REPUBLIQUE ALGERIENNE DEMOCRATIQUE & POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR & DE LA RECHERCHE SCIENTIFIQUE

RAPPORT DU PROJET DE FIN D'ÉTUDES

Pour obtenir le diplôme de

Post-Graduation Spécialisé en sécurité informatique

Préparé par :

Sakhri Hichem , Derrar Omar

Sous la direction de :

Maître assistante Bensefia Hassina (Encadreur)

Un système de Détection d'Intrusion hybride auto-apprenant à base d'ensemble de classifieurs

Soutenue le : 20/02/2022

Devant le jury composé de :

M. NOUALI Omar : Président

Mme. GUEMRAOUI Lila : Examinatrice & **Melle. ZEMMAHE Amina** : Examinatrice

Année Universitaire : **2019 - 2020**

Un système de Détection d'Intrusion hybride auto-apprenant à base d'ensemble de Classifieurs

Sakhri Hichem, Derrar Omar

Mémoire soumis en vue de l'obtention du diplôme de

Post-Graduation Spécialisé

Alger

Fev 2022

REMERCIMENTS

Nous remercions tous d'abord Allah tous puissant qui nous a donné la santé, le courage et la patience afin de pouvoir accomplir ce modeste travail.

Nous tenons dans un premier temps à exprimer notre profonde reconnaissance à notre encadreur Melle Hassina BENSEFIAmaitre assistanteà la Faculté des mathématiques et de l'informatique (UBBA), pour avoir accepté de diriger ce travail et qui nous a accompagnés tout au long de cette période de réalisation. Nous ne serons assez la remercier pour sa disponibilité, son soutien indéfectible, son enthousiasme scientifique et son encouragement qui nous a permis de mener à bien notre travail, surtout dans les moments les plus difficiles.

Nous exprimons toute notre gratitude à tous les membres du jury pour l'honneur qu'ils nous font en participant à l'examen de ce travail, particulièrement à Monsieur Omar NOUALI, le président de notre jury et le responsable Scientifique de la PGS en sécurité informatique du CERIST.

Nous tenons à exprimer nos remerciements à tous nos enseignants PGS et au personnel de la formation du CERIST.

Nos sincères remerciements et nos vives gratitudes vont aux membres de nos familles et en particulier nos parents pour leurs sacrifices envers notre éducation et études.

Enfin, nous remercions toutes les personnes qui ont contribué de prêt ou de loin à la concrétisation de ce modeste travail ainsi qu'à toute personne qui fera l'effort de lire ce document.

شكر وتقدير

أول مشكور هو الله عز وجل، ثم والداي على كل مجهوداتهم منذ ولادتي إلى هذه اللحظات وعائلتي الصغيرة.
يسرني أن أوجه شكري لكل من نصحني أو أرشدني أو وجهني أو ساهم معي في إعداد هذا البحث بإيصالي للمراجع والمصادر المطلوبة في أي مرحلة من مراحله، وأشكر على وجه الخصوص للمشرفة الأستاذة المساعدة بجامعة محمد البشير الابراهيمي برج بوعريريج / حسينة بن صافيةعلى كل المجهودات التي بذلتها معنا من خلال النصح و التصحيح وعلى اختيار العنوان والموضوع، كما أن شكري موجه لإدارة مركز البحث في الاعلام الالي و التقني و الأستاذنوالي عمر على المجهودات المبذولة من طرفه ولأساتذتنا الكرام في المركز لتوفير أفضل بيئة للتدريس في أفضل الأحوال التي تلائم طلبة العلم.

صخري هشام

في البداية، الحمد والشكر لله، جل في علاه، فإليه ينسب الفضل كله في الإكمال -والكمال يبقى لله وحده -هذا العمل.
وبعد الحمد لله، أتوجه بالشكر إلى والداي على وباية بوشملة على كل مجهوداتهم، دعمهم ونصحهم لي دائما، وإلى عائلتي الكبيرة والصغيرة وعلى رأسهم زوجتي على صبرها ومسنادتها لي طوال فترة التربص فجزاهم الله عني خير الجزاء.
كما أتوجه بالشكر والتقدير للمشرفة الأستاذة المساعدة بجامعة محمد البشير الابراهيمي برج بوعريريج / حسينة بن صافية التي كانت بعد إله عزوجل المعين الأول لنا على إتمام وإنجاز هذه المذكرة فلها كل التقدير والإمتنان.
كما أن شكري موجه لإدارة مركز البحث في الاعلام الالي والتقني، والأستاذ نوالي عمر على المجهودات المبذولة من طرفه ولأساتذتنا الكرام في المركز لتوفير أفضل بيئة للتدريس في أفضل الأحوال التي تلائم طلبة العلم.

دردار عمر

ملخص

الهدف من هذا المشروع هو تصميم وتطوير نظام كشف التسلل (IDS) على أساس التسلسل الهرمي للمصنفات والذي يجمع بين طريقتين لكشف التسلل: الطريقة الشاذة والطريقة القائمة على التوقيع ومن ثم التأهيل الهجين. يتمتع نظام IDS هذا بالقدرة على اكتشاف أشكال جديدة من الهجمات وأشكال جديدة من السلوك الطبيعي أثناء تشغيله (في الوقت الفعلي) ولديهاالقدرة على التعلم الإلكتروني التلقائي بالتزامن مع تشغيل نظام كشف التسلل.

هذاالأخيريستغل أداء مجموعات المصنفات وكذلك عدم تجانس المصنفات التي تشكلها، والتي هي شبكات عصبية من نوع شبكات المطرقة التكيفية.(AHN)

تم تنفيذ نظام IDS الخاص بنا باستخدام Matlab وتبعه التحقق من الأداء عبر مجموعة البيانات القياسية في كشف التسلل .NSL KDD 2012 النتائج مرضية، فهي تثبت فعالية النهج المقترح.

الكلمات المفتاحية: نظام كشف التسلل ،(IDS) شبكات المطرقة التكيفية (AHN)،مجموعات المصنفات، مسافة«NSL-KDD."Minkowski

Abstract

The objective of this project is to design and develop an intrusion detection system (IDS) based on a hierarchy of classifiers and which combines the two intrusion detection methods: the anomaly and the signature-based method hence the hybrid qualification.

This IDS has the power to detect new forms of attacks and new forms of normal behavior during its operation (in real time). It has automatic e-learning capability in conjunction with IDS operation. It exploits the performance of the sets of classifiers as well as the heterogeneity of the classifiers which constitute it, which are neural networks of the Adaptive Hamming Nets (AHN) type.

The implementation of our IDS was carried out with Matlab and it is followed by a validation of the performances via the standard data set in intrusion detection NSL KDD 2012. The results are satisfactory, they prove the effectiveness of the proposed approach.

Keywords: Intrusion Detection System (IDS), Adaptive Hamming Nets (AHN), Classifier Ensembles, Minkowski Distance, NSL-KDD.

Résumé

Ce projet a pour objectif la conception et le développement d'un système de détection d'intrusion (Intrusion Detection System, IDS) basé sur une hiérarchie d'ensemble de classifieurs et qui combine les deux méthodes de détection d'intrusion : la méthode basée anomalie et la méthode basée signature d'où la qualification hybride.

Cet IDS a un pouvoir de détection des nouvelles formes d'attaques et des nouvelles formes de comportement normal durant son fonctionnement (en temps réel). Il est doté d'une capacité d'apprentissage en-ligne automatique conjointement au fonctionnement de l'IDS.

Il exploite la performance des ensembles de classifieurs ainsi que l'hétérogénéité des classifieurs qui le constituent qui sont des réseaux de neurones de type Adaptatif Hamming Nets (AHN).

L'implémentation de notre IDS a été effectuée avec Matlab et elle est suivie par une validation des performances via le data set standard en détection d'intrusion NSL KDD 2012. Les résultats sont satisfaisants, ils prouvent l'efficacité de l'approche proposée.

Mots clés : Système de détection d'intrusion (IDS), Adaptive Hamming Nets (AHN), les ensembles de classifieurs, Distance de Minkowski, NSL-KDD.

Table des matières

Liste des figures

Liste des tableaux