

Avant-propos

1. Introduction	11
2. Structure du livre	12

Chapitre 1

Nouveautés du système d'exploitation

1. Introduction	15
2. Winlogon	17
2.1 Architecture	17
2.2 Fournisseurs d'informations d'authentification	18
3. Renforcement des services.	19
3.1 Isolation des sessions	19
3.2 Renforcement des contrôles d'accès.	21
3.3 Comptes de service	21
3.3.1 Système local.	21
3.3.2 Service Réseau	22
3.3.3 Service Local	22
3.3.4 Comptes utilisateurs du domaine.	23
3.4 SID de service.	23
3.5 SID restreints	24
4. Renforcement contre les débordements de pile	25
4.1 DEP	25
4.2 ASLR	28
5. Processus protégés.	29
6. MIC	31
7. Windows Resource Protection (WRP)	33
8. Contrôle des périphériques	34
8.1 Menaces existantes	34
8.2 Blocage par stratégies de groupe	35
8.3 Exemple	38
8.3.1 Blocage d'une classe d'installation de périphériques	40
8.3.2 Blocage d'un ID de périphérique.	44

2 ————— La sécurité sous Windows Vista

9. Améliorations dans la cryptographie	44
9.1 CNG	44
9.2 Cartes à puce	44
9.3 EFS	45
9.4 Services de chiffrement	45
10. Changements spécifiques à Windows 64 Bit	46
10.1 Signature des pilotes de périphériques	46
10.2 PatchGuard (Protection contre la modification du noyau)	46

Chapitre 2

Les nouveaux outils

1. Le Centre de sécurité	47
1.1 Surveillance des fonctions de sécurité du système	47
1.2 Paramétrage	51
2. Windows Defender	53
2.1 Présentation	53
2.2 Paramètres d'analyse automatique	56
2.3 Analyse en temps réel	58
2.4 Utilisation de la communauté Microsoft Spynet	59
2.5 Visualisation et modification des logiciels autorisés ou mis en quarantaine	60
2.6 Explorateur de logiciels	63
2.7 Analyse	65
3. Outil de suppression d'applications malveillantes	66

Chapitre 3

Le pare-feu Windows

1. Présentation	69
1.1 Rappels essentiels	69
1.2 Nouveautés du pare-feu de Windows Vista	71

2.	Paramétrage	73
2.1	Présentation des outils d'administration	73
2.1.1	Panneau de contrôle.	73
2.1.2	Boîte de dialogue de paramétrage.	74
2.1.3	Centre de sécurité	77
2.1.4	Console de logiciel enfichable.	77
2.1.5	Stratégies de groupe.	79
2.1.6	Script.	80
2.1.7	Netsh.	81
2.2	Paramètres globaux.	83
2.2.1	Paramétrage par défaut IPSEC	86
2.2.2	Échange de clé	87
2.2.3	Protection des données.	89
2.2.4	Méthode d'authentification	91
2.3	Configuration des règles	92
2.3.1	Profils	92
2.3.2	Règles	93
2.3.3	Ordre d'application des règles	93
2.4	Scénarii.	94
2.4.1	Restriction d'accès à un service particulier	94
2.4.2	Mode Isolation.	106
2.4.3	Exemptions d'authentification	107
2.4.4	Mode Tunnel.	108

Chapitre 4
Le réseau sous Windows Vista

1.	Le partage de fichiers et d'imprimantes	109
1.1	Présentation générale	109
1.2	Authentification	111
1.3	Intégrité	113
1.4	Paramétrage	116
1.4.1	Activation/désactivation des partages.	116

4 ————— La sécurité sous Windows Vista

1.4.2	Partage et visualisation.	120
1.4.3	Interopérabilité	123
2.	La protection des accès réseau	124
3.	Les réseaux sans fil	125
3.1	Présentation	125
3.2	Risques liés aux réseaux sans fil	126
3.2.1	Utilisation frauduleuse du réseau Wi-Fi et accès Internet	126
3.2.2	Interception de données et modifications.	127
3.3	Protocoles de chiffrement des réseaux sans fil	127
3.3.1	WEP.	127
3.3.2	WPA	129
3.4	Sécurisation des réseaux sans fil	133
3.5	Améliorations dans Windows Vista.	135

Chapitre 5 Contrôle des comptes utilisateurs

1.	Introduction	137
2.	Définitions	140
2.1	SID.	140
2.2	Jetons d'accès (Access Token)	141
2.3	Privilèges et droits.	142
3.	Fonctionnement de UAC	144
3.1	Explication du fonctionnement	144
3.2	Architecture en détail	149
3.2.1	Utilisation du Shell	149
3.2.2	ShellExecute vs CreateProcess	152
3.3	Virtualisation	152
3.4	Contrôle d'intégrité.	156
3.5	Élévation des privilèges	157
3.5.1	Interface graphique	157
3.5.2	Fichiers Manifest	158
3.5.3	Par programmation	161

3.6	Changements	163
3.6.1	Compte administrateur	163
3.6.2	Groupe Utilisateurs avec pouvoir	164
4.	Configuration	164
5.	Questions fréquentes	166

Chapitre 6

Les contrôles d'accès

1.	Définitions	169
1.1	Objets	169
1.2	ACL	169
1.3	ACE	170
1.4	Descripteur de sécurité	170
1.5	DACL	170
1.6	SACL	170
1.7	SDDL	171
1.8	Héritage	171
1.9	Ordre et priorité d'application des ACE	172
1.10	Création et application de permissions	174
2.	Groupes et SID spéciaux	184
2.1	TrustedInstaller	185
2.2	CREATEUR PROPRIETAIRE	186
2.3	DROITS DU PROPRIÉTAIRE	186
2.4	GROUPE CREATEUR	187
2.5	INTERACTIF	187
2.6	LIGNE	187
2.7	REMOTE INTERACTIVE LOGON	187
2.8	RESEAU	188
2.9	SERVICE	188
2.10	SERVICE RÉSEAU	188
2.11	SERVICE LOCAL	188
2.12	SYSTEM	188
2.13	TACHE	189
2.14	UTILISATEUR TERMINAL SERVER	189

6 ————— La sécurité sous Windows Vista

2.15	Utilisateurs du Bureau à distance	189
2.16	Utilisateurs du modèle COM distribué	189
2.17	Utilisateurs avec pouvoir.	191
3.	Changements dans Windows Vista	192
3.1	SID de refus dans le jeton d'accès	192
3.2	ACL sur le système de fichiers.	193
3.3	Documents and Settings.	194
3.4	Partages.	196
3.5	Niveau d'intégrité	197
3.6	Audit	197
3.7	Outils	199

Chapitre 7

Internet Explorer

1.	Les nouveautés d'Internet Explorer	201
1.1	Introduction	201
1.2	Le filtre anti-hameçonnage	202
1.3	La barre de statut	204
1.4	Infocard	204
1.5	Le gestionnaire de modules	205
1.6	ActiveX.	207
2.	Le mode protégé	208
3.	Les paramètres des zones de sécurité	214
3.1	Définition des zones	214
3.2	.NET Framework	217
3.3	Authentification utilisateur.	217
3.4	Autoriser l'installation de .NET Framework	218
3.5	Composants dépendants du .NET Framework.	218
3.6	Contrôles ActiveX et plug-ins	219
3.7	Divers	221
3.8	Script	225
3.9	Téléchargement.	226
4.	Les paramètres de sécurité avancée	227

5. Le paramétrage par stratégie de groupe	231
5.1 Fonctionnalités de sécurité	232
5.2 Panneau de configuration d'Internet Explorer	236

Chapitre 8 BitLocker et EFS

1. BitLocker.	237
1.1 Introduction à BitLocker	237
1.2 Présentation des menaces	238
1.2.1 Données contenues dans un fichier	239
1.2.2 Données contenues dans une base de données	239
1.2.3 Comptes utilisateurs et mots de passe	239
1.2.4 Données pour accéder au réseau privé d'une entreprise.	241
1.2.5 Données confidentielles contenues en mémoire	242
1.2.6 Vidage mémoire d'une application ou du système	243
1.2.7 PageFile	244
1.2.8 Fichier d'hibernation	244
1.2.9 Clés de chiffrement et certificats numériques.	244
1.3 Fonctionnement de BitLocker	245
1.4 BitLocker avec TPM	249
1.5 BitLocker avec USB.	250
1.6 BitLocker avec TPM et code PIN.	250
1.7 BitLocker avec TPM et USB	251
1.8 BitLocker avec TPM et USB et code PIN.	251
1.9 Déploiement de BitLocker	251
1.9.1 Mode d'authentification.	252
1.9.2 Paramétrage et déploiement	253
1.9.3 Gestion des clés de chiffrement	257
2. EFS.	257
2.1 Introduction à EFS	257
2.2 Fonctionnement d'EFS	259
2.2.1 Opérations de chiffrement et déchiffrement de fichier	259
2.2.2 Paramétrage de l'Explorateur Windows.	261

8 ————— La sécurité sous Windows Vista

2.2.3	Fonctionnement	262
2.3	BitLocker et EFS	265
2.4	Plans de restauration	266
2.4.1	Sauvegarde du certificat de chiffrement	266
2.4.2	Agent de récupération EFS	272
2.4.3	Agent de récupération de certificats	273
2.5	GPO EFS	274

Chapitre 9

Stratégies de groupe de sécurité

1.	Introduction	277
2.	Les nouveautés dans Vista	279
2.1	Nouveau format	279
2.2	Multiplés stratégies de groupe locales	281
2.3	Particularités	284
2.3.1	Diagnostics	284
2.3.2	Auditpol.	286
2.3.3	Scripts de logon	287
2.4	Windows Vista Security Guide	287
3.	Les paramètres de sécurité	287
3.1	Stratégies de compte	288
3.1.1	Stratégies de mot de passe	288
3.1.2	Stratégie de verrouillage de compte	289
3.2	Stratégies d'audit	290
3.3	Attribution des droits utilisateurs	292
3.4	Options de sécurité	293
3.5	Stratégies de restriction logicielle	294

Chapitre 10

Développement sécurisé dans Windows Vista

1. Synthèse	297
2. Pratiques de développement	298
2.1 Script de login	298
2.2 Demande d'élévation à distance	299
2.3 Fichiers manifest	299
2.4 Windows Installer	299
2.5 Isolation des privilèges de l'interface utilisateur	300
2.6 Virtualisation	301
2.6.1 Généralités	301
2.6.2 Variables d'environnement et chemins standards	302
2.7 Les contrôles ActiveX	302
2.8 Kit de compatibilité applicative de Microsoft	302
2.9 Scripts	303
2.10 Interface graphique	304
2.11 Signer votre code	306

Annexe

1. Liste de sites	307
Index	310