RÉGIS SENET

Introduction à BackTrack 3

Degré de difficulté

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

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 corrections de bug.

BackTrack est une distribution GNU/Linux issue de Whax et ASC (*Auditor Security Collection*) c'est aussi un système d'exploitation de type Slackware, reposant sur une interface KDE.

La version 3.0 Beta, étant la version actuelle, intègre un noyau 2.6.21.5 permettant entre autres 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 nécessaires 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 clés WEP/ WPA et autres tests (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 *Live CD*, 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 *Live CD* permet d'avoir tous les outils indispensables à la sécurité

Figure 1.

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).

informatique sans laisser aucune trace.

Voici une liste non exhaustive de quelques mises 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. 2.6.21.5),
- Amélioration de la compatibilité des cartes Wifi,
- Amélioration du script de configuration de Xorg,
- Mise à jour des repos d'exploit et des exploits du Framework metasploit,
- Démarrage réseau possible depuis la version USB (PXE Boot),
- Amélioration de la comptabilité sur Mac avec la reconnaissance de la carte airport D'autres mises à jour 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.

Récupération d'informations

Des statistiques nous ont montré qu'une attaque à l'aveugle sur un système distant est dans 99% des cas totalement inefficaces. 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 nous donne 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 *il manque un verbe ?* 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 utiles pour une attaque ultérieure. *je ne vois pas de référence vers le service finger.*

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 cibles en incluant les services vulnérables à des attaques permettant la prise de contrôle de la machine, l'accès à des informations sensibles, les erreurs de configuration, les patchs de sécurité non

Figure 2.

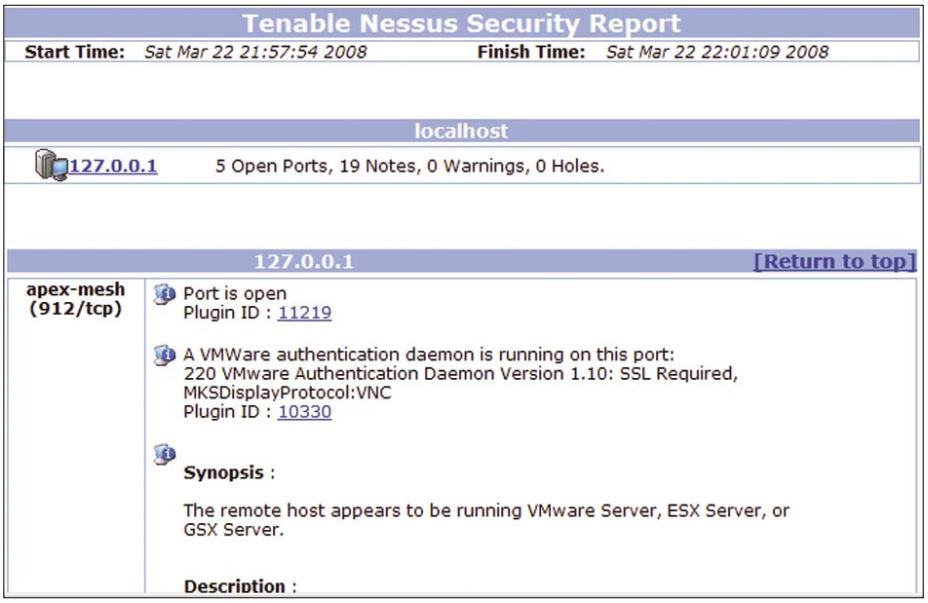

Figure 3.

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 et 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 scanners existants, 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, telle que l'inclusion de fichiers, l'exécution de commandes.

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

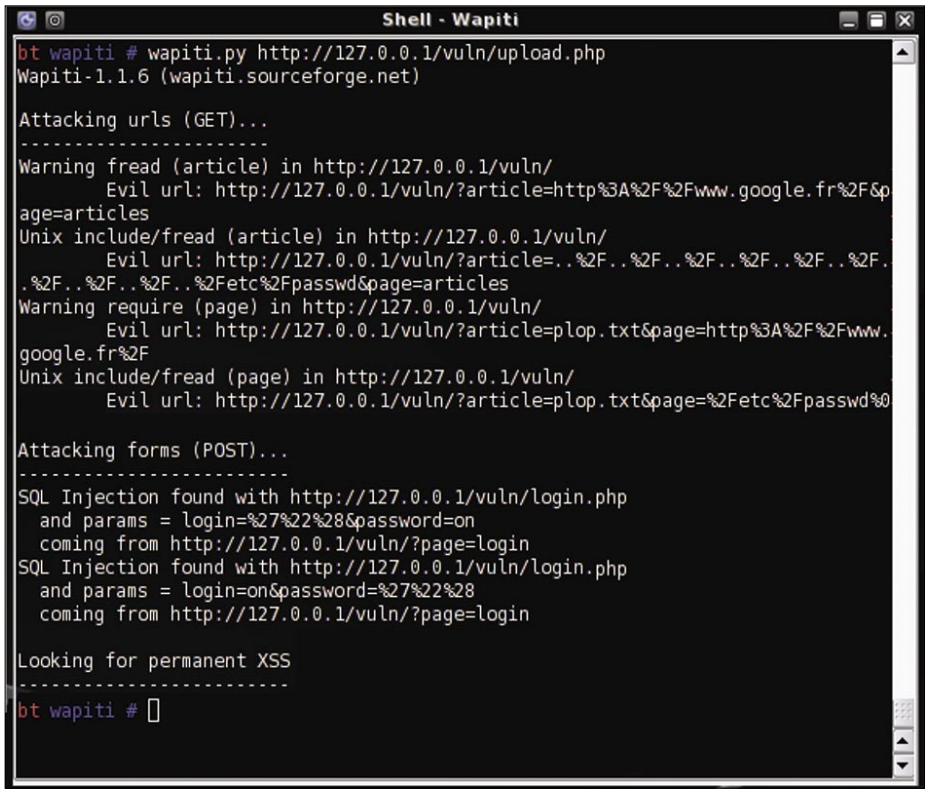

Figure 4.

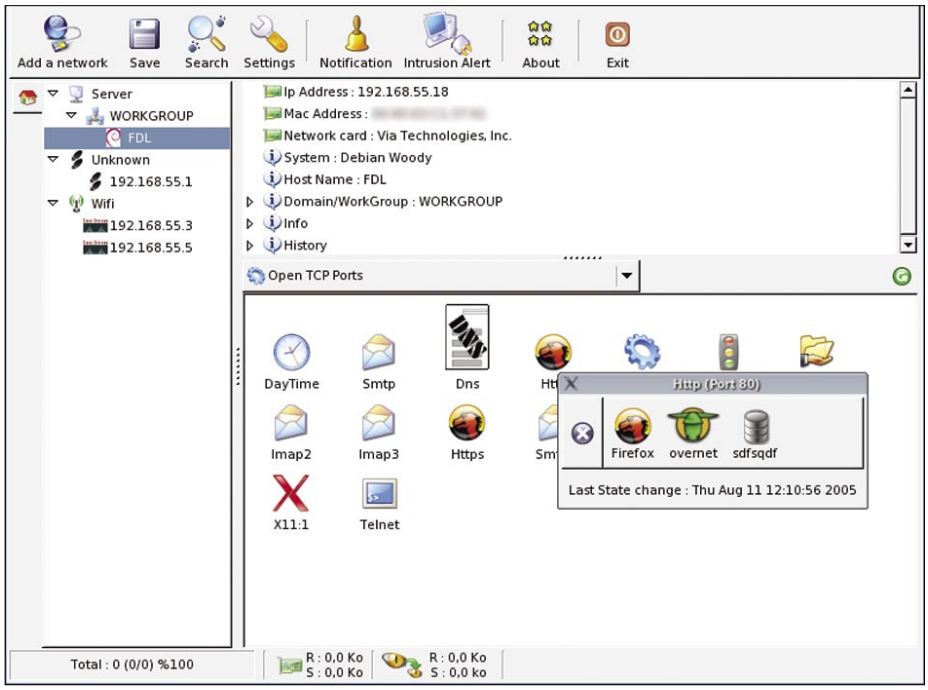

Figure 5.

Collecte d'information – Réseau

Il est possible d'utiliser l'outil *Autoscan* afin de lancer une série de scans à travers le réseau, pour détecter tout matériels et programmes (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.

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 quant 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 récupérées 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 systèmes tel que des Buffer Overflow, ou bien des dénis de service alors qu'avec un scan de vulnérabilités avec Wapiti vas nous emmener vers des attaques Web

Nous allons présenter un cas concret d'attaques de site Web.

Nous allons donc utiliser une structure

d'attaque en deux étapes :

- Récupération d'informations,
- Utilisation de ses informations pour attaquer un site Web.

Récupération d'informations

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

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 redirigés 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. À partir de ce moment, il est possible de réaliser de nombreuses attaques permettant par exemple de rediriger tout 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 es plus importantes dans notre cas figurant le Code Pénal.

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

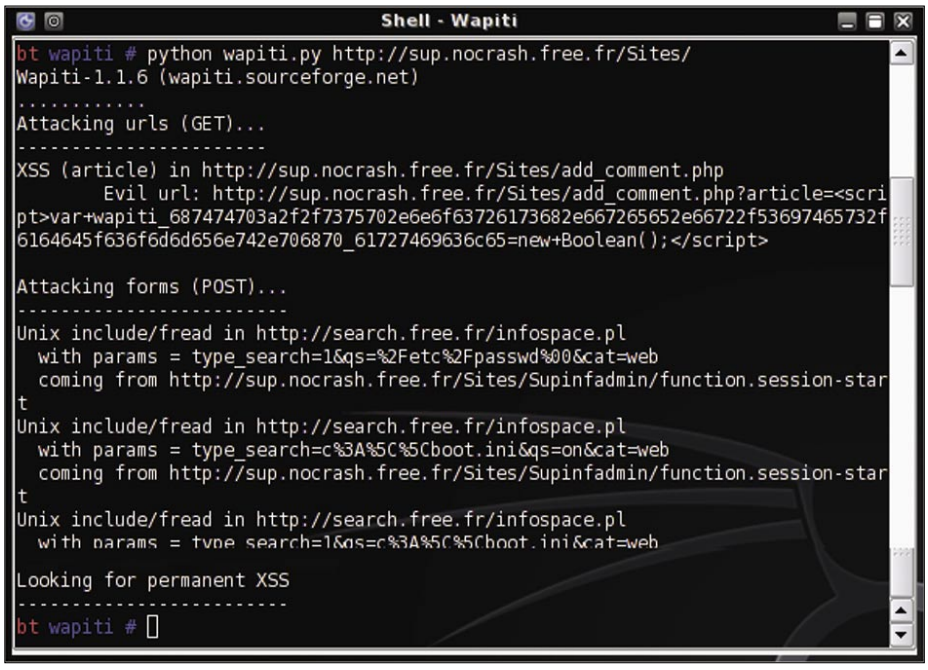

Figure 6.

Figure 7.

Figure 8.

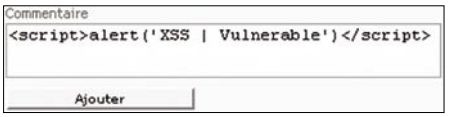

Figure 9.

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

Régis Senet
Régis Senet est actuellement étudiant en troisième année 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*

[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.