

République Algérienne Démocratique et Populaire  
Ministère de l'Enseignement Supérieur et de la Recherche  
Scientifique  
Le Centre de Recherche sur l'Information Scientifique et Technique  
( CERIST )

Mémoire du Projet de fin d'études

Pour l'obtention du diplôme  
De Post Graduation Spécialisée ( PGS ) en Sécurité Informatique

Sujet :



**Etude & Classification des Vulnérabilités de  
Windows 2000 & Linux**

Encadré par : H.KHEMISSA

Etudié par : BENBARTAOUI Abdelhamid  
BENDRISSOU Mohamed

Devant le jury composé de :

Président : Pr. N. BADACHE  
Membre : S. BENMEZIANE  
Membre : D. TANDJAOUI  
Rapporteur : H. KHEMMISSA

PROMOTION 2003

# RESUME

Chaque jour, les laboratoires de recherche de vulnérabilités publient des nouvelles failles sur les systèmes d'exploitation. Ces failles peuvent être exploitées, pour un premier temps, par les "Hackers" connaisseurs pour réaliser des accès non autorisés ou des dénis de services sur ces systèmes.

Aussitôt qu'elles soient connues par les Hackers des outils d'attaque les exploitant sont développés. Ce qui augmente le nombre d'attaques en exponentiel.

Pour régler ces problèmes de sécurité des correctifs sont développés. Ainsi avoir un système mis à jour par ces correctifs est une exigence primordiale pour se prémunir des différents risques. Le suivi des alertes et des correctifs est la tâche demandée aux administrateurs, afin d'assurer la sécurité de leurs systèmes.

Des organismes et des sites Internet spécialisés exposent la liste des nouvelles vulnérabilités détectées et leurs correctifs correspondants. Ou encore plus, ils se spécialisent dans l'étude technique des failles systèmes. Ils proposent des outils logiciels qui permettent de diagnostiquer l'état des serveurs en simulant les différents scénarios d'attaques répertoriés dans une base de données mise à jour.

Notre étude consiste à étudier les vulnérabilités des systèmes Windows 2000 et Linux et les classer par degré de nuisance. Cette étude servira de base pour le diagnostic, le suivi et l'administration des systèmes.

*Mots clés : vulnérabilité, Windows 2000, Linux, exploits, sécurité informatique.*

# SOMMAIRE

## **INTRODUCTION**

### **Chapitre I : Description de Windows 2000**

<b>1) Présentation.</b>	<b>1</b>
<b>2) Description du noyau et du processus de démarrage.</b>	<b>2</b>
2.1) <i>Noyau de Windows 2000</i>	2
2.2) <i>Le processus de démarrage sous Windows 2000</i>	3
2.3) <i>Les processus par défaut dans Windows 2000</i>	5
<b>3) Sécurité.</b>	<b>7</b>
3.1) <i>Identification et Authentification</i>	7
3.2) <i>Contrôle d'accès</i>	8
<b>4) Les vulnérabilités.</b>	<b>9</b>
a) <i>Prise d'empreinte</i>	9
b) <i>Recensement</i>	9
c) <i>Infiltration</i>	9
d) <i>Deni de service</i>	9
<b>5) Classification de Windows 2000.</b>	<b>10</b>
5.1) <i>Rappel sur les normes de classification des produits</i>	10
a) <i>La norme américaine TCSEC</i>	10
b) <i>Norme européenne ITSEC</i>	10
c) <i>Norme ISO 15408</i>	11
5.2) <i>Classification de Windows 2000</i>	11

### **Chapitre II : Description de Linux**

<b>I) Introduction</b>	<b>12</b>
I.1) <i>Fichiers d'initialisation</i>	12
I.2) <i>Répertoires importants</i>	12
I.3) <i>Processus.</i>	13
I.4) <i>init, inittab</i>	13
I.5) <i>Les fichiers rc</i>	13
I.6) <i>Mode mono-utilisateur</i>	14
I.7) <i>Arrêter le système</i>	14

<b>II) Sécurité</b>	<b>15</b>
<i>II.1) Choix du mot de passe</i>	15
<i>II.2) Le temps d'ouverture pour le compte « root »</i>	16
<i>II.3) Fichier « /etc/inetd.conf »</i>	17
<i>II.4) TCP_WRAPPER</i>	18
<i>II.5) Fichier « /etc/host.conf »</i>	19
<i>II.6) Fichier « /etc/services »</i>	20
<i>II.7) Fichier « /etc/securetty »</i>	21
<i>II.8) Les comptes spéciaux</i>	21
<i>II.9) Blocage de la commande su</i>	22
<i>II.10) Limiter les ressources</i>	23
<i>II.11) Fichiers sans propriétaires</i>	23
<i>II.12) Chercher les fichier « .rhosts »</i>	24
<i>II.13) Scanneurs d'insécurité réseau</i>	24

### **Chapitre III : Etude et Classification des vulnérabilités**

<b>Etude des Vulnérabilités :</b>	<b>31</b>
1)- Définition d'une vulnérabilité	31
1.1) Services vulnérables	31
1.2) Scripts vulnérables	31
1.3) Débordement de tampon	31
<i>1.3.1) Principes du Buffer Overflow</i>	35
<i>1.3.2) Exploitation d'un Buffer Overflow</i>	40
<i>1.3.3) Portée de ce type de vulnérabilité</i>	41
<i>1.3.4) Comment se protéger ?</i>	42
<i>1.3.4.1) Contrôle statique de code</i>	42
<i>1.3.4.2) Rendre la pile non exécutable</i>	43
<i>1.3.4.3) Contrôle automatique de longueur des buffers</i>	43
<i>1.3.4.4) Contrôle d'intégrité des pointeurs</i>	43
<i>A) StackGuard</i>	44
<i>B) StackShield</i>	44
<i>1.3.5) Veille technologique</i>	45
<i>1.3.6) Exemple d'une attaque exploitant une Vulnérabilité Buffer Overflow</i>	45
2)- Evolution de la sécurité d'un système	47
3)- La vulnérabilité dans le temps	48

<b>Classification &amp; Evaluation d'une Vulnérabilités :</b>	<b>49</b>
1)- Proposition d'une métrique d'évaluation du degré de sévérité des Vulnérabilités	49
<i>1.1)- Nos critères d'évaluation</i>	<i>49</i>
<i>1.2)- Le degré de sévérité de la vulnérabilité</i>	<i>52</i>
<i>1.3)- Exemple d'évaluation de vulnérabilités</i>	<i>53</i>
<i>1.4)- Formulaire de Vulnérabilité</i>	<i>55</i>