République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université M'hamed BOUGARA de BOUMERDES

Faculté des Sciences
Département d'Informatique

MEMOIRE DE MAGISTER

Spécialité : Informatique
Option : Spécification de Logiciel et Traitement de l'Information

Présenté par :

M^elle Ghenima BOURKACHE

Thème

Un IDS réparti basé sur une société d'agents intelligents

Soutenu devant le jury:

Mr. M. Mezghiche	Pr à l'université de Boumerdes	Président
Mr. Y.M. Djouadi	M.C à l'université de Tizi-Ouzou	Examinateur
Mr. Y. Challal	M.A à l'université de Bab ezzouar	Examinateur
Mr. K. Tamine	HDR. à l'université de Limoges	Rapporteur

Année Universitaire : 2006/2007

ملخص

يكون أمن شبكات الإعلام الآلي عرضة لشتى الإختلالات التي تتمثل خاصة في الازدحامات، التدخلات الغير السليمة والهجمات. لهذا فإنّه من الضروري تزويد هذه الأنظمة بوسائل وآليات قادرة على منع هذه الظاهرة.

من أجل الكشف على كلّ محاولة لخرق سياسة الأمن يجب القيام بمراقبة الأنظمة بطريقة مستمرة ومنتظمة و ذلك باستعمال طرق الكشف عن التعدّيات.

أصبحت أنظمة و طرق الكشف عن التعدّيات منتشرة في أنظمة المعلومات التي حضيت بمكانة هامّة في تصميم إستراتيجية الأمن.

على الرغم من سمعة هذه الوسائل، فإنّ غالبية أنظمة كشف التعدّيات أحادية ومركزية، بينما جمع المعلومات في الشبكة يكون موّزعا. لهذا فإنّ هدفنا يتمحور في الكشف الموزع والذكي للتعدّيات.

في هذا الصدد، نقترح نموذجا لتحقيق نظام لكشف التعدّيات، الذّي يكون موزعا وسلوكيا، وهذا باستعمال طريقة التصنيف القائمة على سير النمل التي تعمل على مبدأ مجموعة من العملاء المتنقلين الذين يتصفون بميزة ردّ الفعل، حيث تكون هذه المجموعة مكرسة للكشف الموزع، والذكي على التعديات في الشبكة.

يهدف هذا النموذج إلى حلّ المشاكل الناتجة عن الأنظمة المركزية للكشف على التعديات.

الكلمات الرئيسية: شبكة الإعلام الآلي، الأمن ،أنظمة كشف التعديات، عملاء متنقلين، أنظمة متعددة العملاء.

Abstract

The networks are increasingly susceptible to be a target of various disorders, against their security, such as the congestions, malevolent accesses and the attacks. To this end, it becomes inescapable to provide these systems of tools and mechanisms able to inhibit these disordered states.

The intrusion detection systems are became very largely deployed in the information systems and they gained an important place in the design of the strategy of security.

In spite of the reputation of these tools, the majority of intrusion detection systems are monolithic and centralized whereas the data-gathering on network is distributed. To this end, our objective lies in the scope of distributed and intelligent intrusion detection.

In this spirit, we propose a model for build a distributed and behavioural intrusion detection system by using a method of classification based on the functioning of ants -ANTClass- and functioning on the principle of a society of reactive mobile agents dedicated to the distributed and intelligent intrusion detection in a network.

This model aims at solving the problems included by the centralized intrusion detection systems.

Keywords: data-processing networks, security, intrusions detection systems, IDS, reactive mobile agents, Multi-agents systems, MAS.

Résumé

Les réseaux informatiques sont de plus en plus susceptibles d'être la cible de dérèglements divers, à l'encontre de leur sécurité, tels que les congestions, les accès malveillants et les attaques. A cet effet, il devient inéluctable de munir ces systèmes d'outils et de mécanismes capables d'inhiber ces dérèglements.

Afin de détecter toute tentative de violation de la politique de sécurité, une surveillance permanente ou régulière des systèmes peut être mise en place : ce sont les Systèmes de Détection d'Intrusions (IDS).

Les systèmes de détection d'intrusions sont devenus très largement déployés dans les systèmes d'informations et ils ont gagné une place importante dans la conception de la stratégie de sécurité.

Malgré la réputation de ces outils, la plupart des systèmes de détection d'intrusions sont monolithiques et centralisés alors que la collecte des données sur le réseau est distribuée. A cet effet, notre objectif s'inscrit dans le cadre d'une détection d'intrusions distrubuée et intelligente.

Dans cet esprit, nous proposons un modèle pour construire un système de détection d'intrusions réparti comportemental en utilisant une méthode de classification basé sur le fonctionnement des fourmis – ANTClass – et fonctionnant sur le principe d'une société d'agents mobiles réactifs dédiée à la détection d'intrusions distribuée et intelligente dans un réseau.

Ce modèle vise à résoudre les problèmes induits par des systèmes de détection d'intrusions centralisés.

Mots clés : réseaux informatiques, Sécurité, système de détection d'intrusions, IDS, agents mobiles réactifs, systèmes multi-agents, SMA.