Conclusion génerale

La sécurité de réseaux demeure l'un des problèmes les plus cruciaux que connaissent les entreprises contemporaines vu la vulgarisation accrue d'internet et des réseaux locaux.

Néanmoins, Il ne sera jamais possible de sécuriser totalement un système d'information, car il y'aura toujours des hackers qui veillent continuellement à découvrir de nouvelles failles dans le système. Cependant, veiller à minimiser ces cas par la mise en place d'outils adéquats capables de dépister et neutraliser d'éventuelles anomalies est actuellement en plein succès.

Notre objectif premier, faut-il le rappeler, était de réaliser un IDS basé sur l'algorithme de classification non supervisé. On visait donc à sécuriser un réseau local en utilisant en particulier la méthode de classification (CAH).

Une nouvelle solution pour la détection d'intrusions basée sur l'algorithme CAH, en effet, nous avons proposé un système de détection d'intrusions réseaux (NIDS) que nous l'avons baptisée ***IDSCAH « Système de*** D***étection d'Intrusions à base CAH »,*** basé sur la méthode non supervisée *CAH.*

Le système ***IDSCAH*** proposé vise à répondre aux normes de la sécurité de réseaux, il ***nécessite*** une phase d'apprentissage, pour cela, nous avons appliqué l'algorithme *CAH* sur la base d'apprentissage et de test *KDD* pour surveiller le système.

Afin de tester ***IDSCAH***, nous avons utilisé une base de données standard dite base de test KDD contenant des connexions normales, et des connexions considérées comme étant des attaques de type (DOS, Probing, R2L, URL). Cette base de test est très appropriée pour évaluer un système de détection d'intrusions de type comportemental, puisqu'elle contient des attaques qui ne figurent pas dans la base d'apprentissage KDD.

Les principales métriques qui présentent un intérêt pour évaluer le système proposé et développés durant ce projet sont le taux de détection et le taux de faux positifs, en d'autres termes les attaques signalées, les attaques ratées par le système. Un système de détection d'intrusions performant est le système qui fournit le meilleur compromis de ces deux facteurs c'est-à-dire celui qui pourrait détecter toute utilisation malveillante du système en générant le minimum de fausses alertes.

Ce projet nous a été d'un grand apport pédagogique et scientifique, puisqu'il nous a permis de découvrir et bien assimiler plusieurs notions telles que la sécurité informatique, ses fonctionnalités et ses mécanismes, de comment aborder les problèmes de classification.

Nous avons proposé une architecture se basant sur l'algorithme de classification CAH. L'idée de base était de classifier les connexions de la base de données KDD'99 pour former

les clusters des connexions normales et les clusters des attaques, puis la détection se fait en comparant les connexions arrivant sur le système informatique aux clusters établit.

En guise de perspectives, nous tenons à mettre l'accent sur certains aspects qui méritent, selon point de vue, d'être explorés toujours en ce qui concerne la détection d'intrusions. Ces pistes se résument essentiellement aux points suivants :

- ✓ Finaliser le test de CAH sur toute la base de données KDD'99.
- ✓ L'hybridation avec d'autres méthodes fondées sur l'approche de détection par scénarios.
- ✓ La coopération avec d'autres méthodes capables de traiter les attributs qualitatifs des connexions TCP/IP de la base KDD'99.