

Les éléments à télécharger sont disponibles à l'adresse suivante :  
**<http://www.editions-eni.fr>**  
Saisissez la référence ENI de l'ouvrage **EPSADEB** dans la zone de recherche  
et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

## 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

## Chapitre 1 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 . . . . . 27
  - 2.2 Infrastructure à clé publique ou PKI . . . . . 28
  - 2.3 Certificat X.509 . . . . . 30
  - 2.4 La suite OpenSSL . . . . . 35
  - 2.5 Autorité de certification . . . . . 38
- 3. Les certificats . . . . . 47
  - 3.1 La certification SSL . . . . . 47
  - 3.2 Les certificats multiples . . . . . 47
  - 3.3 Mise en œuvre d'un certificat SSL . . . . . 48
  - 3.4 L'alternative "Let's Encrypt" . . . . . 51

3.5	Tests de la configuration avec SSL Labs	53
4.	Serveur web	55
4.1	Généralités	55
4.2	Sécurisation	57
4.3	Chiffrement et certificat du serveur web	65
4.4	Tunnels sécurisés	66
5.	Les serveurs Wiki	69
5.1	Introduction	69
5.2	Permissions d'accès au Wiki	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

## **Chapitre 2**

### **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. . . . . 168
  - 5.3 Configuration du domaine. . . . . 170
  - 5.4 Administration du domaine. . . . . 173

**Chapitre 3**  
**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

## Chapitre 4

### 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

**Chapitre 5**  
**Sécurisation de l’Internet des objets**

- 1. Définitions et présentation..... 321
  - 1.1 Qu’est-ce que l’IoT ?..... 322
  - 1.2 Le "big data"..... 323
  - 1.3 Données et protection ..... 323
  - 1.4 Architecture IoT ..... 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’IoT..... 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 . . . . .	378
4.2	Installation de la base de données . . . . .	379
4.3	Installation de l'outil de collecte . . . . .	381
4.4	Installation de l'interface utilisateur . . . . .	383
4.5	Mise en œuvre de la communication . . . . .	387

## Chapitre 6

### 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 . . . . . 439
  - 5.2 Utilisation basique . . . . . 440
  - 5.3 Sauvegarde de bases de données . . . . . 441
  - 5.4 Synchronisation distante . . . . . 443
  - 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

Les éléments à télécharger sont disponibles à l'adresse suivante :  
**<http://www.editions-eni.fr>**  
Saisissez la référence ENI de l'ouvrage **EPSIDEB** dans la zone de recherche  
et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

## Avant-propos

1. Objectifs . . . . .	9
2. Public visé . . . . .	10
3. Prérequis et connaissances nécessaires . . . . .	11
4. Structure de l'ouvrage . . . . .	11
5. Normes et règles de nommage . . . . .	13

## Chapitre 1 Outils de sauvegarde

1. Gestion de sauvegarde simple . . . . .	15
1.1 Généralités sur les sauvegardes . . . . .	15
1.1.1 Les supports . . . . .	16
1.1.2 Plan de reprise informatique . . . . .	18
1.1.3 Politique de sauvegarde . . . . .	20
1.2 Suite OpenSSH . . . . .	21
1.3 Tunnels SSH . . . . .	25
1.3.1 Tunnels SOCKS . . . . .	25
1.3.2 Tunnels par port . . . . .	26
1.3.3 Tunnels X . . . . .	27
1.3.4 Tunnels IP . . . . .	27
1.4 Commande de copie sécurisée . . . . .	28
1.5 Automatisation de sauvegarde avec copie sécurisée . . . . .	30
1.6 Échanges de fichiers sécurisés . . . . .	33
1.6.1 Échanges via sftp . . . . .	33
1.6.2 Échanges via vsftp . . . . .	34
2. Synchronisation avec rsync . . . . .	38
2.1 Présentation . . . . .	38
2.2 Quelques cas d'utilisation simple . . . . .	41



# 2 \_\_\_\_\_ Debian GNU/Linux

Maîtrisez la sécurité des infrastructures

2.3	Sauvegarde complète de machine	42
2.4	Somme de contrôle et mode avancé	44
2.5	Utilisation en tant que service	46
3.	Sauvegarde UrBackup	47
3.1	Fonctionnalités et architecture	47
3.2	Interface applicative	48
3.3	Fonctionnement sécurisé	51
3.4	Nouveaux clients	53
4.	Outil AMANDA	56
4.1	Architecture AMANDA	56
4.2	Configuration du serveur AMANDA	58
4.3	Configuration des clients	64
4.4	Vérification des bandes	66
5.	Sauvegarde d'entreprise	68
5.1	Solution BACULA	68
5.2	Installation	70
5.3	Configuration des services	71
5.3.1	Service de stockage	71
5.3.2	Service du directeur	73
5.3.3	Configuration des clients	79
5.4	Sauvegarde des postes client	80
5.5	Changement de répertoire de sauvegarde	89
6.	Gestionnaire de clonage	90
6.1	Installation	90
6.2	Utilisation et sauvegarde	92
6.3	Méthode de restauration	94

## Chapitre 2

### Outils d'audit et d'analyse

1.	Gestion de ressource	97
1.1	Équipements et matériels	97
1.2	Environnement	105
1.3	Réseau	112

- 2. Analyse du réseau ..... 118
  - 2.1 Renifleur réseau ..... 119
  - 2.2 Outil nmap ..... 120
  - 2.3 Utilisation de nmap ..... 120
  - 2.4 L’outil nmap et le Wi-Fi ..... 123
- 3. Analyse des paquets ..... 124
  - 3.1 Généralités et définitions ..... 124
  - 3.2 L’outil tcpdump ..... 125
  - 3.3 L’outil wireshark ..... 127
  - 3.4 L’outil scapy ..... 135
- 4. Détection d’intrusion ..... 139
  - 4.1 Utilisation d’un IDS ..... 139
  - 4.2 Outil snort ..... 142
  - 4.3 Gestion d’un IDS via pfsense ..... 148
  - 4.4 Outil suricata ..... 152
- 5. Test de pénétration ..... 155
  - 5.1 Présentation ..... 155
  - 5.2 Installation ..... 156
  - 5.3 Initialisation ..... 157
  - 5.4 Configuration ..... 159
  - 5.5 Rapport d’audit ..... 163
- 6. Utilitaire de test et de détection d’intrusion ..... 164
  - 6.1 Les audits pentesting ..... 164
  - 6.2 Outil Backbox en live-CD sur VirtualBox ..... 166
  - 6.3 Exploration de BackBox ..... 168
  - 6.4 Configuration de backbox ..... 171

**Chapitre 3**  
**Outils de surveillance et supervision**

- 1. Surveillance basique ..... 175
  - 1.1 Présentation et définitions ..... 175
  - 1.2 Installation de Glances ..... 178
  - 1.3 Modes d’utilisation ..... 180
  - 1.4 Configuration de Glances ..... 182
  - 1.5 Alternative à Glances ..... 184

2.	Supervision d'un système de calcul	188
2.1	Fonctionnalités	188
2.2	Installation	190
2.3	Configuration	191
2.3.1	Le fichier gmetad.conf	191
2.3.2	Le fichier gmond.conf	192
2.4	Sécurisation	194
2.5	État et statistiques	198
2.6	Alternative légère : cacti	199
3.	Supervision évoluée	207
3.1	Généralités	207
3.2	Installation	208
3.3	Configuration	209
3.4	Initialisation	211
3.5	Utilisation	216
4.	Supervision complète.	218
4.1	Présentation.	218
4.2	Installation	220
4.3	Configuration Apache2	221
5.	Alternative à Nagios	227
5.1	Généralités	227
5.2	Prérequis d'installation	228
5.3	Installation et configuration	229

## Chapitre 4

### Services système et administration

1.	Introduction	237
2.	Serveur de temps	237
2.1	Présentation.	237
2.2	Installation du serveur NTP	238
2.3	Installation du client NTP	241
2.4	Démarrage et vérifications	242
2.5	Sécurisation NTP	244

- 3. Matrices RAID . . . . . 245
  - 3.1 Installation mdadm . . . . . 247
  - 3.2 Création de matrices RAID . . . . . 247
  - 3.3 Cas d'usage . . . . . 251
- 4. Partages Linux . . . . . 261
  - 4.1 Paramétrage serveur . . . . . 262
  - 4.2 Paramétrage client . . . . . 264
  - 4.3 Partages hétérogènes depuis Windows . . . . . 266
    - 4.3.1 Montages SAMBA . . . . . 266
    - 4.3.2 Montages cifs . . . . . 270
- 5. Outils d'administration. . . . . 272
  - 5.1 Gestion des applications AMP. . . . . 272
  - 5.2 Utilisation de l'outil phpMyAdmin. . . . . 274
  - 5.3 Sécurisation de phpMyAdmin. . . . . 275
  - 5.4 Mise en œuvre de webmin. . . . . 277
  - 5.5 Sécurisation de webmin . . . . . 278
  - 5.6 Notifications des nouvelles mises à jour . . . . . 283
- 6. Les mécanismes de wrapper . . . . . 284
  - 6.1 Principe de fonctionnement. . . . . 284
  - 6.2 Installation du wrapper . . . . . 287
  - 6.3 Configuration du fichier inetd.conf. . . . . 287
  - 6.4 Les utilitaires du wrapper. . . . . 288
- 7. Les mécanismes de statistiques. . . . . 291
  - 7.1 Notion de comptabilité . . . . . 291
  - 7.2 Service accton . . . . . 291
  - 7.3 Les statistiques de la comptabilité. . . . . 292
  - 7.4 Utilisation de LBSA . . . . . 293

## Chapitre 5 De la redondance au cluster

- 1. Redondance . . . . . 295
  - 1.1 Présentation des volumes SAN . . . . . 296
  - 1.2 Snapshot sur LVM . . . . . 304
  - 1.3 Carte d'interface réseau et bonding. . . . . 304
  - 1.4 Synchronisation des disques . . . . . 309

# 6 **Debian GNU/Linux**

Maîtrisez la sécurité des infrastructures

1.5	Duplication des services	314
2.	Mise en œuvre d'un cluster	320
2.1	Utilisation de LVS	320
2.2	Utilisation de KeepAlived	323
2.3	Utilisation de heartbeat	328
3.	Haute disponibilité	329
3.1	Architecture à initialiser	329
3.2	Installation de corosync	331
3.3	Configuration de corosync	332
3.4	Configuration de pacemaker	334
4.	Application aux bases de données	335
4.1	Installation	336
4.2	Utilisation et configuration	338
4.3	Système maître/esclave : londiste	342
4.4	Réplication PostgreSQL	346
4.5	Mise en œuvre de la réplication	348

## **Chapitre 6**

### **Loadbalancing et qualité de service**

1.	Équilibrage de charge	357
1.1	Comment optimiser le trafic ?	357
1.2	Équilibrage de charge pfsense	359
1.3	Installation de pfsense	360
1.4	Configuration et accès aux fonctionnalités	365
2.	Configuration de pfsense	366
2.1	Configuration de base	366
2.2	Configuration d'interface réseau	369
2.3	Fonctionnalités supplémentaires	372
2.4	Activation de l'équilibrage de charge	373
2.5	Gestion des règles d'accès	377
3.	Sécurisation de pfsense	381
3.1	Déploiement d'un tunnel VPN site-à-site	381
3.2	Mise en œuvre	385
3.3	Tests de la configuration	391

- 3.4 Sauvegarde/restauration de la configuration ..... 392
- 3.5 Installation d'Open-VM-Tools ..... 394
- 4. Qualité de service. .... 396
  - 4.1 Généralités ..... 396
  - 4.2 Approche directe ..... 397
  - 4.3 Mise en œuvre de trickle ..... 404
  - 4.4 Mise en œuvre de wondershaper ..... 406
- 5. Intégration d'un bac à sable ..... 407
  - 5.1 Le sandbox. .... 407
  - 5.2 Utilisation de seccomp ..... 410
  - 5.3 Mise en œuvre de firejail ..... 411
  - 5.4 Compléments de firejail ..... 412

**Chapitre 7**  
**Outils forensic**

- 1. La science de l'analyse forensic ..... 415
  - 1.1 Le contexte ..... 415
  - 1.2 Les objectifs. .... 416
  - 1.3 Catégorisation des outils ..... 418
  - 1.4 Dans quels cas utiliser l'analyse forensic ? ..... 427
- 2. Kali linux ..... 429
  - 2.1 Fonctions et rôles ..... 429
  - 2.2 Installation de la suite Kali Linux ..... 430
  - 2.3 Configuration et exploitation ..... 437
  - 2.4 Exemples d'utilisation ..... 441
- 3. Caine live ..... 447
  - 3.1 Fonctions et rôles ..... 447
  - 3.2 Initialisation de Caine Live ..... 450
  - 3.3 Configuration et exploitation ..... 459
  - 3.4 Exemples d'utilisation ..... 461
- 4. Deft Linux ..... 464
  - 4.1 Fonctions et rôles ..... 464
  - 4.2 Installation de Deft Linux ..... 468
  - 4.3 Configuration et exploitation ..... 474

4.4	Exemples d'utilisation.....	480
5.	Helix.....	483
5.1	Fonctions et rôles.....	483
5.2	Installation d'Helix.....	486
5.3	Configuration et exploitation.....	489
5.4	Exemples d'utilisation.....	490
5.5	Liste d'outils d'analyses forensic.....	492

## Conclusion

1.	Niveaux évolutifs.....	495
2.	Gestion de statistiques et de journaux.....	496
3.	Bilan des opérations.....	498
4.	Pour conclure.....	499
	Glossaire.....	501
	Index.....	515

Les éléments à télécharger sont disponibles à l'adresse suivante :  
**<http://www.editions-eni.fr>**  
Saisissez la référence ENI de l'ouvrage **EPSSYDEB** dans la zone de recherche  
et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

## 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

## Chapitre 1 Introduction

- 1. Pourquoi Debian ? . . . . . 13
  - 1.1 Sécurité du système d'information . . . . . 16
  - 1.2 Sécurité de l'information . . . . . 17
  - 1.3 Où trouver la distribution Debian ? . . . . . 19
  - 1.4 Quelles « saveurs » de distribution Debian ? . . . . . 22
  - 1.5 Exemple d'installation : iolive . . . . . 24
- 2. Généralités sur la sécurité . . . . . 30
  - 2.1 Sécurité et sûreté de fonctionnement . . . . . 30
  - 2.2 Supervision et surveillance . . . . . 31
  - 2.3 Traçabilité . . . . . 32
  - 2.4 Considération du coût et du risque . . . . . 32
- 3. Quels sont les éléments à sécuriser sur GNU/Linux . . . . . 34
  - 3.1 Le BIOS . . . . . 34
    - 3.1.1 Démarrage . . . . . 35
    - 3.1.2 Paramétrage . . . . . 36
    - 3.1.3 Cas des machines virtuelles . . . . . 37
    - 3.1.4 Utilisation d'UEFI . . . . . 39



3.2	Le bootloader . . . . .	40
3.3	Le noyau linux . . . . .	42
3.4	Les modules . . . . .	44
3.5	L'image au démarrage : initrd . . . . .	45
3.6	Les pseudo-systèmes de fichiers . . . . .	47
3.6.1	/proc . . . . .	47
3.6.2	/sys . . . . .	48
3.7	La mémoire . . . . .	48
4.	Suppression des anciens noyaux . . . . .	50
4.1	Phase d'initialisation init . . . . .	50
4.2	Scripts d'initialisation avec en-têtes LSB . . . . .	53
4.3	Parallélisation avec systemd . . . . .	54
5.	La sécurité fondamentale . . . . .	59
5.1	Sécurisation des comptes utilisateurs . . . . .	60
5.2	Empêcher les comptes inutiles . . . . .	61
5.3	Mettre en œuvre une gestion de mot de passe . . . . .	62
5.4	Fermer les services inutiles . . . . .	64
5.5	Effectuer les mises à jour . . . . .	66

## **Chapitre 2** **Outils noyau et initialisation**

1.	Protection dès la phase de démarrage . . . . .	69
1.1	Sécurisation du BIOS . . . . .	69
1.2	Présentation de GRUB . . . . .	71
1.3	Sécurisation de GRUB . . . . .	75
1.4	Utilisation de GRUB . . . . .	79
1.5	Boot on SAN . . . . .	80
2.	Protection du noyau . . . . .	82
2.1	Le noyau linux . . . . .	82
2.2	Architecture d'un noyau . . . . .	87
2.3	Les anneaux de protection . . . . .	88
2.3.1	Architecture 32 bits sans virtualisation . . . . .	88
2.3.2	Architecture 32 bits virtualisée . . . . .	89
2.3.3	Architecture 64 bits sans virtualisation . . . . .	90
2.3.4	Architecture 64 bits virtualisée . . . . .	90

- 2.4 Protections naturelles du noyau . . . . . 92
- 3. Installation de partition chiffrée. . . . . 99
  - 3.1 Utilisation de LUKS . . . . . 101
  - 3.2 Utilisation d’EncFS . . . . . 105
- 4. Gestionnaire de volumes logiques . . . . . 107
  - 4.1 Description du LVM. . . . . 107
    - 4.1.1 Création de volumes physiques . . . . . 110
    - 4.1.2 Création de groupes de volumes . . . . . 110
    - 4.1.3 Création de volumes logiques . . . . . 111
  - 4.2 Partition LVM chiffrée . . . . . 113
  - 4.3 Utilisation des snapshots sur LVM . . . . . 116
  - 4.4 Sauvegardes LVM . . . . . 116
  - 4.5 Le gestionnaire LVM au niveau du SAN . . . . . 118
  - 4.6 Vérification des volumes logiques . . . . . 120
  - 4.7 Sécurisation des attributs . . . . . 124
- 5. Commandes de base . . . . . 125
  - 5.1 De quoi s’agit-il ? . . . . . 125
  - 5.2 Utilisation des séquences alternatives. . . . . 127
  - 5.3 Mise en place de conteneurs . . . . . 128
  - 5.4 Application de docker : conteneur web. . . . . 133
  - 5.5 Sécurisation des conteneurs . . . . . 134
- 6. Industrialisation des installations . . . . . 137
  - 6.1 Installation de VirtualBox Guest additions . . . . . 142
  - 6.2 Installation de VMTtools . . . . . 143
  - 6.3 Fonctions de clonage . . . . . 144

**Chapitre 3**  
**Outils de base**

- 1. Protection des connexions frauduleuses . . . . . 147
  - 1.1 Utilisation de fail2ban . . . . . 148
  - 1.2 Configuration de fail2ban . . . . . 149
  - 1.3 Interface cliente de fail2ban . . . . . 152
  - 1.4 Interface web de fail2ban . . . . . 154

2.	Protection contre les rootkits	155
2.1	Définition d'un rootkit	155
2.2	Utilisation de samhain	157
2.3	Utilisation de rkhunter	158
2.4	Vérification d'intégrité	161
3.	Protection des fichiers critiques	164
3.1	Comment évaluer la criticité ?	164
3.2	L'utilitaire AIDE	165
3.3	Les règles concernant AIDE	168
3.4	L'outil tripwire, alternative à aide	170
4.	Protection des ports de service	176
4.1	Qu'est-ce qu'un port de service ?	176
4.2	Installation de portsentry	179
4.3	Activation de portsentry	181
5.	Protection des accès	181
5.1	Comment définir un accès ?	181
5.2	Délégation d'accès	184
5.3	Délais de grâce du mot de passe	187
5.4	Gestionnaire de fenêtres	188
6.	Protection des journaux	195
6.1	Paramétrage des logs courants	195
6.2	Surveillance des logs avec logwatch	202
6.3	Vérification des traces avec logcheck	207
6.4	Vérification des traces du noyau	210
6.5	Centralisation des traces avec loganalyzer	211
6.6	Nouvelle gestion des services et de la journalisation	217

## **Chapitre 4** **Outils Serveur**

1.	Protection des limites	225
1.1	Compteurs de ressources	225
1.2	Quantifier les ressources	229
1.3	Gestion de quotas	230
1.4	Confinement et chroot	234
1.5	Gestion des attributs	237

- 2. Protection du paramétrage ..... 239
  - 2.1 Protection contre le spoofing IP ..... 241
  - 2.2 Sécurisation du trafic réseau ..... 241
  - 2.3 Utilisation avancée de sysctl ..... 243
  - 2.4 Paramétrage divers de sécurisation ..... 244
  - 2.5 Protection et surveillance de répertoires critiques ..... 247
- 3. Contrôle d'accès ..... 250
  - 3.1 Les droits standards ..... 250
  - 3.2 Les droits étendus ..... 253
  - 3.3 Sauvegarde des droits étendus ..... 258
  - 3.4 Protection des processus ..... 259
- 4. Protection des sessions ..... 263
  - 4.1 Authentification standard ..... 263
  - 4.2 Authentification par modules PAM ..... 267
  - 4.3 Utilisation des modules PAM ..... 271
- 5. Sécurisation des services ..... 272
  - 5.1 Différents modèles de sécurité ..... 272
  - 5.2 Sécurité des services ..... 273
  - 5.3 Utilisation de SELinux ..... 276
  - 5.4 Les cgroups ..... 279
  - 5.5 Utilisation de AppArmor ..... 282
- 6. Sécurité des Serveurs d'impression ..... 285
  - 6.1 Généralités ..... 285
  - 6.2 Installation ..... 286
  - 6.3 Utilisation ..... 287
  - 6.4 Sécurisation du service ..... 293

**Chapitre 5**  
**Outils réseau**

- 1. Protection des flux réseau ..... 295
  - 1.1 Présentation du réseau ..... 295
  - 1.2 Filtrage des paquets ..... 300
  - 1.3 Utilisation de netfilter ..... 304
  - 1.4 Sauvegarde et restauration des règles ..... 307

1.5	Réseau et connexions sans fil . . . . .	311
1.5.1	Utilisation du Wi-Fi . . . . .	311
1.5.2	Utilisation du Bluetooth . . . . .	316
2.	Sécurisation d'accès aux services . . . . .	318
2.1	Gestion des zones . . . . .	319
2.2	Gestion des sources . . . . .	320
2.3	Gestion des services . . . . .	322
2.4	Gestion des règles . . . . .	323
3.	Système de proxy mandataire . . . . .	325
3.1	Présentation . . . . .	326
3.2	Mise en œuvre de squid . . . . .	330
3.3	Le proxy HAProxy . . . . .	337
3.4	Le proxy SOCKS . . . . .	340
4.	Protection du réseau . . . . .	344
4.1	Introduction . . . . .	344
4.2	Installation de Free RADIUS . . . . .	345
4.3	Configuration de Free RADIUS . . . . .	346
4.4	Cas d'utilisation de Free RADIUS . . . . .	349
5.	Réseau privé virtuel . . . . .	351
5.1	Installation et configuration . . . . .	352
5.2	Infrastructures à clés publiques . . . . .	354
5.3	Installer un conteneur OpenVPN . . . . .	361

## Chapitre 6

### Outils antivirus

1.	Système antiviral de base . . . . .	365
1.1	Cibles à protéger . . . . .	365
1.2	Installation de ClamAV . . . . .	370
1.3	Utilisation de Linux Malware Detect . . . . .	372
1.4	Protection des stations Linux . . . . .	375
1.5	Alternative pour la protection des stations . . . . .	378
2.	Système antiviral forensic . . . . .	381
2.1	Installation de clamtk . . . . .	381
2.2	Utilisation de ClamAV avancée . . . . .	384

- 2.3 Installation de clamassassin . . . . . 385
- 2.4 Installation de clamSMTP . . . . . 386
- 3. Protection complète des répertoires \$HOME . . . . . 388
  - 3.1 Le contexte . . . . . 388
  - 3.2 La mise en œuvre . . . . . 389
- 4. Protection contre les spams . . . . . 392
  - 4.1 Présentation . . . . . 392
  - 4.2 Installation de l'outil . . . . . 393
  - 4.3 Configuration du service de messagerie . . . . . 394
  - 4.4 Gestion des règles d'apprentissage . . . . . 395
  - 4.5 Sauvegarde/restauration de la base SpamAssassin . . . . . 399
- 5. Protection contre les tempêtes ARP . . . . . 400
  - 5.1 Présentation des risques . . . . . 400
  - 5.2 Installation de l'outil de détection . . . . . 402
  - 5.3 Utilisation de l'outil de détection . . . . . 402

**Chapitre 7**  
**Outils de mise à jour**

- 1. Mise en place d'un repository . . . . . 405
  - 1.1 Gestionnaire de paquets . . . . . 406
  - 1.2 Utilisation avancée d'aptitude . . . . . 412
  - 1.3 Gestion de la cohérence . . . . . 414
  - 1.4 Mise à jour de sécurité . . . . . 416
  - 1.5 Création de dépôts . . . . . 419
- 2. Gestion des signatures GPG . . . . . 421
  - 2.1 Le projet GnuPG . . . . . 421
  - 2.2 Champ d'application et signature de clés GnuPG . . . . . 422
  - 2.3 Vérification d'authenticité des paquets . . . . . 423
  - 2.4 Authenticité des dépôts . . . . . 425
- 3. Déclaration et remontée de bugs . . . . . 430
  - 3.1 Cas d'un nouveau bug . . . . . 430
  - 3.2 Modification de rapport . . . . . 433
  - 3.3 Suivi de version . . . . . 434
  - 3.4 Intégrité et reporting . . . . . 436

3.5	Dépannage	437
4.	Automatisation pilotée par Puppet	440
4.1	Définitions et architecture	440
4.2	Installation de Puppet	445
4.2.1	Installation du service principal (puppetmaster)	445
4.2.2	Installation du serveur PuppetDB	449
4.2.3	Installation du serveur Web Frontend	450
4.3	Configuration de Puppet	451
4.4	Mise en œuvre d'une classe Puppet	456
5.	Gestion de version	460
5.1	Présentation de git	460
5.2	Installation de git	463
5.3	Configuration de git	464
5.4	Application et utilisation de git	466
6.	Systèmes de distributions	470
6.1	Fonctionnement de xCAT2	470
6.2	Installation de xCAT2	473
6.3	Configuration xCAT2	476
6.4	Alternative de distribution FAI	477

## Conclusion

1.	Niveaux évolutifs	483
2.	Bilan des opérations	485
3.	Pour conclure	487
	Glossaire	489
	Index	500