INTRODUCTION GENERALE

L'informatique et en particulier Internet jouent un rôle grandissant dans notre société. Un grand nombre d'applications critiques d'un point de vue de leur sécurité est déployé dans divers domaines comme le domaine militaire, la santé, le commerce électronique, etc. La sécurité des systèmes informatiques devient alors une problématique essentielle tant pour les individus que pour les entreprises ou les états.

A cet égard, Afin de détecter toute tentative de violation des mécanismes de la sécurité, une surveillance permanente ou régulière des systèmes peut être mise en place : ce sont les Systèmes de Détection d'Intrusions (IDS).

Ces systèmes sont devenus très largement déployés dans les systèmes informatiques et ils ont gagné une place importante dans la conception de la stratégie de sécurité. Ils sont généralement utilisés pour surveiller l'accès et le flux d'information, dans le but de déterminer tout comportement malicieux, que ce soit de l'intérieur ou de l'extérieur de système d'informations, et rendre cette information disponible aux administrateurs de la sécurité. En option, les systèmes de détection d'intrusions peuvent réagir contre ces comportements malicieux et prendre des contre-mesures.

Afin de remplir les objectifs des IDS, diverses méthodes de détections d'intrusions ont été proposées, parmi ces méthodes, nous citons la classification.

Plusieurs travaux ont été menés sur les algorithmes de classifications. Cependant, les algorithmes de classifications exploités jusqu'à présent dans le domaine de la sécurité possédant eux même des limites qui peuvent entacher la détection d'intrusions. Afin de résoudre les limites des IDS en général, la Détection d'intrusions doit s'orienter vers des nouvelles techniques de détection pour mieux assurer la sécurité de réseaux. Pour cela, nous proposons une nouvelle procédure de détection d'intrusions, qui consiste à utiliser des algorithmes de classification ascendante hiérarchique (CAH).

L'algorithme CAH est l'un des algorithmes rarement appliqué sur la base KDD'99, pour cela nous le choisissons, en premier lieu, pour concevoir et développer un système de détection d'intrusion qui sera expérimenté sur les données de cette base puis les résultats fournis seront comparés aux résultats donnés par l'application d'un autre système, sur les mêmes données.

Notre travail consiste à réaliser un IDS basé sur l'algorithme de classification non supervisé. Dans l'objectif est de sécuriser un réseau local en utilisant en particulier la méthode de classification (CAH).

Notre travail consistera principalement à :

- ✓ Normalisation statistique de la base de données kdd99.
- ✓ Proposer une architecture appliquant l'algorithme CAH sur la base KDD'99.
- ✓ Normalisation de donnés capturés par un sniffer (wirehark).
- ✓ Extraction les champs importants de ces données puis les utiliser dans la classification.

Pour cela, on a réparti notre travail en quatre chapitres, comme suite :

Le premier chapitre se compose de trois parties, la première s'articule sur une généralité sur la sécurité, et la deuxième partie est consacrée aux IDS. Nous présentons la définition, l'architecture globale et le mode de fonctionnement des IDS, ainsi que la classification de ses derniers et enfin les méthodes de détection des intrusions, et la troisième partie est consacré aux méthodes de classification. En premier lieu, nous allons commencer par les définitions, puis les types de méthodes de classification. Ensuite, nous détaillerons la méthode de classification ascendante hiérarchique.

Le deuxième chapitre présente un état de l'art sur la classification dans le domaine de détection d'intrusion de sécurité de réseau.

Le troisième chapitre présent la conception de notre projet, il montre les différentes étapes à suivre pour réaliser l'application.

Le dernier chapitre présente les différents outils qui vont servir à l'implémentation de notre projet, ainsi que l'implémentation de ce dernier et les résultats obtenus.