

Avant-propos

1. Objectifs	9
2. Public visé	10
3. Prérequis et connaissances nécessaires	10
4. Structure de l'ouvrage	11
5. Normes et règles de nommage	12

Sécurisation d'applications web

1. Cryptographie	13
1.1 Présentation et définitions	13
1.2 Algorithmes et protocoles	14
1.3 Fonctions de hachage	16
1.4 Législation et cadre juridique	22
1.5 Les limites de la cryptographie	25
2. Infrastructure PKI	27
2.1 Introduction	

2.2 Infrastructure à clé publique ou PKI	27
2.3 Certificat X.509	28
2.4 La suite OpenSSL	30
2.5 Autorité de certification	35
3. Les certificats	38
3.1 La certification SSL	47
3.2 Les certificats multiples	47
3.3 Mise en œuvre d'un certificat SSL	47
3.4 L'alternative "Let's Encrypt"	48
3.5 Tests de la configuration avec SSL Labs	51
4. Serveur web	53
4.1 Généralités	55
4.2 Sécurisation	55
4.3 Chiffrement et certificat du serveur web	57
4.4 Tunnels sécurisés	65
5. Les serveurs Wiki	66
5.1 Introduction	69
5.2 Permissions d'accès au Wiki	69
	73

5.3 Apparence du Wiki	77
5.4 Personnalisation de la page d'accueil	80
5.5 Sécurisation du serveur web	86
6. Publications WordPress	95
6.1 Introduction	96
6.2 Gestion de contenu	97
6.3 Installation de WordPress	98
6.4 Personnalisation du thème	101
6.5 Sécurisation du blog	105
Sécurisation d'annuaires	
1. Sécurisation de l'annuaire de noms DNS	109
1.1 Généralités sur le serveur de noms	110
1.2 Attaques visant le serveur de noms	111
1.3 Recommandations générales	112
1.4 Mise en œuvre d'un serveur DNS simple	113
1.5 Emprisonnement du serveur de noms	118
1.6 Mise en place du protocole TSIG et DNSSEC	124
2. Mise en œuvre d'un annuaire OpenLDAP	128

2.1 Architecture d'un annuaire LDAP	129
2.2 Sécurité d'utilisation	133
2.3 Sécurisation du backend	136
2.4 Installation d'un serveur LDAP minimal	138
2.5 Réplication des données	146
2.6 Chiffrement des échanges	150
3. Alternative de l'annuaire LDAP : NIS	153
3.1 Service NIS	153
3.2 Restriction d'utilisateurs ou de groupes	156
3.3 Sécurisation du service NIS	157
3.4 Initialisation d'un serveur NIS esclave	158
4. Service d'adressage dynamique DHCP	159
4.1 Fonctionnalités du service DHCP	159
4.2 Sécurisation du service DHCP	161
4.3 Utilisation du failover	162
4.4 Association avec le protocole DNSSEC	163
5. Solution évoluée : SAMBA 4	167
5.1 Introduction	167
5.2 Installation de la solution	167

5.3 Configuration du domaine	168
5.4 Administration du domaine	170
	173

Sécurisation des données et du stockage

1. Introduction à la donnée	175
1.1 Qu'est-ce qu'une donnée ?	175
1.2 Référentiel et métadonnées	176
1.3 Gestion de la donnée	178
1.4 Cycle de vie de la donnée	182
2. Notion de stockage	183
2.1 Les bases de données	183
2.2 Constitution d'une base de données	184
2.3 Les composants d'une base	185
3. Protection des bases de données	187
3.1 Sécurisation de PostgreSQL	187
3.2 Sécurisation de MariaDB	198
3.3 Sécurisation de Cassandra	210
3.4 Sécurisation de MongoDB	217

4. Comment protéger le stockage	223
4.1 Différents types de stockage	223
4.2 Axes de sécurisation du SAN	226
4.3 Axes de sécurisation du stockage NAS	228
5. Mise en œuvre d'un serveur NAS OpenMediaVault	230
5.1 Présentation	230
5.2 Prérequis à l'installation	231
5.3 Installation d'OpenMediaVault	233
5.4 Configuration d'OpenMediaVault	240
5.5 Sécurisation d'OpenMediaVault	248

Sécurisation de la messagerie

1. Les différentes fonctions	253
1.1 La messagerie électronique	253
1.2 L'agent de transfert des messages	256
1.3 L'agent de distribution des messages	258
1.4 L'agent des messages utilisateurs	262
2. Configuration avancée	264

2.1 Le mécanisme anti-relayage	264
2.2 Daemon chrooté	264
2.3 Gestion des filtres anti-spam	267
2.4 Filtrage des en-têtes	268
3. Intégration en base de données	270
3.1 Initialisation	270
3.2 Configuration SQL	272
3.3 Filtrage de messages non conformes	275
3.4 Authentification SASL	276
3.5 Génération de certificats	280
4. Sécurisation des clients de messagerie	281
4.1 Installation d'Enigmail	281
4.2 Configuration d'Enigmail	283
4.3 Génération de la paire de clés	286
4.4 Échanges de clés	289
4.4.1 Export de clé publique	290
4.4.2 Import de clé publique	292
4.5 Échanges de messages chiffrés	292
5. Passerelle complète anti-spam sécurisée	296

5.1 Description du modèle et installation	296
5.2 Configuration du "grey listing"	300
5.3 Configuration de la validation de signature	300
5.4 Configuration du MTA	301
5.5 Configuration de MailScanner	308
5.5.1 Nettoyage des courriels	312
5.5.2 Fichiers de configuration supplémentaires	313
5.5.3 Outil MailWatch	314
5.6 Fonctionnement de la plateforme complète	317

Sécurisation de l'Internet des objets

1. Définitions et présentation	321
1.1 Qu'est-ce que l'loT ?	322
1.2 Le "big data"	323
1.3 Données et protection	323
1.4 Architecture loT	325
1.5 Sécurité du réseau LoRaWAN	330
2. Protocole de distribution	336
2.1 Le protocole MQTT	336

2.2 Implémentations de MQTT	341
2.3 Failles connues	342
2.4 Récapitulatif des risques	344
3. Évolution de la cryptographie	345
3.1 Infections de l'loT	345
3.1.1 Fonctionnement d'un botnet	345
3.1.2 Exemple de botnet : mirai	349
3.2 Constat technologique	357
3.3 Cryptographie légère	360
3.3.1 Algorithmes de chiffrement par bloc	360
3.3.2 Algorithmes de chiffrement par flot	362
3.3.3 Fonction de hachage	363
3.4 Nouvelle piste à explorer : blockchain	364
3.5 Éprouver la sécurité d'objets connectés	368
3.5.1 Conception d'un micronoyau	371
3.5.2 Base de confiance	373
3.5.3 L'isolation des programmes sensibles	373
3.5.4 Génération de preuves formelles	374
4. Mise en œuvre d'objets connectés	376
4.1 Installation de la pile Tick	

4.2 Installation de la base de données	378
4.3 Installation de l'outil de collecte	379
4.4 Installation de l'interface utilisateur	381
4.5 Mise en œuvre de la communication	383
	387

Sécurité et Cloud

1. Présentation et définitions

	391
1.1 Qu'est-ce que le Cloud ?	391
1.2 Types de Cloud	393
1.3 Problématiques liées au Cloud	394
1.4 Les niveaux de services	395
1.5 Debian et le Cloud	399
1.5.1 Classification des données	400
1.5.2 Externalisation du contenu	401
1.5.3 Administration à 360° des données	401
1.5.4 Administration de l'écosystème	403
1.5.5 Sauvegarde de l'écosystème	404

2. Installation de Dropbox

	405
2.1 Installation en ligne de commande	405

2.2 Installation via GDebi	407
2.3 Configuration Dropbox	408
2.4 Sécurisation de Dropbox	409
3. Mise en place d'un SIEM	409
3.1 Initialisation du SIEM	410
3.2 Structure interne du SIEM	411
3.3 Règles de corrélation	414
3.4 Module de gestion de logs	415
3.5 Module de présentation web	416
4. Déploiement OpenStack	420
4.1 Présentation et technologie	420
4.2 Réseau et virtualisation	424
4.3 Mise en œuvre de Keystone	427
4.4 Mise en œuvre de Glance	430
4.5 Mise en œuvre de Nova	432
4.6 Mise en œuvre de Cinder	435
4.7 Intégration de l'interface Horizon	437
5. Sauvegardes Duplicity	439
5.1 Introduction et description	

5.2 Utilisation basique	439
5.3 Sauvegarde de bases de données	440
5.4 Synchronisation distante	441
5.5 Sauvegarde chiffrée	443
5.6 Communication avec le Cloud	445
Conclusion	
1. Niveaux évolutifs	449
2. Évolution de la sécurisation	450
3. Bilan des opérations	452
4. Cybersécurité 2.0	453
5. Pour conclure	454
Glossaire	455
Index	469