Ultimate Hacking : McAfee propose une formation aux DSI

L'objectif de ces cours est de montrer aux responsables informatiques des entreprises petites ou grandes, comment se protéger de façon pro active contre les méthodes utilisées par les Hackers.

L'un des aspects les plus originaux de la formule est la mise en pratique de hack pendant les cours. Des démonstrations sont faites et chaque étudiant doit réaliser des tentatives d'intrusion. Ainsi, les DSI seront plus à même de repérer d'éventuelles fraudes ou failles dans un réseau ou sur un poste du réseau et ainsi être plus réactif, voire même d'anticiper les menaces. Une partie de l'enseignement est également consacrée aux méthodes de réparations des failles et aux techniques qui existent pour isoler ou réduire le risque. Les démonstrations peuvent être réalisées sur n'importe quels OS, de Solaris en passant par les Windows, Linux ou le MacOS X soi-disant impénétrable d'Apple. Les machines utilisées ont d'ailleurs un double boot, Linux/Windows. Comme l'explique Martin Pivetta, Business Development Manager et spécialiste des techniques de Hacking et de l'intrusion : *« pour nos cours, nous utilisons différents outils de sécurité, aussi bien open source que propriétaires, car les hackers utilisent tous les outils possibles. »* Le placement des produits étiquetés McAfee ne semble pas la priorité de ces cours qui ont véritablement une fonction pédagogique. **Comprendre la méthode du Hacker performant** Hacker peut être un métier à plein temps pour les informaticiens attirés vers l'obscur. Et ce n'est pas un travail de tout repos. Il demande de la patience, de la ruse et de longues nuits devant l'écran, un grand thermos de café chaud à portée de la main. Pour saisir comment une Hacker obtient des informations, il faut se pencher sur sa méthodologie. Voici comment elle se décompose. Dans un premier temps, notre garnement de la Toile va procéder au Footprint, l'empreinte. Traduction: il va essayer d'obtenir un maximum d'information sur sa cible. C'est en quelque sorte la phase préparatoire durant laquelle l'espionnage est de rigueur. Pour illustrer cette méthode on peut imaginer que plutôt de s'attaquer directement à un grand groupe surprotégé, il va chercher à s'infiltrer dans le réseau d'une de ses filiales et chercher de l'information en procédant à des scans, le tout le plus discrètement possible. Car rester invisible est une des difficultés les plus grandes du hacking. Une fois que les informations récupérées sont soigneusement rangées sous la forme de tableau (excel) notre hacker méticuleux va s'introduire dans le système s'adonner au pillage, interagir sur le réseau par exemple en rentrant sur un groupe de travail (option groupe de travail sous Google) pour y récupérer des noms, des fonctions, tout est bon ou presque. Une fois son travail terminé, il efface toute trace de son passage et parfois tous les documents de votre disque dur. Martin Pivetta, insiste sur le fait que les utilitaires de base sont très performants, même avec des commandes simples l'on peut obtenir des informations précieuses sur un groupe (par exemple avec un simple tracert ou Ping). Enfin, trouver des informations sur le net est à la portée de presque tous les internautes (Google Hacking, Whois, DNS et même les sites publics) et des programmes comme Neotrace ou Super Scan permettent de faire des reconnaissances de réseau d'une grande précision. Après cette formation de quatre à cinq jours, l'administrateur réseau doit être capable de repérer des modifications suspectes, et procéder à sa « checklist » pour trouver la faille et se protéger des attaques DDos, des chevaux de Troie, des keyloggers, des spywares , des rootkits, et autres menaces. Martin Pivetta confie *« dans certains cas l'on voit même le hacker en train d'essayer*

d'agir. Dans ces cas-là, autant être rapide et savoir ce que l'on fait. »