

UNIVERSITÉ MOHAMMED V - AGDAL
FACULTÉ DES SCIENCES
Rabat



THÈSE DE DOCTORAT

Présentée par

Ali RADI

Titre : Conception d'un Nouveau Système de Prévention d'intrusion basé sur une Politique de Sécurité à trois Niveaux

Discipline : Sciences de l'ingénieur
Spécialité : Informatique et Télécommunications
U.F.R : Informatique et Télécommunications
Période d'accréditation : 2005/2008
Directeur de l'UFR : Prof. Driss Aboutajdine
Directeurs de thèse : Prof. Driss Aboutajdine (FS-Rabat, Maroc)

Soutenance :

Date : 26/11/ 2011

Heure : 15H

Lieu : Al Bayter

Devant le jury :

Président :

Driss ABOUTAJDINE, Professeur à la Faculté des Sciences - Rabat, Maroc

Examineurs :

M. Mohammed MARRAKI, Professeur à la Faculté des Sciences-Rabat, Maroc

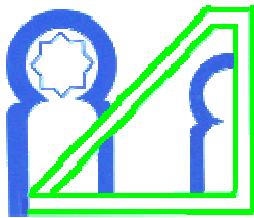
M. Abdelmalek AZIZI, Professeur à la Faculté des Sciences - Oujda, Maroc

M. Boubker REGRAGUI, Professeur à l'ENSIAS, Maroc

M. Mohammed ESSAIDI, Professeur à la Faculté des Sciences - Tétouan, Maroc

Invité :

M. Azzeddine RAMRAMI, M. Azzeddine RAMRAMI, Architecte Sécurité -
NAOSecurity.com, Sophia-Antipolis, France



UNIVERSITÉ MOHAMMED V - AGDAL
FACULTÉ DES SCIENCES
Rabat



Résumé La conception et la mise en œuvre des systèmes de détection d'intrusions (IDS) demeurent un important axe de recherche dans le domaine de la sécurité des systèmes informatiques (SI). Malgré les progrès indéniables enregistrés, il y a encore beaucoup à faire pour améliorer la sécurité des réseaux informatiques d'aujourd'hui. Pour cela, de nombreux mécanismes ont été développés. En général, ces systèmes sont vulnérables aux attaques, à la fois, des utilisateurs non autorisés (attaques externes) ainsi qu'aux attaques des utilisateurs autorisés (attaques internes) qui abusent des privilèges qui leur sont octroyés. Dans cette thèse, notre contribution consiste en la conception et la mise en œuvre d'un système de prévention d'intrusions basé sur une politique de sécurité à trois niveaux. Cette approche, très intéressante même pour les SI complexes, permet aux administrateurs des SI et aux responsables de la sécurité des SI, à la fois, la protection du SI des attaques externes et des attaques internes. Ces dernières sont aussi importantes car d'après plusieurs études et recherches, elles représentent plus de 60% du total des attaques des SI. Aussi, des actions proactives sont possibles dans notre approche, ce qui n'est pas le cas avec la majorité des IDS.

Cependant, l'analyse manuelle de l'énorme volume de données générées par les IDS est impraticable. Pour surmonter ce problème et pour l'évaluer, dans notre approche nous avons proposé l'utilisation des techniques d'apprentissage supervisées, en l'occurrence, les Séparateurs à Vaste Marge (SVM). Les résultats des différentes expérimentations basées sur les trois techniques d'apprentissage supervisées (les SVM, l'analyse en composantes principales et les arbres de décision) pour l'amélioration la détection d'intrusions et leurs comparaisons sont soigneusement présentés et discutés.

Mots-clefs (6) : Système d'Information, Détection d'intrusion, Politique de sécurité, Apprentissage Supervisé, Séparateurs à Vaste Marge, Analyse en Composantes Principales.
