وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي 08ماي 1945 سيدي بلعباس
École Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbès

Mémoire

En vue de l'obtention du diplôme d'**ingénieur d'état**

Filière : **Informatique**

Spécialité : **Ingénierie des Systèmes Informatiques (ISI)**

Thème

Design and Deployment of a Network Anomaly Detection System.

Réalisé par:
Mr BENCHIEKH Moustafa Choukri
Mr BENHABRA Abdesselam

Soutenu le : 00/00/2019 Devant le jury composé de

M/Mme/Mlle XXX	Président
M/Mme/Mlle XXX	Encadreur
M/Mme/Mlle XXX	Examinateur

Année Universitaire
2019/2020

Abstract

Computer security plays an important role in everybody's life, especially when it comes to connected applications and services. Therefore, securing the network connectivity from being compromised by untrusted parties and malicious usage has a great significance in maintaining their efficient functioning. Considered as one of the primary defense lines of network security and expected to be adapting to the dynamically changing threat patterns, Intrusion detection systems have been developed with different techniques by researchers from various disciplines like mathematics, machine learning, and data mining in order to achieve a good immunity against attacks and reliable detection of anomalies. In this thesis, we propose an Artificial Neural Network-based anomaly detection application. In addition to the benign class, the proposed method deals with fourteen attack classes and unlike most methods, our work has been trained using an up to date dataset. As a result, the proposed system is capable of achieving an accuracy of 99% and a false positive rate of 1%.

ملخص

يلعب أمان الكمبيوتر دورا مهما في حياة الجميع ، لا سيما عندما يتعلق الأمر بالتطبيقات والخدمات المتصلة. لذلك فإن تأمين اتصال الشبكة من التعرض للخطر من قبل أطراف غير موثوق بها والاستخدام الضار له أهمية كبيرة في الحفاظ على كفاءة أدائها. نظرا لكونها أحد خطوط الدفاع الأساسية لأمن الشبكة ومن المتوقع أن تتكيف مع أنماط التهديد المتغيرة ديناميكيا ، تم تطوير أنظمة اكتشاف التسلل باستخدام تقنيات مختلفة بواسطة باحثين من مختلف التخصصات مثل الرياضيات والتعلم الآلي واستخراج البيانات من أجل تحقيق مناعة جيدة ضد الهجمات والكشف الموثوق به عن الحالات الشاذة. في هذه الأطروحة ، نقترح تطبيق اكتشاف الشذوذ في الشبكات والمستند إلى الشبكة العصبية الاصطناعية. بالإضافة إلى البيانات الغير مؤذية ، تتعامل الطريقة المقترحة مع أربعة عشر فئة هجوم وعلى عكس معظم الطرق ، تم تدريب عملنا باستخدام مجموعة بيانات حديثة. ونتيجة لذلك فإن النظام المقترح قادر على تحقيق دقة ٩٩ ٪ ومعدل موجب خاطئ ١٪ .