



# Détection d'intrusion de réseau

- **Author :** Stephen Northcutt
- **Publisher :** Vuibert Informatique, 2004
- **pages :** 479 pages
- **N° Class :** 621/816

En dépit des efforts des experts en sécurité, les réseaux sont sujets à un nombre croissant d'attaques de plus en plus sophistiquées. Cet ouvrage vous apprendra à les détecter et à les contrer, en faisant de vous un analyste en détection d'intrusion. Les auteurs, experts réputés en sécurité réseau, communiquent leur expérience dans cet ouvrage. Ils présentent en détail les techniques d'analyse de trafic, les signatures d'attaque, l'utilisation d'outils d'analyse, le paramétrage de la sécurité d'un système, la gestion manuelle ou automatique des intrusions, la mise en œuvre d'un projet de sécurité d'entreprise, etc. Cette nouvelle édition aide notamment à : comprendre TCP dans un contexte réel ; analyser un trafic réseau ; obtenir des informations sur une attaque à partir de champs IP ou de protocoles de plus haut niveau ; reconnaître signatures d'intrusion, dénis de service, motifs d'attaque courants, et à se préparer à gérer des motifs inconnus ; utiliser TCPdump et Snort pour distinguer trafics normaux et anormaux ; paramétrer un système pour assurer sa sécurité ; apprendre à utiliser des réponses manuelles et automatiques aux intrusions ; intégrer un modèle de détection d'intrusion dans le système d'information d'une entreprise.