Nouvelle Approche de Corrélation d'Alertes basée sur la Fouille Multidimensionnelle

Hanen BRAHMI, Imen BRAHMI, Sadok BEN YAHIA

Faculté des Sciences de Tunis.
Département des Sciences de l'Informatique.
Campus Universitaire 1060.
{hanenbrahmi; imen.brahmi}@gmail.com, sadok.benyahia@fst.rnu.tn

Résumé. En réponse aux problèmes posés par la complexité croissante des réseaux et des attaques, les Systèmes de Détection d'Intrusions (SDIs) constituent une bonne alternative pour mieux sécuriser un système informatique. Cependant, les SDIs existants présentent des lacunes en terme de génération excessive d'alertes. Réellement, la majorité de ces alertes ne correspondent pas à des attaques (fausses alertes, alertes redondantes, etc.). Ainsi, la corrélation d'alertes est un processus d'analyse appliqué à des journaux d'alertes. Dans cet article, nous proposons une nouvelle approche pour la corrélation d'alertes basée sur le couplage entre la fouille de données et les outils OLAP (*On Line Analytical Processing*). L'idée intuitive derrière cette approche est de profiter des avantages de la fouille de données multidimensionnelles afin de rehausser l'analyse des alertes et introduire une solution puissante pour faire face aux défauts des SDIs. Les expérimentations, que nous avons menées, montrent l'efficacité de notre nouvelle méthode de corrélation d'alertes.

1 Introduction

Avec le développement accru des réseaux de communication, les risques causés par les attaques sur les systèmes informatiques deviennent un réel problème pour les entreprises et les organisations. Par conséquent, afin de protéger les systèmes d'éventuelles attaques, de nouvelles approches appelées *Systèmes de Détection d'Intrusions* (SDI) ont fait leur apparition. Ces outils ont pour objectif d'analyser le traffic réseau et de détecter les comportements malveillants (Singhal et Jajodia, 2010).

Le revers de la médaille de l'utilisation des SDIs réside dans la génération excessive des alertes. La majorité de ces dernières ne correspondent pas réellement à des attaques (fausses alertes, alertes redondantes, etc.). En effet, le volume des données contenues dans un journal d'alertes est très important. De plus, il augmente d'une manière très rapide puisque plusieurs giga-octets d'alertes peuvent s'accumuler par jour sur certains systèmes (Sadoddin et Ghorbani, 2006). Afin de faire face à ce problème, des approches de *corrélation d'alertes* ont été proposées.

La *corrélation d'alertes* est l'analyse des alertes déclenchées par un ou plusieurs SDIs afin de fournir une vue synthétique et de haut niveau des événements malveillants intéressants