Introduction à BackTrack 3

Cet article explique...

- L'utilisation de BackTrack.
- La récupération d'information
- Les différents outils présents sur BackTrack

Ce qu'il faut savoir...

- Le fonctionnement d'un Live CD
- Système Unix/Linux (Les bases)

Auteur

Régis SENET est actuellement étudiant en troisième à l'école Supérieur d'informatique Supinfo. Actuellement stagiaire chez Gardien Virtuel à Montréal, il découvre la sécurité informatique d'un point de vue entreprise. Il s'intéresse beaucoup aux tests d'intrusion.

Page d'accueil : http://www.remote-exploit.org/backtrack.html

1) Qu'est-ce que BackTrack 3 ?

Développée dans le cadre du projet suisse baptisé **RemoteExploit** par les développeurs *Mati Aharoni* et *Max Moser*, BackTrack a vu le jour pour la première fois le 5 février 2006 sous sa version 1.0 Beta.
Le 14 décembre 2007, la version 3.0 Beta est apparue apportant de nombreuses modifications, améliorations et correction de bug.
BackTrack est une distribution **GNU/Linux** issue de **Whax** et **ASC** (**Auditor Security Collection**) possédant un système d'exploitation de type **Slackware**, le tout sur une interface KDE.
La version 3 .0 Beta, étant la version actuelle, intègre un noyau 2.6.15.5 permettant entre autre une meilleure prise en charge des processeurs DualCore.
A l'heure actuelle, le groupe **Remote-Exploit** ne cesse d'améliorer son produit fort de sa réussite.

L'objectif de BackTrack est de fournir une distribution compacte regroupant l'ensemble des outils nécessaire aux tests de sécurité d'un réseau ou d'application.

Avec ces 300 outils, BackTrack aborde tous les domaines liés aux sécurités modernes allant de l'audit réseau à l'analyse et l'identification de vulnérabilités en passant par divers outils de récupération d'informations.
(Fuzzers / Testeurs de sécurité des réseaux filaires / Testeur des réseaux wifi ...)

BackTrack est principalement connu et utilisé à des fins d'audit de réseaux sans fil wifi. Son développement est axé sur la prise en charge de cartes wifi supportant le mode Monitoring, ce qui permet la capture de paquets, nécessaire pour le crack de clé WEP/ WPA et autres test (suite de logiciel aircrack-ng par exemple)

BackTrack contient aussi des applications basiques comme un lecteur multimédia, traitement de texte ... ce qui en fait un système d'exploitation polyvalent.

L'un des principaux intérêts de BackTrack est d'être disponible sous forme d'un **Livecd**, c'est à dire qu'un ordinateur peut booter directement sur le cd sans avoir à se préoccuper d'une quelconque installation avec la possibilité d'exécuter chaque outil immédiatement.
Ainsi, tout se passe dans la mémoire RAM de l'ordinateur n'entrainant aucune intervention sur le disque dur permettant ainsi de l'utiliser sans risque de perte de données ou autre.
Ce Livecd permet d'avoir tous les outils indispensables à la sécurité informatique sans laisser aucune trace.

Voici une liste non exhaustive de quelques mise à jour sur la nouvelle version:

- Développement d'une image USB ainsi qu'un ISO.
- Correction de la compatibilité des Dual core (en partie grâce au nouveau kernel - 2.6.15.5).
- Amélioration de la compatibilité des cartes Wifi.
- Amélioration du script de configuration de Xorg.
- Update des repos d'exploit et des exploits du Framework metasploit.
- PXE boot réseau ajouté (USB Version)
- Amélioration de la comptabilité sur Mac avec la reconnaissance de la carte airport

D'autre updates sont à venir dans la version stable de BacKTrack 3.0.

Après cette introduction à BackTrack, nous allons pouvoir enfin mesurer toute sa puissance en comprenant comment est ce que nous pouvons nous en servir pour récupérer des données et par la suite les utiliser.

2) Récupération d'informations

Des statistiques nous ont montré qu'une attaque à l'aveugle sur un système distant est dans 99% des cas totalement inefficace. Il est absolument nécessaire d'entamer une collecte d'informations sur le système visé, dans le but d'élargir ses possibilités d'attaques et de s'offrir ainsi plus de flexibilité sur le choix des méthodes d'attaque. La stratégie est aussi importante que la manœuvre elle-même. Manœuvrer sans but précis est une perte de temps.
La règle des « **5P** » constitue le squelette type de toutes attaques informatiques distantes.
Le premier **P** correspond à « **Probe** » qui peut se traduire par « **enquêter** ».

Savoir mener des recherches efficaces sur Internet est la clé de la réussite. Personne n'a la science infuse, mais le rassemblement des masses de données sur un seul et même réseau permet à n'importe qui d'avoir accès à n'importe quel savoir.

Il existe de nombreux moyens de se renseigner sur la cible en fonction du type de cible dont il s'agit ainsi que des informations que nous désirons récupérer.

Nous pouvons nous attarder sur les récupérations d'informations les plus fréquentes.

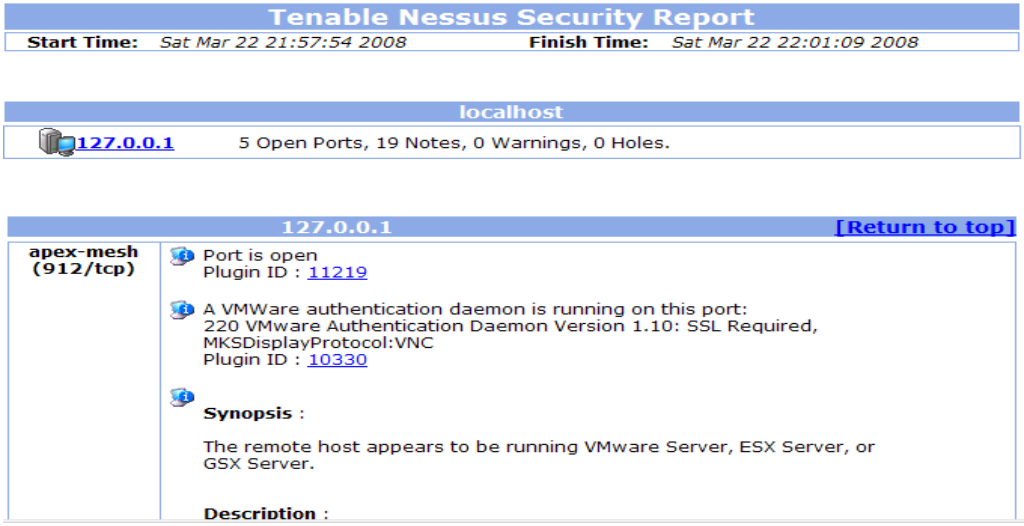
Collecte d'information - Système
Il est possible d'utiliser l'outil **Nmap** afin de se renseigner sur les ports ouverts d'un système distant afin de savoir le type d'attaque qu'il est possible de lancer.
En effet, Nmap va nous donner une liste de « service » s'exécutant sur la machine et dont il est possible de soutirer des informations.

Suite à un Scan des ports sur une machine, distante, nous pouvons les ports ouverts ce qui peut aiguiller nos attaques. En effet une attaque sur un port protégé sera nettement plus difficile.

Dans notre exemple, nous pouvons voir que le port 79 est ouvert, ce qui peut être une très bonne chose pour toute collecte d'information.
En effet, le port 79 est un utilitaire Internet qui permet à quelqu'un d'obtenir des informations sur vous, y compris votre nom complet, votre login et autres informations de profilage.
Ces informations peuvent s'avérer très utilise pour une attaque ultérieure.

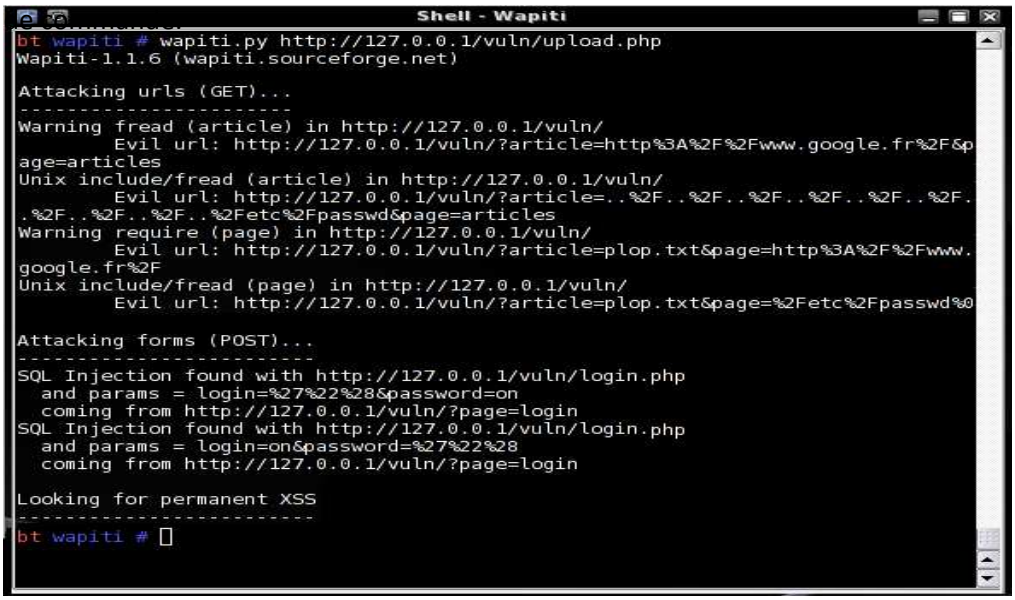
Collecte d'information - Vulnérabilité système

Il est possible d'utiliser l'outil **Nessus** afin de détecter les vulnérabilités sur un système cible distant. Il signale les faiblesses potentielles ou avérées sur les machines cible en incluant les services vulnérables à des attaques permettant la prise de contrôle de la machine, l'accès à des informations sensibles, les fautes de configuration, les patchs de sécurité non appliqués, les mots de passe par défaut, quelques mots de passe communs, et l'absence de mots de passe sur certains comptes systèmes etc.



Collecte d'information - Vulnérabilité Web

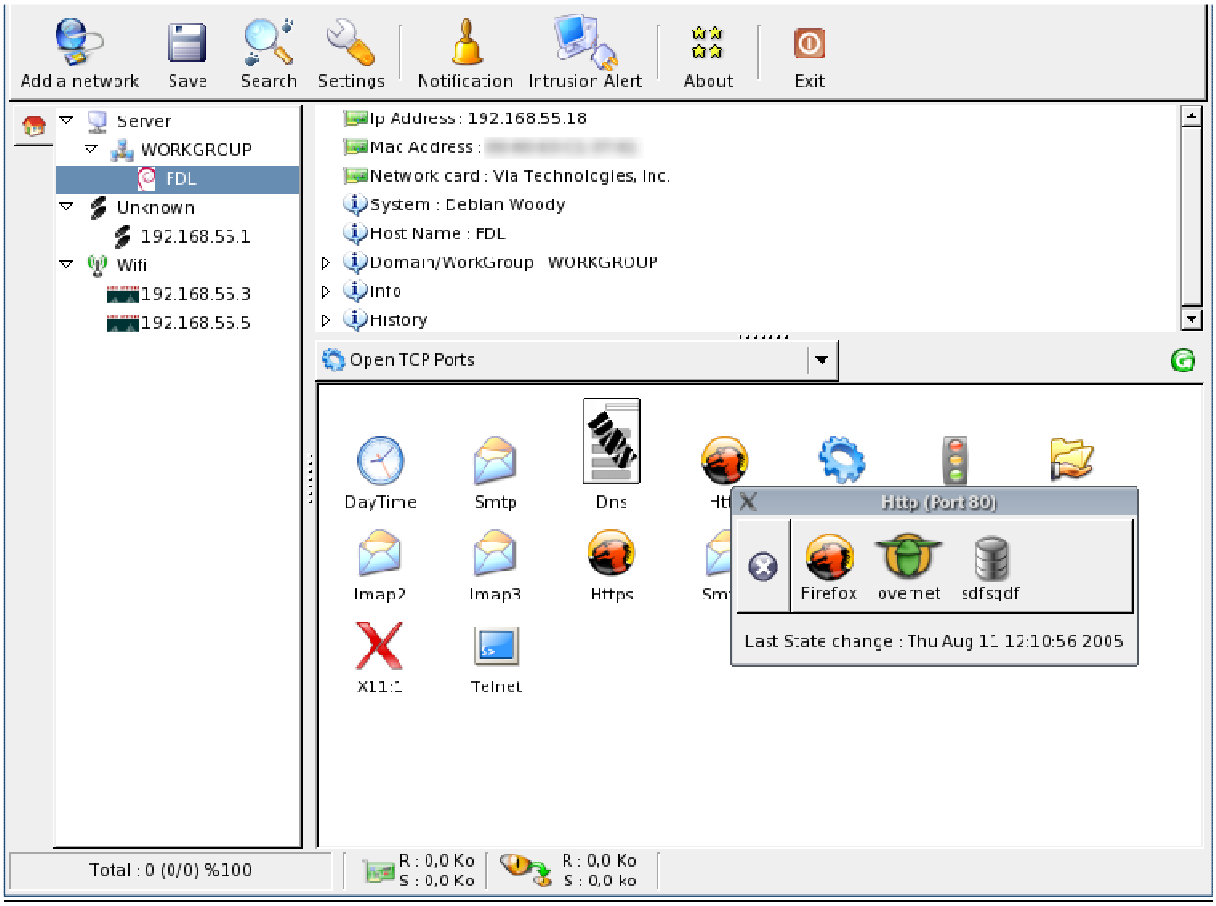
Il est possible d'utiliser l'outil **Wapiti** afin de détecter les vulnérabilités d'un site Web afin de savoir par ou attaquer. Wapiti s'attaque à l'interface du site afin d'y déceler des vulnérabilités inhérentes aux langages dynamiques. Parmi la multitude de scanner existant, celui-ci propose une étude relativement complète. Ainsi, parmi les failles les plus communes, on peut citer des vulnérabilités de type SQL, de type XSS et également d'autres vulnérabilités, tel que l'inclusion de fichier, l'exécution



On peut voir que la page est vulnérable a des attaques de type Injection SQL ainsi qu'à des attaques de types Injection XSS ce qui va pouvoir orienter nos choix rapidement.

Collecte d'information - Réseau

Il est possible d'utiliser l'outil **Autoscan** afin de lancer une série de scan à travers le réseau, pour trouver tout matériel (routeur, pare-feu...), et toutes machines connectées. Ses principales caractéristiques sont de reconnaître les systèmes d'exploitation de ses hôtes, ainsi qu'une série d'informations intéressantes (Ports ouverts, nom de la machine, détection de ressources partagées,...). De plus Autoscan peut émuler un client Telnet, et Nessus.



Il est à présent possible de connaître toute la structure du réseau allant des machines hôtes aux Access Point Wifi en passant par les routeurs.

3) Utilisations de ses informations

Comme nous avons put en parler précédemment, une attaque informatique classique se déroule en 5 étapes et la plupart du temps respecte la règle des 5 P.
Après avoir vu la première partie qui rappelons le est **Probe** correspondant à la récupération d'informations sur la cible, nous allons maintenant nous intéresser à la deuxième partie tous aussi important : **Penetrate** qui quand à elle correspond à l'utilisation des données récupérées afin de pouvoir pénétrer le système cible.

Le type d'attaque que nous allons lancer va dépendre du type d'informations que nous avons récupéré dans l'étape précédente. La récupération d'information ne doit donc pas être prise à la légère afin de maximiser les chances de pénétration du système cible.

En effet, après un scan de vulnérabilité avec Nessus, nous allons plutôt nous attaquer à des vulnérabilités système tels que des Buffer Overflow, ou bien des dénis de service alors qu'avec un scan de vulnérabilité avec Wapiti vas nous emmener vers des attaques Web

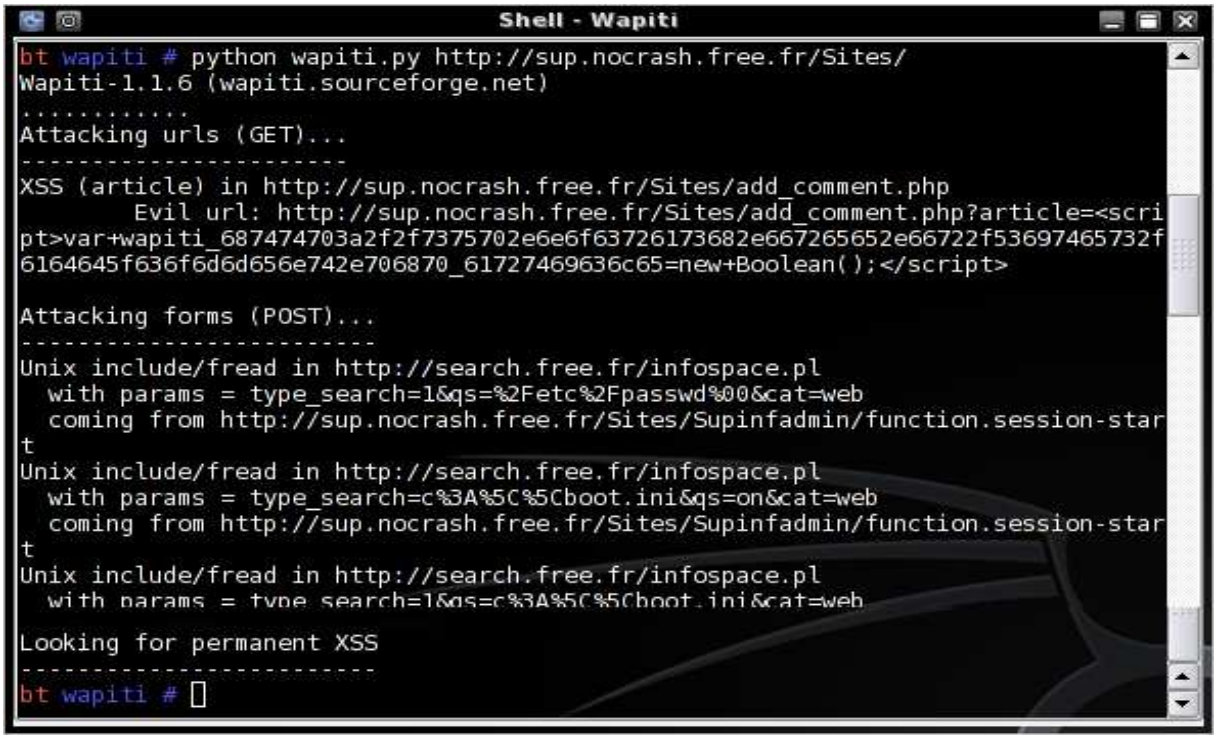
Nous allons présenter un cas concret d'attaques Web.

Nous allons donc utiliser une structure d'attaque en deux étapes :

1 - Récupération d'informations
2 - Utilisation de ses informations pour attaquer un site Web

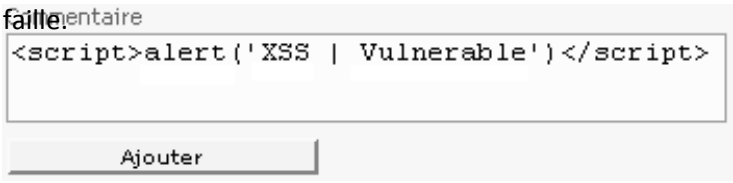
1 - Récupération d'informations

Pour la récupération de données, nous allons utiliser Wapiti sur le site cible.



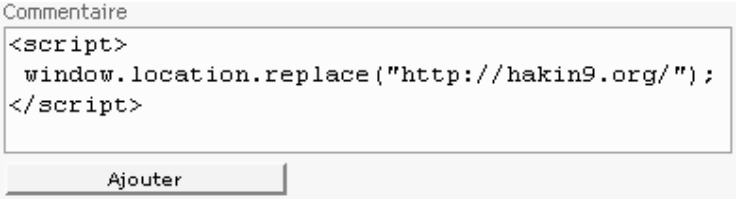
2 - Utilisation de ces informations

Nous pouvons voir qu'une des pages du site (**add_comment.php**) est sensible à des attaques de type XSS. Nous allons donc essayer de réaliser une injection simple afin de vérifier la présence de cette faille.



Une fois le commentaire ajouté, nous sommes automatiquement redirigé sur une page ou nous pouvons voir l'affichage suivant :

Nous avons donc la confirmation que le code est sensible à des attaques de types XSS.
A partir de ce moment, il est possible de réaliser de nombreuses attaques permettant par exemple de rediriger tous le trafic du site vers un autre site avec le code suivant :



Avant de vous lancer à corps perdu dans la collecte d'information ainsi que l'attaque de cibles que ce soit des sites internet ou bien de machines cliente ou même des serveurs, vous devez savoir que nul n'est censé ignorer la loi. Personne n'est capable de retenir les 8000 lois et 110 000 décrets mais il est nécessaire que connaître les parties qui nous intéressent afin de savoir ce qui est autorisé et ce qui ne l'est pas. Nous allons ici simplement présenter un bref rappel des lois présentent dans le Code Pénal les plus importantes dans notre cas de figure :

Recherche de failles et d'exploits
Sans doute la plus importante activité du piratage, la recherche de failles et d'exploit consiste à trouver les erreurs dans les programmes et les façons de les utiliser pour obtenir que le programme ait un comportement différent de celui prévu. La recherche de failles consiste uniquement à rechercher l'erreur et à inventer une technique pour l'utiliser. En aucun cas, il ne s'agit d'utiliser cette technique concrètement. Logiquement, rien dans le code pénal n'interdit la recherche de failles ni la création d'exploits. C'est un moyen pour autoriser la recherche en sécurité informatique, et permettre aux entreprises de pouvoir se défendre contre le piratage.

Intrusion
L'intrusion est le fait, par un moyen quelconque, d'accéder à un système informatique et de l'utiliser. Il s'agit donc ici, notamment, de l'utilisation d'un exploit sur un serveur, de la pose de backdoor, de rootkits et autres. Ceci est interdit. S'introduire et/ou rester dans un système informatique est punissable de 3 ans d'emprisonnement et de 30 000 euros d'amendes. Un durcissement de la peine est prévu en cas de modification de données ou une altération du fonctionnement.
La tentative de piratage est punie comme si l'acte avait été commis

Défaçage
Le défaçage consiste à changer un site web. Techniquement, il s'agit de changer les fichiers du site web. En pratique, les internautes se retrouveront avec une autre page que celle attendue. Ça peut aller du simple ajout de "HacK3D by NoCrash" à un changement complet de la page. Ceci est interdit [Art. 323-2 et 323-3], et puni durement. En effet, le fait de fausser le fonctionnement d'un système informatique [Art. 323-2] et le fait d'ajouter/modifier/supprimer des données [Art. 323-3] sont tous deux punis de 5 ans d'emprisonnement et de 75 000 euros d'amende.

Utilisation des données
Par utilisation des données, nous entendons la collecte d'informations, leur traitement et leur commerce. Quand il s'agit de données personnelles, ces actions sont punies de 5 ans d'emprisonnement et d'une amende variable [Art. 226-16 à 226-24]. Il s'agit de dispositions de la loi relative aux fichiers et aux libertés.
Cependant, le fait de donner/vendre ces données peut s'assimiler à du recel [Art. 321-1] et est puni de 5 ans de prison et de 375000 d'amende.

Le code pénal a bien verrouillé le domaine du hacking. Les articles 323-1 à 323-7 sont suffisamment généraux pour s'appliquer dans presque tous les cas. (En fait, seul le phreaking et le cracking ne sont pas concernés par le code pénal). Depuis 2004 et la LCEN, les peines ont été augmentées et la loi durcie. En effet, depuis la LCEN, les teams risquent l'association de malfaiteurs, le travail en groupe est quasi illégal et la diffusion d'informations et de technique est assez risquée. La LCEN, a aussi rajouté quelques zones de flous. Ces zones de flou concernent surtout l'article 323-3-1, avec son motif légitime et autres notions assez vagues. La jurisprudence devrait faire son apparition d'ici quelques temps avec quelques affaires en cours.

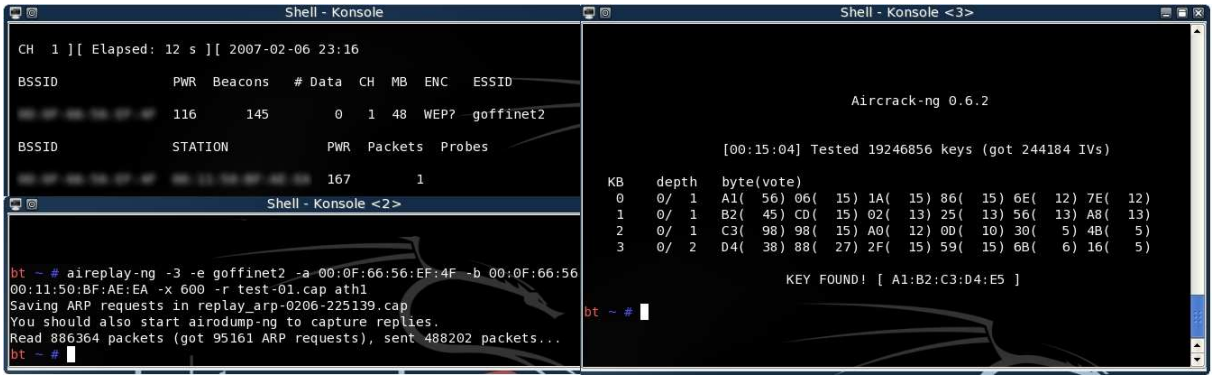
4) Le WIFI 802.11g/b et le Bluetooth

A l'heure actuelle, la plupart des providers (Free, Alice, Wanadoo etc.) fournissent dans leurs offres un modem Wifi (livebox, freebox etc.). Malheureusement, la plupart de ces box Wifi applique par défaut un cryptage WEP (**Wired Equivalent Privacy)** lorsque l'on active le sans fil.
Depuis plusieurs années, la sécurité WEP est une sécurité obsolète et il est devenu simple de cracker des clés WEP en moins de 5 minutes depuis 2005 ainsi que des clés WPA (attaque par dictionnaire)

Comme nous avons put le dire précédemment, la version 3.0 apporte une grande amélioration concernant la compatibilité des cartes Wifi. En effet, avant de pouvoir réaliser des attaques contres des clés WEP/WPA, il est nécessaire de passer sa carte wifi en mode monitoring pour pouvoir permettre l'injection de paquet. Lors de sa première sortie, avec la version 1.0, très peu nombreuses étaient les cartes compatibles avec le mode monitor. Les cartes de type atheros sont en règle générale très bien reconnu. Si par malchance, vous ne disposez pas d'une carte wifi supportant l'injection de paquet, il vous est possible d'acheter un adaptateur externe le permettant.

Il vous sera possible de trouver tous les logiciels vous permettant les attaques contres des réseaux WEP/WPA. Nous pouvons bien sur la célèbre suite aircrack-ng (anciennement aircrack) composé d'airodump-ng (capture de paquets), aireplay-ng (injection de paquet), aircrack-ng (crack de clé)

La puissance de cette suite à déjà était mise en pratique de nombreuse fois avec de nombreuses vidéo disponible actuellement sur le net.

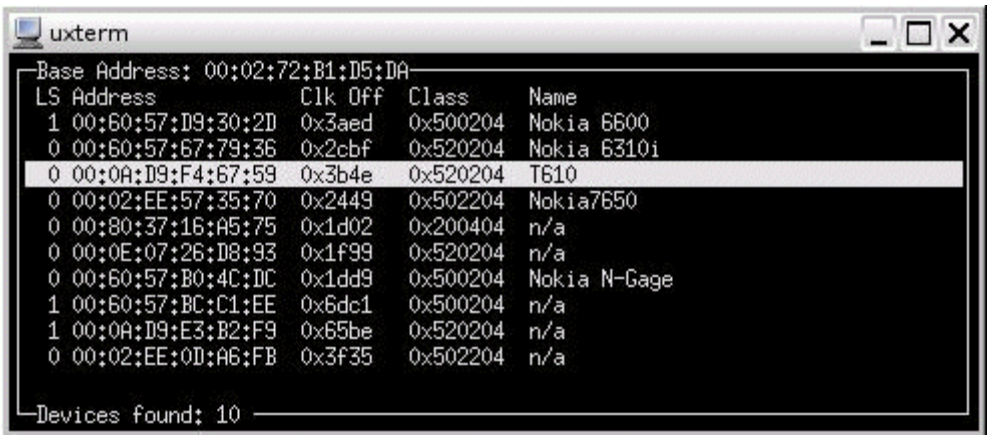


Depuis 2007, un nouvel outil permet de réaliser le crack d'une clé WEP de manière complètement automatisé. Il s'agit de wesside-ng. Wesside-ng se charge ensuite de s'authentifier sur le réseau cible, d'obtenir un PRGA (Pseudo Random Generator Algorithm), il détermine le plan d'adressage du réseau, injecte des ARP request et enfin crack la clef WEP grâce aux ARP générés par le réseau wifi en utilisant une attaque par fragmentation.

De nombreux outils tels que tels Kismet, Airsnort, coWPAtty, FakeAP sont également disponible.

Comme nous avons put le dire, la compatibilité de BackTrack concernant les réseaux sans fils ne cesse d'augmenter pour rendre de plus en plus de matériels et constructeur compatible.
Nous avons démontré la puissance de BackTrack vis à vis de raisons Wifi et le danger que cela pouvait entraîner, mais il existe d'autre type de réseau sans fil. En effet, depuis sa toute première apparition en 1994, le Bluetooth ne cesse de prendre de l'ampleur pour actuellement se retrouver dans de nombreux périphériques informatiques tels que des imprimantes et dans la plupart des récents téléphones cellulaires. De nos jours, les téléphones cellulaires sont devenus une très grande source d'informations (Carnet d'adresse, numéro de téléphone privé, messages).
Comme le Wifi, le Bluetooth n'est à présent plus une technologie sure. En effet de nombreux logiciel exploitant les vulnérabilités du Bluetooth ont vu le jour ces dernières années.

Des outils tels que *Ghettotooth*, *BTscanner* ou *RedFang* sont des scanneurs de Bluetooth permettant de récupérer de nombreuses informations sans avoir à se connecter sur le système cible (marque du constructeur, adresse mac, nom du périphérique...). Encore une fois, nous appliquons bien la recherche d'informations avant toutes autres actions.



Des outils tels que BlueBugger, BlueSnarfer, BTcrack quand à eux, sont des outils permettant l'exploitation de failles du protocole Bluetooth entrainant la possibilité de prendre possession d'un téléphone cellulaire sans le consentement de son propriétaire et de manière invisible.
Il sera alors possible de passer des appels, envoyer/lire des SMS, lire/modifier/supprimer les entrées du carnet d'adresse, se connecter à Internet etc.
Ces outils font de vos informations confidentielles, des informations lisibles par un pirate

```
root@3[~]# bluesnarfer -s SM -r 1-10 -b 00:02:EE:AD:A5:2B
device name: Dz2
custom phonebook selected
+  1 - InfoTalk : 2300
+  10 - ServiceCenter : 2202
bluesnarfer: release rfcomm ok
```

Le moyen le plus sur de ne pas avoir de problème avec ces logiciels, qui comme vous avez put le comprendre mettent vos informations personnelles à découvert, est de simplement désactiver le Bluetooth une fois que vous n'en avez plus l'utilité et éviter d'accepter des communications Bluetooth lorsque vous n'êtes pas sur du destinataire.

5) BackTrack, le couteau suisse de la sécurité

Comme nous avons put le dire précédemment, l'objectif de BackTrack est de fournir une distribution compacte regroupant le maximum d'outils nécessaire aux tests de sécurité d'un réseau ou d'application.
Le nombre d'outils liés à la sécurité informatique ne cesse de croître avec les versions de BackTrack. Dans la version 3.0, nous disposons d'approximativement 300 outils décomposés en 16 catégories. Voici les parties qu'il nous est possible d'utiliser dans de nombreux cas :

Analyse de réseau sans fil

Comme nous avons put le présenter précédent, BackTrack permet de nombreuse analyse des réseaux sans fils tels que le Wifi ou bien le Bluetooth.
Pour l'analyse et le crackage de Wifi, BackTrack dispose de la célèbre suite **aircrack-ng** qui à déjà réalisé ses preuves ainsi que de nouveaux outils tels que **wesside-ng**.

Pour l'analyse et le crackage de Bluetooth, BackTrack dispose d'outils connus tels que **BTscanner** et **BlueSnarfer** permettant respectivement l'analyse et le crackage de réseau Bluetooth

Anonymat

Afin d'éviter de nombreux démêlés judiciaires, il peut être une bonne chose de ne pas laisser de traces sur les différents systèmes comme dans les fichiers de logs par exemple.

Le logiciel **TOR** permet d'être complètement invisible sur le net sans laisser la moindre trace. *Tor est un projet qui aide à la défense contre l'analyse de trafic, une forme de surveillance de réseau qui menace les libertés individuelles et l'intimité, les activités commerciales et relationnelles, et la sécurité d'état. Tor vous protège en faisant rebondir vos communications à l'intérieur d'un réseau distribué de relais maintenus par des volontaires partout dans le monde : il empêche qu'une tierce personne scrutant votre connexion internet connaisse les sites que vous avez visités, et empêche les sites que vous avez visités de connaitre votre position géographique.*

Attaque de mot de passe

Comme pour toute distribution de sécurité qui se respecte, BackTrack dispose d'un large panel de possibilité d'attaque contre les mots de passe que ce soit des attaques « en ligne » ou bien « locale ». Concernant les attaques en lignes, nous pouvons noter la présence du puissant **Hydra**. Hydra est actuellement considéré comme l'un des meilleurs brute forceur en ligne.

Concernant les attaques hors lignes, BackTrack dispose de **RaimbowCrack**.
RaimbowCrack est un casseur de mot de passe basé sur les raimbows tables ce qui le rend excessivement puissant. Avec un tel logiciel, le crackage d'un mot de passe de prend plus que quelques minutes et ne nécessite pas de grosse ressources à mettre en œuvre.

Collecte d'informations

Comme nous avons put le voir précédemment, il existe de nombreuses techniques de collection d'informations. Il faut toujours prendre très au sérieux cette partie qui est la base de toute attaques de petite ou de grande envergure.
Suivant le type d'informations que nous désirons rechercher, nous avons la possibilité de choisir parmi les nombreux outils que nous propose BackTrack.
Wapiti va nous permettre de récupérer des informations sur les failles Web alors que **Nessus** va nous permettre de visualiser les vulnérabilités d'un système d'exploitation ainsi que ces services alors que **nmap** va simplement nous renseigner sur les ports ouverts.

Pénétration

Comme nous avons put en parler précédemment, l'étape suivant la récupération d'information est en règle générale la pénétration de la cible. Pour cela, BackTrack met à notre disposition de célébrissime **Métasploit**. Métasploit est un projet qui rassemble tous les développeurs d'exploit qui partagent leurs découvertes à travers le monde. Il contient une base de données d'environ 300 exploits, capable de simplifier les tests d'intrusion sur des failles importantes. Metasploit 3.0 a également commencé à inclure des outils de fuzzing, pour découvrir des vulnérabilités de logiciels en premier lieu, plutôt que de simplement être fait pour l'exploitation de celles-ci.

Reverse engineering

Le **reverse engineering** ou **rétro-ingénierie** est l'activité qui consiste à étudier un programme pour en déterminer le fonctionnement interne ou sa méthode de fabrication afin de pouvoir par exemple s'octroyer des accès ou des fonctionnalités ne nous étant pas autorisé initialement. Dans le monde underground, le reverse engineering est communément appelé cracking. Pour réaliser le cracking, il est nécessaire de se munir de plusieurs types de logiciels tels qu'un **désassembleur** permettant d'inspecter le code compilé en assembleur, un **débogueur** permettant de visualiser l'état du programme en cours d'exécution et **un éditeur hexadécimal** permettant de modifier le programme.
BackTrack nous propose des outils très performant en matière de cracking avec pour débogueur/désassembleur le célèbre **Ollydbg** et comme éditeur hexadécimal le tout aussi célèbre **Hexedit**.

Sniffers

Comme nous pouvons le savoir, les sniffers sont des logiciels qui peuvent récupérer les données transitant par le biais d'un réseau local. Ils permettent de facilement consulter des données non-chiffrées et peuvent ainsi servir à récupérer des mots de passe ou toute autre information. BackTrack dispose de trois des sniffers les plus connus et les plus performants. En effet, on peut retrouver **Dsniff**, **Ettercap-ng** (anciennement Ettercap) et **Wireshark** (anciennement Ethereal). Ces trois outils sont excessivement puissant et permettent des analyses de trafic très précis.

7) Conclusion

BackTrack est à l'heure actuelle la distribution la plus aboutie en matière de sécurité informatique. BackTrack se qualifient tant par le nombre impressionnant d'outils que leur par qualité reconnu par les professionnels. Ces nombreux développeurs et sa large communauté permettent d'avoir une distribution de plus en plus stable avec une compatibilité accrue avec les différents constructeurs de matériels. BackTrack a gagné une grande notoriété et c'est pourquoi, en 2006, BackTrack a été élu comme étant la première distribution de sécurité par insecure.org.
Nous attendons à présent la sortie officielle de la version 3.0 stable prévu d'ici quelques mois.