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

Design and implementation of an intrusion detection system

Présenté par **:**

- Mr Attatfa Abdelghani
- Mr Chelouf Soufyane

Soutenu le : **06/10/2020** Devant le jury composé de :

- M Belfedhal Alaa Eddine — Président
- M Kechar Mohamed — Encadreur
- Mlle Souyah Amina — Examinatrice

Année Universitaire : 2019 / 2020

Abstract

With the rise of the internet in recent years, the number of users has greatly increased. The Internet serves countless personal and professional needs for individuals and societies. However, this interconnection of computers also allows malicious users to use these resources for malicious purposes, exposing current computer networks to an increasing number of security threats, with new types of attacks appearing continuously and increasing in number, severity and impact. One of the most important attacks is the zero-day attack, which occurs on the same day that a weakness is detected in a software. This weak point is exploited before a patch by the creator of the software, so their signature is unknown in this moment by security software manufacturers.

For These reasons, network administrators are looking for effective security solutions that can protect the company's network. In this context, the IDS(Intrusion Detection System) is a good solution for the protection of computer networks.

ملخص

مع تطور الإنترنت في السنوات الأخيرة، وتضاعف عدد المستخدمين بشكل كبير.أصبحت شبكة الإنترنت تخدم عدداً لا يحصى من الاحتياجات الشخصية والمهنية للأفراد والمجتمعات. ومع ذلك، يسمح هذا الاتصال المتبادل بين أجهزة الكمبيوتر للمستخدمين غير الاخلاقيين باستخدام هذه الموارد لأغراض ضارة وغير اخلاقية، مما يعرض شبكات الكمبيوتر الحالية لعدد متزايد من تهديدات الأمان والهجمات، مع ظهور أنواع جديدة من الهجمات بشكل مستمر ومتزايد من حيث العدد والخطورة والتأثير. ومن أهم الهجمات هجوم يوم الصفر، الذي يحدث في اليوم نفسه الذي يتم فيه اكتشاف ضعف في البرنامج. يتم استغلال هذه النقطة الضعيفة قبل التصحيح من قبل منشئ البرنامج، لذا فإنها لا تملك توقيع معروف في هذه اللحظة من قبل الشركات المصنعة لبرامج الأمان.

ولهذه الأسباب، يبحث مسؤولو الشبكة عن حلول أمان فعالة يمكنها حماية شبكة الشركة. وفي هذا السياق، يعد نظام IDS (نظام اكتشاف الاختراق) حلاً جيدًا لحماية شبكات الكمبيوتر.