**République Algérienne Démocratique et Populaire**

Ministère de l'enseignement supérieur et de la recherche scientifique

**Université des Sciences et de la Technologie Houari Boumediene**

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 MEKLICHE 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 MEKLICHE 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 esprimer 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

# Table des figures

# Liste des tableaux

# 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