

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Des Sciences et de Technologie Houari Boumediène



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

**Mémoire de projet de fin d'études
Pour l'obtention du diplôme
D'ingénieur d'état en informatique**

SUJET

**HONEYPOT POUR ANALYSER LE
TRAFIC MALVEILLANT DANS UN
RESEAU LOCAL**

Thème proposé et encadré par :

**Mme SOUAD BENMEZIANE (chargée de
recherche, CERIST)**

Etudié par :

- **GUENANE FOUAD AMINE**
- **MESDOUR ABDENOUR**

Soutenu le : 24 juin 2009

Devant le jury composé de:

- **K. BENABADJI Président,**
- **N. HADDOUCHE Examinatrice,**
- **Y.ZAFFOUNE Examineur,**

Année universitaire : 2008-2009

N° d'ordre : 86/2009

Sommaire

INTRODUCTION GENERALE :	4
1. Introduction a la sécurité informatique	5
1.1 Définition d'une menace.....	5
1.2 Objectif de la sécurité informatique.....	6
2 Menaces et attaques informatiques	7
2.1 Introduction aux attaques.....	7
2.2 Type d'attaques.....	8
2.3 Définition des virus.....	9
2.4 Exemples de virus.....	10
3 Mécanisme de sécurité informatique :	11
3.1 Introduction :.....	11
3.2 Quelques dispositifs de sécurité.....	12
Chapitre 2 : Menaces/ Attaques / Attaquants	16
Introduction	17
1. Menaces	18
2. Attaquants	19
2.1 Profils des attaquants.....	19
2.2 Objectifs d'un attaquant.....	20
2.3 Types d'attaquants :.....	20
2.4 Profils détaillés des attaquants de Systèmes d'Informations.....	21
3 Attaques	22
3.1 Les entités les plus menacées.....	23
3.2 Les éléments menacés lors d'une attaque.....	24
3.3 Les vecteurs d'attaques.....	25
Chapitre 3 : Honeypots / Honeynets	28
Introduction	29
1. Honeypot	29
1.1 Définition des honeypots.....	29
1.2 Types de honeypots.....	30
1.3 Le niveau d'interaction.....	31
1.4 Honeypots virtuels.....	31
2 Honeynet	32

2.1	Définitions d'un Honeynet	32
2.2	Architecture réseaux des honeynets et descriptions de ces différents modules.....	33
2.3	Les différentes générations de honeynets	35
3	Outils de développement	38
3.1	Sous linux.....	39
3.2	sous Windows	39
4	Comment déployer un honeypot	40
Chapitre 4 : conception d'une architecture de honeypots pour lutter contre les Spams		43
Introduction :		44
1.	Spam : définition	44
2.	Les impacts	45
3.	Techniques de lutte contre les spams	46
3.1	La liste noire	47
3.2	La liste blanche	47
3.3	La liste grise	47
4	Le mode de fonctionnement des spammeurs	47
4.1	La collecte d'adresse e-mail	48
4.2	Open proxies	49
4.3	Open relays	49
5	Utilisation des honeypots pour lutter contre les spams	50
5.1	Honeypot et collecte d'informations	51
5.2	Honeypot :open proxy et open relay	52
6	Présentation de l'architecture typique d'un serveur de messagerie	52
6.1	Rôle du proxy	52
6.2	Rôle du serveur de messagerie	52
6.3	Pourquoi le protocole SMTP ?	53
6.4	Schéma de l'architecture	53
7	Architecture générale du réseau émulé et présentation des différents modules	54
8.1	Honey-Proxy	55
8.2	Relay-pot	55
8.3	Module d'interprétation et d'analyse	56
8.4	Module de mise à jour	58
8.5	Module de statistique	58
8.	Conclusion :	59

Chapitre 5 : implémentation d'une architecture de honeypots pour lutter contre les Spams.....	60
Introduction :	61
1. Principe et outils de développement.....	61
1.1 Principe de virtualisation	61
1.2 Virtual-Box.....	63
1.3 VM-ware Workstation	64
1.4 Système d'exploitation Linux Ubuntu	64
2 Le SPRP (Smart Proxy & Relay Pot):	65
3 Module d'interprétation.....	69
3.1 Expression régulière	70
3.2 Principe de base	71
3.4 Base de données	74
4 Module de mise à jour	75
5 Module statistique.....	76
Bibliographie	78
ANNEXE	80
1. Définition de proxy	81
2. Différents types de serveurs.....	81
3. Définition de plusieurs protocoles que les proxies utilisent	81
3.1 SSH.....	82
3.2 SMTP	82
4 Quelques exemples de proxies utilisés.....	85
4.1 Proxy http	85
4.2 Proxy SSH	85
4.3 Proxy SMTP	85
4.4 Proxy multi-protocoles	85