

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	Examineur
Mr Halim KHELALFA	Examineur
Mr Omar NOUALI	Examineur

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

INTRODUCTION GENERALE	1
-----------------------------	---

Chapitre 1 : Les Firewalls

I. INTRODUCTION	5
II. DEFINITIONS D'UN FIREWALL.....	5
III. L'EMPLACEMENT D'UN FIREWALL	6
IV. LES CATEGORIES DE FIREWALL.....	7
IV.1. LE FIREWALL LOGICIEL.....	7
IV.2. LE FIREWALL HARDWARE.....	7
V. LES COMPOSANTS D'UN FIREWALL	8
V.1. LA POLITIQUE DE SECURITE DU RESEAU	8
V.1.1. <i>La politique d'accès aux services</i>	8
V.1.2. <i>La politique de conception du firewall</i>	9
V.2. L'AUTHENTIFICATION AVANCEE	9
V.3. LE FILTRAGE DE PAQUET.....	10
V.3.1. <i>Les avantages du filtrage de paquet</i>	11
V.3.2. <i>Les limitations du filtrage de paquet</i>	11
V.4. LES PASSERELLES D'APPLICATION	12
V.4.1. <i>Les avantages des passerelles d'application</i>	12
V.4.2. <i>Les limitations des passerelles d'application</i>	13
VI. LES PRINCIPALES ARCHITECTURES DE FIREWALLS.....	13
VI.1. LE ROUTEUR FILTRE.....	13
VI.2. L'HOTE BASTION.....	14
VI.3. L'HOTE FILTRE.....	14
VI.4. LE SOUS RESEAU FILTRE	15
VII. LES AVANTAGES D'UN FIREWALL	16
VIII. LES LIMITATIONS D'UN FIREWALL	16
IX. CONCLUSION	17

Chapitre 2 : Network Forensics

I. INTRODUCTION	18
II. L'EVALUATION DE LA SECURITE DES RESEAUX	18
III. LA NOUVELLE VISION A LA SECURITE DES RESEAUX	19
III.1. LA SURVEILLANCE DU RESEAU	19
III.2. LA MISE EN APPLICATION DE LA LOI	19
IV. FORENSICS.....	20
IV.1. SIGNIFICATION DE FORENSICS	20
IV.2. DEFINITION DE FORENSICS	20
IV.3. LE ROLE DE L'EXPERT EN FORENSICS	20
IV.4. LES DISCIPLINES DE FORENSICS.....	21
IV.4.1. La pathologie légale	21
IV.4.2. La sérologie légale.....	21
IV.4.3. La balistique légale.....	21
IV.4.4. L'anthropologie légale	21
IV.4.5. La psychologie légale	21
IV.4.6. La géologie légale.....	22
V. LE BESOIN DE FORENSICS DANS LA SECURITE INFORMATIQUE.....	22
VI. L'INFORMATIQUE LEGALE	22
VII. NETWORK FORENSICS.....	23
VIII. LES ETAPES DU PROCESSUS DE NETWORK FORENSICS	23
VIII.1. LA COLLECTE DE LA PREUVE.....	23
VIII.1.1. Définition de la preuve.....	23
VIII.1.2. L'emplacement de la preuve	23
VIII.1.3. La source de la preuve	24
VIII.2. L'INVESTIGATION	24
IX. CONCLUSION	24

Chapitre 3 : Les fichiers logs

I. INTRODUCTION	25
II. DEFINITION DE « FICHER LOG ».....	25
III. LE FORMAT D'UN FICHER LOG	25
IV. LES FORMATS STANDARDS DE FICHIERS LOGS	26

IV.1. LE FORMAT W3C ETENDU	27
IV. 2. LE FORMAT LOG COMMUN	27
V. LES CRITERES DE CREATION DE FICHIERS LOGS	28
VI. LES NOMS DES FICHIERS LOGS.....	29
VII. LA CORRELATION DES FICHIERS LOGS	29
VIII. LA SYNCHRONISATION DU TEMPS	30
IX. LES PROBLEMES LIES AUX FICHIERS LOGS.....	30
X. LA PROTECTION DES FICHIERS LOGS	30
XI. LA ROTATION DES FICHIERS LOGS.....	31
XII. L'IMPORTANCE DES FICHIERS LOGS.....	32
XIII. L'INTERPRETATION DES FICHIERS LOGS.....	32
XIV. CONCLUSION	33

Chapitre 4: Les systèmes experts

I. INTRODUCTION	34
II. DEFINITION D'UN SYSTEME EXPERT	34
III. ARCHITECTURE D'UN SYSTEME EXPERT	34
III.1. LA BASE DE CONNAISSANCES.....	35
III.2. LA BASE DE FAITS	35
III.3. LE MOTEUR D'INFERENCE	35
III.4. L'INTERFACE EXPERT.....	36
III.5. L'INTERFACE UTILISATEUR.....	36
III.6. LE MODULE D'EXPLICATION.....	36
IV. LA PROBLEMATIQUE DE LA CONNAISSANCE.....	36
IV.1. L'ACQUISITION DES CONNAISSANCES	36
IV.2. LA REPRESENTATION DES CONNAISSANCES	36
IV.2.1. <i>La représentation procédurale</i>	37
IV.2.2. <i>La représentation déclarative</i>	37
V. LES MODES DE RAISONNEMENT DU MOTEUR D'INFERENCE.....	40
V.1. LE CHAINAGE AVANT	40
V.2. LE CHAINAGE ARRIERE.....	41
V.3. LE CHAINAGE MIXTE.....	41

VI. LE CYCLE DE BASE DU MOTEUR D'INFERENCE	41
VI.1. LA PHASE D'EVALUATION.....	41
VI.1.1. <i>La sélection</i>	42
VI.1.2 <i>Le filtrage</i>	42
VI.1.3. <i>La résolution de conflits</i>	42
VI.2. LA PHASE D'EXECUTION.....	42
VII. QUELQUES EXEMPLES DE SYSTEME EXPERT	42
VIII. LES LIMITES DES SYSTEMES EXPERTS	42
IX. CONCLUSION	43

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

I. INTRODUCTION	44
II. LES FICHIERS LOGS D'UN FIREWALL	44
III. FIREWALL FORENSICS	45
IV. LE CONCEPT DE PORT	45
IV.1. LES PORTS RESERVES.....	45
IV.2. LES PORTS ENREGISTRES.....	45
IV.3. LES PORTS DYNAMIQUES OU PRIVES.....	46
V. LE FORMAT D'UN FICHIER LOG D'UN FIREWALL	46
VI. NOTRE APPROCHE	48
VII. LA SOURCE D'EXPERTISE	49
VIII. L'ACQUISITION DU SAVOIR-FAIRE ET L'EXTRACTION DES CONNAISSANCES	49
VIII.1. LES PORTS DESTINATIONS.....	49
VIII.1.1. <i>Port 0</i>	49
VIII.1.2. <i>Port 1</i>	50
VIII.1.3. <i>Port 7</i>	50
VIII.1.4. <i>Port 11</i>	51
VIII.1.5. <i>Port 19</i>	51
VIII.1.6. <i>Port 21</i>	52
VIII.1.7. <i>Port 22</i>	52
VIII.1.8. <i>Port 23</i>	53
VIII.1.9. <i>Port 25</i>	53
VIII.1.10. <i>Port 53</i>	54
VIII.1.11. <i>Port 67 / 68</i>	54

VIII.1.12. Port 69.....	55
VIII.1.13. Port 79.....	56
VIII.1.14. Port 98.....	56
VIII.1.15. Port 109.....	56
VIII.1.16. Port 110.....	57
VIII.1.17. Port 111.....	57
VIII.1.18. Port 113.....	58
VIII.1.19. Port 119.....	58
VIII.1.20. Port 135.....	58
VIII.1.21. Port 137.....	59
VIII.1.22. Port 139.....	59
VIII.1.23. Port 143.....	59
VIII.1.24. Port 161/162.....	60
VIII.1.25. Port 177.....	61
VIII.1.26. Port 513.....	61
VIII.1.27. Port 535.....	62
VIII.1.28. Port 635.....	62
VIII.1.29. Port 1080.....	62
VIII.1.30. Port 1114.....	63
VIII.1.31. Port 2049.....	63
VIII.1.32. Port 3128.....	63
VIII.1.33. Port 1524.....	64
VIII.1.34. Port 6970.....	64
VIII.1.35. Port 5632.....	65
VIII.1.36. Port 13 223.....	65
VIII.1.37. Port 17027.....	65
VIII.1.38. Port 32770-32900.....	66
VIII.1.39. Port 33434-33600.....	66
VIII.1.40. Port 41508.....	66
VIII.2. LES PORTS SOURCES.....	67
VIII.2.1. Port [1-5].....	67
VIII.2.2. Port 20.....	68
VIII.2.3. Port 53.....	68
VIII.2.4. Port 123.....	68
VIII.2.5. Port 4000.....	69
VIII.2.6. Ports 27910-27961.....	69
VIII.2.7. Ports $\geq 61\ 000$	69
VIII.3. LES MESSAGES ICMP.....	70
VIII.3.1. Type =0.....	70
VIII.3.2. Type =3 et Code=0.....	70
VIII.3.3. Type=3 et Code=3.....	71
VIII.3.4. Type=3 et Code=4.....	71
VIII.3.5. Type=4.....	71
VIII.3.6. Type=5.....	72
VIII.3.7. Type=8.....	72
VIII.3.8. Type =11 et Code =0.....	72
VIII.3.9. Type= 11 et code= 1.....	73
VIII.3.10. Type =12.....	73
VIII.4. LES EXPLORATIONS A LA RECHERCHE DE CHEVAUX DE TROIE.....	73
VIII.5. LES PORTS DES JEUX.....	77

VIII.6. ADRESSAGE IP	78
VIII.6.1. L'adresse IP 255.255.255.255	78
VIII.6.2. Les adresses privées	79
VIII.6.3. Adresse IP 127.x.x.x	79
VIII.6.4. Adresse IP 0.0.0.0	80
VIII.6.5. Adresse IP 169.254.x.x	80
IX. LA REPRESENTATION DES CONNAISSANCES	81
IX.1. LE CHOIX DU FORMALISME DE REPRESENTATION	81
IX.2. LA FORMALISATION DES CONNAISSANCES	81
X. LA BASE DE CONNAISSANCES	82
X.1. LE MODE DE RAISONNEMENT DU SYSTEME EXPERT	82
X.2. LE SHELL DE SYSTEME EXPERT A UTILISER	82
X.3. UN EXEMPLE DE DEROULEMENT D'UNE SESSION D'EXECUTION	83
XI. CONCLUSION	86

La base de connaissances

I. LES REGLES SPECIFIQUES AUX PORTS DESTINATION	86
II. LES REGLES SPECIFIQUES AUX PORTS SOURCE	90
III. LES REGLES SPECIFIQUES AUX MESSAGES ICMP	91
IV. LES REGLES SPECIFIQUES AUX ADRESSES IP	91
CONCLUSION GENERALE	93
REFERENCES BIBLIOGRAPHIQUES	95