



*Mémoire pour l'obtention du diplôme
de Post-Graduation Spécialisée en Sécurité Informatique*

Thème

Réalisation d'un système de renforcement de politiques de sécurité fondé sur les meilleures pratiques

Elaboré par:

- AISSOU Hamza
- TABERKOKT Mourad

Encadré par :

- Mr. BOUABID Mohamed Amine

Soutenu devant le juré :

- Mme. A. ELMAOUHAB, Présidente, Directrice de la division R&D Réseaux, CERIST.
- Mme. F. CHEKAOUI, Examinatrice, Attachée de Recherche, division R&D Réseaux, CERIST.
- Mme. H. LADOUR, Examinatrice, Attachée de Recherche, division R&D Réseaux, CERIST.

-Juin 2016-

Remerciements

Ce mémoire est le fruit d'un travail acharné au sein du CERIST et comme un tel travail nécessite la contribution de plusieurs personnes, nous profitons de cette occasion pour les remercier à travers ces quelques phrases.

Nous tenons tout d'abord à remercier notre promoteur Monsieur BOUABID Mohamed Amine pour la confiance qu'il nous a témoignée en nous proposant ce sujet, sa disponibilité tout au long du projet, ses encouragements et sa patience. Les discussions scientifiques qu'il a su générer, ses remarques et ses suggestions nous ont permis de finaliser ce document.

Nous exprimons toute notre profonde gratitude pour le personnel du service formation du CERIST et nous les remercions.

Nous remercions les membres du jury pour avoir bien voulu juger notre travail.

Table des matières

TABLES DES MATIERES

Introduction générale.....	05
CHAPITRE I : SECURITE DE L'INFORMATION ET POLITIQUE DE SECURITE.....	07
I.1. Introduction.....	08
I.2. Principe de sécurité	08
I.3. Principe de norme.....	11
I.3.1. Définitions.....	11
I.3.2. Types de norme ISO/CEI 270xx.....	12
I.3.3. Structure de la norme ISO/CEI 270xx.....	13
I.3.4. Autre normes et standard.....	15
I.4. Principe de sécurité normative.....	15
I.4.1. Définitions.....	15
I.4.2. Besoin d'un SMSI.....	16
I.4.3. Fonctionnement du SMSI (modèle du PDCA).....	16
I.4.4. Mesures de sécurité SMSI.....	17
I.5. Conclusion.....	17
CHAPITRE II: GUIDE METHODOLOGIQUE DESTINE AUX SYSTEMES LINUX ET LES SERVICES RESEAUX.....	18
II.1. LES BONNES PRATIQUES EN TERMES D'INSTALLATION ET DE CONFIGURATION D'UN SYSTEME GNU/LINUX.....	19
II.1.1. Introduction.....	19
II.1.2. La sécurité physique et environnementale.....	19
II.1.3. Configuration matérielle avant l'installation.....	20
II.1.4. Installation du système.....	20
II.1.5. Configuration et services système.....	22
II.2. GUIDE DES BONNES PRATIQUES POUR SECURISER UN SERVICE WEB	26
II.2.1. Introduction	26
II.2.2. Sécurisation du serveur web	26
II.2.3. Sécurisation des communications.....	28
II.2.4. Implémentation d'une infrastructure réseau sécurisée	29
II.2.5. Administration sécurisée du serveur web	31
II.3. GUIDE DES BONNES PRATIQUES POUR SECURISER UN SERVEUR DE MESSAGERIE.....	34
II.3.1. Introduction	34
II.3.2. Choix des serveurs de messagerie.....	34
II.3.3. Disques et partitionnement du serveur de messagerie	34
II.3.4. Suppression de la documentation sur le serveur.....	34
II.3.5. Sécuriser l'environnement réseau.....	34
II.3.6. Sécuriser les serveurs de la messagerie	36
II.4. GUIDE DES BONNES PRATIQUES POUR UN USAGE SECURISE D'OPENSSE.....	38
II.4.1. Introduction.....	38
II.4.2. Cryptographie	38
II.4.3. Durcissement système	39
II.4.4. Authentification et contrôle d'accès utilisateur.....	40
II.4.5. Protocole et accès réseau	41
II.4.6. IGC OpenSSH	41
CHAPITRE III : LA MISE EN PLACE D'UN GESTIONNAIRE DE CONFIGURATION.....	43
III.1. La gestion de configuration.....	44
III.1.1. Introduction	44
III.1.2. Les outils de gestion de configuration automatique.....	44

III.1.3. Solutions open source existantes.....	44
III.1.4. Choix de l'outil.....	46
III.1.5. Études comparatives	46
III.2. Configuration automatisée avec puppet.....	48
III.2.1. Introduction a Puppet.....	48
III.2.2. Fonctionnement.....	48
III.2.3. Structure de Puppet.....	50
III.3. Réaliser une implémentation pratique via puppet.....	51
III.3.1. Installation de Puppet.....	51
III.3.2. Configuration de Puppet.....	52
III.4. Les modules puppet.....	55
III.4.1. Le module.....	55
III.4.2. Création des modules.....	55
III.4.3. Structure des modules crée.....	56
III.4.4. Exemple de module SSH.....	57
CONCLUSION GENERALE	64
REFERENCES BIBLIOGRAPHIQUES	66
ANNEXES	68