Un 'rootkit open source' pour Linux !

Immunity distribue un logiciel permettant de tester des intrusions sous Linux, du nom de **Debug Register RootKit**. Ce produit est placé sous licence GPL. En fait, il ne s'agit ni plus ni moins que d'un ***rootkit***, un programme qui s'installe en mode administrateur et permet de cacher des portes dérobées. À l'aide d'un *rootkit*, un pirate peut prendre le contrôle d'une machine à l'insu de l'utilisateur.

DR RootKit est un module qui utilise les registres de débogage présents dans les processeurs Intel x86 (architecture IA32). Il fonctionne avec les noyaux Linux 2.6 et peut cacher des processus, des *sockets* réseau et des fichiers.

Bien évidemment, le but n'est pas de proposer un outil aux pirates, mais une implémentation de référence d'un *rootkit*, permettant aux spécialistes de la sécurité de **trouver des parades à ce genre de menaces**, ou de mettre à l'épreuve leurs outils de sécurité et de détection. À cet effet, DR RootKit est supporté par la suite de tests Canvas Professional de l'éditeur, laquelle est disponible pour Windows, Linux, Mac OS X, *etc.*

Comme toujours dans le monde de la sécurité, la limite est cependant étroite entre un code source censé tester une machine afin de mieux la sécuriser et l'utilisation de ce même code source à des fins inavouables. **Gageons que les utilisateurs de Canvas Professional ne sont pas tous des administrateurs systèmes soucieux de la sécurité de leurs serveurs.**

La plupart des distributions Linux ne favorisant pas par défaut l'utilisation systématique et continue du compte administrateur, DR RootKit ne représente aucune menace réelle (son installation ne peut s'effectuer qu'avec les droits du compte *root*). Ouf.