

# SÉCURITÉ DES RÉSEAUX WINDOWS

Protection des réseaux  
Microsoft® en entreprise



**01**  
INFORMATIQUE

157  
Étienne Busnel

DUNOD

2-005-645-1

# SÉCURITÉ DES RÉSEAUX WINDOWS

## Protection des réseaux Microsoft® en entreprise

Étienne Busnel

*Consultant et responsable de l'offre Sécurité  
des Systèmes d'Information chez EDS*



DUNOD

# Table des matières

Avant-propos . . . . .	XI
------------------------	----

## Première partie – Contexte et présentation

<b>Chapitre 1 – Appréhender la sécurité des systèmes d'information . . . . .</b>	<b>3</b>
1.1 Contexte de la sécurité des systèmes d'information . . . . .	3
1.2 Méthodes de gestion de la sécurité . . . . .	5
1.3 Démarche synthétique . . . . .	11
1.4 Identifier les vulnérabilités . . . . .	11
1.5 Déterminer les éléments sensibles . . . . .	13
1.6 Prendre en compte l'existant . . . . .	14
1.7 Confronter les besoins, les risques et l'existant . . . . .	14
1.8 Mettre en place des moyens de protections techniques et organisationnels . . . . .	15
<b>Chapitre 2 – Présentation de Windows NT, 2000, XP, 2003 . . . . .</b>	<b>17</b>
2.1 Fonctionnalités attendues . . . . .	17
2.2 Système privilégié . . . . .	18
2.3 Comparaison . . . . .	19

2.4	Évaluation . . . . .	19
2.5	Détails sur Windows XP . . . . .	22
2.6	Détails sur Windows 2003 Server . . . . .	29

## Deuxième partie – Fonctionnalités de sécurité

<b>Chapitre 3 – Authentification</b> . . . . .	<b>37</b>
3.1 Caractéristiques de l'authentification . . . . .	37
3.2 Architecture d'authentification . . . . .	39
3.3 NTLM . . . . .	42
3.4 Kerberos . . . . .	47
3.5 Certificats X.509 et cartes à puce . . . . .	55
<b>Chapitre 4 – Chiffrement et signature</b> . . . . .	<b>57</b>
4.1 Généralités . . . . .	57
4.2 Implémentation par Microsoft . . . . .	67
4.3 Infrastructure de gestion de clé (PKI) . . . . .	67
4.4 Protection des fichiers . . . . .	78
4.5 Protection des flux réseau . . . . .	86
<b>Chapitre 5 – Gestion des utilisateurs</b> . . . . .	<b>105</b>
5.1 Introduction . . . . .	105
5.2 Utilisateur . . . . .	106
5.3 Mots de passe . . . . .	109
5.4 Droits . . . . .	111
5.5 Options de sécurité . . . . .	117
<b>Chapitre 6 – Gestion des droits d'accès</b> . . . . .	<b>123</b>
6.1 En théorie . . . . .	123
6.2 En pratique . . . . .	127
<b>Chapitre 7 – Gestion de l'audit et de la journalisation</b> . . . . .	<b>137</b>
7.1 Stratégie d'audit . . . . .	137
7.2 Configuration de l'audit des objets . . . . .	138

7.3	Détail des événements enregistrés . . . . .	140
7.4	Exploitation . . . . .	147
7.5	Administration . . . . .	152
<b>Chapitre 8 – Partage de fichiers . . . . .</b>		<b>153</b>
8.1	Gestion des droits d'accès . . . . .	153
8.2	Intégrité . . . . .	154
8.3	Authentification . . . . .	155
8.4	Implémentation réseau . . . . .	156
<b>Chapitre 9 – Administration . . . . .</b>		<b>157</b>
9.1	Rappel de Windows NT 4.0 . . . . .	157
9.2	Gestion des stratégies de groupes . . . . .	158
9.3	Active Directory . . . . .	159
9.4	Protection de la disponibilité . . . . .	160
<b>Chapitre 10 – Accès distants (RAS) . . . . .</b>		<b>165</b>
10.1	Configuration de base . . . . .	165
10.2	Verrouillage du compte . . . . .	166
10.3	Protocoles . . . . .	166
10.4	L2TP . . . . .	167
<b>Chapitre 11 – Implémentation des protocoles réseau . . . . .</b>		<b>171</b>
11.1	TCP/IP . . . . .	172
11.2	NetBT . . . . .	177
11.3	DNS . . . . .	177

### Troisième partie – Les attaques sur les réseaux Windows

<b>Chapitre 12 – Contexte . . . . .</b>		<b>181</b>
12.1	Situation de Microsoft . . . . .	181
12.2	Vision des pirates . . . . .	182
12.3	Stratégie Microsoft . . . . .	182

<b>Chapitre 13 – Failles de sécurité</b> . . . . .	189
13.1 Failles type . . . . .	189
13.2 Suivi et correction des failles . . . . .	195
<b>Chapitre 14 – Attaques courantes</b> . . . . .	201
14.1 Recueil d'informations « libres » . . . . .	201
14.2 Visibilité d'une machine Windows sur le réseau . . . . .	202
14.3 Authentification : vulnérabilités et moyens d'accès illicites . . . . .	204
14.4 Accès aux fichiers . . . . .	206
14.5 Partage de fichiers (SMB) . . . . .	210
14.6 Virus . . . . .	211

#### Quatrième partie – Recommandations de mise en œuvre

<b>Chapitre 15 – Installation</b> . . . . .	217
15.1 Protection du BIOS . . . . .	217
15.2 Multisystème et réseau . . . . .	217
15.3 Système de fichiers . . . . .	218
15.4 Composants . . . . .	219
15.5 Mots de passe . . . . .	220
15.6 ERD . . . . .	221
15.7 Services Packs, Hotfixes . . . . .	222
<b>Chapitre 16 – Configuration</b> . . . . .	225
16.1 Protection physique . . . . .	225
16.2 Protection des objets . . . . .	226
16.3 OS/2 et POSIX . . . . .	232
16.4 Suppression des données . . . . .	233
16.5 Sécurisation du réseau . . . . .	235
16.6 Partages . . . . .	241
16.7 Désactivation des services non nécessaires . . . . .	241
16.8 Minimisation de la visibilité réseau . . . . .	243
16.9 Gestion des utilisateurs . . . . .	248

16.10 Gestion des stratégies . . . . .	252
16.11 Restrictions d'accès . . . . .	254
16.12 Audit, gestion des logs . . . . .	263
<b>Chapitre 17 – Exploitation . . . . .</b>	<b>265</b>
17.1 Suivi de la configuration . . . . .	265
17.2 Gestion des utilisateurs . . . . .	265
17.3 Gestion des sauvegardes . . . . .	266
17.4 Gestion des logs . . . . .	266
17.5 Veille technologique et gestion des correctifs . . . . .	266
17.6 Tests de vulnérabilités . . . . .	267

### Annexes (téléchargeables sur le site [www.dunod.com](http://www.dunod.com))

#### A – Description du protocole NTLM

##### A.1 Protocole

##### A.2 Message « Negotiate »

##### A.3 Détail des options

##### A.4 Message « Challenge »

##### A.8 Détail des options

##### A.9 Message « Authenticate »

##### A.10 Ré-authentification

##### A.11 Algorithme de défi

##### A.12 Algorithme de réponse

#### B – Détail des certificats X.509 v3 et CRL v2

##### B.1 Norme X.509 v3

##### B.2 Extensions de certificat

##### B.3 Champs de base d'une CRL

##### B.4 Extensions d'entrée de CRL

##### B.5 Extensions de CRL

C – Différences de droits entre le groupe « Utilisateurs avec pouvoir »  
et le groupe « Utilisateurs »

D – Événements audités

E – Démarrage d'une machine

F – Détail de l'implémentation EFS

F.1 Chiffrement de fichier

F.2 Déchiffrement

Index . . . . . 269