الجمهورية الشعبية الديمقراطية الجزائرية
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

En vue de l'obtention du diplôme de **Master**

Filière : **Informatique**

Spécialité : **Systèmes d'information et Technologies Web (SIW)**

Thème

Approches et Techniques de Détection d'Intrusion

Présenté par **:**

- Mr KHELLADI Abderrahmane
- Mr SELMI Anwar

Soutenu le : **06/07/2020** Devant le jury composé de :

-	M. BELFEDHAL Alaa Eddine	MCB	Président
-	M. MALKI Abdelhamid	MCB	Encadreur
-	M. BENDAOUD Fayssal	MCB	Examinateur
-	M. KAZI TANI Mohammed Yassine	MCB	Examinateur

Année Universitaire : 2019 / 2020

Résumé

Actuellement, la sécurité des technologies de l'information et de la communication suscite une préoccupation croissante au sein de la communauté scientifique, car toute attaque ou anomalie dans le réseau peut affecter considérablement de nombreux domaines tels que la sécurité nationale, le stockage des données privées, la protection sociale, économiques, etc. Par conséquent, la détection des anomalies est devenue un problème important qui a été étudié dans divers domaines de recherche et domaines d'application. Pour cette raison de nombreuses techniques et approches différentes ont été proposées et introduites. Dans ce travail, l'objectif principal est de passer en revue les aspects les plus importants liés à la détection des anomalies, plus précisément sur les réseaux, nous présentons une étude bibliographique sur les techniques, méthodes et systèmes les plus pertinents dans ce domaine de recherche, tout en regroupant ces derniers en différentes catégories. De plus, pour chaque catégorie d'approches, nous identifions ces avantages et ces inconvénients. Afin de rendre notre mémoire plus lisible et plus compréhensible, nous introduisons dans la première partie : (1) détection d'anomalies et ses notions connexes, (2) concepts de base liés à la détection d'intrusions réseau, (3) notions de base du machine learning et ses techniques, (4) un aperçu autour du Big Data et ses outils de traitements. Nous consacrons la deuxième partie à l'étude des différentes approches de détection d'anomalies réseau, à savoir : approches basées sur les statistiques, approches basées sur la classification et celles basées sur le clustering, en concluant avec d'autres approches moins importantes basées sur d'autres solutions.

Mots clés : Détection d'anomalies, Détection d'intrusions, IDS, Sécurité réseau, Machine Learning, Big Data, Approches de détection d'anomalies.

Abstract

Currently, the security of information and communication technologies is a growing concern in the scientific community, since any attack or anomaly in the network can significantly affect many areas such as national security, storage of private data, social protection, economic problems, etc. Consequently, the detection of anomalies has become an important problem which has been studied in various fields of research and fields of application. For this reason many different techniques and approaches have been proposed and introduced. In this work, the main objective is to review the most important aspects related to the detection of anomalies, more precisely on networks, we present a bibliographical study on the techniques, methods and systems that are the most relevant in this field of research, while grouping these into different categories. In addition, for each category of approach, we identify its advantages and disadvantages. In order to make our memory more readable and more comprehensible, we introduce in the first part : (1) detection of anomalies and its related notions, (2) basic concepts related to the detection of network intrusions, (3) notions of basis of machine learning and its techniques, (4) an overview around Big Data and its processing tools. We dedicate the second part to the study of different approaches to detecting network anomalies, namely : statistical-based approaches, classification-based approaches and those based on clustering, concluding with other less important approaches based on other solutions.

Keywords : Anomaly detection, Intrusion detection, IDS, Network security, Machine Learning, Big Data, Anomaly detection approaches.history