## *Résumé :*

La détection d'intrusions est la capacité d'un système informatique de déterminer automatiquement, à partir d'événements relevant de la sécurité, qu'une violation de sécurité se produit ou s'est produite dans le passé. Pour ce faire, la détection d'intrusions nécessite qu'un grand nombre d'événements de sécurité soient collectés et enregistrés afin d'être analysés.

Il existent deux approches pour la détection d'intrusion : l'approche comportementale et l'approche par scénarios. L'approche comportementale consiste à décrire le comportement (profil) usuel d'un utilisateur et ce, afin de détecter toute action anormale ou inhabituelle de cet utilisateur. L'approche comportementale permet de détecter des attaques inconnues. L'approche par scénarios consiste à définir des comportements anormaux et ce, afin d'analyser les données susceptibles d'être des attaques. L'approche par scénarios utilise souvent une base de scénarios d'attaques.

Dans ce travail, on s'intéresse à l'approche par scénarios. Notre but est de déterminer les attaques potentiellement présentes dans le fichier d'audit qui contient une masse très importante d'événements.

En effet, le problème d'analyse du fichier d'audit de sécurité est un problème NP-complet, c'est pourquoi nous proposons une approche méta-heuristique basée sur les algorithmes génétiques et le recuit simulé.

L'approche méta-heuristique pour la détection d'intrusions, que nous proposons, permettra de rechercher les scénarios d'attaques prédéfinies dans les traces d'audit. Le but de cette approche est de déterminer la présence d'une ou plusieurs signatures d'attaques dans les données d'audit.



**Mots-clés :** Détection d'intrusion, approche comportementale, approche par scénarios, algorithme mimétique, sécurité, attaques.



## *Abstract :*

The intrusions detection is the capacity of a computer system to determine automatically, from an audit file that a violation of security occurs or has been occurred in the past. With this intention, the intrusions detection requires that a great number of data, events or users activities are collected and saved in order to be analyzed.

There are two main models of intrusion detection:

- An anomaly detection approach: where the detection is performed by detecting changes in the patterns of utilization or behavior of system and users.
- A misuse detection approach: where detection is performed by exploiting known attacks called signature.

In this work, we are interested in the misuse approach. Our goal is to determine the potentially attacks presented in the audit file which contains a very important mass of events. Indeed, the problem of the audit file analysis is an Np-complete, this is why we propose a metaheuristic approach based on the genetic algorithms and the simulated annealing.

The metaheuristic approach for the intrusions detection, which we propose, will make it possible to seek the attacks scenarios predefined in the audit traces. The approach aim is to determine the presence of an attacks signature in the audit data.



**Keywords :** Intrusion detection, Misuse Detection, Anomaly Detection, Mimetic algorithm, security, attacks.



## ملخص :

كشف التعدي على النظام المعلوماتي هو قدرة هذا النظام على تحديد وبطريقة آلية عن طريق تحليل الأحداث، حصول إنتهاك لأمن النظام المعلوماتي. ولهذا فكشف أي تعدي يتطلب جمع قدر كبير من المعطيات و الأحداث و نشاطات المستعملين، تخزينها و من ثم تحليلها.

هناك طريقتين لكشف التعدي على النظام المعلوماتي :

- طريقة تعتمد على نمذجة السلوك العادي للمستعمل، وأي عمل يخرج عن نطاق هذا السلوك يعتبر نشاط غير عادي.
- الطريقة الثانية تعتمد نمذجة السلوكات غير العادية، و تحليل المعطيات المخزنة لتحديد هل هناك تعدي أم لا.

في هذا العمل نهتم بتطوير طريقة لتحديد الهجومات المحتملة على النظام المعلوماتي من خلال تحليل سجل الأحداث الخاص بالنظام، و الذي يحتوي على كمية كبيرة من المعطيات بحيث يصعب إستعمال خوارزميات البحث العادية.

الطريقة المقترحة تعتمد على البحث عن سيناريوهات الهجومات المعروفة في سجلات أحداث النظام بإستعمال خوارزم يعتمد على تقنيتين للذكاء الإصطناعي، و هما الخوارزميات الجينية و التبريد المقلد.



**الكلمات المفتاحية :** كشف التعدي، الكشف بالسلوك، الكشف بالسيناريو، الخوارزميات المقلدة، الأمن المعلوماتي، الهجومات.