RESUME :

Les systèmes de détection d'intrusion visent à détecter des attaques contre les systèmes informatiques et les réseaux ou généralement contre des systèmes d'information. En effet, c'est difficile de fournir des systèmes d'information prouvable sécurisé et pour les maintenir dans un état sécurisé pendant leur vie et utilisation.

La détection d'intrusions nécessite qu'un grand nombre d'événements de sécurité soient collectés et enregistrés afin d'être analysés.

Deux approches pour la détection d'intrusion ont été proposées : 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, elle permet de détecter des attaques inconnues. L'approche par scénarios consiste à définir des événements anormaux et ce, afin d'analyser les données susceptibles d'être des attaques, elle utilise souvent une base de scénarios d'attaques.

Dans ce mémoire nous proposons un algorithme de recherche locale stochastique pour la recherche des scénarios d'attaques prédéfinis dans le fichier d'audit de sécurité. Au début nous présentons un état de l'art sur la sécurité informatique, et les systèmes de détection d'intrusions. En suite nous présentons les algorithmes de recherche locale stochastique et leurs fonctionnements. Par la suite, nous présentons une formalisation du problème d'analyse de fichier d'audit sous forme d'un problème contraint FASPAS, et nous proposons une approche de recherche locale stochastique pour ce problème. Enfin, et pour prouver l'efficacité de cette approche, nous présentons une étude comparative entre notre approche et celle de M. SAHMADI présenté dans [59].

Mots clés :

Détection d'intrusion, approche comportementale, approche par scénario, algorithme de recherche locale stochastique (SLS), sécurité, attaques.