REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'enseignement supérieur et de la recherche scientifique

Centre de Recherche de l'Information Scientifique et Technique

C.E.R.I.S.T

MEMOIRE

Pour l'obtention du Diplôme de Post-Graduation Spécialisée en

Sécurité Informatique

THEME

La conception d'une base de connaissances pour l'aide à l'investigation dans Firewall Forensics

Présenté par :

Melle : Hassina BENSEFIA

Encadrée par :

Mme : Sakina LOUNI

Devant le jury :

Mr Hamid KHEMISSA	**Président**
Mme Sakina LOUNI	**Rapporteur**
Mme Souad BENMEZIANE	**Examinateur**
Mr Halim KHELALFA	**Examinateur**
Mr Omar NOUALI	**Examinateur**

Mai 2002

Remerciements

Je tiens à exprimer ma profonde et sincère reconnaissance envers l'honorable institution, l'Institut National de formation en Informatique(INI), plus particulièrement à son Directeur Général, Monsieur Abderrazak HENNI, pour m'avoir encouragée et autorisée à suivre une post-graduation dans un domaine de pointe qui est la sécurité informatique. Que l'INI trouve ici l'expression de toute ma gratitude pour l'aide et la confiance qui m'ont été accordées pour mener à bien cette post-graduation.

Je tiens à adresser mes vifs remerciements :

- *A Monsieur M.. Halim KHELALFA, chargé de recherche au C.E.R.I.S.T, pour m'avoir proposé un thème d'actualité ;*
- *A Madame Sakina LOUNI pour avoir accepté de diriger ce travail et pour toutes les remarques faites pour la finalisation de ce mémoire ;*
- *A madame Houria ZAIDI, responsable du service formation du C.E.R.I.S.T, pour sa disponibilité, sa compréhension et ses encouragements durant toute la période de notre PGS.*
- *A mes enseignants de la PGS pour le grand effort qu'ils ont fait pour nous transmettre le savoir ;*
- *A madame et messieurs les membres du jury de cette PGS.*

Mes meilleurs remerciements vont également à :

- *Mes collègues à L'INI qui m'ont aidé et m'ont encouragé sans cesse ;*
- *Mes camarades de post-graduation pour leur amitié et leur soutien moral ;*
- *Les Personnels de la bibliothèque et du service reprographie de l'INI ;*
- *Tous ceux qui m'ont aidé de loin ou de près à élaborer ce travail..*

TABLE DES MATIERES

Chapitre 2 : Network Forensics

Chapitre 3 : Les fichiers logs

Chapitre 4: Les systèmes experts

Chapitre 5 : La conception d'une base de connaissances pour l'interprètation des fichiers logs d'un Firewall

La base de connaissances