

REPUBLICQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE  
Ministère de l'enseignement supérieur et de la recherche scientifique  
Université Mouloud Mammeri Tizi Ouzou  
Faculté de génie électrique et d'informatique  
Département d'informatique

## MEMOIRE

De fin d'études

En vue de l'obtention du diplôme d'ingénieur d'état en informatique

Option : informatique industrielle

### Thème

Conception et réalisation d'une boîte d'outils

D'audit de sécurité dans les réseaux

Informatiques

Proposé et dirigé par :

Melle M.BELKADI, Enseignant à l'université Mouloud Mammeri de Tizi-ouzou.

Mr. TANDJAOUI, Membre de recherche au CERIST.

Réalisé par : **Mr. Nabil LAKRIM**

**Mr. Redhouane GUEBLI**

Devant le jury :

Président Mr LALAM

Examineurs : Mr MADIOU

Mme AOUDJIT

Promotion 2005/2006

## Sommaire

<b>INTRODUCTION GENERALE.....</b>	<b>1</b>
-----------------------------------	----------

### **CHAPITRE I : La sécurité Informatique.**

<b>I.1. Introduction :.....</b>	<b>3</b>
<b>I.2 Définition de la sécurité informatique :.....</b>	<b>4</b>
<b>a. Confidentialité des données : .....</b>	<b>4</b>
<b>b. Authentification : .....</b>	<b>4</b>
<b>c. Intégrité des données :.....</b>	<b>5</b>
<b>d. La disponibilité :.....</b>	<b>5</b>
<b>I.3.Définition des vulnérabilités :.....</b>	<b>5</b>
<b>a. Les débordements de tampon :.....</b>	<b>6</b>
<b>b. Chaîne d'attaque :.....</b>	<b>6</b>
<b>c. Mot de passe par défaut :.....</b>	<b>6</b>
<b>d. Mauvaise configuration :.....</b>	<b>6</b>
<b>e. Révélation de la zone mémoire :.....</b>	<b>7</b>
<b>f. Information sur le réseau :.....</b>	<b>7</b>
<b>g. Divulgarion de versions :.....</b>	<b>7</b>
<b>I.4. Les menaces :.....</b>	<b>7</b>
<b>I.4.1. Les menaces accidentelles :.....</b>	<b>7</b>
<b>I.4.2. Les menaces intentionnelles :.....</b>	<b>7</b>
<b>I.4.3. Les menaces passives :.....</b>	<b>8</b>
<b>I.4.4. Les menaces actives : .....</b>	<b>8</b>
<b>I.5. Les attaques :.....</b>	<b>8</b>
<b>I.5.1. Définition :.....</b>	<b>8</b>
<b>I.5.2. Classification des attaquants :.....</b>	<b>8</b>
<b>I.5.2.1.Les Scripts Kiddies :.....</b>	<b>8</b>
<b>I.5.2.2. Les hackers :.. ..</b>	<b>9</b>
<b>I.5.3. Les principaux types d'attaques : .....</b>	<b>9</b>
<b>a. IP Spoofing : .....</b>	<b>9</b>
<b>b. Le Craquage de mots de passe :.....</b>	<b>9</b>
<b>c. Le reniflement des paquets : .....</b>	<b>9</b>
<b>d. ARP Spoofing: .....</b>	<b>10</b>
<b>e. DNS Spoofing :.....</b>	<b>10</b>
<b>•DNS ID Spoofing: .....</b>	<b>10</b>
<b>•DNS Cache_Poisonig : .....</b>	<b>10</b>
<b>f. Les Scripts:.....</b>	<b>11</b>
<b>• Injection SQL :.....</b>	<b>11</b>
<b>g. Les bugs : .....</b>	<b>12</b>
<b>• Buffer overflow : .....</b>	<b>12</b>
<b>h. Les dénies de services : .....</b>	<b>12</b>
<b>h.1. Les dénies de services applicatifs : .....</b>	<b>12</b>
<b>h.2. Les dénies de services réseaux : .....</b>	<b>12</b>

• SYN flooding :.....	12
• UDP flooding :.....	13
• Attaques basées sur la fragmentation:.....	13
• Techniques de broadcasts dirigés:.....	14
• Dénie de service distribué:.....	14
i. Virus :.....	14
i.1. Les virus furtifs :.....	15
i.2. Les virus cryptés :.....	15
i.3. Les virus mutants:.....	15
i.4. Les virus de pièges :.....	15
i.5. Les rétrovirus :.....	15
i.6. Les chevaux de Troie et bombes logiques :.....	15
i.7. Les vers :.....	16
i.8. Les accès cachés :.....	16
I.6. La politique de sécurité :.....	16
a. Politique de sécurité administrative :.....	17
b. Politique de sécurité physique :.....	17
c. Politique de sécurité logique :.....	17
I.6.1. Les principales techniques de défense et de sécurité :.....	18
a. Authentification : .....	18
b. Cryptographie :.....	18
c. Mécanisme de signature numérique :.....	18
d. Firewalls :.....	18
e. Antivirus :.....	19
f. VPN(Réseau Privé Virtuel) :.....	19
g. Les IDS :.....	20
I.7.L'audit de sécurité :.....	20
I.7.1. La qualité d'une solution d'audit de sécurité:.....	21
I.7.2. Une approche proactive :.....	21
I.7.2.1. Phase de découverte :.....	21
I.7.2.2. Phase de détection :.....	21
I.7.2.3. Phase d'analyse des résultats :.....	21
I.7.2.4. Phase de remède :.....	22
I.7.2.5. Journal d'audit de sécurité :.....	22
Conclusion :.....	23

## CHAPITRE II : Méthodologies d'audit de la sécurité informatique

<b>II.1. Introduction :</b>	<b>24</b>
<b>II.2. Définition :</b>	<b>24</b>
<b>II.3. La méthode Marion :</b>	<b>25</b>
<b>II.3.1. Objectif de la méthode :</b>	<b>25</b>
<b>II.3.2. Fonctionnement de la méthode :</b>	<b>25</b>
<b>II.3.3. Déroulement de la méthode :</b>	<b>26</b>
• <b>Phase 0 « Préparation » :</b>	<b>26</b>
• <b>Phase 1 « Audit des vulnérabilités » :</b>	<b>26</b>
• <b>Phase 2 « Analyse des risques » :</b>	<b>27</b>
• <b>Phase 3 « Plan d'action » :</b>	<b>28</b>
<b>II.3.4. Commentaire sur la méthode :</b>	<b>28</b>
<b>II.4. La méthode Mehari :</b>	<b>30</b>
<b>II.4.1. Les fondements de la démarche :</b>	<b>30</b>
<b>II.4.2. La traduction de la démarche dans la méthode :</b>	<b>30</b>
<b>II.4.2.1. Plan stratégique de sécurité :</b>	<b>32</b>
• <b>Métrique des risques et objectifs de sécurité :</b>	<b>32</b>
• <b>Etablir une classification globale des ressources :</b>	<b>32</b>
• <b>Définir une politique de sécurité :</b>	<b>32</b>
• <b>Présenter une charte de management :</b>	<b>32</b>
<b>II.4.2.2. Plan opérationnel de sécurité :</b>	<b>32</b>
a. <b>La phase préparatoire :</b>	<b>32</b>
b. <b>L'audit de l'existant :</b>	<b>32</b>
c. <b>L'évaluation de la gravité des scénarios :</b>	<b>32</b>
d. <b>L'expression des besoins de sécurité :</b>	<b>32</b>
<b>II.4.2.3. Plan opérationnel de l'entreprise :</b>	<b>33</b>
a. <b>Choix d'indicateur représentatifs :</b>	<b>33</b>
b. <b>Elaboration d'un tableau de bord de la sécurité de l'entreprise :</b>	<b>33</b>
c. <b>Rééquilibrage et arbitrage entre entités :</b>	<b>33</b>
<b>II.4.2.4. Commentaire sur la méthode :</b>	<b>33</b>
<b>II.5. La méthode EBIOS :</b>	<b>34</b>
<b>II.5.1. La traduction de la démarche dans la méthode :</b>	<b>36</b>
<b>II.5.1.1. Etude du contexte :</b>	<b>36</b>
a. <b>Etude de l'organisme :</b>	<b>36</b>
b. <b>Etude du système cible :</b>	<b>36</b>
c. <b>Détermination de la cible de l'étude de sécurité :</b>	<b>36</b>
<b>II.5.1.2. Expression des besoins de sécurité :</b>	<b>36</b>
a. <b>Réalisation des fiches de besoins :</b>	<b>36</b>
b. <b>Synthèse des besoins de sécurité :</b>	<b>37</b>
<b>II.5.1.3. Etude des menaces :</b>	<b>37</b>
a. <b>Etude des origines des menaces :</b>	<b>37</b>

b. Etude des vulnérabilités :.....	37
c. Formalisation des menaces : .....	37
II.5.1.4. Identification des objectifs de sécurité : .....	37
a. Confrontation des menaces aux besoins : .....	37
b. Détermination des objectifs de sécurité : .....	38
c. Détermination des niveaux de sécurité :.....	38
II.5.1.5. Détermination des exigences de sécurité :.....	38
a. Détermination des exigences de sécurité fonctionnelles : .....	38
b. Détermination des exigences de sécurité d'assurance :.....	38
II.5.2. Commentaire sur la méthode :.....	38
II.6. La méthode Ferros : .....	40
II.6.1. Les avantages de la méthode Ebios pour la rédaction d'une Feros: .....	40
II.6.2. Rédaction d'une Feros en utilisant Ebios : .....	40
II.6.3. Schéma de passage de la méthode Ebios vers la méthode Feros :.....	41
II.6.4. Les critères de choix d'une méthode : .....	44
II.6.5. Conclusion :.....	44

### CHAPITRE III : La Méthode Ebios

III.1.Introduction .....	45
1. Un outil de gestion des risque.....	45
2. Un outil de négociation et d'arbitrage.....	45
3. Un outil de sensibilisation.....	45
4. Un outil compatible avec les normes internationales .....	45
5. De nombreux utilisateurs.....	45
6. Une utilisation pour des systèmes à concevoir et des systèmes existants :.....	45
7. Une approche exhaustive :.....	46
8. Un outil réutilisable.....	46
9. Une démarche adaptative .....	46
III.2. Les étapes de la méthode EBIOS : .....	47
III.2.1. Étude du contexte : .....	47
Activité 1.1. Étude de l'organisme : .....	47
1.1.1 Présenter l'organisme : .....	47
1.1.2 Lister les contraintes pesant sur l'organisme :.....	47
1.1.3 Lister les références réglementaires applicables à l'organisme : .....	47
1.1.4 Faire une description fonctionnelle du SI global : .....	47
Activité 1.2. Étude du système-cible : .....	47
1.2.1 Présenter le système cible : .....	47
1.2.2 Lister les enjeux : .....	47
1.2.3 Lister les éléments essentiels : .....	47
1.2.4 Faire une description fonctionnelle du système cible : .....	48
1.2.5 Lister les règles de sécurité : .....	49

<i>Activité 1.3. Détermination de la cible de l'étude de sécurité :</i>	49
1.3.1 <i>Lister et décrire les entités du système :</i>	49
1.3.2 <i>Croiser les éléments essentiels et les entités :</i>	49
III.2.2. <i>Expression des besoins de sécurité :</i>	51
<i>Activité 2.1. Réalisation des fiches de besoins :</i>	51
2.1.1 <i>Choisir les critères de sécurité à prendre en compte :</i>	51
2.1.2 <i>Déterminer l'échelle de besoins :</i>	51
2.1.3 <i>Déterminer les impacts pertinents :</i>	51
<i>Activité 2.2. Synthèse des besoins de sécurité :</i>	52
2.2.1 <i>Attribuer un besoin de sécurité par critère de sécurité à chaque élément essentiel.....</i>	52
III.2.3. <i>Étude des menaces.....</i>	52
<i>Activité 3.1 – Étude des origines des menaces :</i>	54
3.1.1 <i>Lister les méthodes d'attaque pertinentes :</i>	54
3.1.2 <i>Caractériser les méthodes d'attaque par les critères de sécurité qu'elles peuvent affecter :</i>	54
3.1.3 <i>Caractériser les éléments menaçants associés par leur type et leurs causes :</i>	54
3.1.4 <i>Ajouter une valeur représentant le potentiel d'attaque de l'élément menaçant :</i>	54
<i>Activité 3.2. Étude des vulnérabilités :</i>	55
3.2.1 <i>Identifier les vulnérabilités des entités selon les méthodes d'attaque : ..</i>	55
3.2.2 <i>Estimer éventuellement le niveau des vulnérabilités :</i>	55
<i>Activité 3.3. Formalisation des menaces :</i>	56
3.3.1 <i>Formuler explicitement les menaces :</i>	56
3.3.2 <i>Hiérarchiser éventuellement les menaces selon leur opportunité :</i>	57
III.2.4. <i>Identification des objectifs de sécurité :</i>	59
<i>Activité 4.1. Confrontation des menaces aux besoins :</i>	59
4.1.1. <i>Déterminer les risques en confrontant menaces et besoins de sécurité :.....</i>	59
4.1.2 <i>Formuler explicitement les risques :</i>	60
4.1.3. <i>Hiérarchiser les risques selon l'impact sur les éléments essentiels et l'opportunité des menaces :</i>	60
<i>Activité 4.2. Formalisation des objectifs de sécurité :</i>	61
4.2.1 <i>Lister les objectifs de sécurité :</i>	61
4.2.2 <i>Justifier la complétude de la couverture :</i>	61
4.2.3 <i>Classer éventuellement les objectifs de sécurité en deux catégories : ....</i>	61
<i>Activité 4.3. Détermination des niveaux de sécurité :</i>	61
4.3.1 <i>Déterminer le niveau de résistance adéquat pour chaque objectif de sécurité :</i>	61
III.2.5. <i>Détermination des exigences de sécurité :</i>	64
<i>Activité 5.1. Détermination des exigences de sécurité fonctionnelles :</i>	64
5.1.1 <i>Lister les exigences de sécurité fonctionnelles :</i>	64

5.1.2. Classer les exigences de sécurité fonctionnelles en deux catégories : ..	64
Activité 5.2. Détermination des exigences de sécurité d'assurance : .....	65
5.2.1 Lister les exigences de sécurité d'assurance : .....	65
5.2.2. Classer éventuellement les exigences de sécurité d'assurance en deux catégories : .....	65
Conclusion : .....	66

## **CHAPITRE IV : Conception**

<b>IV.1. Introduction :</b> .....	67
<b>IV.2. Description du fonctionnement de la boîte d'audit :</b> .....	67
<b>IV.3. Le serveur (Le noyau) :</b> .....	67
<b>IV.3.1. Description des différents modules composant le noyau :</b> .....	69
1. Module des communications : .....	69
2. Module d'authentification et SGBD : .....	69
3. Module d'analyse : .....	70
a. Module de détection des machines actives : .....	70
b. Module de détection des ports ouverts : .....	70
c. Module de détection des systèmes d'exploitations : .....	70
4. Module d'attaque : .....	70
5. Module de besoin de sécurité : .....	70
6. Module de détermination de mesures de sécurités : .....	70
7. Module de rapport : .....	71
8. Module de mise à jour : .....	71
<b>IV.3.2. Description des étapes de l'audit de sécurité exécuté sur le serveur :</b> .....	71
<b>IV.4. Le client :</b> .....	74
<b>IV.4.1. Description des modules composant le client :</b> .....	74
1. Le module de communication : .....	74
2. Le module générateur de rapport : .....	74
<b>IV.4.2. Description du cheminement des étapes d'un audit sur le client :</b> .....	74
<b>IV.5. Objectif :</b> .....	75
<b>IV.5.1. Présentation de UML :</b> .....	75
<b>IV.5.1.1. Cas D'utilisation :</b> .....	76
<b>IV.5.1.2. Représentation :</b> .....	76
<b>IV.5.1.3. Diagramme de séquences :</b> .....	77
<b>IV.5.1.4. Diagramme de collaboration :</b> .....	77
<b>IV.5.1.5. Diagramme de classes :</b> .....	78
a. Représentation et notions de bases : .....	78
b. Classe et objet : .....	78
c. Attribut et opération : .....	78
d. Association : .....	78
e. Agrégation et composition : .....	78

f. Généralisation, Super Classe, Sous Classe : .....	79
IV.5.1.6. Diagramme de composants : .....	79
IV.5.1.7. Diagramme de déploiement : .....	79
IV.5.1.8. Diagramme d'état : .....	80
IV.5.1.9. Diagramme d'activité : .....	80
IV.6. Diagramme de cas d'utilisation de notre système : .....	81
1. L'administrateur :.....	81
2. Le client : .....	81
3. Identification et authentification : .....	81
4. Connexion : .....	81
5. Détection des machines actives : .....	81
6. Détection des ports ouverts : .....	81
7. Identification des systèmes d'exploitation : .....	81
8. Audit du système cible : .....	81
9. Gestion des bases de données des utilisateurs : .....	81
10. Gestion des bases de données des vulnérabilités: .....	81
11. Gestion des bases de données des besoins de sécurité : .....	82
12. Gestion des bases de données des mesures de sécurité : .....	82
IV.7. Diagrammes d'activités de notre outil :.....	84
IV.8. Diagrammes de séquences de notre système :.....	88
IV.9. Description des bases de données utilisées : .....	90
1. La base de données des utilisateurs :.....	90
2. Base de données des vulnérabilités :.....	90
3. Base de données des besoins de sécurité : .....	92
4. Base de données des mesures de sécurité : .....	93
<b>CHAPITRE V: Développement.....</b>	<b>94</b>
V.1. Introduction :.....	94
V.2. Les outils :.....	94
V.2.1. Environnement matériel :.....	94
V.2.2. Environnement de développement :.....	94
V.2.2.1. Système d'exploitation :.....	94
V.2.2.1.1. Description générale de Linux : .....	94
V.2.2.1.2. Gestion réseau sous Linux : .....	94
V.2.2.1.3. Sécurité sous Linux :.....	95
a. L'authentification:.....	95
b. Le contrôle d'accès :.....	95
V.2.2.1.4. Linux et les Threads :.....	95
V.2.2.2. Langage de programmation :.....	95
a. Description de JAVA :.....	95
b. Caractéristiques de JAVA :.....	96



c. <i>Le JDK</i> :	96
d. <i>L'API (interface de programmation d'application)</i> :	97
V.2.2.3. <i>Environnement de programmation du langage java</i> :	97
a. <i>NetBeans IDE 4.0</i> :	97
b. <i>Borland Jbuilder 2005 developer</i> :	97
c. <i>MYSQL</i> :	97
c.1. <i>Outils graphique de MySQL</i> :	98
V.2.2.4. <i>ICMP Broadcast (Teste de connectivité d'une machine)</i> :	98
V.2.2.5. <i>Nmap</i> :	98
1. <i>TCP SYN Scan : ( Test des ports ouverts)</i> :	99
2. <i>TCP Fingerprint (Détection d'OS)</i> :	99
V.2.2.6. <i>Le langage de script de tests (NASL)</i> :	100
V.3. <i>Principe de fonctionnement</i> :	100
V.3.1. <i>Interface serveur d'administration</i> :	101
V.3.2. <i>Lancement du serveur</i> :	101
<i>Exemple de plug-in (nasl)</i> :	105
V.3.3 <i>Lancement d'un Audit</i> :	106
V.3.4 <i>Bases de données</i> :	106
V.4. <i>Conclusion générale et perspective</i> :	111

## ANNEXE

<i>Annexe (A) les Méthodes d'Audit</i> :	113
<i>Annexe (B) La Norme CVE</i> :	117
<i>Annexe (C) NMAP</i> :	122
<i>Annexe (D) Le Langage NASL</i> :	125

## Bibliographie