présentation 7
2. Nouveautés d'AES par rapport au TKIP 8
3. Récapitulatif 8
II Faiblesses 9
III Solutions 9
IV Types de craquage existant 9
V Test 11
VI Conclusion 14
BIBLIO 14

I Présentation du WPA (Wi-Fi Protected Access)

Le Wi-Fi Protected Access (WPA et WPA2) est un mécanisme pour sécuriser les réseaux sans-fil de type Wifi.

1. Origine du WPA

1. Wi-Fi Alliance (WPA)

La Wi-Fi Alliance est une association d'entreprises, qui possède les droits sur le sigle Wi-fi et qui certifie le matériel portant ce sigle. Les certifications des implantations du WPA ont commencé en avril 2003 et sont devenues obligatoires en novembre 2003.

Le WEP faisant l'objet de trop nombreuses faiblesses, la Wi-Fi Alliance et l'IEEE ont donc décidé de garantir plus de sécurité tant pour le transfert des données que pour l'authentification des utilisateurs en créant une nouvelle solution de sécurisation de réseau WiFi.

La norme IEEE 802.11i a tardé à être validée. Du coup, en fin 2002, la Wi-Fi Alliance a défini un sous-ensemble de ce qu'allait être 802.11i, sous la désignation de WPA.

2. 802.11i (WPA2)

La norme IEEE 802.11i, est un amendement à la norme IEEE 802.11 ratifié le 24 juin 2004 plus connu sous le nom de WPA2, traite du renforcement de la sécurité des échanges au niveau des réseaux informatiques locaux utilisant une liaison sans fil (WLAN).

La norme IEEE 802.11i (ou WPA2) fournit un chiffrement plus élaboré que celui de la solution intérimaire WPA (Wi-Fi Protected Access).

Pour la mise en place de ces nouvelles sécurités, il faut faire attention au matériel (point d'accès) utilisé car le WPA ne nécessite qu'une mise jour du firmware du point d'accès tandis que le WPA2 nécessite un matériel adéquat.
De nos jours, tous les nouveaux matériels disposent de la sécurité WPA2.

2. Présentation

1. Types

Il existe 2 types de WPA, la version personal la plus utilisée, mais aussi la version enterprise utilisant un serveur d'authentification.

1. WPA personal : clés partagées (PSK)

1. Schéma et explication de connexion, d'authentification

Le mode personal permet de mettre en oeuvre une infrastructure sécurisée basée sur le WPA sans utiliser de serveur d'authentification. Le WPA personal repose sur l'utilisation d'une clé partagée, appelées **PSK** pour Pre-shared Key, renseignée dans le point d'accès ainsi que dans les postes clients. En effet, le WPA permet de saisir une « passphrase » (phrase secrète), traduite en PSK par un algorithme de hachage.

Voici le schéma d'une connexion WiFi de base, c'est-à-dire que le client envoie une requête d'authentification au point d'accès, celui-ci lui répond et en cas d'authentification réussi, le client renvoie une requête pour s'associer au point d'accès.
Si celui-ci accepte, le client est connecté au point d'accès.

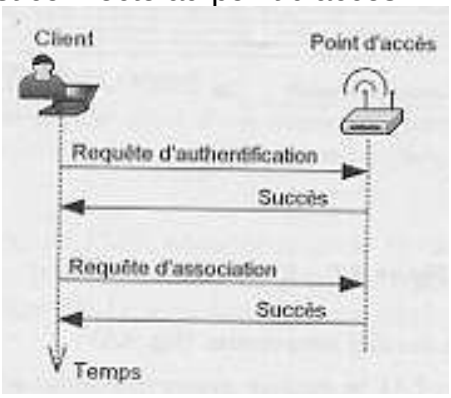

Figure 1 : Association WiFi

2. Explication des différentes clés utilisées

Voici le schéma de la négociation des clés durant la phase de la connexion au point d'accès.
Tout d'abord le client et le point d'accès se mettent d'accord sur une clé PTK (Pairwise Transient Key) dérivée de la PMK (Pairwise Master Key).
Désormais les échanges sont cryptés avec la clé PTK dans un tunnel sécurisé.
Ce qui permet au point d'accès d'envoyer la clé GTK (Group Transient Key) utilisée pour crypter le trafic broadcast et multicast avec une requête EAPol-Key.
Avec cette clé le client peut dorénavant décrypter le trafic de groupe et ensuite accéder au réseau en ayant des communications cryptées.

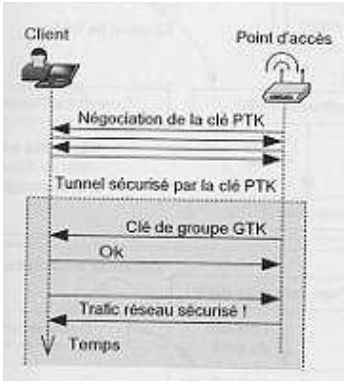

Figure 2 : Négociation des clés temporaires

Un moment important de la communication est le four-way handshake, c'est-à-dire 4 messages non cryptés donc vulnérables aux attaques car ils contiennent les échanges permettant de négocier la clé PTK.
Ces messages sont d'ailleurs utilisés au moment du craquage de la clé WPA (cf V Test).
Voici le schéma du four-way handshake :
- Tout d'abord le point d'accès envoie son nonce (numéro utilisé qu'une seule fois) au client en clair.
- Ensuite le client génère la clé PTK avec ses éléments, et envoie son propre nonce au point d'accès en rajoutant un code de contrôle d'intégrité.
- Puis le point d'accès génère la clé PTK à l'aide du nonce du client. Il utilise la clé générée pour vérifier le code d'intégrité envoyé par le client et si le code est bon (sinon il y a échec de la connexion), il envoie un message au client pour lui dire en rajoutant un code d'intégrité.
- Pour finir, le client vérifie le code d'intégrité et si le code est bon c'est qu'ils ont la bonne et même clé PMK. Il envoie ensuite un message au client pour lui dire qu'il est prêt à démarrer la session.
Le tunnel sécurisé est donc créé ce qui permet désormais de réaliser des échanges cryptés.

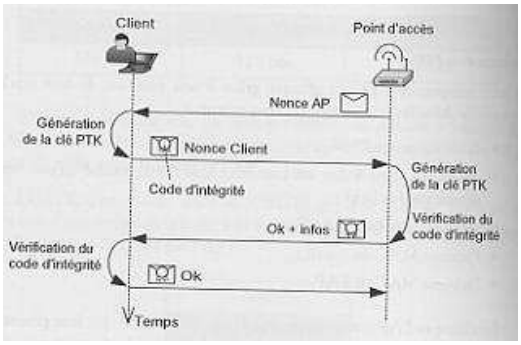

Figure 3 : Négociation de la clé temporaire PTK avec le four-way handshake

Plusieurs clés sont donc utilisées pour se connecter à un réseau.
Tout d'abord la première clé (PSK ou EAP suivant le protocole utilisé) devient la clé maitresse appelé PMK.
Ensuite, la clé PTK, c'est la dérivée avec une fonction de hashage de la clé PMK.
La clé de groupe GTK quant à elle est générée par le point d'accès après hashage de la clé GMK.

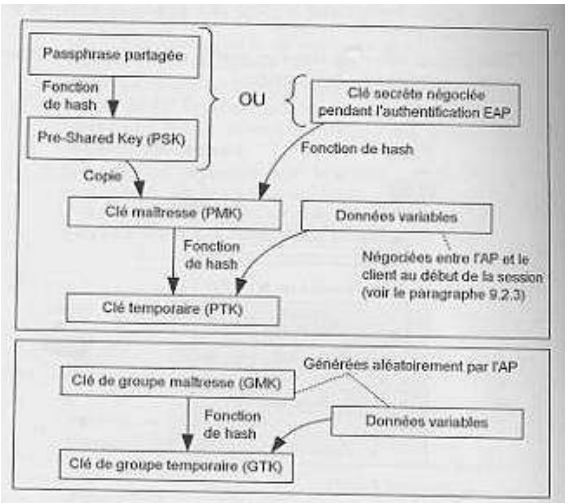

Figure 4 : Hiérarchie des clés du WPA et du WPA2

2. WPA enterprise : architecture 802.1x (RADIUS avec EAP)

1. Schéma et explication de connexion, authentification

Le mode enterprise impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification, généralement un serveur RADIUS (Remote Authentication Dial-in User Service), et d'un contrôleur réseau (le point d'accès).
Le but du protocole EAP utilisé ici est d'identifier les utilisateurs avant de les laisser rentrer sur le réseau à l'aide de multiples méthodes d'authentification : mot de passe, carte à puce, certificats électroniques, …

Voici le schéma expliquant comment marche la connexion WiFi avec un serveur d'authentification (version WPA enterprise).
Ici les clients sont reliés au point d'accès mais ensuite pour accéder au réseau il faut s'authentifier sur un serveur d'authentification.

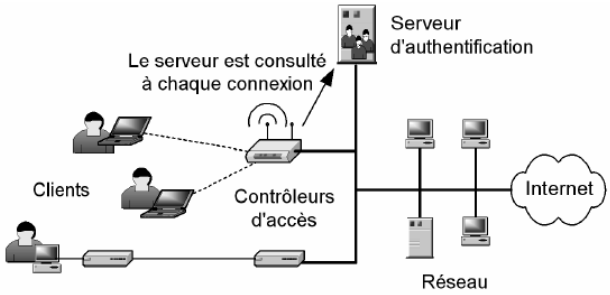

Figure 5 : Vue d'ensemble du protocole EAP

Le schéma suivant est celui d'une connexion WiFi avec 802.1x.
Tout d'abord le client envoie une requête EAPol Start pour démarrer l'échange ayant pour but l'authentification au point d'accès qui vérifie l'identité du client à l'aide d'un serveur d'authentification.
Au cours de l'authentification, le client et le serveur s'accorde sur le protocole de cryptage des données et la clé de 256 bits utilisée (PMK).
Après l'échange des clés entre le serveur, l'AP et le client, l'échange continue désormais dans un tunnel sécurisé.
L'authentification réussie, le serveur envoie une requête de succès EAP au client pour son association au point d'accès.

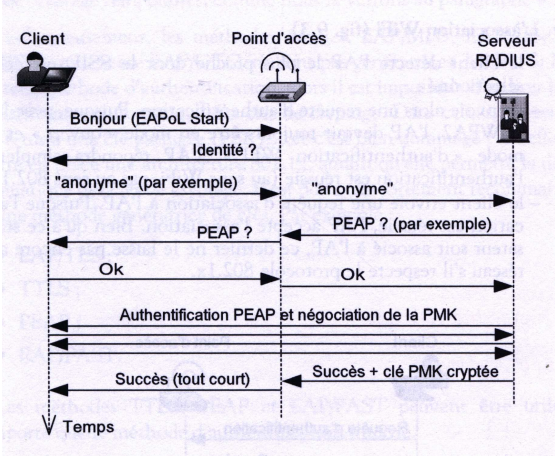

Figure 6 : Authentification 802.1x

Ce schéma est celui d'une connexion WiFi via un serveur d'authentification EAP avec un certificat.
Tout d'abord le serveur envoie une requête d'authentification au client, celui-ci lui répond soit avec un mot de passe soit avec une carte à jeton soit avec un certificat (ici le client ne disposant pas de carte à jeton, il propose au serveur une autre alternative d'authentification et celui-ci choisit le certificat).
Après vérification par le serveur, le client renvoie une requête pour s'associer au point d'accès.
Si le serveur accepte, le client est connecté au réseau.

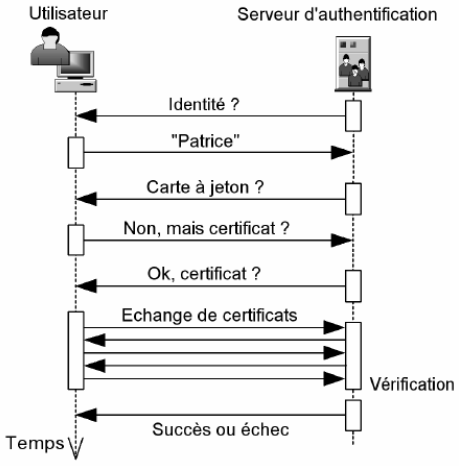

Figure 7 : Dialogue avec EAP

2 .Types EAP

EAP (Extensible Authentication Protocol) est un protocole d'identification très souple (mots de passe, carte à puce, certificats électroniques, …) utilisé dans différents contextes, pas seulement dans le cadre du WiFi et qui est défini par IEFT (Internet Engineering Task Force) en mars 1998 (RFC 2284) puis corrigé en juin 2004 (RFC 3748).

Le principe est basé sur 3 acteurs, c'est-à-dire que si un client cherche à accéder au réseau, un contrôleur d'accès lui barrera le chemin jusqu'à ce qu'il s'identifie auprès du serveur d'authentification.

Le contrôleur d'accès du type point d'accès sert d'intermédiaire pour la communication entre le client et le serveur d'authentification.

Il existe une multitude de méthodes d'authentification avec EAP qui se diffèrent par l'utilisation d'un certain protocole d'authentification (ex : CHAP), fonction de hachage (ex : MD5), protocole de sécurisation des échanges (ex : TLS), … mais les principales sont répertoriées dans le tableau suivant.

Tableau récapitulatif des types EAP les plus courants.

Types EAP

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Authentification du serveur	Aucune	Password Hash	Clé publique (certificat)	Clé publique (certificat)	Clé publique (certificat)
Authentification du client	Password Hash	Password Hash	Clé publique (Certificat , carte à puce)	CHAP, PAP, MS-CHAP(v2), EAP	EAP(EAP-MS-CHAPv2 ou clé publique)
Distribution dynamique des clés	Non	Oui	Oui	Oui	Oui
Risques sécurité	Vol de session. Attaque dictionnaire. Obtention du login client et Attaque MiM	Attaque dictionnaire et obtention du login client	Obtention de l'identité client	Attaque MiM	Attaque MiM

Figure 8 : Tableau récapitulatif des types EAP

2. Cryptages

Il existe 2 types de cryptage, le protocole TKIP pour le WPA, et le protocole AES pour le WPA2.

1. WPA : TKIP

1. Présentation

TKIP (Temporal Key Integrity Protocol) est un protocole de communication utilisé pour la protection et l'authentification des données transitant sur un réseau WiFi.
WPA spécifie notamment l'utilisation de ce chiffrement qui recourt au même algorithme (RC4) que WEP, mais renouvelle la clé tous les dix mille paquets.
TKIP est donc plus performant que le WEP.

2. Nouveautés par rapport au WEP (clé RC4)

On utilise le même algorithme de cryptage RC4 que le WEP seulement il est plus performant.
Un mécanisme a été mis en place pour éviter d'utiliser des clés RC4 faibles, l'utilisation du contrôle d'intégrité Michael est plus puissant que le contrôle d'intégrité IVC du WEP, le vecteur d'initialisation est plus long (48 bits au lieu de 24 bits pour le WEP) et est aussi utilisé pour contrer les attaques de relecture et enfin les clés de cryptage sont différentes à chaque paquet, et sont distribuées suivant un mécanisme plus souple et plus sûr que celui du WEP.

2. WPA2 : TKIP et AES (CCMP)

1. Présentation

CCMP (Counter-Mode/CBC-Mac protocol) est une méthode de chiffrement qui utilise AES (Advanced Encryption Standard), un algorithme de chiffrement.
La combinaison des deux est la sécurité la plus performante.

2. Nouveautés d'AES par rapport au TKIP

Le cryptage AES est le plus sécurisé, mais provoque certains problèmes de compatibilité avec quelques matériels.
C'est le plus fort standard de chiffrage autorisé par Wi-Fi.
Il dispose comme avantages d'une authentification forte reposant sur le protocole 802.1X, d'un mécanisme de distribution automatique des clés, d'un contrôle d'intégrité puissant et d'un mécanisme empêchant toute attaque de relecture.
Si on choisit de se connecter en réseau mixte TKIP+AES alors le cryptage sera utilisé avec l'algorithme le moins fort des deux, soit TKIP. Ce n'est donc pas une bonne solution de sécurité.

Tableau récapitulatif des protocoles, algorithmes de cryptages et algorithmes de contrôle d'intégrité des différentes solutions de sécurités WiFi.

Solution	Protocole	Cryptage	Intégrité
WEP	WEP	RC4	CRC
WPA	TKIP	RC4	Michael
WPA2	TKIP	RC4	Michael
WPA2	CCMP	AES	CBC

3. Récapitulatif

Tableau récapitulatif des solutions de chiffrement plus précis que le précédent.

	WEP	*TKIP*	*CCMP*
Chiffrement	RC4	RC4	AES
Taille de la clé	40 ou 104 bits	128 bits (chiffrement) 64 bits (authentification)	128 bits
Taille IV	24 bits	48 bits	48 bits
Clé par paquet	Non (seul l'IV fait varier la suite chiffrante)	Oui	Pas nécessaire
Intégrité de l'en-tête du paquet	Non	SA et DA protégés par Michael	CCM
Intégrité des données du paquet	CRC32	Michael	CCM
Détection des rejeux	Non	Sequencement des IV obligatoire et rejeu impossible	Sequencement des IV obligatoire et rejeu impossible
Gestion des clés	Aucune	IEEE 802.1X	IEEE 802.1X

Figure 9 : Récapitulatif des solutions de chiffrement

II Faiblesses

- **Celles du PSK :**

C'est la solution la plus simple mais elle ne convient qu'aux petits réseaux infrastructure ou les réseaux Ad Hoc.
Ces défauts sont dus aux mots de passe trop court, au partage de la clé avec tous les utilisateurs ce qui diminue la sécurité et le fait que tous les utilisateurs peuvent espionner le trafic des autres et dans le cas où le nombre d'utilisateur est grand, le système devient lourd à gérer.

- **Celles de TKIP :**

Par exemple celle du protocole Michael qui dispose d'un code d'intégrité MIC (Message Integrity Protocol) trop court et donc qui peut être attaquable en quelques heures.

- **Celles d'EAP :**

La sécurité du 802.1x peut être compromise de 3 façons différentes : en attaquant la méthode EAP utilisée (contre la méthode d'authentification il existe l'attaque de dictionnaire en ligne ou hors ligne), en détournant une session après sa création ou encore en s'interposant entre le client et le serveur d'authentification (attaque MiM).

III Solutions

- Celles pour PSK :

Il faut utiliser un mot de passe long, une vingtaine de caractères est recommandé ou au moins une douzaine si c'est des lettres aléatoires et aussi ne pas avoir trop d'utilisateur à gérer sur un même point d'accès.

- Celles pour TKIP :

La contre mesure de Michael est que si un paquet est modifié par un pirate le contrôle d'intégrité Michael le détectera et l'AP sera bloquée pendant 60 secondes. Ceci permet d'éviter qu'un pirate modifie des millions de paquets dans l'espoir que l'un d'entre eux passera le contrôle d'intégrité.

- **Celles pour EAP :**

Il faut créer un tunnel sécurisé, améliorer la validité du certificat (exemple : un par poste) et avoir une bonne sécurité interne du type carte à jeton en utilisant un cryptage puissant du type WPA et WPA2.

IV Types de craquage existant

Les principales failles utilisées pour le craquage sont celle de l'authentification avec le MAC spoofing pour détourner une session, les failles ARP utilisées pour une attaque MiM (Man in the Middle) et les attaques DoS (déni de service).

- **Le MAC Spoofing**

C'est une technique d'attaque qui permet de changer son adresse MAC par une autre pour pouvoir accéder à un routeur ou un serveur qui dispose d'une restriction d'accès par adresse MAC soit en se cachant du réseau soit en usurpant l'identité d'un autre ordinateur.

- **Attaques MiM** (Man in the Middle)

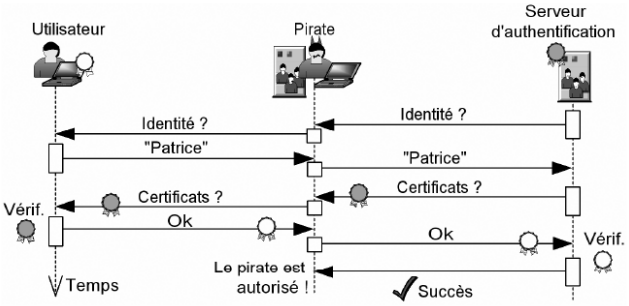

Figure 10 : Exemple d'attaque MiM contre l'authentification EAP

La principale attaque man in the middle consiste à exploiter une faiblesse du protocole ARP (*Address Resolution Protocol*) dont l'objectif est de permettre de retrouver l'adresse IP d'une machine connaissant l'adresse physique (adresse MAC) de sa carte réseau.
L'objectif consiste à s'interposer entre deux machines du réseau et de transmettre à chacune un paquet ARP falsifié indiquant que l'adresse ARP (adresse MAC) de l'autre machine a changé, l'adresse ARP fournie étant celle de l'attaquant.
Les deux machines cibles vont ainsi mettre à jour leur table dynamique appelée Cache ARP. On parle ainsi de « ARP spoofing».
De cette manière, à chaque fois qu'une des deux machines souhaitera communiquer avec la machine distante, les paquets seront envoyés à l'attaquant, qui les transmettra de manière transparente à la machine destinatrice.
Cette attaque fait intervenir trois acteurs : le client, le serveur et l'attaquant. Le but de l'attaquant est de se faire passer pour le client auprès du serveur et de se faire passer pour le serveur auprès du client. Il devient ainsi l'homme du milieu. Cela permet de surveiller tout le trafic réseau entre le client et le serveur, et de le modifier à sa guise pour l'obtention d'informations (mots de passe, accès système, etc.).

- **Attaques DoS**

Le déni de service ou Denial of Service (DoS) est, d'une manière générale, l'attaque qui vise à rendre pendant un temps indéterminé une application informatique tel qu'un serveur incapable de répondre aux requêtes de ses utilisateurs.

Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés.
Les attaques de type DoS peuvent être évitées en repérant l'adresse de la machine hostile, dans le cas d'une attaque à distance, et de bannir celle-ci. Les paquets IP provenant de cette machine seront donc désormais rejetés directement sans être traités.

- **Attaques par dictionnaire** (en ligne et hors ligne)

L'attaque par dictionnaire est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Elle consiste à tester une série de mots de passe potentiels, en utilisant des fichiers externes contenant des phrases, mots, nombres, noms ou citations, les uns à la suite des autres, en espérant que le mot de passe utilisé pour le chiffrement soit contenu dans les dictionnaires.

Ce type d'attaque est très rapide. Un mot de passe mal choisi est vite découvert.

- **Attaques par force brute**

L'attaque par force brute est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons de caractères possibles. Cette méthode de recherche exhaustive ne réussit que dans les cas où le mot de passe cherché est constitué de peu de caractères. Ces programmes tentent toutes les possibilités de mot de passe dans un ordre aléatoire afin de berner les logiciels de sécurité qui empêchent de tenter tous les mots de passe dans l'ordre.

Cette méthode garantit de trouver un mot de passe mais prend du temps.

La solution est d'avoir un mot de passe complexe.

V Test

Le test consiste au craquage du WPA-PSK avec un live cd comprenant des logiciels pour créer du flux sur le point d'accès et sniffer le réseau pour récupérer assez de trames pour pouvoir ensuite à l'aide d'une base de données (dictionnaire,...) trouver le mot de passe. Il existe désormais sur internet des fichiers dictionnaires (payant pour ceux que j'ai trouvé) contenant 15 millions de clés spécifiques au livebox ou encore 20 millions de clés spécifiques au neufbox.

Pour craquer une clé, il faut tout d'abord regarder le réseau disponible, choisir le point d'accès que l'on veut attaquer, ensuite on l'attaque tout en écoutant le réseau et en forçant la déconnexion du client pour capturer le handshake (des trames spécifiques de connexions qui contiennent la clé cryptée) lorsqu'il se reconnecte, puis on compare la clé cryptée récupérée avec un fichier dictionnaire.

Ici, l'interface wifi (caractérisée par le protocole 802.11b/g) est reconnue en tant que wlan0. Il faut la basculer en mode monitor afin d'écouter les réseaux wifi.

Figure 11 : Mode monitor de l'interface WiFi

Airodump-ng permet d'écouter les réseaux wifi et éventuellement d'enregistrer les paquets dans un fichier de capture.

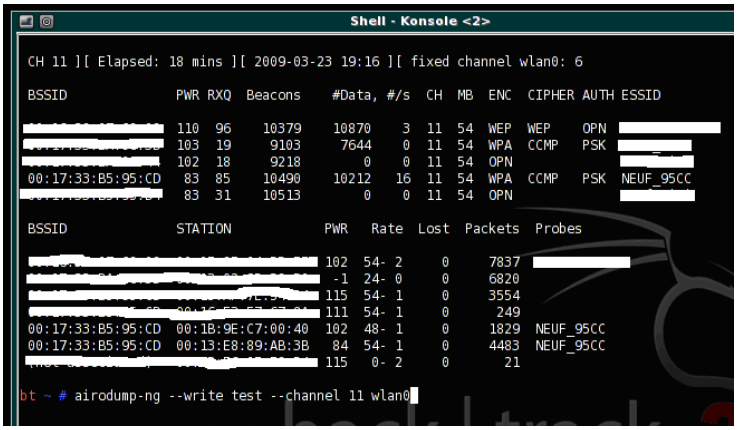

Figure 12 : Ecoute de tout le réseau

Ici, airodump-ng a écouté tous les canaux, et a affiché les points d'accès utilisant le cryptage WPA, sans écrire de fichier de capture.

Maintenant je cible mon point d'accès émettant sur le canal 11 en écrivant les paquets capturés dans un fichier nommé out-01.cap.

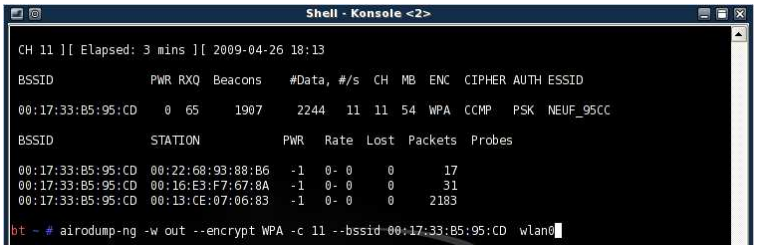

Figure 13 : Ecoute du réseau de ma box

Il y a 3 stations connectées.

Pour réussir un crack wpa, il est primordial qu'une station soit connectée, en effet le **four-way handshake** est nécessaire au crack car c'est un ensemble de paquets émis par le point d'accès et la station lorsque celle ci se connecte et il ne peut être capturé que si une station est connectée au point d'accès.
Une méthode de crack (méthode passive) consiste à cibler un point d'accès, et à écouter le réseau pendant des heures en attendant qu'un client se connecte.
Une autre méthode consiste à utiliser aireplay-ng et son attaque -0 (désauthentication) pour forcer la déconnexion du client et capturer le handshake lorsqu'il se reconnecte (le gestionnaire de réseau wifi de windows est reglé par défaut pour se reconnecter automatiquement à un point d'accès en cas de déconnexion, l'attaque -0 exploite cette faille).
Pour réaliser la dernière méthode il faut ouvrir 2 nouveaux shells avec dans le premier, une commande aireplay-ng pour envoyer des requêtes de désauthentification à la station et dans le second, une commande aireplay-ng pour envoyer des requêtes de désauthentification au point d'accès.

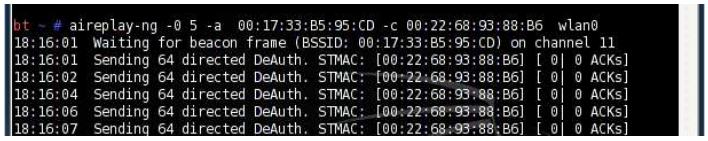

Figure 14 : Attaque sur la station

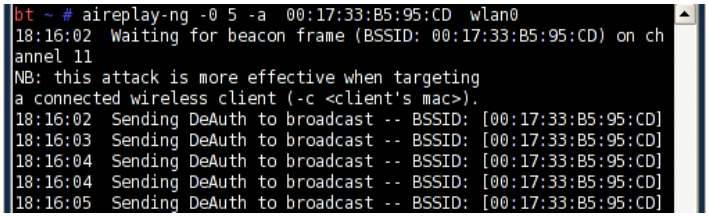

Figure 15 : Attaque sur le point d'accès

Si l'attaque a réussi, le WPA handshake devrait apparaitre en haut à droite de la fenêtre du shell airodump-ng.

Selon la qualité de la réception, la capture du handshake peut etre immédiate, ou très fastidieuse. Il se peut qu'il faille renouveler les attaques à de nombreuses reprises avant d'obtenir le tant attendu handshake.

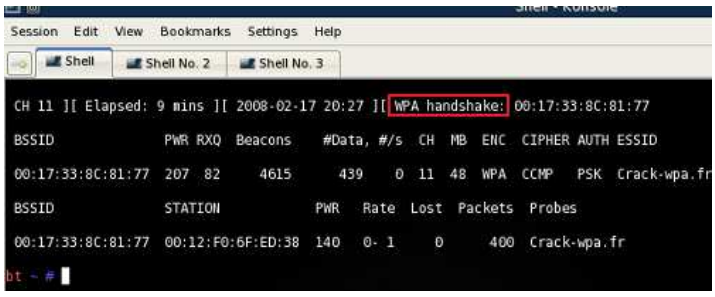

Figure 16 : Handshake récupéré, image d'un tutorial

Le crack peut commencer, il se lance avec la commande suivante:

aircrack-ng -w nom-du-fichier-dictionnaire nom-du-fichier-de-capture
Le crack se lance, aircrack-ng va tester tous les mots de passe contenus dans le fichier dictionnaire.

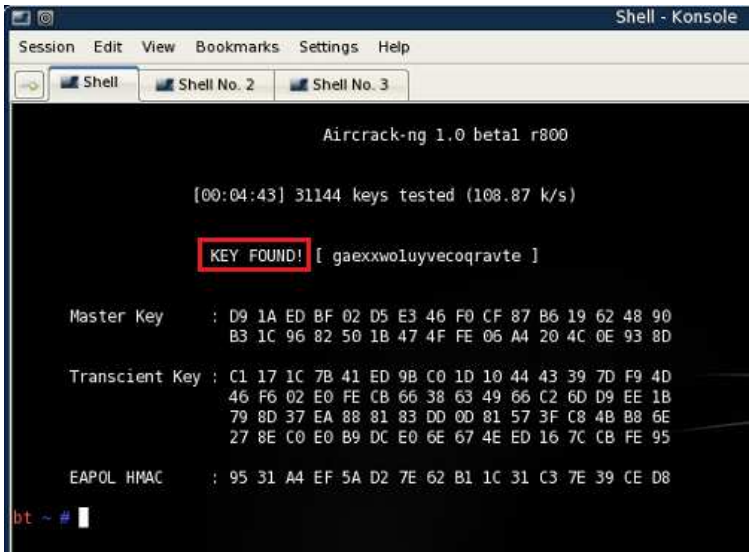

Figure 17 : Craquage de la clé WPA à l'aide d'un dictionnaire, image d'un tutorial

La clé WPA a donc bien été craquée mais à l'aide d'une bonne réception, d'un bon fichier dictionnaire et d'un mot de passe sans caractères aléatoires.

VI Conclusion

Ce projet m'a permit d'en apprendre plus sur le fonctionnement du WPA que ce soit au niveau des différents types qu'au niveau de ses éléments (cryptages, protocoles, authentification,…) et sur les différentes étapes de connexion surtout au niveau de la négociation des clés.
Mon test de craquage, n'a pas aboutit, je n'ai pas pu récupérer le WPA handshake malgré mes nombreuses attaques et le fait que mon point d'accès était à moins d'un mètre de mon ordinateur. Comme quoi il n'est pas si aisé que ça de craquer une clé WPA, encore faut il aussi avoir un bon dictionnaire pour la retrouver.

La clé WPA est donc un bon mécanisme pour sécuriser les réseaux, en particulier le WPA2 malgré le fait que la WPA-PSK semble déjà craquable d'après les tutoriaux sur internet. La meilleure solution reste d'utiliser une bonne sécurisation du réseau grâce à WPA et WPA2 et surtout à avoir un mot de passe complexe.

Il m'a également appris à effectuer de la recherche documentaire avec plus de précision et de qualité, que se soit en anglais, le plus souvent, ou en français, bien que j'ai trouvé dès le début un livre à la bibliothèque qui était vraiment très bien fait.

BIBLIO

Documents papier et powerpoint :

- WIFI Déploiement et Sécurité : La Qos et le WPA livre par Aurélien Géron (2006)
- Analysis and Countermeasure on Vulnerability of WPA Key Exchange Mechanism (2004) (documents récupérés à M. GERARD YVES)
- WPA / WPA2 : Une sécurité fiable pour le Wi-Fi ? Présentation powerpoint réalisée par le Groupe Sécurité Unix et Réseau (14 Juin 2005)
- Wi-Fi CERTIFIED for Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi Networks, pdf par Wi-Fi Alliance(2007, 2008, 2009)
- Faille dans le protocole WPA-WPA2, pdf par Gentoo-Québec.org, Sylvain Alain (février 2009)

Site

- www.wi-fi.org : Site officiel de l'Alliance Wi-Fi
- http://www.crack-wpa.fr/tutoriel-crack-wpa.php : Tutoriel pour le craquage de WPA-PSK par attaque de dictionnaire avec un livecd
- http://fr.wikipedia.org/wiki/Wi-Fi_Protected_Access : Page wikipedia sur la protection des réseaux Wi-fi. J'ai aussi lu d'autres pages wikipédia concernant les protocoles utilisés par le WPA et les attaques.
- http://www.itworld.com/security/57285/once-thought-safe-wpa-wi-fi-encryption-cracked : Article sur une conférence de novembre 2008 montrant des faiblesses du WPA
- www.commentcamarche.net/contents/wifi/wifi-wpa.php3 : Page du site comment ça marche sur le WPA, j'ai aussi lu d'autres pages du site concernant les protocoles utilisés pas le WPA et les attaques.
- http://www.linux-france.org/prj/inetdoc/securite/tutoriel/tutoriel.securite : publication inetdoc.LINUX