



## Sécurité informatique - Ethical Hacking: Apprendre l'attaque pour mieux se défendre

- Author : ACISSI.
- Publisher : Editions ENI, 2009
- pages : 355 pages
- N° Class : 621/178

Ce livre sur la sécurité informatique (et le ethical hacking) s'adresse à tout informaticien sensibilisé au concept de la sécurité informatique mais novice en la matière. Il a pour objectif d'initier le lecteur aux techniques des attaquants pour lui apprendre comment se défendre. Après une définition précise des différents types de hackers et de leurs objectifs, les auteurs présentent la méthodologie d'une attaque et les moyens de repérer les failles par lesquelles s'insérer dans un système. Le chapitre sur le Social Engineering, ou manipulation sociale, illustre pourquoi les failles humaines représentent plus de 60% des attaques réussies. Les failles physiques, qui permettent un accès direct aux ordinateurs visés ainsi que les failles réseaux et Wi-Fi sont présentées et illustrées avec à chaque fois des propositions de contre-mesures. La sécurité sur le web est également présentée et les failles courantes identifiées à l'aide d'outils qui peuvent facilement être mis en place par le lecteur sur ses propres systèmes. L'objectif est toujours d'identifier les failles possibles pour ensuite mettre en place la stratégie de protection adaptée. Enfin, les failles systèmes sous Windows ou Linux sont recensées puis les failles applicatives avec quelques éléments pour se familiariser au langage assembleur et ainsi mieux comprendre les possibilités d'attaque. Les auteurs de ce livre composent une équipe de personnes de conviction qui se donnent pour mission de rendre la sécurité informatique accessible à tous : "apprendre l'attaque pour mieux se défendre" est leur adage. Hackers blancs dans l'âme, ils ouvrent au lecteur les portes de la connaissance underground.