

**MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE  
LA RECHERCHE SCIENTIFIQUE**

***CENTRE DE RECHERCHE SUR L'INFORMATION  
SCIENTIFIQUE ET TECHNIQUE***

***C.E.R.I.S.T.***

**Mémoire pour l'Obtention  
du Diplôme de Post-Graduation Spécialisée  
En Sécurité Informatique**

**ETAT DE L'ART :  
LES SYSTEMES DE DETECTION  
D'INTRUSIONS**

**Présenté Par :**

M<sup>me</sup>. BENSLIM nee BENMERZOUG Ghania  
M<sup>elle</sup>. ESSED Nabila

**Promoteur :**

Mr. AHMED Nacer M.

**Jury :**

M. BENHAMADI	President
M <sup>e</sup> . BENMEZIANE	Membre
M. NOUALI	Membre

**Session : Juin 2001**

# SOMMIAIRE

<b>INTRODUCTION</b> .....	<b>5</b>
<b>CHAPITRE I : Concepts et Définitions de Base</b>	
<b>I.1 .La sécurité en générale</b> .....	<b>8</b>
I.1.1- Les regles de sécurité d'un système d'information .....	<b>8</b>
I.1.2- Pourquoi les systèmes sont-ils vulnérables? .....	9
I.1.3- Méthodes et Outils Utilisees par les Attaquants .....	10
I.1.3.1- Les Methodes .....	10
I.1.3.2- Les Outils .....	10
I.1.4- Technique de Protection des Informations .....	12
I.1.5- Les mécanismes de sécurité sur un exemple de réseau .....	13
I.1.5.1- Description du reseau a sécuriser .....	13
I.1.5.2- Identifier les informations a proteger .....	14
I.1.5.3- Politique de sécurité .....	14
I.1.5.4- Sécurité <b>minimum</b> .....	14
I.1.5.5- Le probleme des accès distants .....	15
I.1.5.6- Firewall et proxy .....	15
I.1.5.7- Logiciel de detection systematique d'erreurs .....	16
I.1.5.8- Système de detection d'intrusions .....	16
I.1.5.9- Apres sécurisation .....	16
1.2- Les systèmes de detections d'intrusions (IDS) .....	17
1.2.1- Définition de l'intrusion .....	17
1.2.2- Définition de la Detection d'intrusions .....	18
1.2.3- Definition d'un IDS .....	18
1.2.4- Les composants d'un IDS .....	19
1.2.5- Rôle de la Detection d'intrusions .....	20