

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche
Scientifique

Centre de Recherche sur l'Information Scientifique et Technique



Mémoire de fin d'études
Pour l'obtention du diplôme de post graduation spécialisée en
sécurité informatique

Thème :

Honeypots: Etude, Déploiement et Tests

Présenté par : Mr Ahcène Boukorça

Encadré par:

Mme: Benmeziane Souad
Mr : Ait Djoudi Rafik

Devant le jury

Djamel TANDJAOU
Hassina BENSEFIA
Lyes KHELLADI

Président
Examinatrice
Examineur

Décembre 2006

Sommaire

Sommaire

Introduction générale	1
Concepts de la sécurité informatique	3
1.1. Définition de la sécurité informatique	3
1.2. Objectifs de la sécurité informatique	3
1.3. Termes et définitions	4
1.3.1. Actifs	4
1.3.2. Vulnérabilités	4
1.3.3. Menaces	4
1.3.4. Attaques	4
1.3.5. Contre-mesures	4
1.4. Menaces potentielles	5
1.4.1. Piratages	5
1.4.2. Codes malveillants	6
1.4.3. Détournements du système de sécurité	7
1.4.4. Perturbateurs de services	7
1.4.5. Spam	8
1.4.6. Sites Web factices	8
1.5. Outils de sécurité évolués	8
1.5.1. Proxy	8
1.5.2. Translation d'adresses réseau (NAT)	9
1.5.3. Firewalls	9
1.5.4. Systèmes de détection/prévention d'intrusion (IDS/IPS)	10
1.5.5. Antivirus	12
1.5.6. Tunneling (VPN)	12
1.5.7. Accès à distance	13
1.5.8. Honeypots	13
Conclusion	13
Honeypots et honeynets	15
2.1. Définition de honeypot	15
2.2. Historique des honeypots	15
2.3. Utilités des honeypots	16
2.4. Limites des honeypots	18
2.5. Types de honeypots	19
2.5.1. Honeypots de production	19
2.5.2. Honeypots de recherche	19
2.6. Principe de fonctionnement des honeypots	20

2.6.1. Prévention des attaques	20
2.6.2. Détection des activités malicieuses.....	21
2.6.3. Réaction aux attaques	21
2.6.4. But de recherche	22
2.7. Classification des honeypots	22
2.7.1. Honeypots à faible interaction	22
2.7.2. Honeypots à moyenne interaction	23
2.7.3. Honeypots à forte interaction	24
2.8. Définition des honeynets	25
2.9. Fonctionnement des honeynets.....	26
2.9.1. Contrôle de données.....	26
2.9.2. Capture de données.....	27
2.9.3. Analyse de données	27
2.9.4. Collecte de données	27
2.10. Types de honeynets.....	27
2.10.1. Première génération de honeynets	28
2.10.2. Deuxième génération de honeynets.....	29
2.10.3. Troisième génération de honeynets	30
2.10.4. Honeynets virtuels	31
2.10.4. Honeynets distribués.....	33
2.11. Projets honeynets.....	33
2.11.1. Les projets “HONEYNET”	33
2.11.2. Le Honeynet Research Alliance.....	33
2.11.3. Le projet HOSUS (Honeypot Surveillance System).....	34
Conclusion	34
Etude de quelques solutions honeypots	34
3.1. Honeypots commerciaux.....	34
3.1.1. ManTrap	34
3.1.2. Specter	37
3.2. Honeypots gratuits	39
3.2.1. BackOfficer Friendly.....	39
3.2.2. Argos	41
3.2.3. Deception Toolkit.....	43
3.2.4. Népenthes.....	43
3.2.5. Honeyd	44
3.4. Comparaison entre les outils présentés	45
Conclusion	46
Etude et tests de Honeyd.....	47
4.1. Présentation de Honeyd	47
4.2. Fonctionnement de Honeyd.....	48
4.2.1. Fichiers de configuration	48
4.2.2. Scripts de services	49
4.2.3. Routing Topologies.....	50

4.2.4. Logging -----	50
4.3. Architecture interne de Honeyd.....	51
4.4. Réception de paquets de réseau	53
4.5. Installation et paramétrage de Honeyd.....	54
4.5.1. Installation -----	54
4.5.2. Configuration-----	54
4.6. Exploitation de logs	55
4.6.1. Analyse de Logs -----	55
4.6.2. Sécurisation-----	55
4.7. Tests de Honeyd	55
4.7.1. Description de la plateforme de test-----	56
4.7.2. Configuration de Honeyd-----	58
4.7.3. Analyse de log -----	64
Conclusion	66
Emulation du serveur web wikayanet -----	67
5.1 Description du serveur web wikayanet	67
5.2. Architecture de honeynet émulant wikayanet.....	67
5.3. Mise en œuvre de honeynet émulant wikayanet.....	69
5.3.1. Description de la plateforme de test-----	69
5.3.2. Fichier de configuration -----	69
5.3.2. Services émuls par Honeyd -----	70
5.3.3. Description d'une attaque émulée par le honeypot proposé -----	73
5.4. Test de honeypot émulant le serveur web	74
5.5. Analyse de log	76
Conclusion	78
Conclusion générale -----	79
Bibliographie-----	80
Annexe-----	82