



Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie Houari Boumediène

Faculté d'Electronique et d'Informatique

Département d'Informatique

## Projet de fin d'étude pour l'obtention du diplôme Master

Option

Réseaux et Systèmes Distribués

**Thème**

**Détection des sites web malicieux avec les honeyclients**

Sujet proposé par :

Mme. SBENMEZIANE

Présenté par :

Mr DIFALLAH Adlane.

Mr KERRAOUCH YOUCEF.

Soutenu le : 26/06/2011

Devant le jury composé de :

Mr A.AISSANI. Président

Mr D.BAHLOUL. Membre

Mme L.ALIOUANE. Membre

Binôme N° /014/2011

## Table des matières

Partie I : Etat de l'art .....	1
Chapitre I : Infection de sites web .....	1
I.1. Introduction.....	1
I.2. Généralité sur la sécurité informatique.....	1
I.2.1. Différents types de pirates informatiques .....	2
I.2.2. Motivations des Hackers .....	4
I.2.3. Le besoin de sécuriser les sites web .....	5
I.3. Code malicieux .....	7
I.3.1. Virus .....	7
I.3.2. Virus réticulaire (Botnet) .....	8
I.3.3. Ver (Worm).....	8
I.3.4. Cheval de Troie (Trojan).....	9
I.3.5. Bombes logiques .....	9
I.3.6. Porte dérobée (backdoor) .....	10
I.3.7. Logiciel espion (spyware) .....	10
I.3.8. Défacement .....	10
I.3.9. Ingénierie sociale (Social engineering) .....	11
I.3.10. Exploit.....	12
I.3.11. Attaques sur le Web et sur les données .....	12
I.4. Méthodes de diffusion.....	14
I.4.1. Vers XSS.....	14
I.4.2. Email.....	15
I.4.3. Faux résultats de recherche .....	15
I.4.4. Malvertising – Les bannières publicitaires infectées .....	16
I.5. Méthodes de détection .....	17
I.5.1 Antivirus .....	17
I.5.2 Pare-feu.....	18
I.5.3 Systèmes de détection des intrusions (IDS).....	19
I.6. Conclusion .....	19
Chapitre II : Honeypots .....	20
II.1. Introduction .....	20
II.2. Présentation des honeypots .....	20

II.3. Historique .....	23
II.4. Fonctionnement des honeypots .....	24
II.4.1. Principe de fonctionnement .....	24
II.4.2. La surveillance .....	24
II.4.3. Collecte d'information .....	25
II.4.4. Analyse d'informations .....	25
II.5. Les type des honeypots .....	25
II.5.1 Honeypots de production .....	25
II.5.2 Honeypots de recherche .....	25
II.5.3. À faible interaction (virtuel) .....	26
II.5.4. À moyenne interaction (hybrides) .....	26
II.5.5. À forte interaction (physique) .....	27
II.6. Les honeynets .....	27
II.6.1. Le contrôle de données .....	27
II.6.2. La capture de donnée .....	28
II.7. Les honeynet virtuel .....	28
II.8. Honeyclient.....	29
II.8.1. Présentation des honeyclients : .....	29
II.8.2. Architecture des honeyclients: .....	29
II.8.3. Types des honeyclients .....	29
II.9. Intérêt et inconvénient .....	30
II.9.1. Les intérêts.....	30
Honeypots est une conception très simple qui leur donne des puissants avantages .....	30
II.9.2. Les inconvénients .....	31
II.10. Les outils honeypots .....	31
II.10.1. UML (User-Mode Linux) .....	31
II.10.2. VMware .....	32
II.10.3. VirtualBox .....	32
II.10.4. Sniffer (renifleurs) .....	32
II.10.5. IDS.....	32
II.10.6. Le pare-feu.....	32
II.10.7. Serveur de log .....	33
Syslog est un daemon dédié à l'enregistrement des journaux (log) .....	33
II.11. Les projets « honeypots » .....	33

II.11.1. Glastopf .....	33
II.11.2. HoneyBot.....	33
II.11.3. Scada (Supervisory Control And Data Acquisition) .....	33
II.11.4. Le projet HONEYNET .....	34
II.12. Conclusion .....	35
Partie II : Contribution .....	36
Chapitre III : Conception du système de détection des sites web malicieux avec les honeyclients .....	36
III.1. Introduction .....	36
III.2. Analyse et spécification des besoins.....	37
III.2.1. Problématique.....	37
III.2.2. L'architecture générale du Honeyclient .....	38
III.2.3. Le diagramme de cas d'utilisation global : .....	43
III.2.3.1. Identification des acteurs du système.....	43
III.2.3.2. Identification des cas d'utilisation du système :.....	44
III.2.3.3. Diagramme de séquence .....	46
III.4. Conclusion.....	48
Chapitre IV : Mise en œuvre du système de détection des sites web malicieux avec les honeyclients .....	49
IV.1 Introduction.....	49
IV.2 Mise en œuvre.....	50
IV.2.1 Présentation du moteur de recherche NUTCH .....	51
IV.3 Présentation du moteur d'analyse ClamAV.....	54
IV.4 Présentation de l'architecture de la base d'archives .....	55
IV.5 Contraintes liés à la mise en œuvre de l'application.....	56
IV.5 Présentation de l'interface de l'application .....	57
IV.7 Conclusion .....	58
Conclusion générale .....	59
Bibliographie.....	60
Annexe 1 : Installation et configuration du moteur de recherche Nutch-1.2.....	62
Annexe 2 : Installation et configuration de l'antivirus ClamAV .....	69
Résumé.....	70
Abstract.....	70