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 de **Master**

Filière : **Informatique**

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

Thème

Network Anomaly Detection

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

Due to the immense growth of applications with connected users and services in the last decade, monitoring networks and guarding them by identifying security vulnerabilities along with detecting anomalies has become the fundamental daily task of network administrators. Keeping an eye on the network traffic and bandwidth usage have proved its great efficiency when it comes to differentiating malicious network behavior from the normal one. Besides that and as the primary defense line of the network infrastructure, intrusion detection systems are expected to adapt to the dynamically changing threat patterns, thus, various techniques have been developed by researchers from different disciplines like mathematics, machine learning, and data mining in order to achieve a good immunity against attacks and reliable detection of anomalies.

ملخص

مع التقدم الهائل والسريع للتكنولوجيا في عصرنا الحالي وتعميم الرقمنة وكثرة مستخدميها، أصبحت مراقبة الشبكات وحمايتها أمرا الزاميا وضروريا لحياتنا اليومية، وهذا ماجعل مهمة الكشف عن الشذوذ في الشبكة مهمة أساسية في الحياة اليومية للمسؤولين عنها كونها خط الدفاع الأساسي لبنيها التحتية. وقد أثبتت مراقبة حركة مرور الشبكة واستخدام عرض النطاق الترددي فعالية كبيرة في التميز بين سلوك الشبكة الخبيث عن السلوك العادي، كما ان تكيف أنظمة الكشف عن الشذوذ مع أنماط التهديد المتغيرة ديناميكيا ،وتطور علم الرياضيات والتعلم الآلي والتنقيب عن البيانات وتخصصات اخرى، افاد الباحثين في تطوير تقنيات واساليب مختلفة من أجل تحقيق الحصانة ضد الهجمات وكشف موثوق عن الشذوذ.

Resume

Suite à l'immense croissance des applications avec des utilisateurs et des services connectés au cours de ces dernières années, la surveillance des réseaux et leur protection par l'identification des vulnérabilités de sécurité ainsi que la détection des anomalies sont devenues des tâches essentielles pour les administrateurs de réseau. Par ailleurs, en tant que première ligne de défense de l'infrastructure du réseau, les systèmes de détection des intrusions sont capables de s'adapter à l'évolution dynamique des menaces. Ainsi, les chercheurs de différentes disciplines ont mis au point diverses techniques telles que les mathématiques, l'apprentissage automatique et l'exploration de données afin d'obtenir une bonne immunité contre les attaques et une détection fiable des anomalies