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

MEMOIRE

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

Filière : **Informatique**

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

Thème

Firewalls Logs Analysis Platform and Access Lists Vulnerability Detection System.

Présenté par :

- M. El MOGHERBI Mohammed Fayçal

Soutenu le : **04/07/2022**

Devant le jury composé de :

M. AZZA Mohammed	Président
M. KHALDI Belkacem	Encadreur
M. KHALDI Miloud	Examinateur

Année Universitaire : 2021/2022

Abstract

In today's business environments, information is becoming increasingly easily accessible through a large network of interconnected systems. Therefore, protecting this information and delivering it to the right recipient becomes a critical need for business security.

Firewall logs analysis reveals a lot of information about the security threat attempts at the periphery of the network and on the nature of traffic coming in and going out of the firewall. The analyzed firewall logs information, provides real-time information to the Administrators on the security threat attempts and so that they can swiftly initiate remediation action.

Firewall log monitoring plays an important role in business risk assessment. Analyzing firewall traffic logs is vital to understand network usage. Firewall Analyzer, a firewall monitoring tool, offers many features that help in collecting, analyzing and reporting on firewall logs.

Keywords : Network, log analysis, log monitoring, log collectors, machine learning, anomaly detection.

Résumé

Dans les milieux d'affaires d'aujourd'hui, l'information devient de plus en plus facilement accessible grâce à un vaste réseau de systèmes interconnectés. Par conséquent, la protection de ces informations et leurs transmission au bon destinataire devient un besoin critique pour la sécurité de l'entreprise.

L'analyse des journaux de pare-feu révèle beaucoup d'informations sur les tentatives de menace à la sécurité et sur la nature du trafic entrant et sortant du pare-feu. Ces informations une fois enregistre et analysé , fournit des informations en temps réel aux administrateurs sur les tentatives de menace à la sécurité et leur permet de lancer rapidement des mesures correctives.

La surveillance des journaux des pare-feu joue un rôle important dans l'évaluation des risques commerciaux. L'analyse des journaux du trafic est essentielle pour comprendre l'utilisation du réseau. L' analysateur des pare-feu, un outil de surveillance qui offre de nombreuses fonctionnalités qui aident à collecter, analyser et produire des rapports sur les journaux de pare-feu.

Mots clés : Réseau, analyse des journaux, surveillance des journaux, collecteurs de journaux, apprentissage automatique, détection d'anomalies.
