République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des Sciences et de la Technologie Houari BOUMEDIENE

FACULTE DE ELECTRONIQUE & INFORMATIQUE
DEPARTEMENT D'INFORMATIQUE

Mémoire du projet de fin d'études

Pour l'obtention du diplôme
D'ingénieur d'état en Informatique

Option : **Systèmes & Réseaux**

Thème :

Système de Détection d'Intrusion Comportemental

Thème proposé et encadré par : **Mr NACI Djamel**

Etudié par : **AKIF Yacine & BELHOCINE Farouk**

Devant le Jury composé de :
Mr BELKHIR Président
Mr BEHLOUL Membre
Mr BERBAR Membre

Organisme d'accueil :
Centre de Recherché sur l'Information Scientifique et Technique

PROMOTION 2004/2005
N° 90

Résumé

Le travail à effectuer est dans le domaine de la sécurité réseau, et a pour objectif la conception et la mise en œuvre d'un Système de détection comportemental dans un environnement d'entreprise, ce système s'intéresse aux intrusions internes c'est-à-dire qu'on tente de détecter les attaques réalisées depuis le réseau interne de l'entreprise. Ce qui justifie le choix de se baser sur les attaques internes est le rapport *« Computer Crime and Security Survey »* publié par la **CSI** (*Computer Security Institute*) pour l'année 2000, et qui indique que 90% des responsables de sécurité ont détecté des attaques, il indique également que seulement 25% d'entre eux ont décelé des attaques provenant de l'extérieur. Cette étude montre aussi que 78% des responsables de sécurité ont découvert des accès non autorisés provenant de l'intérieur. De son coté L'ICSA (*International Computer Security Association*) considère que 80% des problèmes de sécurité proviennent de l'intérieur même de l'organisation.[SEC03].

Lors de l'exploitation de la machine, Chaque utilisateur a un comportement unique, On va donc essayer en premier lieu de construire un profil unique pour chaque utilisateur qui définit ce comportement, pour cela on utilisera les événements générés dans le système par cet utilisateur, et la fréquence de chaque événement va constituer une variable aléatoire; ensuite toutes ces variables aléatoires vont être représentées par un histogramme, et ce dernier n'est que le profil.

Le profil est le noyau de l'approche comportementale, puisque la détection se ferra en le comparant au comportement courant. Dans notre Système on compare le profil de l'utilisateur type avec le profil courant; et cette comparaison est réalisée grâce aux fonctions de calcul de distance entre les histogrammes, si cette distance est supérieur a un seuil donné une alerte est générée.

Pour renforcer ce profil on va ajouter des *Sensors* (sondes) réseau et système qui vont fournir des informations supplémentaires sur cet utilisateur comme les sites qu'il a visité, les services qu'il utilise, et le taux de charge du processeur…etc.

Pour prouver l'efficacité de cette méthode (calcule de distance), nous allons effectuer des tests de détection d'intrusion, permettant aussi de fixer quelques paramètres comme la valeur du seuil de détection, la meilleur fonction de calcul de distance…etc.

Mots Clés : Sécurité informatique, attaques réseaux, Intrusion, Profil référentiel, Profil temporaire, Comportement, Fichiers Logs, évènements, Distances statistiques, Histogrammes.

SOMMAIRE

Chapitre III : La Concéption du système de détection comportemental

Chapitre IV : La mise en œuvre du système de détection comportemental

Chapitre V : Tests de la méthode comportementale

Conclusion générale