D113 : une plateforme open-source dédiée à l'analyse des flux et à la détection des intrusions

David Pierrot, Nouria Harbi

Université Lumière Lyon 2, Laboratoire ERIC 69676 BRON Cedex, FRANCE
{david.pierrot1,nouria.harbi}@univ-lyon2.fr

Résumé. Ce travail se situe dans le domaine de la "Cybersécurité", le projet "D113" permet de visualiser en temps réel les flux transitant sur des équipements de filtrage sans avoir recours au traitement manuel des journaux d'événements. Nous centrerons notre démonstration sur la visualisation de grands "graphes" et l'exploitation d'analyses statiques des flux.

1 Introduction

L'explosion d'internet, couplée à l'effet de la mondialisation, a pour résultat d'interconnecter les personnes, les entreprises, les états. Le côté déplaisant de cette interconnexion mondiale des Systèmes d'Information réside dans un phénomène appelé "Cybercriminalité". Des personnes, des groupes mal intentionnés ont pour objectif de nuire dans un but pécuniaire ou pour une "cause", aux informations d'une entreprise, d'une personne voire d'un Etat. Il n'est pas rare que des faits de "cyber-attaques" soient relatés dans les médias envers des grandes sociétés comme "Google","Visa","Sony", "Apple". La sécurité d'un Système d'Information se doit d'être présente afin de garantir la confidentialité, l'intégrité, la disponibilité de l'information. De ce fait, il existe une multitude d'équipements de sécurité qui permettent de détecter les comportements anormaux. Un des principaux équipements de sécurité est le "Pare-Feu" [1] ou plus communément appelé "Firewall". Il a pour mission comme le décrit Al-Shaer et Hamed (2003) de filtrer , selon une politique fondée sur les flux autorisés à pénétrer dans un réseau selon leurs sources, leurs destinations et les services souhaités (navigation internet, transfert de fichiers, etc...). Par son positionnement, il donne une visibilité totale de l'ensemble des flux. Cet équipement offre aussi la possibilité "d'historiser" vers des journaux les flux ayant été autorisés ou interdits. L'exploitation et l'analyse des journaux d'événements liés aux équipements de sécurité sont devenues primordiales pour la maîtrise des flux et la détection des intrusions ainsi que pour la vérification du bien fondé de la politique de filtrage mise en place (Golnabi et al, 2006). Dans ce contexte, les constructeurs d'équipements de filtrage mettent à disposition des logiciels permettant d'analyser les flux. Ces derniers nécessitent un accès et une connaissance dudit équipement. La détection des anomalies et des comportements anormaux est conséquemment réservée à ces seuls utilisateurs. La problématique de la représentation des événements de sécurité est tellement répandue que plusieurs outils ont même été regroupés au

1. équipement de sécurité basé sur le filtrage des entrées/sorties des flux réseau