République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Centre de Recherche sur l'Information Scientifique et Technique

Mémoire pour l'obtention du diplôme

de Post-Graduation Spécialisée en Sécurité Informatique

Thème

Conception et réalisation d'un outil de détection d'intrusion réseau

Elaboré par:

- Mr. BENCHEIKH Abdelfattah

Encadré par :

- Dr. NOUALI Omar, DSI, CERIST

- Mr. KRINAH Abdelghani, DSI, CERIST

Soutenu devant le jury :

-

-

-

-Juillet 2016

Dédicace

Je dédie ce modeste travail :

A la mémoire de celle qui s'était toujours dévouée et sacrifiée pour moi, celle qui avait toujours été là dans mes moments de détresse, celle qui nous a quitté durant cette formation, **ma très chère mère**. que dieu l'accueillera dans son vaste paradis.

A celui qui m'a toujours encouragé et soutenue, **mon très cher père**.

A celle qui m'a toujours aidé, soutenue et encouragé tout au long de ce projet, **ma très chère épouse.**

A **mes très chers anges, Timallah Abderrahmane,Soahaib et Lina** .

A **mes très chers frères et sœurs** qui m'ont énormément encouragée et soutenue.

Abdelfattah

Remerciement

Ce sujet a été proposé par la division de sécurité informatique du Centre de Recherche sur l'Information Scientifique et Technique dans le cadre de projet de fin de formation post-graduation spécialisée en sécurité informatique.

Je tiens avant tout à exprimer ma profonde gratitude, mes sincères remerciements et ma haute considération à mon promoteur Dr NOUALI Omar, Directeur de la division sécurité informatique CERIST, pour la confiance qu'il m'a fait d'accepter d'être mon promoteur.

Je souhaite exprimer ma profonde gratitude, mes sincères remerciements et ma haute considération à mon encadreur Mr KRINAH Abdelghani, Chargé d'étude à la division sécurité informatique CERIST, pour son soutien, ses précieux conseils et sa patience tout au long de ce projet.

Mes vifs remerciements et mes hautes considérations vont également aux membres de jury pour l'honneur d'accepter de consacrer de leur précieux temps afin d'évaluer mon travail.

J'exprime ma haute considération à tous le personnel du service formation du CERSIT et je les remercie.

Je remercie aussi tous ceux qui, de près ou de loin, ont contribué à la réussite de ce travail.

ملخص:

من أجل ضمان تطبيق السياسة الأمنية لأنظمة الإعلام الآلي طور العديد من الأدوات الأمنية المختلفة، من بين هذه الأدوات نجد أنظمة كشف التسلل. أنظمة كشف التسلل هي كل أداة أو وسيلة تساعدنا على التنبؤ أو تحديد أي نشاط غير شرعي أو غير طبيعي في الشبكة. الوظيفة الأساسية لهذه الأنظمة هي تحذير المس ؤول عن الشبكة بوجود تهديدات أو إنتهاكات للسياسة الأمنية ، و بناءاً على ذلك ي تخذ المسؤول التدابير المناسبة وفقاً للمعلومات المتاحة له . من بين هذه الأنظمة من يعتمد تكنولوجيا تقفي أثر الإختراق، و منها من يعتمد تكنولوجيا تحديد سلوك إستغلال الشبكة. إلا أن هذه الأنظمة صعبة التثبيت و في بعض الأحيان لا تسمح بالتخصيص وفق رغبات المسؤول عن الشبكة. من هذا المنطلق قمنا في هذه الأطروحة، بتصميم و إنجاز نظام كشف التسلل عبر الشبكة معتمدين طريقة تعقب الأثر باستخدام تقنية الأنظمة الخبيرة المستعملة في الذكاء الإصطناعي. يمّكن النظام المنجز من المراقبة و الفحص الآني للشبكة، و التنبيه في حال كشف الإختراق، كما يمكن لمستخدم هذا النظام أن يضبط معاييراً للسياسة الأمنية الخاصة به.

مفاتيح البحث: أمن أنظمة الإعلام الآلي، أنظمة كشف التسلل، أنظمة كشف التسلل عبر الشبكة، الهدهد، الأنظمة الخبيرة، الذكاء الإصطناعي.

Résumé:

Afin d'assurer l'application de la politique de sécurité des systèmes d'information, de nombreux outils de sécurité ont été développés, parmi ces outils, on trouve les systèmes de détection d'intrusion. L'IDS (Intrusion Detection System) est l'outil ou le moyen capable de nous aider à identifier les intrusions ou toute activité illégale ou anormale. La fonction principale de ces systèmes est de notifier l'administrateur réseau de toutes tentatives d'attaque ou violation de la politique de sécurité, L'administrateur peut prendre des mesures appropriées en fonction des informations issues de l'IDS. Deux approches utilisées dans ces systèmes la première basé signature , et la deuxième comportementale. Toutefois, ces systèmes sont souvent difficiles à mettre en place et ne permettent pas la personnalisation selon les souhaits de l'administrateur réseau. Dans ce mémoire, nous avons conçu et réalisé un IDS réseau basé signature et nous avons utilisé la technologie des systèmes expert utilisés dans l'intelligence artificielle. Le système réalisé permet la capture et le décodage du trafic réseau en temps réel, l'analyse du trafic décodé, la notification en cas de détection d'intrusion, et l'introduction des règles de politique de sécurité.

Mots clés: Sécurité informatique, Système de détection d'intrusion réseau, IDS, NIDS, Houdhoud, Système experts, Système de détection d'intrusion.

Abstract

To ensure the implementation of the security policy, different security tools have been developed, among these tools include intrusion detection systems. IDS (Intrusion Detection System) is the tool or method that can help us to identify intrusions or any illegal or abnormal network activity. The main function of these systems is to notify the network administrator of any attempts of attack or breach of security policy, the administrator can take the appropriate action based on the information from the IDS. Two approaches are used in these systems, the first one is by signature, the second one is by behavior. However, these systems are often difficult to implement and do not allow customization according to the wishes of the network administrator. In this thesis, we designed and implemented a network detection system signature based, using expert systems techniques known in artificial intelligence. The developed system can capture, decode and analysis network traffic on real-time, notify the administrator in case of intrusion detection. Moreover the administrator can introduce his own security policy rules.

Key words: Intrusion detection systems, IDS, Network intrusion detection systems, NIDS, Houdhoud, Expert system, artificial intelligence.

Liste des figures

Liste des tableaux

Sommaire