

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

Pour l'obtention du diplôme de post graduation spécialisée en  
sécurité informatique

Thème :

# Etude et Déploiement de la sécurité d'un serveur de nom BIND

*Présenter par :*  
*Mr Kessas Aissa*

*Encadre par :*  
*M.Derhab abd elwahid*

*Membre de jury :*

- Mme BENMEZIANE Souad Présidente*
- Mlle BENSAFIA Hassina Membre*
- Mr DJENOURI Djamel Membre*

*Cerist 2006*

## **Sommaire**

Introduction : .....	1
<i>Chapitre 1 : La sécurité d'un system Linux</i> .....	
<i>Introduction</i> : .....	2
1.1. Sécurité du poste de travail .....	2
1.1.1.Évaluation de la sécurité du poste de travail .....	2
1.1.2-Sécurité du BIOS et du chargeur de démarrage : .....	2
1.1.3-Sécurité des mots de passe : .....	4
a)Création d'un mot de passe : .....	5
b) Méthodologie pour la création d'un mot de passe sûr : .....	7
c) Création de mots de passe utilisateurs au sein d'une société .....	7
d) Utilisation forcée de mots de passe hermétiques .....	8
e) Expiration des mots de passe .....	8
1.2. Sécurité du serveur .....	9
1.2.1.Services non sécurisés .....	9
1.2.2. SSH .....	10
1.2.3. Samba .....	11
1.2.4. Httpd .....	11
1.2.5. Partage de données / NFS.....	12
1.2.6. Proxy .....	12
1.2.7. Serveur DHCP.....	12
1.2.8. Serveur NIS .....	13
1.2.9. Configurer un serveur de temps avec ntp.....	14
1.3. Réseaux privés virtuels (VPN) .....	16
1.3.1. VPN et Red Hat Linux.....	17
1.4. IPsec .....	17
1.5. Pare-feu .....	17
1.5.1.Netfilter et iptables .....	18
1.5.2.Utilisation d'iptables.....	18

1.6. La sauvegarde des données .....	19
<i>Conclusion</i> .....	19
Chapitre 2 : Installation du BIND .....	
2.1. Introduction .....	20
2.2. <i>Qu'est-ce donc qu'un serveur DNS?</i> .....	20
2.3. <i>Noms de domaines : leur structure</i> .....	20
2.3.1. <i>Les domaines et Le Nom de Domaine</i> .....	21
2.3.2. <i>Les zones</i> .....	21
2.4. <i>Le rôle d'un serveur DNS</i> .....	22
2.5. <i>Serveur DNS cache : données mémorisées</i> .....	22
2.6. <i>Les messages DNS</i> .....	22
2.7. <i>Les ports utilisés par un serveur DNS</i> .....	22
2.8. <i>Installation et Compilation du bind</i> .....	23
2.8.1. <i>Le fichier /etc/named.conf</i> .....	23
2.8.2. <i>Explication de named.conf</i> .....	24
2.8.3. <i>Les fichiers de zones</i> .....	25
2.8.4. <i>Les fichier resolv.conf et host.conf</i> .....	26
2.8.5. <i>Test de la configuration</i> .....	27
2.8.6. <i>Consultation des fichier log(erreur de lancement du bind)</i> .....	28
2.8.7. <i>Remarques sur un serveur DNS cache</i> .....	29
2.9. <i>DNS BIND : serveur de Zone</i> .....	29
2.9.1. <i>Un serveur DNS pour mon domaine</i> .....	29
2.9.2. <i>Le fichier de zone de mon domaine</i> .....	31
<i>Conclusion</i> .....	33
Chapitre 3 :Présentation Des attaques Aux Serveurs BIND .....	
3.1. <i>Un bref historique</i> .....	34
3.2. <i>Les failles de sécurité du DNS</i> .....	34
3.3. <i>Des attaques sur le protocole DNS</i> .....	34
3.3.1. <i>Attaque de type "man-in-the-middle"</i> .....	35
3.3.2. <i>DNS ID spoofing et DNS Poisonning</i> .....	36

a) <i>DNS ID Spoofing</i> .....	36
b) <i>Attaque par Pollution de cache (DNS Cache Poisoning)</i> .....	38
3.3.3. <i>L'Attaque par déni de service</i> .....	38
<i>Conclusion</i> .....	39
Chapitre 4 : <i>Evaluation des vulnérabilités</i> .....	
4.1. <i>Évaluation des vulnérabilités</i> .....	40
4.2. <i>Principes fondamentaux de sécurité</i> .....	40
4.3. <i>Sécurisation d'un réseau</i> .....	40
4.3.1. <i>Politique de sécurité</i> .....	40
4.4. <i>Architecture de Sécurité, la DMZ</i> .....	41
4.5. <i>Les outils d'administration</i> .....	43
• <i>Nmap</i> .....	43
• <i>tcpdump</i> .....	43
• <i>Snort</i> .....	43
• <i>Nessus</i> .....	43
• <i>Network Promiscuous Card Detector</i> .....	43
4.6. <i>Intervention d'une société de service</i> .....	44
A) <i>Audit de sécurité</i> .....	44
B) <i>Test d'intrusion</i> .....	45
c) <i>Après une intrusion</i> .....	45
4.7. <i>Détection d'intrusions</i> .....	46
a) <i>Définition d'un système de détection d'intrusions</i> .....	46
b) <i>Types d'IDS</i> .....	46
4.7.1. <i>IDS basés sur l'hôte</i> .....	47
<i>Tripwire</i> .....	47
4.7.2. <i>IDS basé sur le réseau</i> .....	47
<i>Snort</i> .....	48
<i>Conclusion</i> .....	48
Chapitre 5 : <i>La Sécurité Du BIND Sécurisation et perspective</i> .....	

5.1. Introduction .....	49
5.2. Sécurisation des transactions avec TSIG .....	50
5.2.1. Génération de la clé .....	52
5.2.2. Configuration TSIG au niveau du serveur primaire .....	53
5.2.3. Synchronisation des horloges .....	54
5.3. Sécurisation des données du DNS avec DNSSec .....	54
5.3.1. L'enregistrement de ressources « KEY » .....	55
5.3.2. L'enregistrement de ressources « SIG » .....	56
5.3.3. L'enregistrement de ressources « NXT » .....	57
5.3.4. L'enregistrement de ressources « DS » .....	59
Conclusion .....	60
Chapitre 6 : Atelier de sécurité du BIND .....	
Introduction .....	61
6.1.Sécurité du poste de travail .....	62
6.2.Configuration du serveur de noms BIND .....	64
6.3. Sécurité du serveur .....	68
6.4.L'architecture proposée .....	70
6.5.Configuration du firewall .....	70
6.6. Sécurisation des transactions avec TSIG .....	72
6.7.Synchronisation des horloges .....	73
6.8.Test de la configuration .....	74
Conclusion .....	77