The HACKADEMY SCHOOL
100% white hat hacking

COURS SECURITE WIFI

Important

Ce polycopié de cours de The Hackademy a pour objectif de contribuer à une meilleure compréhension des risques de sécurité liés à l'usage de l'outil informatique, et ainsi, permettre de s'en protéger plus efficacement. Il sera utile aux administrateurs système et réseau, aux développeurs, et à tout professionnel travaillant avec Internet. Si vous êtes soucieux de comprendre comment un pirate pourrait tenter de vous attaquer afin d'être à même de déjouer ses tentatives, ce cours vous est destiné. Cependant aucune garantie n'est donnée que ce contenu va vous permettre de vous protéger de manière totale, mais vous donnera les éléments pour mettre en place une politique de management sécurité efficace. De plus, ce cours ne peut avoir pour vocation de couvrir l'ensemble des sujets liés à la sécurité de manière exhaustive : nous vous détaillons les méthodes d'attaque courantes, et vous fournissons les éléments pour vous en protéger.

The Hackademy et DMP ne sauraient être tenus pour responsable des dommages éventuels causés par une application des méthodes présentées ici sur un système.

Il est formellement interdit par la loi d'appliquer les techniques d'attaque présentées dans cette formation sur un système que vous ne possédez pas. Vous pouvez cependant les appliquer sur vos systèmes informatiques à des fins de tests de vulnérabilité, en gardant à l'esprit que cela représente toujours des risques pour la stabilité des systèmes audités.

Avertissement

Il est essentiel de comprendre que si ces méthodes sont ici présentées, c'est avant tout dans une optique de compréhension générale de la sécurité et des moyens mis en oeuvre par les pirates, et ce dans le seul et unique but, de pouvoir lutter contre ce danger.

De plus, ces méthodes de protection s'appliquent autant aux entreprises qu'aux particuliers. En effet, en dehors du nombre de documents privés que vous possédez sur votre ordinateur, un éventuel pirate pourrait vouloir se servir de votre système comme d'une passerelle dans le but de ne pas être retrouvé. Dans ce cas, se serait à vous, en tant que personne physique ou morale, de prouver votre innocence. De plus, une politique de sécurité convenable est de réinstaller entièrement votre système en cas de piratage, avec la perte de temps et de finance que cela implique.

Auteurs

Nous tenons à remercier pour leur participation à l'élaboration de cette formation et à l'écriture de ce cours :

- **CrashFr** (crashfr@thehackademy.net)

SOMMAIRE

Chapitre 5 : Attaques

1. Détection des réseaux WiFi
2. Sniffing réseau
3. Falsification d'adresse MAC
4. Mapping réseau
5. Cracking WEP
   A) Attaque passive
   B) Attaque active
8. Cracking WPA
9. Hijhacking
10. D.O.S

Chapitre 6 : Sécurisation

1. Portée du point d'accès
2. Desactivation SSID
3. Filtrage d'adresses MAC
4. Cryptage des données
   A) 802.1x
   B) WPA
   C) WPA2
   D) VPN
5. Leurre AP
6. Portail captif

INTRODUCTION

INTRODUCTION AUX RÉSEAUX SANS FIL

Le premier réseau commercial sans-fil a vu le jour en 1982 aux États-Unis, en France il faut attendre 1986 pour que France Telecom unique opérateur téléphonique à l'époque mette en place un réseau sans fil. Le Wireless est arrivé sur le marché grand public il y a peu de temps, il existe différentes normes pour différentes utilisations. Les réseaux sans fil se développent rapidement dans les entreprises et chez les particuliers sans tenir compte des risques que cela peut engendrer. Car comme n'importe quel réseau, un réseau sans fil est une source potentielle de piratage. Particulièrement les réseaux sans fil qui font transiter les paquets d'informations par l'air contrairement aux réseaux câblés qui utilisent un support matériel (câbles). Les réseaux sans fil restent quand même une solution très économique et simple à mettre en oeuvre, mais encore faut il correctement le configurer pour éviter de se faire pirater. Ce cours devrait vous permettre de mettre en place un réseau sans fil tout en connaissant les dangers qui pourraient se présenter suivant la configuration de celui-ci.

CHAPITRE I

LES NORMES

1. Résumé des normes

La plupart des normes qui nous intéressent (famille 802.11) sont développées par l'association IEEE (http://grouper.ieee.org/). Ces normes sont acceptées ou non pour une utilisation en France par l'ART (http://www.art-telecom.fr/).

- WLAN (Wireless Local Area Networks) : IEEE 802.11, Hiperlan
- WPAN (Wireless Personal Area Network) : Bluetooth
- WMAN (Wireless Metropole Area Network) : IEEE 802.16
- GSM et UMTS : Téléphones cellulaires

2. Les différentes normes

A) Bluetooth (802.15)

Cette norme permet la communication à travers des ondes radios de différents appareils électroniques (mobiles, ordinateurs portables et maisons...). Cette norme a une portée de base de 10 à 30 mètres et un débit de 1Mbps (la version 2 de bluebooth devrait atteindre de 2 à 10Mbps).

B) WiMax (802.16)

Cette norme, validée par le IEEE en 2001 et développée par le « consortium WiMax forum » permet en théorie avec le 802.16a, un débit maximum de 70 mégabits par seconde sur une portée de 50 km. En pratique, cela permet d'atteindre 12 mégabits par seconde sur une portée de 20 km. Pour le moment, le WiMax permet de mettre en place des réseaux point à point et devrait très prochainement se mettre à la mobilité avec le 802.16e. WiMax (Worldwide Interoperability for Microwave Access) est le nom commercial pour cette norme qui n'a pas encore fait ses preuves...

C) Hiperlan

Cette norme propose un débit de 23,5Mbps sur 50 mètres (pour la version 1) et 54Mbps sur 100 mètres (pour la version 2). Cette norme est la concurrente de la norme 802.11a qui fonctionne dans la même bande de fréquence (5 Ghz). L'Hyperlan a certains avantages techniques par rapport à la norme 802.11a mais est apparue après sur le marché.

D) WiFi (802.11)

802.11b

C'est l'extension qui nous intéresse le plus car c'est la plus appropriée et la plus utilisée pour les réseaux privés locaux en France s'étendant à 100 mètres de portée environ. Le 802.11b utilise des fréquences de 2,4Ghz et par conséquence autorise des débits allant jusqu'à 11Mbps (en théorie) et plus suivant les technologies constructeurs. De nos jours, les données peuvent être cryptées en 64, 128 ou 256 bits

grâce au WEP (Wired Equivalent Privacy) pour que les informations qui transitent par le réseau ne puissent être lues avec un simple outil informatique (sniffer). En France, le 802.11b est autorisé dans un cadre et un lieu privé, mais est interdit dans le domaine du public (lieux publics : rue...) mais l'ART a changé sa politique le 7 octobre 2002 et a autorisé l'utilisation du 802.11b dans les lieux publics à titre expérimental et gratuit grâce à des licences attribuées sur une période de 3 ans donc si vous êtes une association et que vous voulez développer un réseau sans fil dans votre ville, déposez votre dossier pour en avoir l'autorisation. Le 802.11b permet d'avoir un vitesse raisonable et cette norme est peu coûteuse.

802.11a

Cette norme fonctionne dans la bande de fréquence des 5 Ghz et peut atteindre un débit maximum de 54 Mbps. Ce qui rend l'extension 802.11a beaucoup plus rapide que l'extension 802.11b. Du fait, que cette norme ai été approuvée en 1999, elle est beaucoup moins utilisée que la norme 802.11b mais cela devrait changer dans les prochaines années à venir... Dans le commerce cette norme est appelée: Wi-Fi5 et commence à voir le jour en France car l'ART l'autorise depuis peu en intérieur.

802.11g

Extension à haut débit (54 Mbps) dans la bande des 2,4 Ghz. C'est donc une extension de la norme 802.11b. C'est d'ailleurs pour cela que les points d'accès 802.11g dans le commerce sont compatibles avec les cartes 802.11b.

Il existe aussi plusieurs groupes techniques chargés d'améliorer la norme 802.11 :

Note :

- 802.11e : amélioration de la prise en compte par la norme 802.11 de la qualité de service
- 802.11f : standardisation des protocoles entre points d'accès
- 802.11h : gestion du spectre pour la norme 802.11a
- 802.11i : amélioration des fonctions de sécurité
- 802.11n : amélioration des performances au niveau de la couche MAC

4. Qu'est-ce que le Wi-Fi ?

Le Wi-Fi est établi par le WECA (Wireless Ethernet Compatibility Alliance) qui a pour but d'assurer l'interopérabilité des produits 802.11 et de promouvoir cette technologie. Pour obtenir la certification Wi-fi, un constructeur doit passer un test d'interopérabilité auprès du WECA. Une fois le test passé avec succès, le constructeur peut utiliser le logo Wi-fi comme une sorte de marque. Le Wi-Fi regroupe tout le matériel 802.11a, b, g.

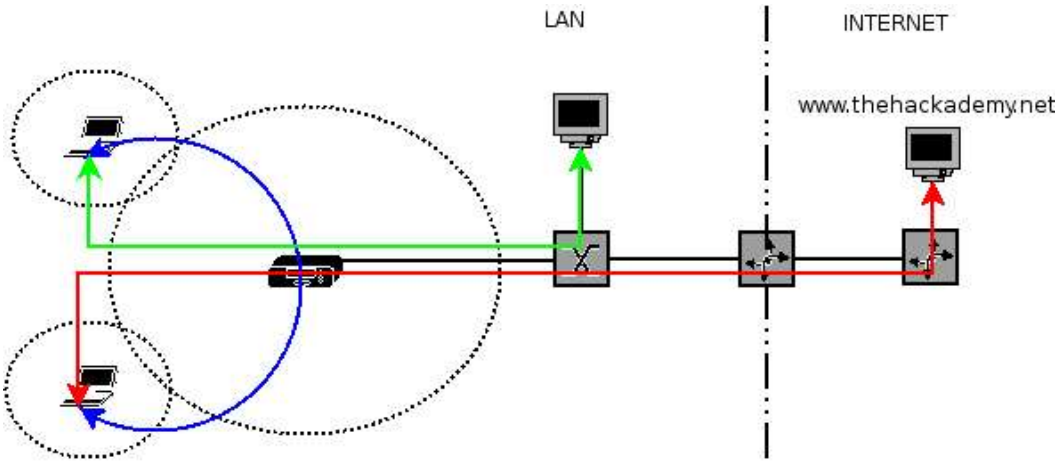
Lorsqu'un matériel a été certifié Wi-Fi, il doit avoir un logo comme celui-ci :

CHAPITRE II

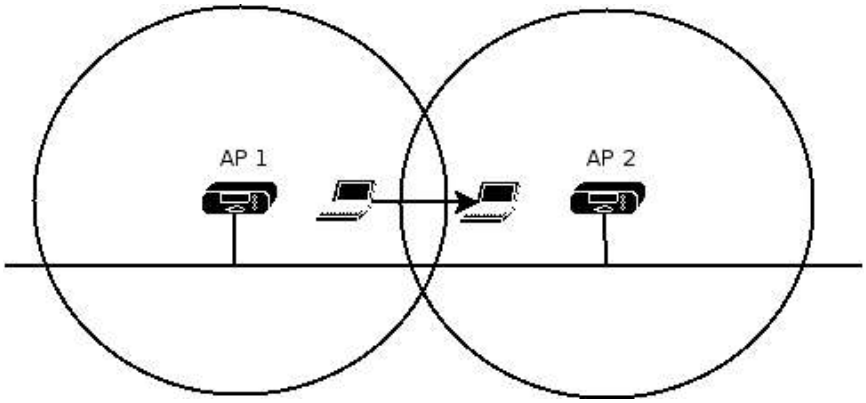
LE MATERIEL

1. Les points d'accès

Il existe différents matériels sur le commerce permettant de construire son propre réseau Wi-fi. Suivant la structure que vous choisirez, vous aurez besoin ou pas de ce que l'on appelle un "point d'accès", "Access Point" ou "AP". Dans une structure à point d'accès (Insfrastructure), le point d'accès a pour rôle de transmettre les différentes requêtes entre les clients du réseau sans fil, mais le point d'accès est aussi et avant tout une sorte de pont entre le réseau câblé et le réseau sans fil. Ce qui permet aux clients Wi-Fi d'accéder au réseau câblé via un hub, switch, passerelle pour utiliser la connexion internet, sachant que certains AP ont aussi la fonction de routeur donc directement connecté au web. Le réseau câblé sera donc connecté sur le port RJ45 de l'AP et les clients du réseau sans fil, utiliseront les antennes de l'AP (ondes hertziennes) pour communiquer avec le réseau câblé ou entre eux.



Les clients peuvent passer d'AP en AP s'il en existe plusieurs de connectés sur la même branche du réseau câblé, sans quitter le réseau (roaming), permettant ainsi de créer des réseaux sans fil très étendus. Ainsi un client peut passer de l'AP1 à l'AP2 si les 2 ont le même SSID et émettent sur le même canal :



Voici un point d'accès bon marché parmi tant d'autres :

Il coûte environ 100 euros et se connecte via Ethernet à votre réseau local. Son bas prix est dû au fait qu'il ne supporte que le 802.11b et que depuis quelques mois on voit apparaître les points d'accès 802.11g dans le commerce.

2. Les cartes

Ensuite il faut équiper les PC qui serviront de clients avec des cartes PCMIA pour les portables, PCI ou USB pour les PC fixe. Ces cartes peuvent être comparées à des cartes ethernet dans un réseau câblé.

Voici une carte PCMCIA pour ordinateur portable :

Cette carte coûte environ 35 euros, compatible 802.11b, débit théorique de 11Mbps, WEP, supportée sous Linux et Windows. Je vous conseille tout de même une carte Orinoco (802.11b) ou autre carte permettant de connecter une antenne externe si vous désirez faire ce que l'on appelle du War-driving.

Pour mettre une carte PCMCIA sur votre PC fixe vous devrez acheter un adaptateur. Il faut faire attention en achetant l'adaptateur PCI car il est propre à chaque carte PCMCIA. Vous ne pourrez pas faire fonctionner votre carte Orinoco en utilisant l'adaptateur PCI Belkin par exemple. Vous pouvez aussi trouver à la place de la carte PCMCIA et son adaptateur, une carte PCI en un seul bloc :

ou une carte externe utilisant le port USB :

Je vous conseille tout de même l'adaptateur PCI avec la carte PCMCIA si jamais vous avez besoin d'utiliser la carte sur un ordinateur portable.

3. Les antennes

Il existe différents types d'antennes. Pour permettre l'utilisation d'une antenne, il vous faudra absolument une carte ayant un connecteur externe comme sur les cartes Orinoco, où viendra se fixer le pigtail. Ci-dessous le connecteur externe d'une carte Orinoco.

Antenne Omnidirectionnel :

Cette antenne permet de capter les différents réseaux se trouvant aux alentours sur une surface formant un cercle ayant comme centre la tige de l'antenne.

Une antenne directionnelle :

L'antenne directionnelle, comme son nom l'indique doit être pointée vers la direction où l'on désire émettre ou recevoir. Cette antenne permet d'avoir une réception plus élevée qu'une antenne omnidirectionnelle, elle sera utilisée pour cibler un réseau particulier.

Il existe d'autres types d'antennes que vous pourrez fabriquer vous même :
http://wireless-fr.org/contributions/antenne-yagi/Antenne-directionnelle.html

Pour acheter des antennes déjà montées :
http://www.fab-corp.com/

Pour ces 2 antennes, il vous faudra ce que l'on appelle un pigtail. Le pigtail, est tout simplement un adaptateur "sortie antenne externe / connecteur antenne de la carte PCMCIA" qui est propre à chaque constructeur de carte. Voici un pigtail Orinoco :

4. Les amplificateurs

Les amplificateurs sont malheureusement interdits en France... Ces amplis permettent d'amplifier le signal en sortie de votre antenne. Les amplis sont très utilisés pour le hijhacking.

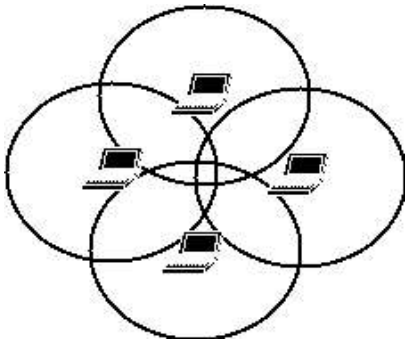
CHAPITRE III

LES MODES

Chaque carte peut fonctionner en plusieurs modes, en général 2 (Ad-Hoc, Infrastructure) mais nous verrons qu'en faisant fonctionner une carte comme un accès point, nous pourrons utiliser d'autres modes.

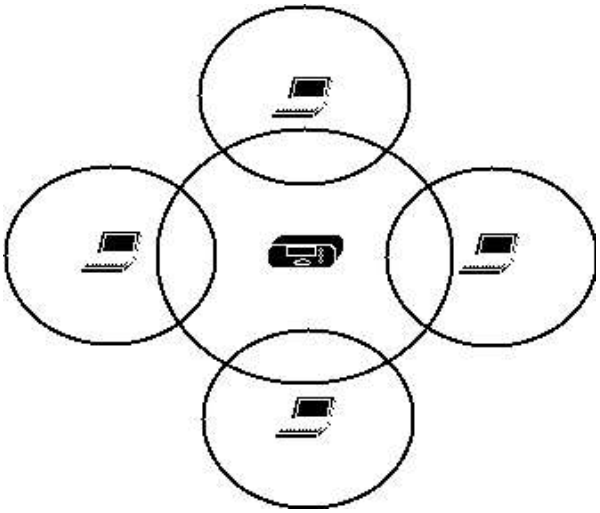
1. Le mode Ad-Hoc (peertopeer)

Ce mode est utilisé dans le cas ou l'on désire construire un petit réseau sans point d'accès. Le seul inconvénient de ce type de réseau c'est sa faible étendue car toutes les machines munies de cartes doivent être à la portée de toutes les autres.



2. Le mode Infrastructure (managed)

Ce mode permet à une machine équipée d'une carte Wi-Fi de communiquer sur un réseau équipé d'un point d'accès qui aura pour rôle de faire transiter les informations entre les différents clients du réseau sans fil. Cette structure a une étendue plus large que la structure Ad-Hoc car il suffit à chaque client d'être à la portée du point d'accès et non pas, de tous les clients car les informations transitent toutes par le point d'accès avant d'être renvoyées vers le client destinataire.



3. Le mode Monitor

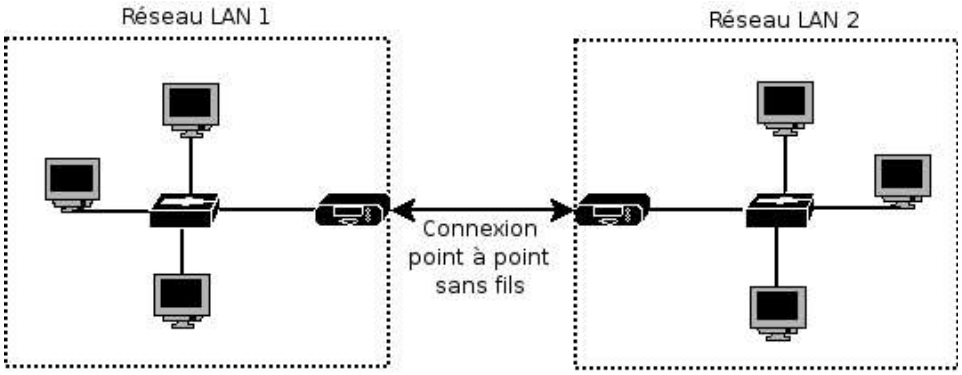
Ce mode est identique au mode promiscious d'une carte ethernet. Il va permettre d'intercepter tous les paquets transitant dans l'air qui ne sont pas forcément à destination de notre machine. Pour activer ce mode, il faudra en général appliquer un patch au pilote de votre carte WiFi.

4. Le mode Master

Ce mode désigne le mode de fonctionnement d'un point d'accès. Nous allons voir à la suite du cours que sous Linux nous aurons la possibilité de transformer une carte PCMCIA en point d'accès avec certains modules / pilotes.

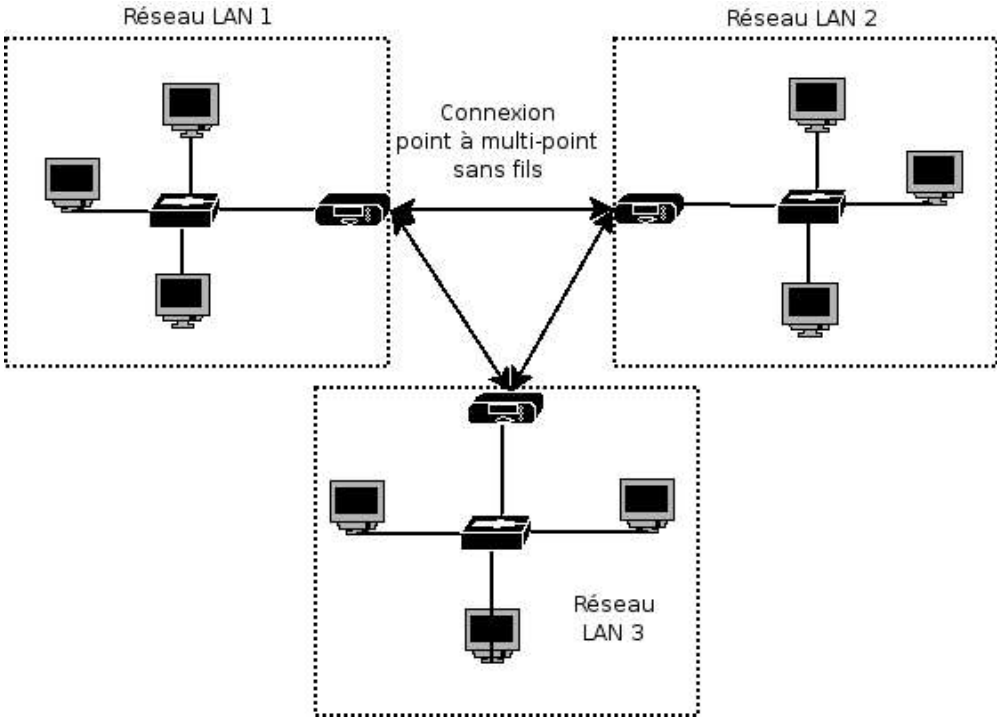
5. Le mode Point to Point

Ce mode permet à 2 points d'accès de créer une connexion réseau point à point. Lorsqu'un point d'accès est en mode « point to point » il ne communique qu'avec un seul autre point d'accès ayant une adresse MAC bien précise, donc aucun client ne peut se connecter sur un point d'accès en mode « point to point ». Ce mode est très couramment utilisé pour relier 2 réseaux filaires d'un bâtiment à un autre d'une même entreprise.



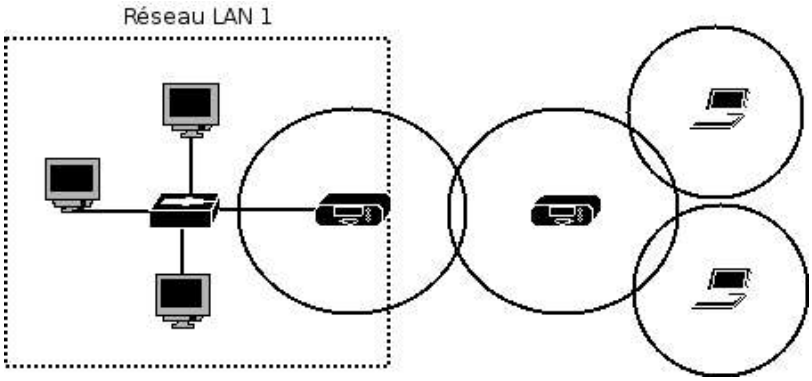
6. Le mode Point to MultiPoint

Ce mode est identique au mode « point to point » à la seule différence qu'au lieu de transmettre les paquets vers un seul point d'accès, il peut communiquer avec plusieurs points d'accès en même temps.



7. Le mode Repeater

Ce mode permet à un point d'accès de transmettre les communications provenant des clients vers un autre point d'accès au lieu de les transmettre vers le réseau câblé. Donc un point d'accès en mode repeater n'a pas besoin d'être connecté au réseau local via un câble RJ45.

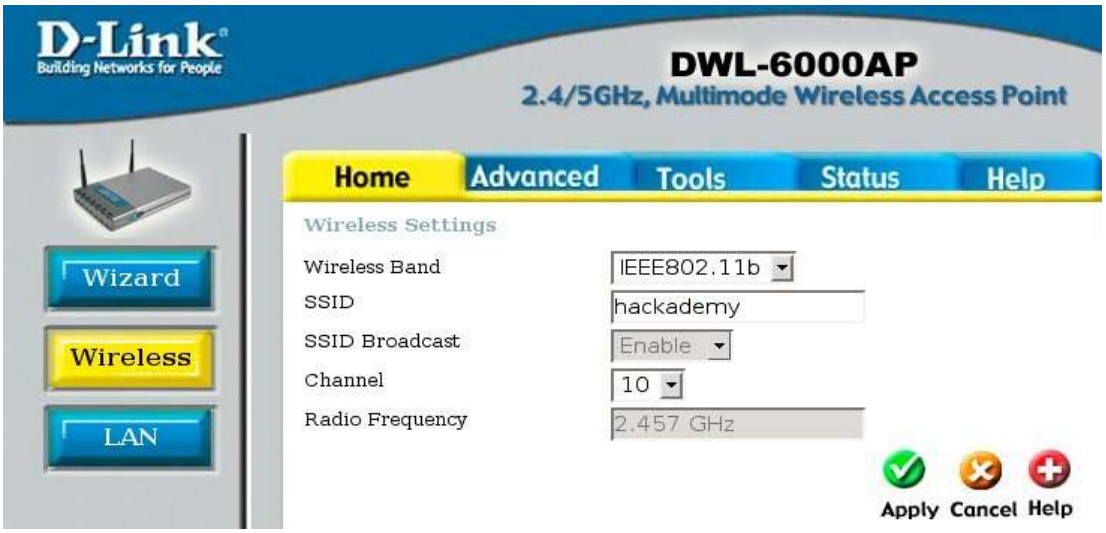


CHAPITRE IV

INSTALLATION

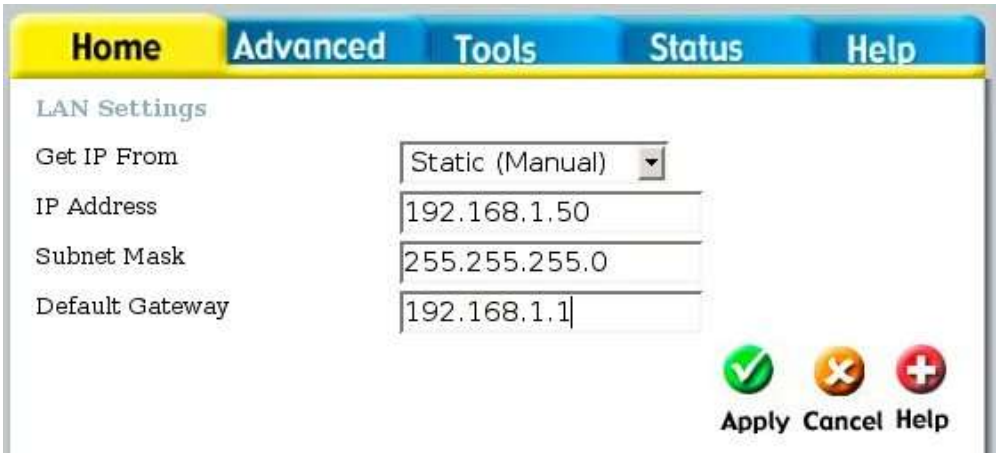
1. Configuration d'un point d'accès

La majorité des points d'accès sont configurables à partir d'un panneau HTTP sur le port 80 (ou via Telnet), il vous suffit donc de vous connecter avec notre navigateur sur son adresse IP par défaut. Nous prendrons comme exemple un D-link. La première chose à configurer est le SSID et le canal sur lequel notre AP fonctionnera du côté sans fil :

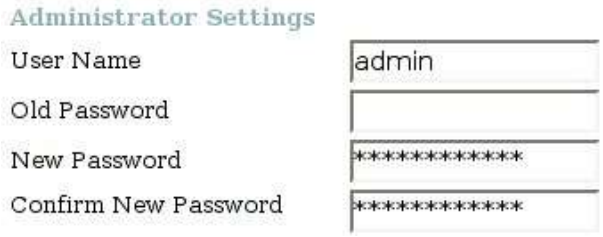


En effet, chaque réseau sans fil de type 802.11 est associé à un SSID (Service Set Identifier) et à un canal qui lui permet de se différencier des autres et qui permet ainsi d'avoir dans la même zone plusieurs réseaux sans fil. Suivant le pays ou vous vous trouvez, vous aurez accès à plus au moins de canaux suivant la norme utilisée (14 canaux au total, 4 autorisés en France de 10 à 13 pour le 802.11b et g).

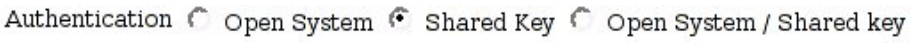
Il va falloir maintenant configurer le côté LAN (filaire) de notre AP. Si vous possédez un serveur DHCP vous pouvez demander à votre AP de récupérer une IP auprès de celui-ci. Dans le cas contraire, vous devrez lui fixer une adresse IP fixe comme ci-desous :



Ensuite vous pouvez modifier le login / password par défaut pour éviter que quelqu'un du réseau s'amuse à modifier la configuration de votre point d'accès :

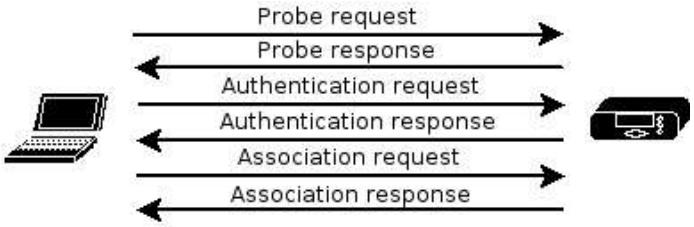


Dans un premier temps, enregistrez vos paramètres et essayez de vous connecter dessus avec un de vos clients Wi-Fi. Si la connection s'éffectue correctement vous pouvez essayer d'activer le WEP pour encrypter les données transistant entre les clients et le point d'accès. Un point d'accès peut utiliser 2 authentifications différentes par défaut pour autoriser ou non un client à se connecter au réseau :



Avant d'étudier en détail ces 2 méthodes, voici comment un client communique avec un point d'accès :

1. Le client envoie en broadcast des requêtes de sonde (probe request) sur chacun des canaux.
2. Le point d'accès répond aux requêtes sonde qu'il reçoit sur son canal par une réponse sonde (probe response).
3. Le client vérifie grâce à la réponse sonde renvoyée par les AP, quel est celui qui à le meilleur signal et lui envoie une requête d'authentification (authentication request).
4. Le point d'accès lui renvoie une réponse d'authentification (authentication response).
5. Si l'authentification s'est correctement déroulée, le client envoie une requête d'association (association request).
6. Le point d'accès répond par une réponse d'association (association response).
7. Le client peut désormais envoyer des données vers le point d'accès.



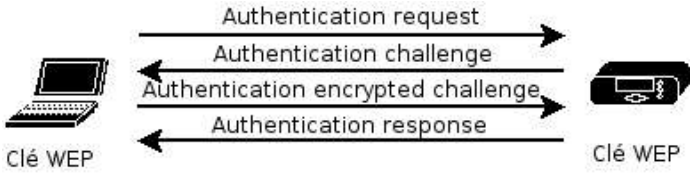
Les requêtes sonde permettent au client de connaître les différents points d'accès disponibles pour le SSID recherché et la vitesse de transmission qu'il supporte. En général, les points d'accès envoient ce que l'on appelle des « Beacon Frames » qui indiquent au client qu'un point d'accès ayant un SSID est disponible dans la zone dans laquelle il se trouve. Mais certains points d'accès permettent de désactiver l'envoi du SSID, c'est pour cela que les clients envoient des requêtes sonde.

Une fois le point d'accès optimal trouvé, le client essaye de s'authentifier auprès de celui-ci.

Comme nous l'avons dit plus haut, la première méthode d'authentification est l'authentification ouverte. Lorsque le point d'accès utilise cette méthode, il n'attend qu'une requête d'authentification avec le bon SSID et rien d'autre. C'est-à-dire, que le point d'accès n'a aucun moyen de vérifier si ce client à réellement le droit d'accéder au réseau ou pas, il suffit juste que le client ait le bon SSID pour être authentifié. Si le WEP est activé en utilisant cette méthode et que le client n'a pas la bonne clé WEP, ses données ne seront pas transmises.

Le seconde méthode, qui est l'authentification à clé partagée oblige le client à spécifier une clé WEP statique qui sera identique à celle spécifiée au niveau du point d'accès. Voici comment se déroule la phase d'authentification avec une clé partagée :

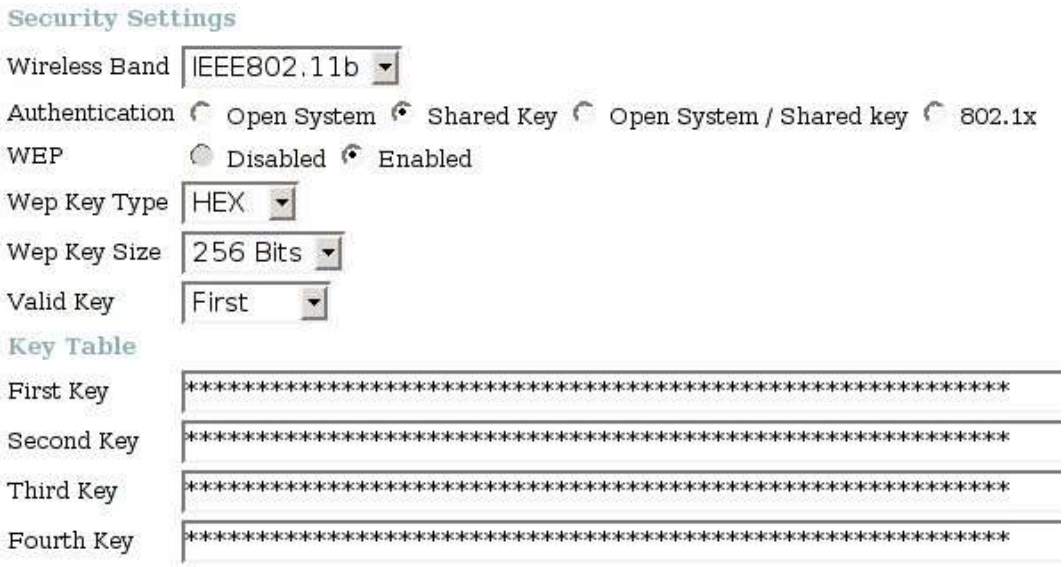
1. Le client envoie une requête d'authentification à clé partagée
2. Le point d'accès renvoie un challenge sous forme de texte en clair
3. Le client encrypte le challenge au format texte avec sa propre clé WEP et renvoie le résultat au point d'accès.
4. Le point d'accès va alors décrypter le message et le comparer à sa version en clair. Si cela correspond, c'est-à-dire que le client à la même clé que le point d'accès, le point d'accès renvoie une réponse valide au client lui permettant d'accèder au réseau.



Le problème avec cette méthode d'authentification, c'est qu'un pirate pourrait sniffer le challenge et sa version encryptée et donc, en déduire le KeyStream que nous verrons dans la chapitre dédié aux attaques sur le protocole WEP. Lorsque vous activez le WEP vous pourrez prédéfinir 4 clés soit sous un format ASCII ou hexadécimal.

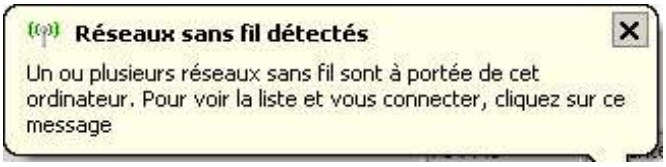
Une clé héxadécimale 64 bits est composée de 10 caractères.
Une clé hexadécimale 128 bits est composée de 26 caractères.
Une clé hexadécimale 256 bits est composée de 58 caractères.

Nous verrons dans le chapitre consacré au WEP que les clé sont en réalité composé de la clé hexadecimal + un vecteur d'initialisation de 24 bits.

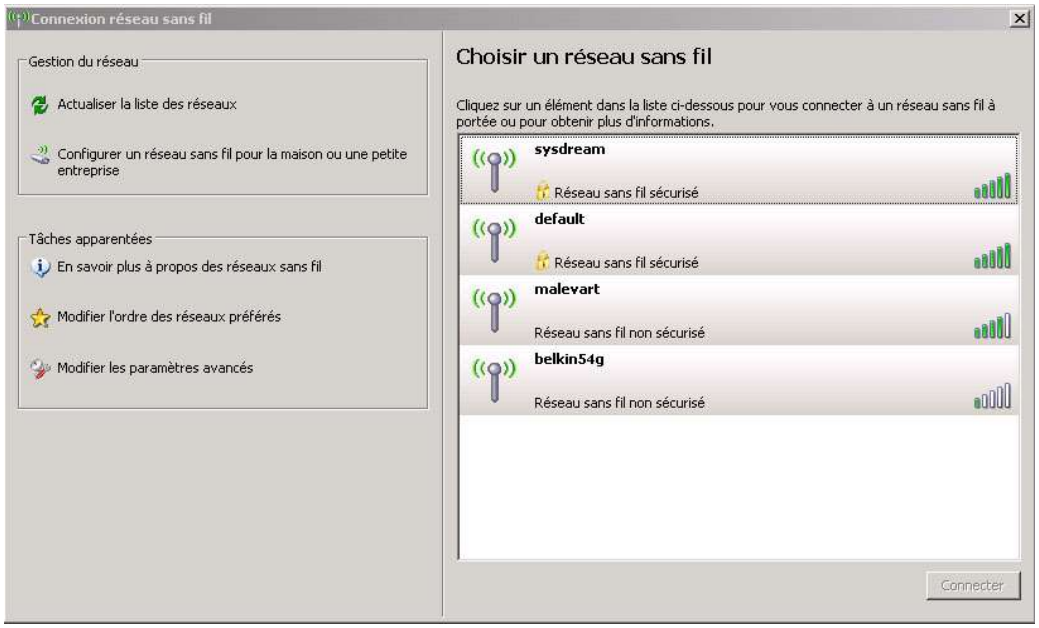


2. Installation sous Windows (XP)

Le wireless est très bien intégré dans XP. Tout d'abord, il faut installer les pilotes livrés avec votre carte Wi-Fi. Une fois cela fait, XP s'occupera de gérer les connexions sans fil à la place du client fourni avec votre carte. Si un ou des réseaux sont à votre portés, il devrait vous afficher un petit panneau d'alerte :

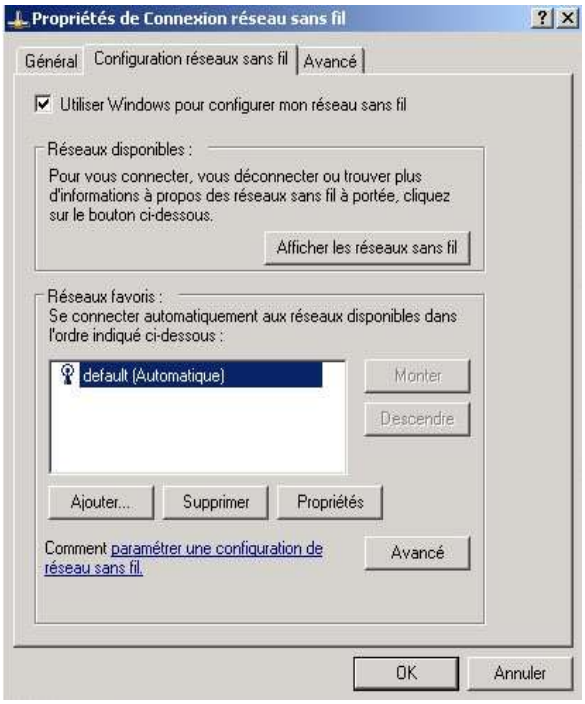


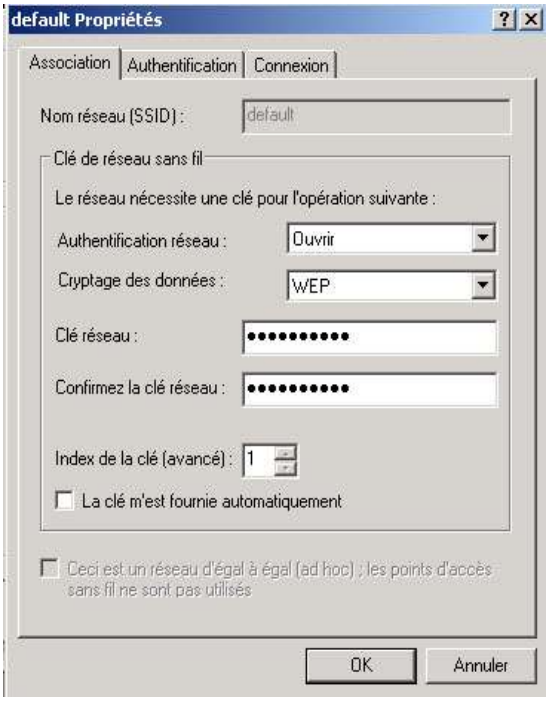
En cliquant sur cette alerte, il devrait vous afficher tous les réseaux disponibles (sous XP avec le SP2) :



Les réseaux avec un petit cadenas indique que le réseau utilise le WEP. Dans ce cas, la clé vous sera demandée à la sélection du réseau. XP gère le wifi avec une liste de réseaux préférés. C'est-à-dire que votre machine se connectera en priorité à ces réseaux par ordre de préférence. Vous pourrez modifier cet ordre en cliquant sur « Modifier l'ordre des réseaux préférés ».

Si vous désirez vous connecter à un nouveau réseau, sélectionnez le sur la partie de droite du panneau et cliquez sur « modifier les paramètres avancés ».





Dans les paramètres avancés vous pourrez configurer le type d'authentification, activer ou non le cryptage et la clé WEP. Si vous utilisez le 802.1x (Chapitre Sécurisation) vous devrez cocher la case « la clé m'est fournie automatiquement ». N'oubliez pas aussi, de modifier les paramètres TCP/IP de votre carte Wi-Fi pour qu'ils correspondent au réseau auquel vous désirez vous connecter.

3. Installation sous Linux (Debian)

Si vous désirez monter un réseau sous linux je vous conseille de contacter le fournisseur afin de savoir si le matériel est supporté. Il existe plusieurs manières pour installer une carte Wi-fi sous Linux, dans ce cours je décrirais l'installation d'une carte Orinoco et d'une carte à base de chipset Prism2 (avec la possibilité d'activer le mode monitor). Pour installer correctement une carte wireless PCMCIA il faut commencer par une recompilation de votre noyau. Les options indispensables à activer dans son kernel sont les suivantes :

- chargement de modules. Activez les 3 options qui se trouvent dans "Loadable module support"
- le support pour le wireless. Activez l'option "Wireless LAN (non-hamradio)" qui se trouve dans "Network device support --> Wireless LAN (non-hamradio)". N'activez pas les pilotes se trouvant en

dessous car il seront inclus dans pcmcia-cs (paquetage PCMCIA externe).
- le support PCMCIA. Désactivez les options "PCMCIA/Carbus support" et "Cardbus support (NEW)" se trouvant dans "General Setup --> PCMCIA/Carbus support".

Sauvegardez votre configuration et recompilez votre noyau.

Maintenant nous allons installer "pcmcia-cs" qui est un module permettant de détecter les différentes cartes insérées dans un de nos ports PCMCIA et de charger le bon pilote correspondant à la carte insérée.

pcmcia-cs-3.2.1.tar.gz --> http://sourceforge.net/projects/pcmcia-cs
patch orinoco (pcmcia-cs-3.2.1-orinoco-patch.diff)--> http://airsnort.shmoo.com/orinocoinfo.html

Ce patch est très utile, car il permet d'activer le mode monitor de la carte Orinoco. Ce mode monitor permet de capturer tous les paquets 802.11 sans association au réseau cible. Si vous n'activez pas le mode monitor, vous ne pourrez pas capturer de paquet tant que vous ne serez pas associé au réseau a sniffer et vous ne verrez pas les « Beacon Frames » (et autres paquets de management) envoyés par les points d'accès. Ce mode est entre autre utilisé par Airsnort comme nous le verrons plus loin, pour sniffer les paquets cryptés transitant sur un réseau sans fil de type 802.11. La première chose à faire est de patcher les pilotes de notre carte Orinoco se trouvant dans les sources de notre module pcmcia-cs. Décompressez pcmcia-cs grâce à la commande :

$ tar zxvf pcmcia-3.2.1.tar.gz

Pour patcher le pilote, copiez le patch Orinoco (fichier .diff) dans le répertoire source du pcmcia-cs et appliquez le :

$ patch -p0 < pcmcia-cs-3.2.1-orinoco-patch.diff

Après avoir appliquer le patch il ne vous reste plus qu'à compiler votre module pcmcia-cs :

$ make config
$ make all
$ make install

Relancez votre système et si tout s'est bien passé votre carte Orinoco devrait être reconnue. Pour le vérifier, installez "wireless-tools" :

http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html

Cet outil permet de configurer votre carte Wireless. Insérez votre carte et tapez "iwconfig", vous devriez voir apparaître les différentes options de votre carte, comme ceci pour une carte Orinoco:

Vous remarquez que cette commande ressemble à "ifconfig" pour un réseau filaire (ethernet) et elle s'utilise de la même manière (exemple: iwconfig eth1 essid nom_de_mon_reseau_wifi channel 3 mode managed key icila_cle_wifi) bien sûre, cette ligne ne sert que d'exemple, vous devrez la modifier selon vos besoins/désirs, pour cela consultez la page man de la commande iwconfig (man iwconfig). Vous trouverez aussi la commande « iwlist » qui permet de lister les options de votre carte. Par exemple, si vous voulez connaître les différentes vitesses de transmission de votre carte :

Pour les cartes PCMCIA ou PCI dont le chipset est de type Prism2 utilisez linux-wlan :

http://www.linux-wlan.com/linux-wlan/

Il inclut les pilotes pour les cartes Prism2 et un outil permettant d'activer le mode monitor. Pour configurer notre carte Prism2 nous n'utiliserons plus la commande "iwconfig" mais la commande "wlanctl-ng" fournie avec linux-wlan. Vous pouvez tout de même utiliser "iwconfig" pour vérifier que votre carte est bien reconnue par "pcmcia-cs" :

Ensuite, vous devez configurer votre /etc/pcmcia/config.opts (Debian) et ajouter les lignes de configuration dans /etc/pcmcia/wireless.opts selon les options que vous choisirez, par contre, pour les cartes PCI ou Airbus vous devez aller dans /etc/network/interfaces.

CHAPITRE IV

ATTAQUES

1. Détection des réseaux wifi

Pour détecter les divers réseaux sans fil (et donc leur SSID) qui nous entourent, il suffit de se munir d'un scanner de réseau sans fil. Pour windows, il existe par exemple Netstumbler qui est gratuit. Ce scanner combiné avec Mappoint et Stumverter permet de cartographier les différents points d'accès croisés sur notre chemin.

http://www.netstumbler.com

Pour Linux, utilisez kismet (qui est porté aussi sous windows), qui en plus de détecter les réseaux, permet de sniffer les paquets et peut aussi être combiné avec un GPS pour afficher les AP sur une carte du monde. Le résultat du sniffing sera enregistré dans un fichier consultable avec tcpdump ou ethereal (format libpcap). En bref, c'est le meilleur scanner/sniffer que vous trouverez pour les réseaux wireless.

http://www.kismetwireless.net

Vous pourrez aussi essayer "Mognet" qui est un sniffer/scanner codé en Java donc fonctionnant sur divers OS.

http://chocobospore.org/mognet/

Ci-dessous, le résultat d'un scan effectué avec Netstumbler muni de l'antenne omni-directionnelle. Les points d'accès ayant le WEP actif, on un petit cadenas à gauche de leur nom.

MAC	SSID	Name	Ch...	Vendor	Ty...	En...	SN...	Sign...	Noi...	SNR+	Lati
00095B2B6138	confortissimo		11	Netge...	AP			-89	-98	9	N4E
00095B2BFF...	Wireless		10	Netge...	AP			-89	-94	5	N4E
0090D10180...	BRIDGE		11	Addtron	AP			-78	-101	18	N4E
0090D100B6...	WLANSMC		4	Addtron	AP			-79	-96	16	N4E
0030651F2A...			10	Apple	AP	W...		-94	-99	4	N4E
0030651F1F01	CD Air		10	Apple	AP	W...		-85	-95	10	N4E
0002B39274...	wireless		10	Intel	AP			-81	-102	21	N4E

Après avoir exporté le résultat au format summary, il est possible de cartographier ces résultats en utilisant Stumverter combiné avec Mappoint, dont voici une capture (les réseaux cryptés sont affichés en rouge):

2. Sniffing réseau

Pour le sniffing, nous utiliserons Ethereal car la libpcap qu'il utilise, interprète le 802.11 et elle nous permettra de lire les fichiers dump produits par Kismet. Si vous lancez le sniffer sans activer le mode monitor, vous remarquerez qu'il ne vous affichera pas les « Beacon frames » mais juste ce qui se trouve au dessus de la couche physique. Voici les commandes pour activer le mode monitor :

iwpriv eth1 monitor 2 1	active le mode monitor pour la carte orinoco (eth1) sur le canal 1
wlanctl-ng wlan0 lnxreq_wlansniff channel=1 enable=true	active le mode monitor pour la carte Prism2 (wlan0) sur le canal 1

Vous pouvez le vérifier avec la commande ifconfig en regardant l'adresse MAC de votre carte. Elle devrait être dans un format incorrect :

```
wlan0     Link encap:UNSPEC  HWaddr 00-30-AB-20-26-5E-00-00-00-00-00-00-00-00
-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:82018 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:5606771 (5.3 MiB)  TX bytes:0 (0.0 b)
          Interrupt:5 Base address:0x180
```

Voici le résultat d'une capture sous Ethereal avec le mode monitor d'activé :

No.	Time	Source	Destination	Protocol	Info
9	6.093060	SmcNetwo_9f:c0:e7	Agere_4f:f0:98	IEEE 8	Probe Response
10	6.093967	SmcNetwo_9f:c0:e7	Agere_4f:f0:98	IEEE 8	Probe Response
11	6.094971	D-Link_98:40:80	Agere_4f:f0:98	IEEE 8	Probe Response
12	6.126003	SmcNetwo_9f:c0:e7	Agere_4f:f0:98	IEEE 8	Probe Response
13	6.134807	SmcNetwo_9f:c0:e7	Broadcast	IEEE 8	Beacon frame

Comme vous pouvez le constater, nous recevons bien les « Beacon frames » qui indiquent la présence de divers AP autour de nous.

http://www.ethereal.com (ethereal)
http://www.tcpdump.org (libpcap pour linux)
http://winpcap.polito.it/install/default.htm (winpcap pour windows)

3. Falsification d'adresse MAC

La falsification d'adresse est utilisée pour renforcer l'anonymat mais aussi pour contourner le filtrage présent dans beaucoup de points d'accès. Pour changer notre adresse MAC nous utiliserons macchanger sous Linux et SMAC sur Windows qui permettent de fixer une adresse de façon fixe ou aléatoire.

Sous Linux :

Avant de changer l'adresse, il faut désactiver la carte en faisant :

$ifconfig eth1 down

et une fois l'adresse MAC modifiée :

$ifconfig eth1 up

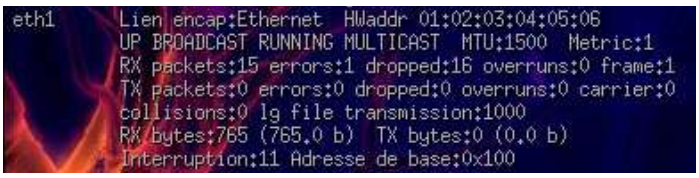
Voici quelques commandes pour macchanger :

$ macchanger -e eth1
Permet de changer de façon aléatoire les 3 derniers octets de la carte eth1, ce qui permet de garder les octets réservés au fabricant.

$macchanger --mac=01:02:03:04:05:06 eth1
Permet de spécifier entièrement la nouvelle adresse MAC associée à la carte eth1.

Vous pouvez aussi spécifier une nouvelle adresse MAC en utilisant ifconfig :
$ifconfig eth1 hw ether 01:02:03:03:04:05:06

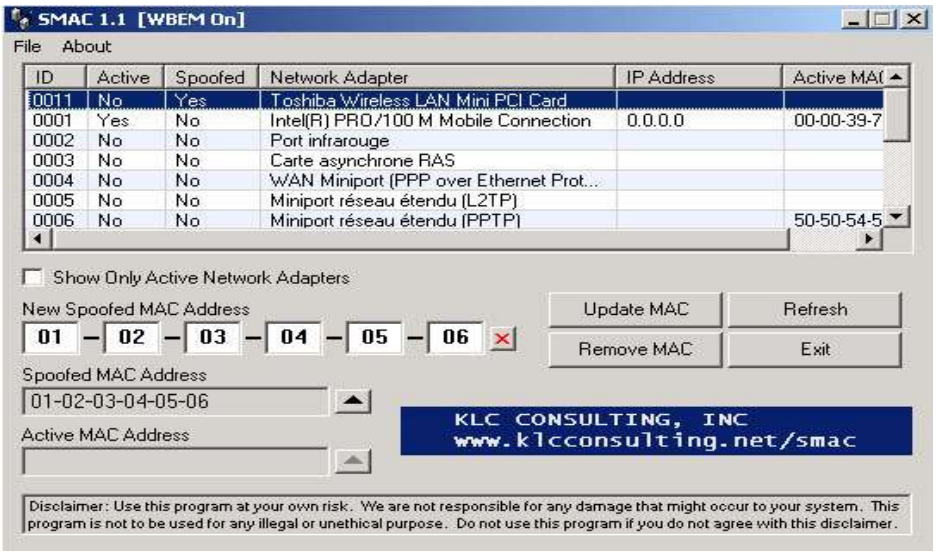
Voici le résultat :



Sous Windows :

Comme sous Linux, nous devrons dans un premier temps désactiver notre interface avant de modifier son adresse MAC avec SMAC. Pour cela aller dans vos connexions réseau et faites un clique droit sur votre interface et cliquez sur désactiver.

Ensuite lancez SMAC, décochez la case « Show Only Active Network Adapters » pour afficher toutes vos interfaces. Sélectionnez la carte à modifier, spécifiez la nouvelle adresse MAC et cliquez sur Update MAC :



Il ne vous reste plus qu'a réactiver l'interface et faire un « ipconfig /all » pour verifier que l'adresse MAC a bien été modifiée :

```
Carte Ethernet Connexion réseau sans fil:

        Statut du média . . . . . . . . . : Média déconnecté
        Description . . . . . . . . . . . : Toshiba Wireless LAN Mini PCI Card
        Adresse physique . . . . . . . . .: 01-02-03-04-05-06
```

La seule différence avec macchanger, c'est que l'adresse est modifié de façon permanente, il faudra relancer SMAC pour réatribuer l'adresse MAC d'origine.

http://www.klcconsulting.net/smac/
http://www.alobbs.com/macchanger

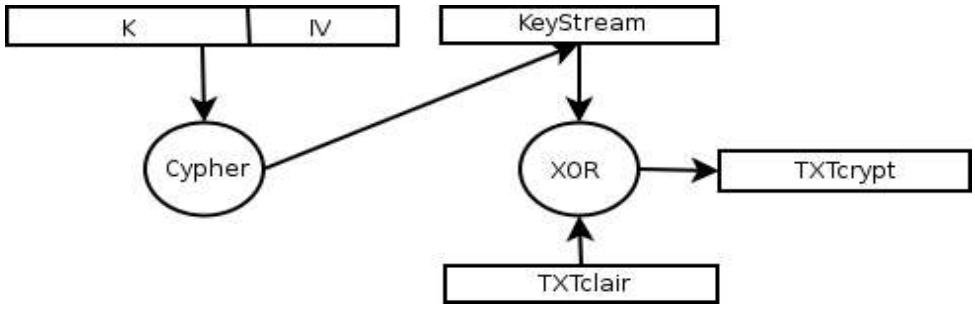
4. Mapping réseau

Thcrut permet de détecter les autres machines présentes sur le réseau en envoyant différents types de requêtes (ARP, DHCP, etc...) mais il permet aussi de faire du fingerprinting. Prenons par exemple le cas où le pirate a réussi à se connecter au réseau mais qu'il ne connaît pas la plage de celui-ci. Il pourrait utiliser thcrut pour découvrir les machines présentent sur le réseau et donc la plage. Il pourra utiliser thcrut pour découvrir la plage 192.168.x.x ou autres plages de réservées aux réseaux locaux en utilisant les requêtes ARP :

http://www.thc.org/thc-rut/

5. Cracking WEP

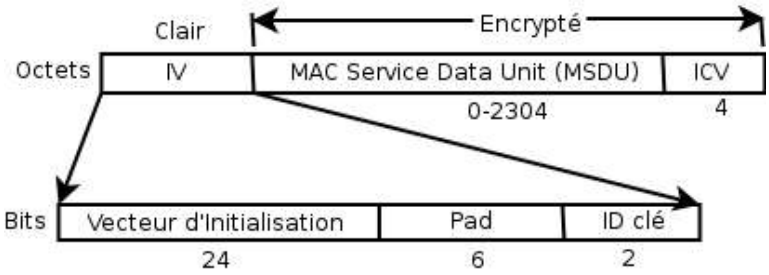
La principale faille des réseaux sans fil, est la libre circulation des données, ces données peuvent ne pas être cryptées, donc lisible par une personne malveillante, pour remédier à cela on peut utiliser le WEP qui crypte vos données grâce à des clés de cryptage statiques au niveau du point d'accès et de chacun des clients avant de les transmettre par les ondes. Le WEP peut utiliser un cryptage 64 bits (en réalité 40), 128 bits (104), 256 bits (232). Bien-sûre, la clé la plus grande est conseillée car plus longue à cracker pour un pirate. Le WEP (Wired Equivalent Privacy) est un protocole de sécurité se trouvant sur la couche liaison du réseau 802.11b. Le WEP utilise l'algorithme RC4, qui a été développé par la RSA Security. Cet algorithme est basé sur les permutations aléatoires des octets. Voici de façon simple comment RC4 encrypte les données pour le WEP :



- K est la clé partagée sur le réseau (clé WEP statique)
- IV un vecteur d'initialisation sur 24 bits. Ce vecteur (transmis en clair) permet de modifier le Keystream pour qu'il soit différent à chaque trame transmise sur le réseau sans fil. Cela permet de rendre le TXTcrypt différent dans le cas où le même TXT clair a été transmit plusieurs fois.
- KeyStream est généré avec les 2 variables ci-dessus par la formule : RC4(IV,K)
- TXTclair est le texte à encrypter

- TXTcrypt est le texte crypté
- ICV est le contrôle d'intégrité (qui se trouve à la fin de TXTcrypt)

Datagramme simplifié d'un paquet WEP :



A) ATTAQUE PASSIVE :

Ceci n'est que de la théorie mais 3 hommes (Fluhrer, Mantin et Shamir) ont révélé 2 types d'attaques possibles :

- La première nommée "invariance weakness" est dû à une faiblesse du RC4 qui permet, quand la clé est de faible taille, de pouvoir déterminer de nombreux bits.
- La seconde nommée "known IV attack" se fait grâce à la connaissance de IV, comme il circule en clair sur le réseau il est facilement récupérable en sniffant et permet ainsi de récupérer 2 paquets utilisant le même KeyStream. Ce qui va lui permettre de déduire le XOR des 2 TXTclair pour effectuer une attaque statistique pour retrouver la clé WEP utilisée. Plus le nombre de paquets utilisant le même Keystream est capturé, plus rapide sera l'attaque statistique.

Les logiciels utilisant ces 2 attaques sont airsnort, aircrack et wepcrack.

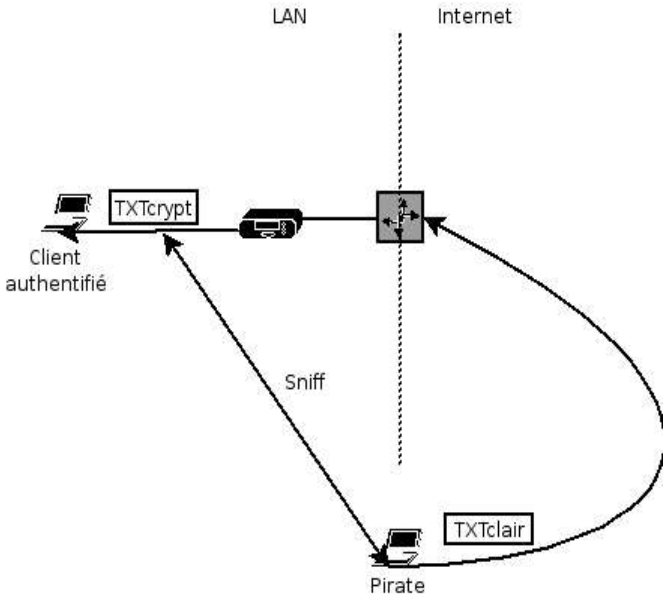
B) ATTAQUE ACTIVE :

Comme nous l'avons vu ci-dessus, le WEP effectue un XOR avec le KeyStream pour obtenir le texte encrypté. C'est ce mécanisme qui va permettre au pirate d'effectuer des attaques actives pour générer un maximum de paquets encryptés et ensuite effectuer une attaque passive.

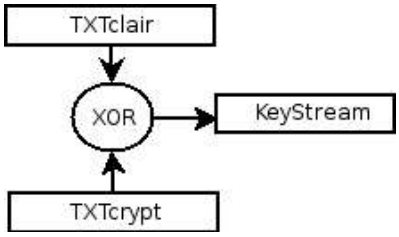
1. Initialization Vector Replay Attacks

   Pour mettre en place cette attaque le pirate devra sniffer en continu le réseau Wifi encrypté qu'il désire cracker. Ensuite viennent une série d'étapes :

   - Le pirate envoie par le net un message en clair dont il connaît le contenu et sa taille (ex : email)
   - Le pirate sniff le réseau à la recherche du message encrypté représentant le message en clair envoyé qu'il peut déterminer grâce à sa taille.



- Le pirate récupère la frame qui correspond à son message encrypté et en déduit le KeyStream.



- Le pirate peut augmenter la taille du KeyStream en utilisant la même paire IV/WEP que la frame récupérée.

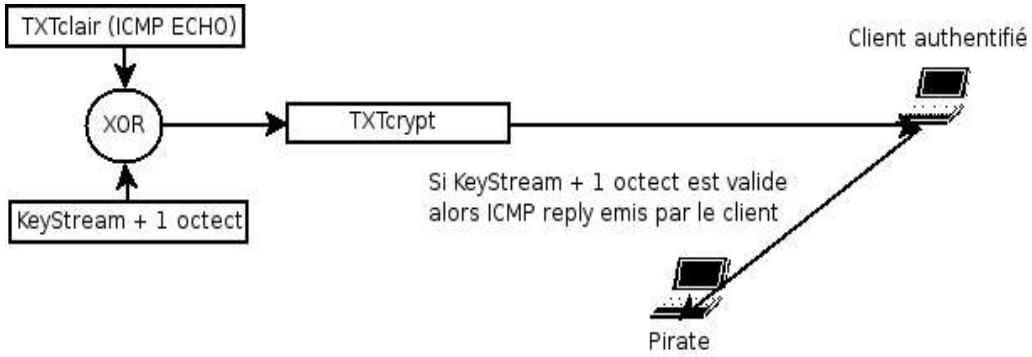
Pour augmenter la taille du Keystream à la taille désirée le pirate devra :

- Forger un paquet (trame) contenant un octet supplémentaire par rapport à la taille du KeyStream déduit précédemment. Cette trame contiendra un « ICMP echo request » car si la trame est correctement forgée, la machine vers laquelle ce paquet sera envoyé, renverra un « ICMP echo reply ».

- L'octet rajouté au KeyStream est facilement déductible car il n'y a que 256 possibilités. Donc le pirate va essayer toutes les combinaisons les une après les autres.

- Si la bonne combinaison est trouvée, un « ICMP echo reply » sera renvoyé.

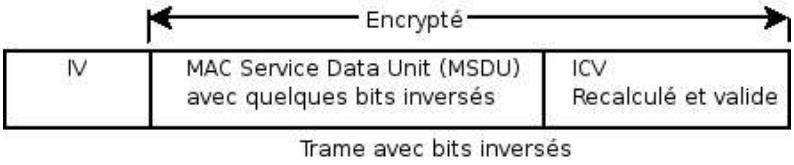
- Ce processus est répété jusqu'à avoir la taille du KeyStream voulu.



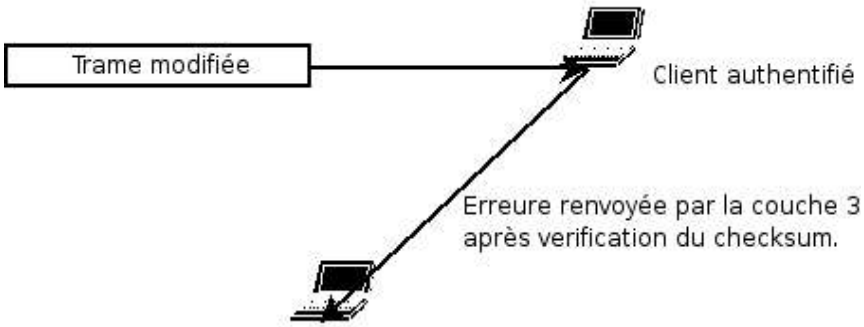
Le pirate pourra ainsi envoyer n'importe quel type de paquet encrypté mais ne pourra pas décrypter de suite les paquets qui lui seront envoyés. Il devra donc effectuer une attaque passive pour récupérer le clé WEP du réseau.

2. Bit-Flipping Attacks

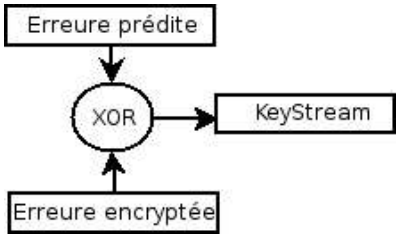
- Le pirate capture une trame encryptée sur le réseau
- Il inverse certains bits du payload et modifie le ICV



- Il transmet la trame modifiée
- Celui qui reçoit la trame, calcul le ICV
- Le destinataire compare le ICV qu'il a calculé à celui contenu dans la trame reçue
- Le destinataire accepte la trame modifiée
- Il désencapsule la trame et la transmet à la couche 3
- A cause des inversions de bits, la checksum de la couche 3 n'est pas valide
- La pile IP du destinataire produit une erreur prévisible
- Le pirate sniff le réseau à la recherche de l'erreur encryptée

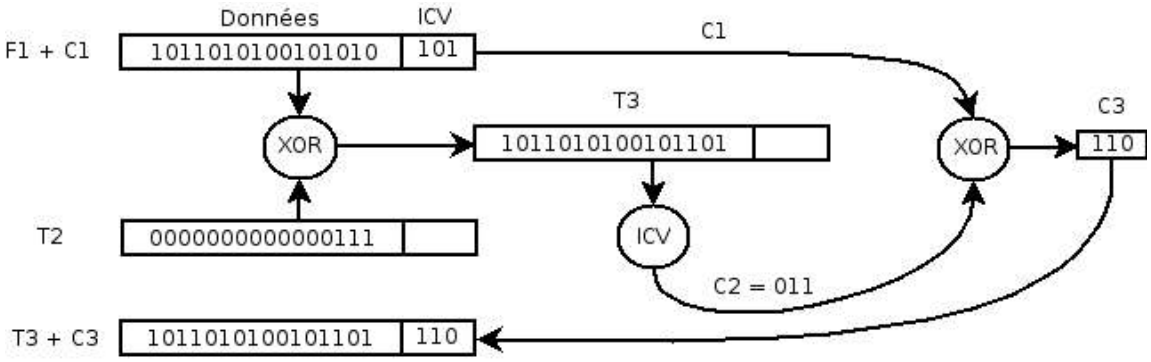


- Une fois l'erreur capturée, le pirate en déduit le KeyStream



Cette attaque est possible car il y a une vulnérabilité au niveau de ICV. Alors comment le hacker peut-il modifier correctement ICV alors que celui-ci est encrypté dans la trame ?

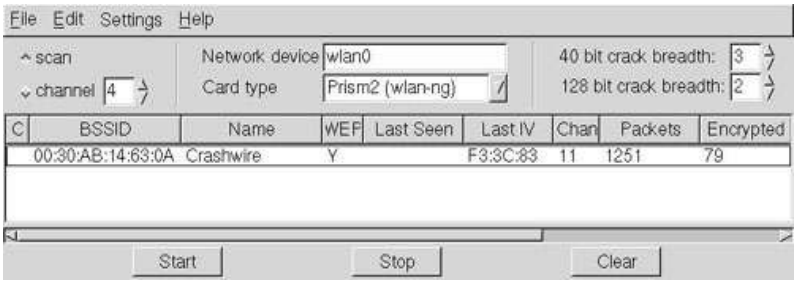
- Une trame cryptée (t1) a un ICV (c1)
- Une nouvelle trame est générée (t2) de la même longueur que t1 mais avec les bits à inverser sur la trame finale
- Une nouvelle trame est calculée (t3) à partir d'un XOR sur t1 et t2. C'est cette trame que le hacker va envoyer.
- L'ICV (c2) est caculé à partir de t2
- Le nouveau ICV (c3) de t3 est déduit à partir d'un XOR sur c1 et c2



Crackeur WEP

- Airsnort
  Airsnort permet de retrouver la clé WEP utilisée pour crypter les données d'un réseau sans fil. Pour cracker la clé WEP, airsnort à besoin de capturer un certains nombre de paquets (5 millions environ pour une clé 64 bits). Plus le trafic sur le réseau sera élevé, plus rapide sera la découverte de la clé WEP et plus le nombre de bits de clé sera élevé, plus le nombre de paquets à capturer sera élevé. Pour que Aisnort puisse fonctionner correctemment, vous devez activer le mode monitor au préalable. Voici une capture de celui-ci en pleine activité :

  http://airsnort.shmoo.com/



- Aircrack

  Plus puissant que Airsnort ce logiciel permet de cracker les clés WEP encore plus rapidement en implémentant l'attaque de Korek.

  http://www.cr0.net:8040/code/network/aircrack/

- Weptools
  Ce nom regroupe deux outils. Un pour cracker les clés WEP, l'autre pour décrypter les paquets. Pour cracker les clés WEP, wep_crack utilise l'attaque par dictionnaire ou par brutforce. wep_decrypt va servir à decrypter les paquets WEP une fois que la clé a été trouvée. Weptools fonctionne à partir des fichiers dump provenant des sniffers utilisant pcap (ethereal, kismet, etc...).
  http://www.lava.net/~newsham/wlan/

- Wepattack

  Voici un autre logiciel permettant d'effectuer des attaques par dictionnaires sur les dumps au format libpcap, donc nous pouvons directement lui fournir les paquets capturés par kismet.

  http://wepattack.sourceforge.net/

- Weplab

  Logiciel regroupant les attaques statistiques et les attaques par dictionnaires.

  http://weplab.sourceforge.net/

6. Cracking WPA

Il existe actuellement un logiciel permettant de cracker les clés WPA si la passphrase est de trop faible qualité et si le WPA fonctionne en mode « authentification par clé partagée ». Ce logiciel est disponible sur http://www.tinypeap.com qui fourni aussi un firmware modifié pour les routeurs linksys permettant d'avoir un serveur RADIUS en local evitant aussi la mise en place d'un serveur RADIUS dédié. Mais le logiciel qui nous interesse pour cette partie du cours est wpa_cracker qui permet de faire un attaque par dictionnaire passive sur le dump d'une authentification par clé partagée. Après avoir fait une capture de l'authentification d'un client en WPA nous pouvont donner celle-ci à wpa_cracker en lui spécifiant quelques informations par rapport au réseau à cracker. Ethereal nous sera d'une grande utilité pour les informations supplémentaires concernant l'authentification EAPOL en 4 poignés de main. En effet, wpa_cracker a besoin d'un certain nombre d'informations (SSID, ANONCE, SONCE, MAC, etc..) contenu dans le protocole EAPOL. Voici le résultat Ethereal avec les 4 paquets qui nous interessent :

Pour une explication détaillé du fonctionnement de wpa_cracker et des informations qu'il necesite veuillez consulter : http://www.tinypeap.com/docs/WPA_Passive_Dictionary_Attack_Overview.pdf .
Pour avoir plus de chance de réussite, il faudra modifier le dictionnaire (en.dic) ainsi que le fichier de definition d'attaque (password.def) qu'il utilise pour retrouver la bonne clé partagée.

7. Hijhacking

Pour détourner les clients d'un réseau sans fil, il suffit de mettre en place un autre point d'accès ayant la meme configuration (SSID, WEP, etc...) que le réseau à détourner et un signal plus puissant que celui où se trouvent les victimes. En effet, par défaut les clients se connectent toujours sur le réseau ayant le signal le plus fort. Pour créer son propre point d'accès il existe :

Hostap
Hostap est un pilote permettant d'activer le mode master sur une carte à base de chipset Intersil Prism2/2.5/3. Ce pilote va donc nous permettre de transformer notre carte en point d'accès sous Linux.

http://hostap.epitest.fi

Ce pilote est livré avec hostapd un daemon qui une fois combiné avec le pilote hostap, permet d'utiliser plusieurs options suplémentaires comme l'authentification 802.1x, WPA, RADIUS, etc...

HermesAP
Hermesap est un ensemble de pilote/patch sous Linux permettant d'activer le mode master sur une carte à base de chipset Hermes (Orinoco).

http://hunz.org/hermesap.html

Dans notre exemple, nous utiliserons Hostapd avec un carte Netgear MA401 (PCMCIA) à base de chipset Prism2. Pour installer Hostapd, vous devrez récupérer les sources de hostap-driver et taper les commandes qui suivent :

$tar zxvf hostap-driver-0.2.4.tar.gz
$cd hostap-driver-0.2.4

Si le module PCMCIA a été compilé en dehors du kernel, vous devrez indiquer dans le Makefile le répertoire où se trouve les sources de PCMCIA.

$make

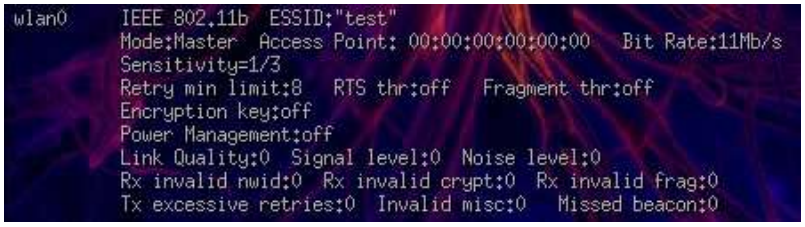
$make install

Vérifiez que le fichier /etc/pcmcia/hostap_cs.conf contient bien le modèle de votre carte.

$/etc/init.d/pcmcia restart

Insérez votre carte et normalement, elle devrait être reconnue et associée au driver hostap_cs. Voilà ce que vous devriez voir apparaître en tapant :

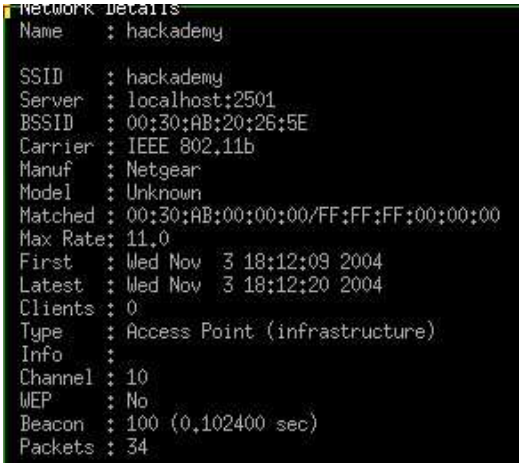
$iwconfig



Comme vous pouvez le remarquer l'interface wlan0 est bien en mode Master et associé au SSID test. Nous allons configurer notre carte pour détourner les clients qui voudraient s'associer au réseau ayant le SSID hackademy sur le canal 10.

$iwconfig wlan0 essid hackademy
$iwconfig wlan0 channel 10
$ifconfig wlan0 192.168.0.100

Voilà, vous avez un point d'accés opérationnel et disponible pour tous les clients se trouvant aux alentours. Voici le résultat sous kismet :



Pour utiliser le 802.1x et le WPA il faudra installer hostapd.

8. D.O.S

Il existe plusieurs D.O.S qui permettent de déconnecter les clients d'un réseau sans fil, de ralentir un AP ou de bloquer complètement le réseau.

1. Canal flooding
Cette attaque est basé sur la saturation de la bande fréquence pour provoquer un maximum de colision et provoquer des erreurs CRC. Pour cela il suffit simplement de mettre plusieurs point d'accès sur le meme canal, jusqu'a saturation.

2. Désautentification flooding
Envois des paquets de désauthentification en spoofant le BSSID se qui a pour conséquence de déconnecter les clients authentifiés.

3. Authentification flooding
Envois des paquets d'authentification vers le point d'accès en spoofant les adresses MAC se qui a pour conséquence dans certains cas de rendre l'accès au réseau impossible (l'AP refuse de nouvelles authentifications) ou de bloquer le point d'accès.

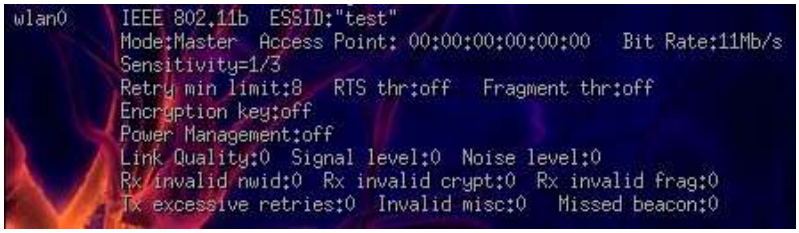
4. WPA flooding
Il est possible de rentre inactif le WPA en envoyant 2 paquets de données non autorisés en moins d'une second. Ce qui rend le réseau inaccessible pour les clients WPA légitimes.

Void11 est un logiciel implémentant 2 D.O.S :

- deauth, qui implémente le désauthentification flooding
- auth, qui implémente l'authentification flooding

Void11 utilise Hostap pour générer les paquets et nécessite la version 0.1.3 sinon vous ne pourrez pas le compiler. Une fois compilé, vous devez activer votre carte en mode master :

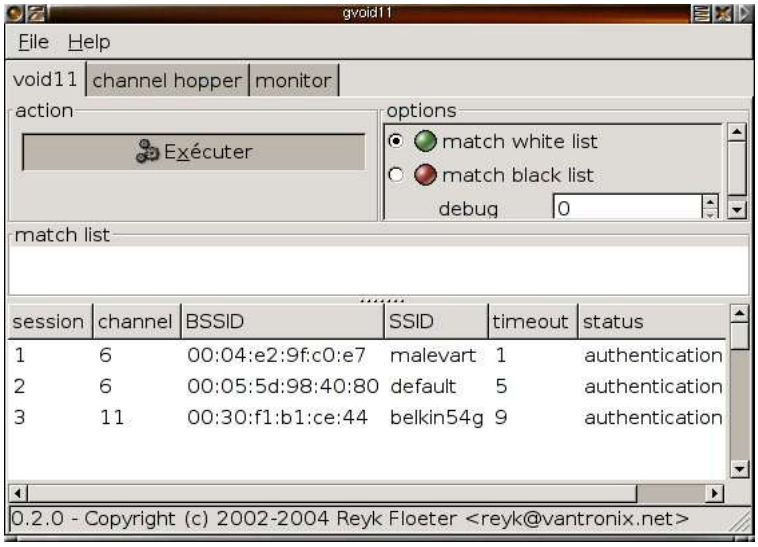
$iwconfig wlan0 mode master



Ensuite il faut activer le daemon de hostap :

$iwpriv wlan0 hostapd 1

Il ne vous manque plus qu'à lancer gvoid11 :

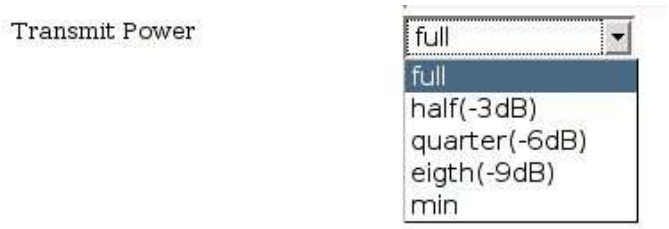

gvoid11
File Help
void11 channel hopper monitor
action
Exécuter
options
match white list
match black list
debug 0
match list
session channel BSSID SSID timeout status
1 6 00:04:e2:9f:c0:e7 malevart 1 authentication
2 6 00:05:5d:98:40:80 default 5 authentication
3 11 00:30:f1:b1:ce:44 belkin54g 9 authentication
0.2.0 - Copyright (c) 2002-2004 Reyk Floeter <reyk@vantronix.net>

CHAPITRE IV

SECURISATION

1. Portée du point d'accès

Il est possible sur certains points d'accès de régler la portée (puissance de transmission) de celui-ci, réglez là de telle façon qu'elle couvre juste votre réseau et pas plus. Votre réseau ne s'étend pas forcément à l'extérieur de votre appartement (sur la voie publique).

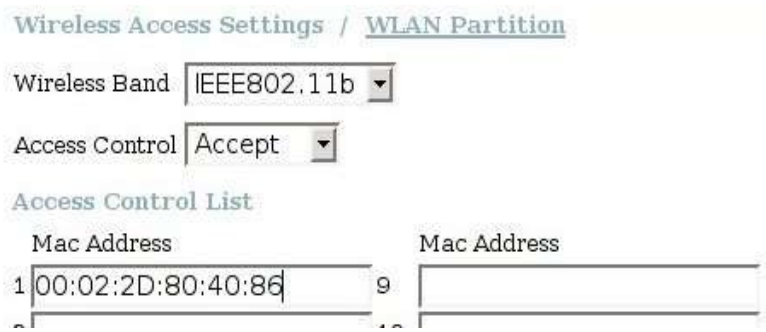


2. Desactivation SSID

Si votre point d'accès vous le permet, il est conseillé de désactiver le SSID du réseau, ce qui rendra la tache plus difficile au pirate car le SSID ne sera plus envoyé dans les « Beacon Frames ». Il sera donc obligé de le récupérer d'une autre façon (sniffing client <--> AP). Il faut aussi eviter de laisser le SSID par défaut pour eviter les attaques par brute force.

3. Filtrage des adresses MAC

Sur certains point d'accès, il est possible d'activer le filtrage par adresse MAC. Ce qui renforce l'authentification en autorisant ou en refusant certaines adresses MAC à se connecter.



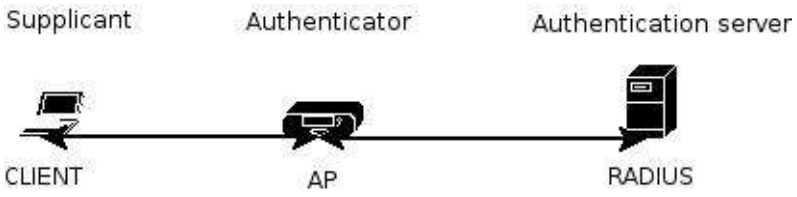
4. Cryptage des données

En effet, le cryptage des données est une priorité au niveau des réseaux sans fil, pour cela, on dispose de plusieurs protocoles. Comme nous l'avons vu plus haut dans le cours, le WEP est efficace dans le cas ou la clé de cryptage est grande, mais cela n'empêchera pas un pirate motivé d'en venir à bout en sniffant assez de paquets ou en effectuant une attaque par dictionnaire car le WEP utilise toujours la même clé pour crypter les données. Pour rendre le WEP plus efficace, vous pouvez utiliser plusieurs protocoles.

A) 802.1x :

Le 802.1x appelé aussi EAPOW (EAP Over Wireless) utilise le protocole EAP (Extensible Authentication Protocol) ou PEAP (Protected Extensible Authentification Protocol) et a été développé à la base pour les réseaux filaires pour empecher l'accès physique (via un switch ou hub) à une personne non autorisée.

Le 802.1x utilise 3 termes qu'il faut connaître pour comprendre l'authentification. L'utilisateur ou client qui désire s'authentifier est appelé « supplicant », le serveur (RADIUS) qui vérifie cet utilisateur est appelé « authentication server» et ce qui se trouve entre les 2 (le point d'accès) est appelé « authenticator ».



L'authentification 802.1x se déroule en 4 phases :

- Lorsqu'un client s'associe au point d'accès, l'authenticator (AP) envoie une requête EAP-Response au serveur d'authentification (RADIUS).
- Le serveur d'authentification renvoie à l'authentificateur un challenge qui est transmis au supplicant au format EAOP.
- Le supplicant renvoie la réponse au challenge à l'authentificateur qui la transmet au serveur d'authentification
- Si le supplicant s'est correctemment authentifié, le serveur d'authentification renvoie un message valide pour permettre au client (supplicant) d'accéder au réseau ainsi qu'une clé WEP générée par l'authentificateur. Dans le cas contraire, un message d'erreur est renvoyé et le client ne peut pas accéder au réseau.

Certains point d'accès (dlink DWL6000AP par exemple) n'ont pas forcément besoin d'un serveur RADIUS pour authentifier les clients car ils implémentent un RADIUS en local. Vous pourrez donc directement spécifier les pseudo/password des utilisateurs qui on le droit d'accéder au réseau :

Comme vous pouvez le remarquer vous devez spécifier une longueur de clé WEP. En effet, le 802.1x au niveau wireless génère automatiquement la clé WEP qui sera utilisée par tous les clients du réseau. Il vous faudra ensuite configurer chacun de vos clients pour se connecter au réseau en utilisant le protocole 802.1x avec EAP ou PEAP pour plus de sécurité (Le 802.1x est implémenté de base dans WinXP) et lui indiquer que la clé WEP vous est fournie automatiquement. Pour Win2000 vous devrez télécharger un patch sur le site de Microsoft pour qu'il puisse supporter le 802.1x ou installer le dernier service pack (SP4) :

http://support.microsoft.com/default.aspx?scid=kb;fr-fr;313664

Voici un bon tutorial si vous désirez mettre en place un serveur radius :

http://www.tldp.org/HOWTO/8021X-HOWTO/index.html

B) WPA (Wi-Fi Protected Access) :

Le WPA fonctionne actuellement sous Windows XP en appliquant un patch que vous pouvez télécharger sur le site de Microsoft ou en installant le SP2 mais attention, certaines carte ne supportent pas le WPA au niveau hardware donc vous serez obligé de changer de carte. Sur les postes clients Linux vous pourrez utiliser wpa_supplicant (supporte aussi le 802.1x) disponible sur :

http://hostap.epitest.fi/wpa_supplicant/

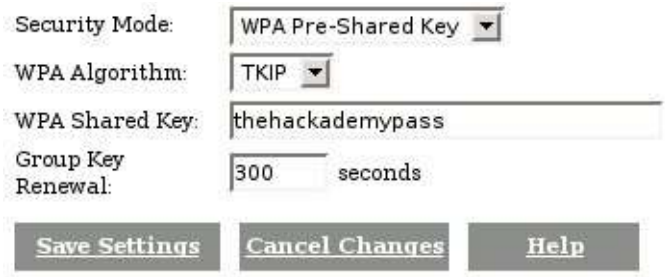
Le WPA est une solution intermédiaire avant que le protocole 802.11i soit finalisé. Cette solution vise à améliorer 2 faiblesses du protocole 802.11, le cryptage des données et l'authentification des utilisateurs. Pour le cryptage des données, le WPA se base sur le protocole TKIP (*Temporal key integrity protocol)* qui inclut un vecteur d'initialisation de 48 bits, un contrôle d'intégrité renforcé MIC *(Message integrity code)* pour empêcher la modification des données à la volé, ainsi qu' un nouveau système de génération de clés (mixage, regénération). En effet, le TKIP utilise une clé temporaire de 128 bits qui est regénérée tous les 10000 paquets échangés. Vous pouvez faire fonctionner le WPA en 2 modes distincts :

- Le mode « Authentification par utilisateur » :
Ce mode est plutôt destiné aux entreprises car il combine le 802.1x donc la possession d'un serveur RADIUS pour l'authentification des utilisateur et le cryptage WPA pour la transmission des données après authentification.

- Le mode « Authentification par clé partagée » (PSK) :
Ce mode est plutot distiné aux particuliers ayant un petit réseau local car il ne nécessite pas de serveur RADIUS pour authentifier les utilisateurs.

Voici un exemple de configuration WPA (PSK) avec un point d'accès Lynksys et une carte client Orinoco sous Linux. Au niveau du point d'accès vous avez besoin de lui indiquer :

- la passphrase à utiliser (la passphrase doit au minimum faire 8 caractères pour généré une clé de 256 bits)
- l'algorithme (TKIP ou AES)
- le temps en milliseconde de renouvellement de la clé



Au niveau du client d'utilise wpa_supplicant donc voici le fichier de configuration :

Comme vous pourrez le remarque, le fichier contient non pas une passphrase mais son equivalent en 256 bits. Pour générer l'équivalent, vous devrez utiliser wpa_passphrase livré avec wpa_supplicant (dans cet exemple le SSID du réseau est « hackademy ») :

Vous n'avez plus qu'a assigner une adresse IP, passerelle à votre carte wifi (ath0 dans mon cas), à lancer wap_supllicant et le tour est joué :

$ ifconfig ath0 192.168.0.10
$ wpa_supplicant -B -i ath0 -c /etc/wpa_supplicant.conf

$ route add default gw 192.168.0.1
$ ping www.google.fr

C) WPA2 :

Fonctionnement exactement comme le WPA mais utilise un algorithme plus puissant qui est AES au lieu de RC4. Le protocole AES est plus fort mais nécessite donc une puissance CPU beaucoup plus importante.

D) VPN :

Les VPN sont une autre solution au problème de sécurité. Il vont vous permettre de créer des réseaux privés virtuels d'une machine à une autre, d'un réseau à un autre ou d'un client à un réseau en utilisant des canaux cryptés. La mise en place de VPN est un cours à lui tout seul, pour cela nous ne l'aborderont pas dans ce cours et c'est une solution très peu utilisée en sans fil, car difficilement gérable quand il y a beaucoup de clients.

5. Leurre AP

Fake AP permet de simuler la présence de plusieurs AP en envoyant des « Beacon Frames » avec différents SSID et adresses MAC. Cet outil permet de rendre la tâche plus difficile au pirate, en effet, il pensera qu'il existe plusieurs AP alors qu'en réalité il en existe qu'un voir aucun... Pour pouvoir utiliser fakeap vous aurez besoin d'installer hostap.

http://www.blackalchemy.to/project/fakeap/

Fakeap se présente sous forme de script Perl. Pour le configurer il vous suffit de l'éditer après l'avoir décompressé :

$tar zxvf fakeap-0.3.1.tar.gz
$cd fakeap-0.3.1
$vi fakeap.pl

Voici les informations importantes à paramétrer :

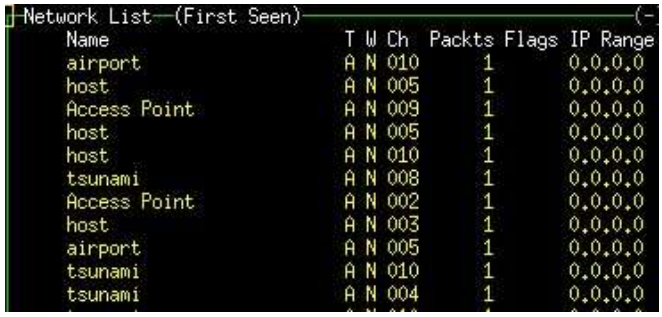
```
my $MAX_CHANNEL = 11;                  # Noth America.  Change for other regions.
my $IWCONFIG    = "/sbin/iwconfig";                    # Change as needed
my $IFCONFIG    = "/sbin/ifconfig";                    # Change as needed
my $CRYPTCONF   = "/home/crashfr/hostap-utils-0.2.4/hostap_crypt_conf";    # Cha
nge as needed

my @words = ( "Access Point", "tsunami", "host", "airport", "linksys" );
my @vendors = ( "00:00:0C:", "00:00:CE:", "00:00:EF:" );
```

IWCONFIG indique le chemin où se trouve iwconfig
IFCONFIG indique le chemin où se trouve ifconfig
CRYPTCONF indique le chemin où se trouve le fichier hostap_crypt_conf
@words indique les faux SSID que fakeap doit émettre
@vendors indique les faux id vendeurs (3 premiers octets des adresses MAC) que fakeap doit émettre

Une fois votre fakeap.pl configuré vous devrez l'activer :

$ifconfig wlan0 up
$perl fakeap.pl --interface wlan0

Voici le résultat sous kismet quand fakeap est actif :



6. Portail captif

Nocat est ce que l'on nomme un portail captif (OpenSource), dans le sens ou dès que le client s'est authentifié auprès du point d'accès il est automatiquement redirigé vers une page HTML lui demandant de s'identifier avec un login/password auprès d'un serveur RADIUS en général (802.1x). Ce genre de portail est très souvent utilisé dans les HotSpot (borne wifi public) pour vérifier si le client à payé son accès au Web car le client n'a pas besoin de configuration spécial mais juste d'un navigateur en état de marche. Une fois le client authentifié auprès de Nocat, les règles de firewalling sont modifiées pour permettre à la machine de se connecter à internet.

http://nocat.net

7. Conclusion

Comme vous l'aurez remarqué en lisant ce cours, il existe plusieurs protocoles permettant de combler les failles du WEP mais lequel utiliser au final ? En faite, cela va dependre du matériel que vous avez à disposition. Si tout votre matériel (point d'accès et carte clientes) vous permet d'utiliser le WPA et que vous avez à disposition un serveur Radius, vous pourrez dans ce cas implémenter une très forte sécurité en utilisant le WPA/RADIUS en mode « Authentification par utilisateur ». Actuellement, c'est le top pour les réseaux sans fil mais le plus dur à mettre en place à cause du serveur RADIUS. Si vous n'avez pas de serveur RADIUS activez le WPA en mode « Authentification à clé partagé » et définissez une passphrase la plus compliqué possible. Si votre matériel ne vous permet pas d'utiliser le WPA, verifier si votre AP supporte un radius en local pour eviter le deploiement de celui-ci et utilisez le 802.1x comme protocole d'authentification. Cette solution est très bien pour empécher un intru de se connecter au réseau mais n'empechera pas le cracking de la clé WEP par une personne motivée, sauf si vous régénérez régulièrement de nouvelles clés WEP (ce que je vous conseille biensur). Si jamais votre AP ne supporte ni le 802.1x, ni le WPA, vous serez obligé d'utiliser le WEP. Dans ce cas, je vous conseil de mettre en place un portail captif, de définir une clé de 256 bits et de la renouveller le plus souvent possible. Voila... le cours arrive à sa fin. N'hesitez pas à me contacter pour tout problème de configuration, sécurisation, compréhension, etc... sur mon adresse email : crashfr@thehackademy.net

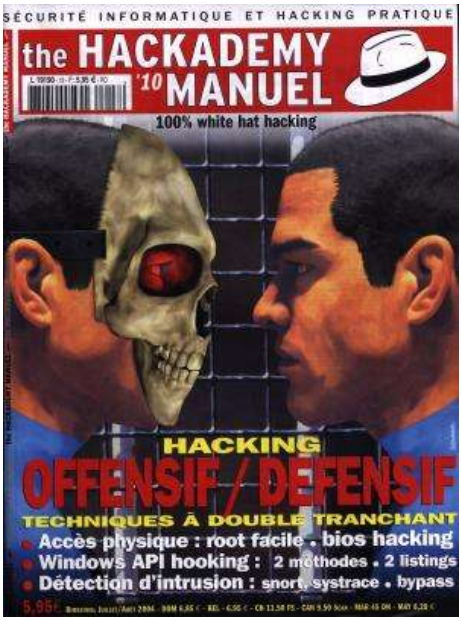
Contact

1 Villa du clos de Malevart 75011 Paris.
Tel: 01 40 21 04 28
e-mail: hackademy@thehackademy.net

26 bis rue jeanne d'Arc 94160 St Mandé
Tel: 01 53 66 95 28
e-mail: abonnements@dmpfrance.com

the HACKADEMY ,c'est aussi:

The hackadermy Journal, The hackademy manuel et d'autres numéros spéciaux!!!!!



Alors n'hésitez pas à vous abonner, en remplissant le formulaire suivant :

FAITES VOTRE CHOIX !

Abonnement Hackademy Journal (tous les mois) :	32 €	☐
Avec CD :	+ 4 €	☐
Abonnement Hackademy Manuel (Tous les deux mois) :	28 €	☐
Avec CD :	+ 4 €	☐
Nos cours par correspondances (Hack1, Hack 2 et Hack3) Les deux volumes de 80 pages livrés chez vous :	84 €	☐
Avec CD :	+ 4 €	☐
Le CD seul :	16 €	☐
Le T shirt historique " Intrusion . exe " :	23 €	☐
TOTAL		

PACKAGE *PUBLICATIONS* :
Abonnement journal + abonnement manuel : 60 €
Dans ce package, le CD est offert ☐
Avec T shirt : +15 euros ☐

PACKAGE *HACKTION* :
Abonnement journal + abonnement manuel +
Cours par correspondance Hack1, 2 et 3 : 130 €
Dans ce package, le CD est offert ☐
Avec T shirt : + 15 euros ☐

TOTAL :

H08

PAIEMENT
☐ par chèque à l'ordre de DMP
☐ par Carte Bleue ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐
Expire en ☐☐

Nom : ..... Prénom : .....
Adresse : .....
..... Code postal : .....
Ville : ..... Pays : .....
E-mail : .....

Envoyez votre bulletin acompagné de votre règlement à l'ordre de D.M.P. à The Hackademy 26 bis rue Jeanne d'Arc 94160 Saint Mandé

Signature

SYSDREAM

Crée par les formateurs de l'hackademy, SYSDREAM est une SSII spécialisée en sécurité informatique.

Nous apportons aux entreprises notre expertise pour assurer aux entreprises la fiabilité et la sécurité de leur infrastructure informatique.

Nos domaines d'intervention:

- **Audit de sécurité:** il permet de faire une expertise globale de votre système (test intrusif, audit technique, audit de vulnérabilité).

- **Les produits Systech sécurité:** Des solutions matérielles destinées à renforcer la sécurité de votre infrastructure, et assurant un suivi performant de tout type d'évènement réseau ou système.

- **Le dévelopement d'applications:** De la maîtrise d'oeuvre à la conception technique, nous pouvons intervenir ou vous conseiller dans toutes les phases du développement de votre application.

www.sysdream.com

Pour toute information: info@sysdream.com