



République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie Houari Boumediene

**Faculté d'Electronique et d'Informatique
Département Informatique**

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

Option

Réseaux et Systèmes Distribués

Thème

**Mise en œuvre d'un honeypot pour la
sécurisation des applications Web**

Sujet Proposé par :

Mme. S. BENMEZIANE

Mr. A. AMIRA

Présenté par :

BADACHE Islam

CHIBANE Mohamed

Soutenu le 26/06/2014

Devant le jury composé de :

Mr. A. AISSANI

Mme. L. KHEROUA

Mme. L. ALIOUANE

Président

Membre

Membre

Binôme N°89/2014

Table des matières

Introduction générale	1
1 La sécurité des application Web	3
1.1 La sécurité informatique	3
1.1.1 Définition de la sécurité informatique	3
1.1.2 Objectif de la sécurité informatique	4
1.1.3 Termes et définitions	4
1.1.4 Types de menaces	5
1.1.5 Mécanismes de sécurité	7
1.2 Les applications Web	12
1.2.1 Le protocole http	12
1.2.2 HTML« <i>HyperText Mark-Up Language</i> »	14
1.2.3 JavaScript	14
1.2.4 PHP	15
1.3 La sécurité des applications Web	16
1.3.1 Les vulnérabilités Web	17
1.3.2 Vérification des applications Web	18
1.4 Conclusion	22
2 Les honeypots	23
2.1 Définition des honeypots	23
2.2 Fonctionnement des honeypots	24
2.2.1 La surveillance	24
2.2.2 La collecte de données	24
2.2.3 L'analyse des données	24
2.3 Types de honeypots	25
2.3.1 Honeypot de production	25
2.3.2 Honeypot de recherche	25
2.4 Classification des honeypots	26

2.4.1	Honeypots à faible interaction	26
2.4.2	Honeypots à moyenne interaction	27
2.4.3	Honeypots à forte interaction	28
2.4.4	Comparaison entre les niveaux d'interaction des honeypots . . .	30
2.5	Les honeynets	30
2.6	Fonctionnement des honeynets	30
2.6.1	Le contrôle de données	31
2.6.2	La collecte de données	31
2.6.3	L'analyse de données	31
2.7	Types de honeynets	31
2.7.1	Première génération de honeynets	31
2.7.2	Deuxième génération de honeynets	33
2.7.3	Troisième génération de honeynets	33
2.7.4	Honeynets virtuels	34
2.8	Outils de développement	35
2.8.1	User Mode Linux(UML)	35
2.8.2	Specter	35
2.8.3	Honeyd	35
2.9	Conclusion	36
3	Conception du système de sécurisations des applications Web	37
3.1	Description générale de l'approche	37
3.2	Architecture générale	39
3.2.1	Distribution des honeypots	40
3.2.2	Faibles retenues	40
3.2.3	Rôle des honeypots	43
3.3	Description des modules de honeypots	44
3.3.1	Module de collecte de données	44
3.3.2	Module d'analyse de données	46
3.3.3	Module de statistique	48
3.4	Conclusion	49
4	La mise en œuvre du système	50
4.1	Description de la plateforme	50
4.1.1	Installation de VMware Workstation	50
4.1.2	Honeyd	51
4.1.3	Installation de honeyd	52
4.2	Configuration et Lancement des honeypots	53

4.2.1	Honeypot de faible interaction : Site web	53
4.2.2	Honeypot de forte interaction : Application DVWA	57
4.3	Analyse des fichiers logs	60
4.3.1	Honeypot de faible interaction	60
4.3.2	Honeypot de forte interaction : Application DVWA	62
4.4	Statistiques et résultats	63
4.5	Etude de cas de déploiement réel d'un honeypot de faible interaction . .	65
Conclusion Générale		67
Bibliographie		70
Annexe		71