

Solutions • **WINDOWS 2000**



Sécurité

sous Windows 2000 Server

THOMAS W. SHINDER

DEBRA LITTLEJOHN SHINDER

D. LYNN WHITE

EYROLLES



2-005-592-1

Sécurité **SOUS Windows 2000** **Server**

THOMAS W. SHINDER

DEBRA LITTLEJOHN SHINDER

D. LYNN WHITE

EYROLLES



Table des matières

Remerciements	V
Les auteurs	VII
Préface	IX
CHAPITRE 1	
Introduction au dispositif de sécurité de Windows 2000 Server	1
Bref aperçu de la sécurité sous Windows 2000 Server	1
Livre blanc sur la sécurité sous Windows 2000	2
Pourquoi des changements en matière de sécurité ?	2
Nouveautés de Windows 2000 Server en matière de sécurité	2
Problèmes et limitations	4
Ce qui n'a pas changé... ..	6
Considérations sur la mise à niveau/migration	6
Plan de sécurité du réseau	6
Test du plan de sécurité du réseau	8
Procédure de mise à niveau/migration	9
Analyse préliminaire	10
Synthèse	11
FAQ	12

CHAPITRE 2

Paramètres par défaut de contrôle des accès	13
Introduction	13
Le groupe Administrateurs	15
Le groupe Utilisateurs	15
Le groupe Utilisateurs avec pouvoir	16
Configuration de la sécurité au cours de l'installation de Windows 2000	16
Autorisations par défaut pour le système de fichiers et le Registre ..	17
Droits par défaut des utilisateurs	30
Appartenance par défaut aux groupes	35
Synthèse	37
FAQ	37

CHAPITRE 3

Authentification Kerberos	39
Introduction	39
Authentification sous Windows 2000	39
Avantages du système d'authentification Kerberos	41
Les normes Kerberos	41
Modifications apportées par Microsoft au système Kerberos	42
Le protocole Kerberos	42
Concepts de base	42
Sous-protocoles	47
Tickets	51
Kerberos et Windows 2000	55
Le Centre de distribution de clé, ou KDC (Key Distribution Center)	55
Stratégie Kerberos	58
Contenu d'un ticket Microsoft Kerberos	59
Délégation de l'authentification	60
Pré-authentification	61
Fournisseurs de sécurité, ou SSP	61
Mémoire cache d'identification	62
Résolution de noms DNS	63
Ports UDP et TCP	63

Données d'autorisation	63
KDC et données d'autorisation	63
Services et données d'autorisation	64
Synthèse	64
FAQ	65

CHAPITRE 4

Sécurisation des réseaux à l'aide des services de sécurité distribués de Windows 2000	67
Introduction	67
La sécurité sous Windows NT	68
La sécurité distribuée de Windows 2000 : tout un nouveau monde !	68
Normes ouvertes	68
Services de sécurité distribués de Windows 2000	70
Active Directory et la sécurité	71
Avantages d'une gestion des comptes via Active Directory	71
Relation existant entre Active Directory et les services de sécurité	78
Protocoles de sécurité de Windows 2000	86
Authentification NTLM	87
Authentification Kerberos	87
Paires de clés privées/publiques et certificats	88
Autres protocoles pris en charge	89
Ouverture de session unique (SSO)	90
L'interface SSPI (Security Support Provider Interface)	91
Windows 2000 et la sécurité Internet	91
Authentification de client via SSL 3.0	92
Authentification d'utilisateurs externes	92
Services de certificats Microsoft	92
CryptoAPI	93
Accès inter-entreprises : partenaires distribués	93
Synthèse	94
FAQ	95

CHAPITRE 5

Jeu d'outils de configuration de sécurité	97
Introduction	97
Vue d'ensemble du Jeu d'outils de configuration de sécurité	98
Composants du Jeu d'outils de configuration de sécurité	98
Service de configuration et d'analyse de la sécurité	98
Configurations de sécurité	100
Base de données de configuration et d'analyse de la sécurité	101
Zones de configuration et d'analyse de la sécurité	103
Interfaces utilisateur du Jeu d'outils de configuration de sécurité	105
Configuration de la sécurité	112
Stratégies de comptes	112
Stratégies locales	113
Journal des événements	114
Groupes restreints	114
Sécurité du Registre	116
Sécurité du système de fichiers	116
Sécurité des services du système	118
Analyse de la sécurité	118
Stratégies de compte et locales	119
Gestion des groupes restreints	120
Sécurité du Registre	120
Sécurité du système de fichiers	120
Sécurité des services système	122
Intégration des stratégies de groupe	122
Configuration de la sécurité dans des objets de stratégie de groupe	122
Autres stratégies de sécurité	123
Utilisation des outils	123
Utilisation du Service de configuration et d'analyse de la sécurité	123
Utilisation de l'Extension Paramètres de sécurité de l'Éditeur de stratégie de groupe	125
Synthèse	125
FAQ	126

CHAPITRE 6

Le système de fichiers cryptés (EFS) de Windows 2000	129
Introduction	129
Utilisation d'un système de cryptage des fichiers	130
Principes fondamentaux du cryptage	131
Principe du système de fichiers cryptés EFS	132
Opérations utilisateur	133
Cryptage de fichier	133
Utilisation d'un fichier crypté	135
Copie d'un fichier crypté	135
Déplacement ou renommage d'un fichier crypté	136
Décryptage d'un fichier	137
L'utilitaire Cipher	138
Cryptage de dossier	139
Opérations de récupération	139
L'architecture du système EFS	141
Les composants du système EFS	141
Le processus de cryptage	142
Les informations de cryptage EFS	145
Le processus de décryptage	147
Synthèse	149
FAQ	150

CHAPITRE 7

Sécurité IP pour Microsoft Windows 2000 Server	153
Introduction	153
Méthodes d'intrusion dans les réseaux	154
Ecoute passive des données sur le réseau (<i>snooping</i>)	154
Trucage de la source (<i>spoofing</i>)	155
Vol de mots de passe	155
Attaques par déni de services	156
Ecoute par interposition non détectée	157
Attaques dirigées contre des applications	157
Compromission de clés	158
Architecture IPSec	158
Vue d'ensemble des services cryptographiques de l'architecture IPSec	159
Services de sécurité IPSec	163
Associations de sécurité et procédures IPSec de gestion de clés	164

Déploiement de la sécurité IP Windows	166
Evaluation des informations	166
Identification de l'« ennemi »	167
Analyse des niveaux de sécurité requis	168
Elaboration de stratégies de sécurité au moyen de consoles IPSec personnalisées	168
Stratégies de sécurité flexibles	170
Stratégies de négociation flexibles	177
Filtres	178
Création d'une stratégie de sécurité	180
Synthèse	189
FAQ	190
CHAPITRE 8	
Cartes à puce	193
Introduction	193
Interopérabilité	194
ISO 7816, EMV et GSM	195
PC/SC Workgroup	195
L'approche Microsoft	195
Smart Card Base Components (composants de base des cartes à puce)	198
Fournisseurs de services	198
Solutions avancées	203
Authentification de clients	203
Ouverture de session interactive par clé publique	203
Courrier électronique sécurisé	208
Synthèse	209
FAQ	210
CHAPITRE 9	
Infrastructure à clé publique de Windows 2000	211
Introduction	211
Concepts	212
Techniques cryptographiques	212
Cryptographie par clé publique : fonctionnalités	214
Protection et certification des clés cryptographiques	217

Composants de l'infrastructure à clé publique de Windows 2000 . . .	221
Autorités de certification	223
Hiérarchies de certificats	223
Déploiement des autorités de certification	225
Approbation dans le cas de plusieurs hiérarchies de CA	226
Activation des clients de domaines	226
Génération de clés	226
Récupération de clés	227
Inscription de certificat	227
Renouvellement de certificats	228
Utilisation de clés et de certificats	228
Itinérance	229
Révocation	229
Fiabilité	229
Stratégie de sécurité pour l'infrastructure à clé publique sous Windows 2000	230
Autorités de certification racine	230
Inscription et révocation de certificats	232
Ouverture de session par carte à puce	232
Vue d'ensemble des applications	233
Sécurité Web	233
Messagerie électronique sécurisée	234
Signature numérique du code	234
Système de fichiers cryptés, ou EFS (Encrypted File System)	235
Ouverture de session par carte à puce	235
Sécurité IP (IPSec)	236
Préparation à la mise en œuvre d'une infrastructure PKI avec Windows 2000	237
Synthèse	238
FAQ	241
CHAPITRE 10	
La sécurité sous Windows 2000 Server en bref	243
Introduction	243
Que recouvre exactement la sécurité sous Windows 2000, et pourquoi faut-il le savoir ?	244
La sécurité informatique dans ses grandes lignes	244
Les différents composants de la sécurité informatique	246

Elaboration d'une stratégie de sécurité	247
Un peu d'histoire : la sécurité sous Windows NT !	248
Modifications importantes apportées à Windows NT	251
Impact du dispositif de sécurité de Windows 2000 sur les industries et les entreprises	251
Avantages et inconvénients du dispositif de sécurité de Windows 2000	252
Avantages de la sécurité sous Windows 2000 Server	253
Inconvénients de la sécurité sous Windows 2000 Server	254
Synthèse	256
FAQ	257
Index	259