



République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université des Sciences et de la Technologie Houari Boumediène

Faculté d'Electronique et d'Informatique

Mémoire de Master

Domaine Mathématiques et Informatique

Filière Informatique

Spécialité

Réseaux et Systèmes Distribués

Thème

***Conception et réalisation d'un Outil de Détection
des Intrusions dans un Réseau***

Réalisé par :

Mr: BENHARRATS Wassim Adel

Mr: HOUAS Amine

Sujet proposé par :

Dr: NOUALI Omar, DSI, Cerist

Mr: KRINAH Abdelghani, DSI, Cerist

Devant le jury :

Mme BENZAID Chafika Présidente

Mme MEKLIICHE Kenza Membre

Binôme N° : 140/2016

REMERCIEMENTS

Arrivés au terme de ce travail, nous ne pouvons que reconnaître l'apport d'un nombre de personnes sans qui ce projet n'aurait pu être mené à bien.

Nos plus sincères remerciements vont d'abord au centre de recherche sur l'information scientifique et technique CERIST et à notre promoteur monsieur Krinah Abdelghani , pour nous avoir guidé tout au long de ce travail par ses conseils judicieux et avisés, pour nous avoir encouragé quand il le fallait et pour le temps précieux qu'il nous a consacré.

Nous tenons également à remercier les membres du jury Madame BENZAID, Madame MEKLIICHE de nous avoir fait l'honneur d'examiner et de juger notre modeste travail.

Que tous ceux qui ont contribué de près ou de loin à l'aboutissement de ce travail, par leurs conseils, leurs encouragements ou leur soutien inconditionnel, trouvent ici l'expression de notre profonde reconnaissance. Une pensée particulière à nos familles.

Hommage

Je tiens à rendre un hommage soutenu à mon grand père Bouamrane Chikh qui nous a quitté récemment. C'était un humaniste à l'esprit large, un intellectuel reconnu et respecté pour son humilité. Toute sa vie il a oeuvré pour transmettre des valeurs telles que l'amour du travail bien fait et le respect de son prochain. Je tiens à exprimer le bonheur et l'honneur que j'ai à être son petit fils. Je lui serai toujours reconnaissant quand au patrimoine qu'il nous a légué à moi et à ma famille et je profite de cette occasion pour dédier à sa mémoire ce modeste travail. Puisse dieu l'accueillir dans son vaste paradis. Allah yarahmek ya djeddi, achaykh Bouamrane . BENHARRATS Wassim

Résumé

Aujourd'hui, la sécurité des réseaux informatiques est devenue primordiale afin de garantir une infrastructure fiable et performante, et d'assurer la confidentialité et l'intégrité des données échangées entre utilisateurs et applications.

Ceci passe par la surveillance du contenu sur le réseau et la détection d'activité douteuse.

Afin de détecter les attaques que peut subir un système, il est nécessaire de disposer d'un outil spécialisé dont le rôle sera de surveiller les données qui transitent sur ce système et qui permettrait à l'administrateur de réagir si des données semblent suspectes, ou susceptibles de nuire au fonctionnement normal du système informatique.

Parmi les solutions existantes, les logiciels qui sont les plus à même d'effectuer cette tâche sont les systèmes de détection d'intrusion : les IDS.

L'objectif de ce projet est de concevoir et réaliser un outil de détection des intrusions dans un réseau informatique. L'application à proposer doit garantir la surveillance du contenu circulant sur le réseau en procédant à la collecte, puis l'analyse des paquets TCP/IP en temps réel.

Les données récupérées doivent être présentées à un administrateur, à travers une interface graphique, lui permettant de repérer les activités suspectes suivant des critères préalablement établis, et lui offrant la possibilité d'agir afin de pallier à la menace, dans le but d'assurer la sécurité de l'infrastructure dont il a la charge.

Mot clés :

Sécurité des réseaux, détection des intrusions, TCP/IP.

Abstract

Today, the security of computer networks has become essential to ensure a reliable and efficient infrastructure, and ensuring the confidentiality and integrity of data exchanged between users and applications.

This requires the monitoring of content on the network and detect suspicious activity.

To detect attacks that can undergo a system, it is necessary to have a specialized tool whose role will be to monitor the data that transmitted through the network this system would allow the administrator to react if data seem suspicious, or could adversely affect the normal operation of the computer system.

Among existing solutions, the software that perform the best this task are intrusion detection systems IDS.

The objective of this project is to design and implement an intrusion detection tool in a computer network. The application must provide to ensure monitoring of content on the network by performing real time collection and analysis of TCP / IP packets .

The data collected should be presented to an admin, through a graphical user interface (GUI), allowing it to identify suspicious activities according to predefined criteria, and offering the possibility to take action to mitigate the threat in order to ensure the security of the infrastructure it is responsible.

Key words :

Networks security, intrusion detection, TCP/IP.

Sommaire

Introduction générale	1
1 Notions de bases sur les réseaux informatiques	3
1.1 Types de réseaux	4
1.1.1 Les réseaux locaux (LAN)	4
1.1.2 Les réseaux métropolitains (MAN)	4
1.1.3 Les réseaux étendus (WAN)	5
1.2 Topologie	5
1.2.1 La topologie physique	6
1.2.2 La topologie logique	9
1.3 Architecture TCP/IP	10
1.3.1 Définition	10
1.3.2 TCP/IP est un modèle en couches	10
1.3.3 Couches TCP/IP	11
1.3.4 Suite de protocoles	13
1.4 Encapsulation	15
1.5 Segment TCP	16
1.5.1 Description des champs	17
1.6 Segment UDP	18
1.6.1 Description des champs	18
1.7 Le datagramme IP	19
1.7.1 Description des champs	20
1.8 La trame Ethernet :	22
1.8.1 Description des champs	23
2 Notions sur les IDS	25
2.1 Introduction	26
2.2 Notions de base de la sécurité	26
2.2.1 La confidentialité :	26
2.2.2 L'intégrité	26
2.2.3 La disponibilité	26
2.2.4 L'authentification	26
2.2.5 Non-répudiation	26
2.3 Terminologie de la sécurité informatique	27
2.4 Types d'attaques	28
2.5 Système de détection d'intrusions	30

2.5.1	Historique	30
2.5.2	Détection d'intrusions	30
2.5.3	Définition IDS	31
2.5.4	Modèle et normalisation :	33
2.6	Méthodes de détection :	34
2.6.1	L'approche par scénario :	34
2.6.2	L'approche comportementale	36
2.7	Classification des IDS	38
2.7.1	Classification selon l'emplacement des sources de données :	38
2.7.2	Classification selon la réponse après détection	40
2.8	Exemples d'IDS	41
3	Conception	44
3.1	Objectifs visés	45
3.2	Description des bénéfiques	45
3.3	Résultats et fonctionnalités attendus	46
3.3.1	Paramétrage	46
3.3.2	Sauvegarde	46
3.3.3	Affichage	46
3.4	Description de la solution proposée	47
3.4.1	Vue d'ensemble de la solution	47
3.4.2	Définition	48
3.4.3	Schéma de l'application	49
3.5	Identification des acteurs	49
3.6	Diagramme de cas d'utilisation	50
3.6.1	Acteur	50
3.7	Diagramme d'activité	52
3.8	Diagramme de séquences	54
3.8.1	Authentification	54
3.8.2	Mise à jour des paramètres	56
3.8.3	Fonctionnement du système	58
3.9	Diagramme des classes	60
3.10	Base de données	61
4	Environnement de développement et réalisation de l'application	62
4.1	Environnement matériel	63
4.1.1	Matériel informatique	63
4.1.2	Equipements de connexion	63
4.2	Environnement logiciel	64
4.2.1	Java	64
4.2.2	jNetPcap	64

4.2.3	Présentation d'eclipse	65
4.2.4	Présentation de SQL	66
4.3	Présentation de l'application détection d'intrusion	67
4.3.1	Fenêtre d'authentification	67
4.3.2	Première utilisation	68
4.3.3	Paramètres de collecte (filtre)	69
4.3.4	Paramètres de détection	70
4.3.5	Collection et Traitements	72
4.4	Exemples d'exécution	73
4.4.1	Authentification	73
4.4.2	Paramètres de détection	74
4.4.3	Paramètres de collecte (filtre)	75
4.4.4	Collecte et traitement	76
4.4.5	Fenêtre d'affichage	80
	Conclusion générale	83
	Bibliographie	84

Table des figures

1.1	Types des Réseaux	5
1.2	Topologie en bus	6
1.3	Topologie en anneau	7
1.4	Topologie en étoile	8
1.5	Topologie Maillé	8
1.6	Couches TCP/IP	11
1.7	Processus d'encapsulation	15
1.8	Segment TCP	16
1.9	Segment UDP	18
1.10	Datagramme IP	19
1.11	Trame Ethernet	22
2.1	Exemple de réseau avec IDS	31
2.2	Problèmes des IDS	32
2.3	Modèle CIDF	33
2.4	Schéma représentant l'approche par scénario	34
3.1	Schéma de conception de l'application	49
3.2	Use case "Administrateur"	51
3.3	Diagramme d'activité"Systeme"	53
3.4	Diagramme de séquence"Authentification"	55
3.5	Paramètres	57
3.6	Diagramme de séquence "Systeme"	59
3.7	Diagramme des classes	60
4.1	Câble Ethernet RJ45	63
4.2	Logo Java	64
4.3	Logo d'eclipse	65
4.4	Logo phpMyAdmin	66
4.5	Page d'accueil	67
4.6	Fenêtre principale	68
4.7	Paramétrage de la collecte (filtre)	69
4.8	Critères de détection	70
4.9	Fenêtre de collecte et traitements	72
4.10	Fenêtre d'authentification	73
4.11	Critères de détection	74

4.12 Fenêtre de filtrage	75
4.13 Choix d'interface réseau	76
4.14 Résultat de la collecte	77
4.15 Exemple d'intrusion	78
4.16 Fenêtre statistique	79
4.17 Affichage sans critères	80
4.18 Affichage avec critères(ip source)	81
4.19 Affichage avec critères(Taille)	82

Liste des tableaux

- 1.1 Suite des protocoles et de leurs couches 13
- 3.1 Rôle des acteurs 49
- 3.2 Taches de l'administrateur 50
- 3.3 Système (Activité) 52
- 3.4 Authentification 54
- 3.5 Paramétrage 56
- 3.6 Fonctionnement système 58

Liste des abréviations

ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
CRC	Cyclic Redundancy Check
CPU	Central Processing Unit
DF	Don't Fragment
DNS	Domain Name System
FCS	Fram Check Sequence
FTP	File Transfer Protocol
FDDI	Fiber Distributed Data Interface
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocole
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv6	Internet Protocol version 6
IPv4	Internet Protocol version 4
IOS	Organisation Internationale de Normalisation
LAN	Local Area Network
MAC	Medium Access Control
MAN	Metropolitan Area Network
MF	More Fragment
OSI	Open System Interconnection
PDA	Personal Digital Assistant
PDU	Protocol Data Unit
QoS	Quality Of Service
RARP	Reverse Address resolution protocol
SFD	Start Trame Delimiter
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
Telnet	Terminal NETwork
TTL	Time To Live

UDP User Datagram Protocol
WAN Wide Area Network
IDS Intrusion Detection System