

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 arges, Timallah Abderrahmane, Souhaib 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.

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 المسؤول عن الشبكة بوجود تهديدات أو إنتهاكات للسياسة الأمنية ، وبناءاً على ذلك يتخذ المسؤول التدابير المناسبة وفقاً للمعلومات المتاحة له . من بين هذه الأنظمة من يعتمد تكنولوجيا تقفي أثر الاختراق، ومنها 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. يمكن النظام المنجز من المراقبة و الفحص الآني للشبكة، والتنبيه في حال كشف الاختراق، كما يمكن لمستخدم هذا النظام أن يضبط معايير 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

Figure I.1 Catégorie des réseaux informatiques	6
Figure I.2 Topologie en bus	6
Figure I.3 Topologie en étoile	7
Figure I.4 Topologie en anneau	7
Figure I.5 Topologie maillé	7
Figure I.6 Composants du réseau informatique.....	8
Figure I.7 Correction des erreurs de transmission	9
Figure I.8 Modèle de communication OSI	13
Figure I.9 Correspondance TCP/IP OSI.....	15
Figure I.10 Structure de l'entête du datagramme IP	17
Figure I.11 UDP Protocole de la couche transport.....	23
Figure I.12 Encapsulation de l'UDP dans un datagramme IP	23
Figure I.13 L'entête UDP	23
Figure I.14 L'entête TCP	25
Figure I.15 Clôture canonique d'une connexion TCP.....	27
Figure I.16 Clôture abrupte d'une connexion TCP	28
Figure I.17 Mécanisme de l'acquittement du protocole TCP	28
Figure I.18 Fenêtre glissante du protocole TCP.....	29
Figure I.19 Exemple de fenêtre glissante du TCP	30
Figure II.1 Taxonomie des IDS	41
Figure II.2 Principe de l'algorithme génétique.....	42
Figure II.3 Paradigme de détection.....	48
Figure II.4 Modèle générique d'un IDS proposé par l'IDWG (Wood and Erlinger, 2012)	49
Figure II.5 Architecture de SNORT	55
Figure III.1 Architecture de la solution proposée	60
Figure III.2 Diagramme de classe de la solution proposée	68

Figure III.3 Diagramme d'activité de la solution proposée	69
Figure III.4 Architecture typique du système basé sur les règles	70
Figure IV.1 Chargement de l'application	84
Figure IV.2 Fenêtre de connexion à la console de la solution	84
Figure IV.3 Message d'échec de connexion	85
Figure IV.5 Menu principal et barre d'outils principale.....	85
Figure IV.4 La fenêtre principale de la solution	85
Figure IV.6 Fenêtre de sélection de fichier de capture PCAP	86
Figure IV.7 Fenêtre de sélection de fichier de capture PCAP	86
Figure IV.8 Fichier de capture sélectionné	87
Figure IV.9 Choix d'une interface réseau pour la capture	87
Figure IV.10 Panneau de capture	89
Figure IV.11 Barre de filtre d'affichage	89
Figure IV.12 Fenêtre de gestion des services réseaux.....	90
Figure IV.13 Fenêtre de gestionnaire de règles de détection	91
Figure IV.14 Panneau d'évènements	91

Liste des tableaux

Tableau I.1 Champs de l'entête du datagramme IP.....	19
Tableau I.2 Classes d'adresse IP v4	21
Tableau I.3 Champs de l'entête TCP	26
Tableau II.1 Tableau comparatif de méthodes de détection.....	45
Tableau II.2 Tableau comparatif des IDS connus	57
Tableau III.1 Aspect fonctionnel de la solution.....	63
Tableau IV.1 Caractéristiques du Java.....	79

Sommaire

Introduction générale	1
PARTIE I. : ETUDE DES RESEAUX INFORMATIQUES	3
CHAPITRE 1 : Réseaux informatiques.....	4
I.1.1 Evolution des réseaux et des télécommunications.....	4
I.1.2 L'internet: le réseau public.....	4
I.1.3 Architecture des réseaux informatiques.....	5
I.1.4 Principales composantes d'un réseau.....	8
I.1.5 Techniques de détection et de correction des erreurs de transmission	9
I.1.6 Modes de communication.....	11
I.1.7 Mode de fonctionnement d'un réseau	11
CHAPITRE 2 : Modèles de communications standards	13
I.2.1 Modèle de communication OSI	13
I.2.2 Le Modèle TCP/IP	14
CHAPITRE 3 : Le protocole IP	17
I.3.1 Le format du Datagramme IP	17
I.3.2 Adressage IP.....	20
I.3.3 Le protocole UDP.....	22
I.3.4 Attribution des ports	24
I.3.5 Le protocole TCP	25
PARTIE II. : SYSTEMES DE DETECTION D'INTRUSION	31
CHAPITRE 4 : Notions de la sécurité informatique.....	32
II.4.1 Propriétés de la sécurité informatique	32
II.4.2 Politique de sécurité.....	33
II.4.3 Les objectifs de la sécurité informatique.....	34
CHAPITRE 5 : Attaques et intrusions informatiques.....	35

II.5.1	Définitions	35
II.5.2	Etapas d'une attaque	35
II.5.3	Classification des attaques informatiques	36
II.5.4	Les contre-mesures.....	38
CHAPITRE 6	: Systèmes de détection d'intrusion	40
II.6.1	Détection d'intrusion.....	40
II.6.2	Système de détection d'intrusion (IDS)	40
II.6.3	Taxonomie des systèmes de détection d'intrusion	40
II.6.4	Méthodologie de détection	41
II.6.5	Le comportement de l'IDS en cas de détection (IDS actif et IDS passif).....	45
II.6.6	La source des données auditées.....	46
II.6.7	Architecture d'un système de détection d'intrusion.....	49
II.6.8	Critères d'évaluation d'un IDS	51
II.6.9	Les différents types des IDS.....	51
II.6.10	Les limites des systèmes de détection d'intrusions	54
II.6.11	Les systèmes de détection d'intrusion les plus répandus.....	54
II.6.12	Comparatif des solutions IDS Connus.....	57
PARTIE III.	:ETUDE CONCEPTUELLE DE LA SOLUTION.....	59
CHAPITRE 7	: Architecture de la solution proposée.....	60
III.7.1	Niveau décisionnel	60
III.7.2	Niveau traitement.....	60
III.7.3	Niveau Données.....	61
III.7.4	Aspect fonctionnel de la solution	61
CHAPITRE 8	:Modélisation de la solution.....	64
III.8.1	Méthodes de conception	64
III.8.2	Modélisation de la solution proposée.....	67
CHAPITRE 9	:Détection basée sur les règles.....	70

III.9.1	Moteur d'inférence.....	70
III.9.2	Conception d'un NIDS basé sur les règles.....	71
III.9.3	Les règles de SNORT.....	72
III.9.4	L'Algorithme RETE.....	74
III.9.5	Principe de fonctionnement de l'analyse basé sur les règles:.....	75
PARTIE IV.	REALISATION ET IMPLEMENTATION DE LA SOLUTION	77
CHAPITRE 10	: Langage et outils de développement.....	78
IV.10.1	Le langage Java	78
IV.10.2	La librairie JNetPcap	79
IV.10.3	Le Java Expert System Shell	79
IV.10.4	Outil de développement Netbeans EDI.....	81
IV.10.5	La base de donnée Apache Derby	81
CHAPITRE 11	: Implémentation de la solution.....	82
IV.11.1	Module FlowCapturer.....	82
IV.11.2	Module FlowDecoder.....	83
CHAPITRE 12	: Présentation de la solution développée.....	84
IV.12.1	Ouverture d'une session.....	84
IV.12.2	la console de la solution.....	85
IV.12.3	Source de capture.....	86
IV.12.4	Filtre de capture	88
IV.12.5	Contrôle d'une capture.....	88
IV.12.6	Le filtre d'affichage	89
IV.12.7	Gérer les services réseaux	90
IV.12.8	Gestionnaire de politique de détection.....	90
IV.12.9	Gestionnaire d'évènements.....	91
Conclusion générale		92