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

MEMOIRE

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

Filière : **Informatique**

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

Thème

Intrusion Detection Systems: Study and Comparison

Présenté par **:**

- Mr Attatfa Abdelghani
- Mr Chelouf Soufyane

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

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

Année Universitaire : 2019 / 2020

Abstract

With the huge rise of the internet and the notable technological development in recent years, the number of users has greatly increased. The internet serves countless personal and professional needs for people and companies. However, this interconnection of computers also allows attackers and malicious users to exploit these resources for malicious purposes, which exposes today's computer networks to an increasing number of attacks and threats security, with new types of techniques and attacks appearing continuously and which are increasing both in number, severity and impact. For these reasons, researchers and systems administrators seek effective and automated security strategies and solutions in order to reduce damage or stop a big part of threats able to protect the corporate network and information systems.

One of the best solution in this context are Intrusion Detection Systems (IDS), which are used for protecting computer networks and information systems.

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.