الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

المدرسة العليا للإعلام الآلي - 08 ماي 1945 – بسيدي بلعباس
Ecole Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbes

Mémoire de Fin d'étude

Pour l'obtention du diplôme d'**ingénieur d'état**

Filière : **Informatique**

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

Thème

Système de détection d'intrusion a base d'apprentissage automatique (IDS)

Présenté par :

Mr. Mohamed Abdeldjebbar ACHER

Mr. Abdellah Anas Derkaoui

Soutenu le : **01/10/2020** Devant le jury composé de :

- M BELFEDHAL Alaa Eddine — Président
- M Mohammed Yassine KAZI TANI — Encadreur
- Mlle Djihed ANANI — Examinatrice

Année Universitaire : 2019 / 2020

ABSTRACT

Intrusion Detection was developed to extend security visibility into the network and monitor the activity of users while they are on the network. An Intrusion Detection System (IDS) can augment security solutions as a dynamic security component by detecting, responding to, and reporting unauthorized activity from data extracted directly from the network. There are two types of methods in IDS, anomaly and misuse, they play complimentary role for a better IDS.

Our goal of this research paper is to make a State of the Art survey for anomaly based IDS and expose a general overview about the machine learning and deep learning approaches used in it. We will see the different between shallow models and deep learning models, expose the latest datasets used for training and testing and give a real-world examples and experiments with their achieved accuracy.

We will conclude this paper by our own contribution in this field.

Résumé

La Détection d'intrusion a été développé pour étendre la visibilité de la sécurité dans les réseaux et surveiller l'activité des utilisateurs pendant qu'ils travaillent sur le réseau. Un système de détection d'intrusion (IDS) peut augmenter les solutions de sécurité en tant que composant de sécurité dynamique en détectant, réagissant aux données extraites directement du réseau et signalant les activités non autorisées. Il existe deux grandes catégories d'IDS, les plus connues sont les détections par signatures et les détections par anomalies, ils jouent un rôle complémentaire pour une meilleure sécurité.

Notre travail consiste à faire un état de l'art sur Les IDS de base anomalies en présentant une vue générale sur les approches de machine Learning et Deep Learning qui sont utilisées dans les IDS. On va voir les différences entre les modèles superficiels de machine Learning et les modèles de Deep Learning, ainsi les différents jeux de données (dataset) et les travaux réalisés dans le monde réel et on va finir par présenter notre propre contribution dans ce domaine.

ملخص

تم تطوير كاشف الاختراق لتوسيع نطاق الأمان في الشبكة ومراقبة نشاط المستخدمين أثناء وجودهم عليها. يعتبر نظام كشف الاختراق مكون أمان ديناميكي من خلال اكتشاف النشاط المحظور المستخرج من الشبكة والاستجابة له والإبلاغ عنه. هناك طريقتان لكشف الاختراق عن طريق الامضاء و المقارنة وعن طريق التعلم وسوء الاستخدام, سويا يلعبان دورا مكملا لحماية افضل.

يتمثل عملنا في القيام بدراسة استقصائية حديثة حول كشف الاختراق عن طريق التعلم و القيام بمقارنة بين مختلف النماذج الموجودة وعرض التجارب الحالية والمستخدمة في العالم و تقديم نموذجنا الخاص.