

Mémoire de fin d'études
pour l'obtention du Diplôme d'Ingénieur d'Etat en
GENIE INFORMATIQUE

Présenté par:

- Djallel ABDELLI
- Mohamed Hocine BOUTERAA

Thème

**CONCEPTION ET REALISATION D'UN
SYSTEME DE DETECTION DES
VULNERABILITES.**

Dirigé par:

BELHADAD Abdelouahab

Année: 2005

SOMMAIRE

PREAMBULE

INTRODUCTION GENERALE

Partie I : ETAT DE L'ART

Chapitre I : L'AUDIT INFORMATIQUE

I. INTRODUCTION.....	1
II. IDENTIFICATION DES RISQUES DE SECURITE.....	1
III. IDENTIFICATION DES RESSOURCES.....	2
III.1. Classement des ressources par ordre de priorité.....	2
III.2. Calcul de la valeur d'une ressource.....	3
IV. IDENTIFICATION DES MENACES.....	3
IV.1. Évaluation de la sécurité.....	3
IV.1.1. Évaluations des opérations.....	4
IV.1.2. Tests d'intrusion.....	4
IV.1.3. Évaluation des vulnérabilités.....	5
IV.1.4. Audit de détection des intrusions.....	6
IV.2. Outils d'évaluation des vulnérabilités.....	6
IV.2.1. Bases de données de listes de vulnérabilités.....	7
IV.2.2. Fonctionnalité de mise à jour.....	7
IV.2.3. Fonctionnalité de personnalisation.....	7
IV.2.4. Sécurité du réseau.....	7
IV.2.5. Sécurité des hôtes.....	7
IV.2.6. Sécurité des applications.....	8
IV.2.7. Sécurité des données.....	8
IV.2.8. Classement par ordre de priorité.....	8
IV.3. Données requises pour le processus d'analyse des risques de sécurité.....	8
IV.3.1. Calcul des facteurs de gravité.....	9
IV.3.2. Mesure de l'effort requis pour exploiter les vulnérabilités identifiées.....	9
IV.3.3. Calcul des facteurs de vulnérabilité.....	9

Chapitre II : LE MODELE CVE

I. INTRODUCTION.....	11
II. CONTRAINTES EMPECHANT L'INTEROPERABILITE.....	12
II.1. Convention de nommage contradictoire.....	13
II.2. Gestion des informations semblables multi sources.....	13
II.3. Gestion des perspectives de la même vulnérabilité.....	13
III. L'INTRODUCTION D'UN NOUVEAU TERME : « EXPOSURES ».....	13
IV. DEFINITION DES TERMES« VULNERABILITES – EXPOSURES ».....	14
V. ENUMERATION COMMUNE DE VULNERABILITES ET EXPOSITIONS.....	14
VI. PROCESSUS D'ETABLISSEMENT DE LA LISTE CVE.....	15
VI.1. Etape de soumission.....	15
VI.2. Etape de candidature.....	15
VI.3. Etape d'entrée.....	16

Chapitre III : LE MODELE OVAL

I. INTRODUCTION.....	18
----------------------	----

II. LE LANGAGE OVAL (OPEN VULNERABILITIES ASSESSMENT LANGUAGE)	19
III. PROCESSUS D'EMPLOI D'OVAL	20
IV. ELABORATION DES REQUETES OVAL	20
V. LES AVANTAGES D'OVAL:	21
VI. EXEMPLE D'OVAL	21
Partie II : CONCEPTION	
Chapitre I : CONCEPTION	
I. APPROCHE GENERALE	24
I.1. Introduction	24
I.2. Phase de découverte	24
I.3. Phase de détection	24
I.4. Phase d'analyse des résultats	24
I.5. Phase de remédiation	25
II. ARCHITECTURE GENERALE DU SYSTEME	25
III. MODELISATION DES ATTAQUES	26
III.1. Introduction	26
III.2. La grammaire du langage	26
III.3. Description du langage	28
III.4. Exemples de scripts d'attaques	28
III.4.1. Script de l'attaque SMURF	28
III.4.2. Script de l'attaque LAND	28
III.4.3. Script de l'attaque PING OF DEATH	29
III.4.4. Script de l'attaque NEW TEAR	29
III.4.5. Script de l'attaque SYN FLOOD	29
III.4.6. Script de l'attaque MAC FLOODING	30
IV. MODELISATION DES BASES DE DONNEES	30
IV.1. Introduction	30
IV.2. La base des vulnérabilités	31
IV.3. La base OVAL	32
IV.4. L'accès aux bases de données	33
V. MODELISATION UML DU SYSTEME	34
V.1. Introduction	34
V.2. Présentation d'UML	34
V.2.1. Modélisation de l'architecture d'un système	35
V.2.2. Les diagrammes d'UML	36
V.3. Architecture logicielle	37
V.4. Diagramme de déploiement	37
V.5. Diagrammes de cas d'utilisation	39
V.5.1. Diagramme de cas d'utilisation (coté serveur)	39
V.5.2. Diagramme de cas d'utilisation (coté client)	40
V.6. Diagrammes d'activités	41
V.6.1. Diagramme d'activités pour le scan IP	41
V.6.2. Diagramme d'activités pour le scan TCP	41
V.6.3. Diagramme d'activités pour le scan non intrusif	42
V.6.4. Diagramme d'activités pour le scan intrusif	44

V.6.5. Diagramme d'activités pour le scan des vulnérabilités	45
V.7. Diagrammes de séquences.....	45
V.7.1. Sélection d'interface réseau.....	45
V.7.2. Ajout d'une attaque.....	46
V.7.3. Suppression d'une attaque	47
V.7.4. Modification d'une attaque.....	47
V.7.5. Consultation des logs.....	47
V.7.6. compilation d'un script d'attaque	48
V.7.7. Ajout d'une requête OVAL	48
V.7.8. Suppression d'une requête OVAL.....	49
V.7.9. Modification d'une requête OVAL	50
V.7.10. Scan IP.....	50
V.7.11. SCAN TCP	51
V.7.12. Scan UDP	53
V.7.13. phase de découverte du scan des vulnérabilités.....	53
V.7.14. Scan vulnérabilités pour les clients et les machines inconnues (test intrusif).....	54
V.7.15. Scan des vulnérabilités seulement pour les clients	55
V.7.16. Analyse des résultats	56
V.7.17. Lancement d'une attaque connue par le système	57
V.7.18. Lancement d'une attaque inconnue par le système	57
V.7.19. Exécuter une attaque.....	58
V.7.20. Test_wrt et test_wft	59
V.7.21. Test_cmp	60
V.8. Diagramme de classes.....	60
V.9. Diagramme d'objets.....	62
Partie III: REALISATION	
Chapitre I: REALISATION	
I. ENVIRENMENT DE DEVELOPEMENT	63
I.1. Langage de programmation Visual C++ 6.0	63
I.2. La bibliothèque WinPCap	63
II. PRESENTATION DU SYSTEME DE DETECTION DES VULNERABILITES	63
II.1. Présentation de l'application (serveur).....	63
II.1.1. présentation générale	63
II.1.2. Présentation détaillée de chaque interface	65
II.2. PRESENTATION DE L'APPLICATION (client)	72
CONCLUSIONS ET PERSPECTIVES	
ANNEXES	
GLOSSAIRE	
BIBLIOGRAPHIE & WEBOGRAPHIE	