



# SÉCURISATION D'UN SERVEUR WINDOWS 2000



**Patrick CHAMBET**

**Jean OLIVE**

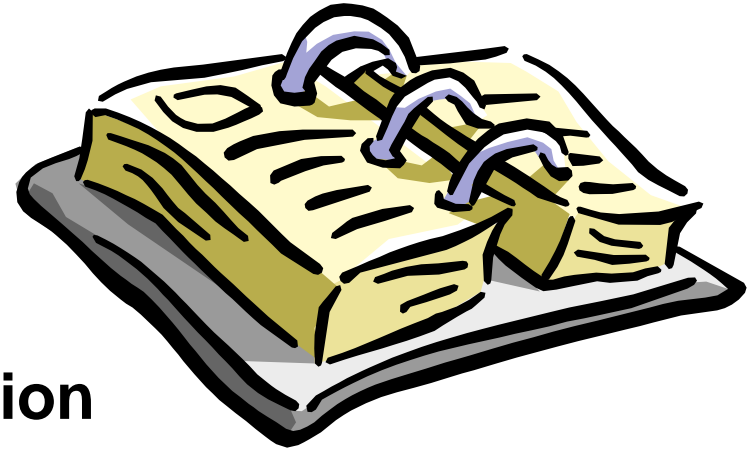
**EdelWeb**

[patrick.chambet@edelweb.fr](mailto:patrick.chambet@edelweb.fr)

[jean.olive@edelweb.fr](mailto:jean.olive@edelweb.fr)

<http://www.edelweb.fr>

- ✓ • Objectifs
- Comparatif avec NT 4.0
- Recommandations de sécurisation
  - Communes à NT 4.0
  - Nouvelles recommandations

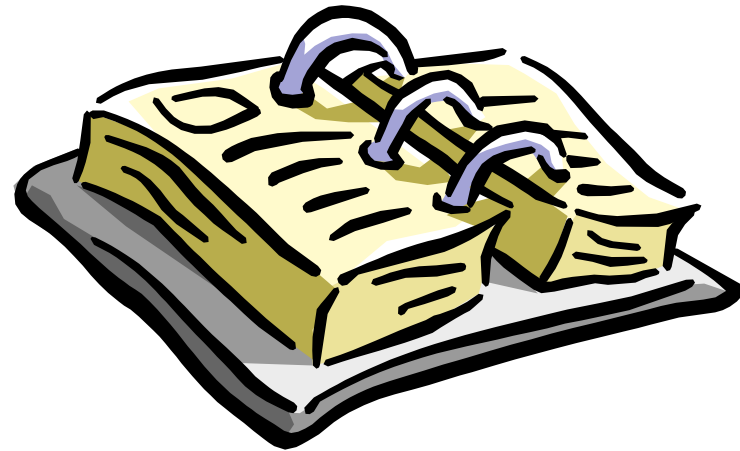




- **Etablir les principales recommandations pour sécuriser un réseau Windows 2000**
- **Présenter des cas pratiques à travers des démonstrations**
- **Présenter des retours d'expérience concernant la sécurisation de serveurs sous Windows 2000**
- **Conclure sur le niveau de sécurité de Windows 2000**



- Objectifs
- ✓ • Comparatif avec NT 4.0
- Recommandations
  - Communes à NT 4.0
  - Nouvelles recommandations



# Comparatif avec NT 4.0

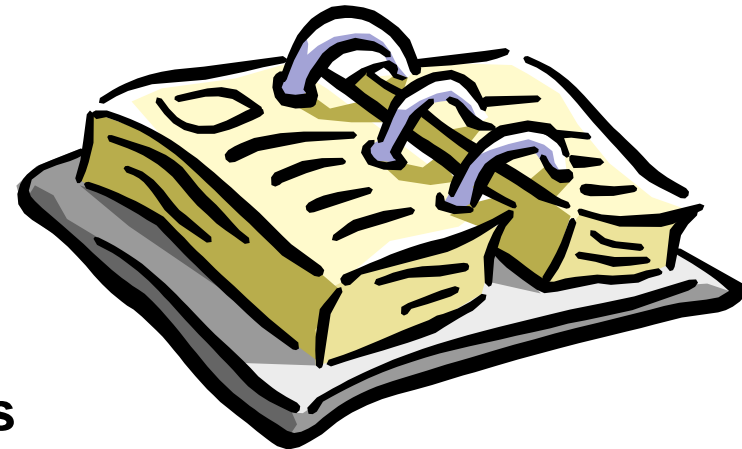


© EdelWeb 2000

<b>Lacunes de NT 4.0</b>	<b>Solutions de Windows 2000</b>
<b>(In)sécurité de NTFS</b>	<b>EFS</b>
<b>Pas de juste milieu entre simple utilisateur et administrateur</b>	<b>Utilisateurs avec pouvoir, délégation</b>
<b>Privilèges grossiers pour la délégation d'administration</b>	<b>Augmentation de la finesse des privilèges</b>
<b>Pour faire fonctionner certaines applications, les utilisateurs doivent disposer de droits étendus</b>	<b>Augmentation de la finesse des droits, délégation</b>
<b>Ecrasement des DLL système par des programmes d'installation</b>	<b>Windows File Protection (WFP)</b>
<b>Autres lacunes et vulnérabilités</b>	<b>Aucune solution</b>
	<b>Nouvelles vulnérabilités</b>



- Objectifs
- Comparatif avec NT 4.0
- ✓ • **Recommandations**
  - Communes à NT 4.0
  - Nouvelles recommandations

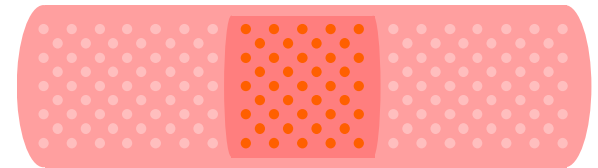


# Recommandations communes: Service Packs



© EdelWeb 2000

- **Appliquer les Service Packs et les Hot Fixes**
  - **Service Pack:**
    - Réunion de nombreux correctifs + nouvelles fonctionnalités
    - Dernière version : SP1
  - **Hot Fix:**
    - Ordre d'installation
    - Version française
    - <http://www.microsoft.com/windows2000/downloads/>
- **Il n'est plus nécessaire de repasser les SP après l'installation de nouvelles applications**

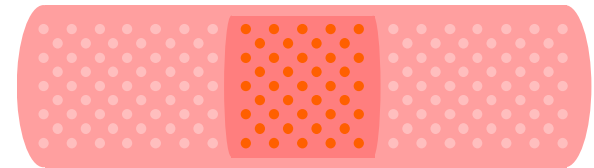


# Recommandations communes: Service Packs



© EdelWeb 2000

- **Le SP1 pour Windows 2000 corrige les vulnérabilités suivantes (pour mémoire):**
  - "Malformed Hit-Highlighting Argument"
  - "VM File Reading"
  - "Virtualized UNC Share"
  - "Desktop Separation"
  - "Malformed TCP/IP Print Request"
  - "Myriad Escaped Characters"
  - "Mixed Object Access"
  - "Malformed Environment Variable"
  - "IP Fragment Reassembly"
  - "Malformed Extension Data in URL"
  - "Undelimited .HTR Request" et "File Fragment Reading via .HTR"
  - "Protected Store Key Length"
  - "HTML Help File Code Execution"
  - "SSL Certificate Validation"
  - "Malformed E-mail Header"
  - "Persistent Mail-Browser Link"
  - "Cache Bypass"



# Recommandations communes: Sécurisation du poste local



© EdelWeb 2000

- Activer le mot de passe de démarrage du BIOS
- Activer le mot de passe de protection du BIOS
- Booter sur le disque dur en premier
- Désactiver les lecteurs de disquettes et de CD-ROM
- Ne pas faire de multi-boot
- Configurer le délai d'affichage du boot à zéro
- Désactiver la touche F8 au démarrage
- Risques:
  - Pas d'EFS sur les fichiers système (SAM, ...)
  - Virus
  - Vol de disque



# Recommandations communes: Compte Administrateur



© EdelWeb 2000

- Renommer le compte Administrateur
- Ajouter un compte leurre aux privilèges réduits
- Utiliser des mots de passe robustes
- Vulnérabilité:
  - Le compte Administrateur ne peut pas être verrouillé
  - Les seules politiques applicables au mot de passe sont :
    - Historique
    - Exigences de complexité
    - Durée de vie minimale / maximale
    - Longueur minimale

Démo

pwdump2.exe



# Recommandations communes: Sauvegardes



© EdelWeb 2000

- **limiter le nombre d'opérateurs de sauvegarde**
- **Séparer les privilèges d'archivage et de restauration**
- **Journaliser l'utilisation de ces privilèges**
  
- **Vulnérabilité:**
  - **Les opérateurs de sauvegarde peuvent outrepasser les restrictions de lecture et d'écriture sur les fichiers**
- **Contrainte :**
  - **La journalisation des privilèges génère un grand nombre d'évènements dans le journal de sécurité**



# Recommandations communes: Privilèges (1)



© EdelWeb 2000

- **limiter le nombre d'utilisateurs disposant du privilège « Accéder à cet ordinateur depuis le réseau »**
- **Vulnérabilité :**
  - Par défaut, ce droit est attribué au groupe "Tout le monde"
- **Contrainte :**
  - Chaque poste doit être paramétré



# Recommandations communes: Privilèges (2)



© EdelWeb 2000

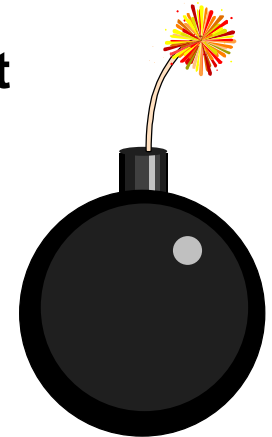
- **limiter le nombre d'utilisateurs disposant du privilège « Gérer le journal d'audit et de sécurité »**
- **Vulnérabilité:**
  - **Les trois privilèges de visualisation, d'effacement et d'ajout de règles d'audit ne sont pas dissociés**
- **Contrainte :**
  - **Néant**

# Recommandations communes: Permissions



© EdelWeb 2000

- **Limiter l'attribution de la permission « Modifier les permissions » sur les répertoires et fichiers système**
- **Vulnérabilité:**
  - **La permission « Aucun accès » à « Tout le monde » peut être appliquée au disque dur, ce qui rend le système inutilisable**
- **Contrainte:**
  - **Modification des permissions par défaut**



# Recommandations communes: Sécurisation des accès réseau



© EdelWeb 2000

- **Partages réseau**
  - Restreindre les permissions d'accès, les partages étant créés en accès complet par défaut
- **Désactiver les partages administratifs (C\$, D\$, ADMIN\$, ...) activés par défaut au démarrage**
  - Désactivation dans la base de registre ou par stratégie
  - Contraintes : certains services distants peuvent ne plus fonctionner



- **Installation**
- **Architecture du réseau**
- **Active Directory**
- **Gestion des utilisateurs**
- **Base de registre**
- **Système de fichiers**
- **Permissions**
- **Sécurisation des accès réseau**
- **Administration distante**
- **DNS, IIS 5.0, Index Server 2.0**
- **Outils: MMC, SCTS, ...**

# Recommandations : Installation



© EdelWeb 2000

- **Préférer une installation “fraîche” plutôt qu’une mise à jour depuis NT 4.0**
- **Isoler les machines pendant l’installation de Windows 2000**
  - **Partages administratifs temporairement sans mot de passe**
- **Changer les permissions sur le répertoire « All Users »**
  - **Vulnérabilité: l’installation de Windows 2000 avec les options « Unattended Install File » et « OEMPreinstall » laisse le répertoire « All Users » en accès complet**



# Recommandations : Architecture du réseau



© EdelWeb 2000

- **Attention aux domaines multiples:**
  - Trafic de réplication
  - Opération de suppression de domaines fils complexe
- **Structurer grâce aux OU et aux Sites**
- **Passer en mode natif dès que possible**
- **Supprimer les clients pré-Windows 2000**



# Coexistence NT 4.0 / Windows 2000



© EdelWeb 2000

PDC	BDC	Clients	
NT 4.0	NT 4.0	Tous (9x/ME, NT, 2000)	Pas d'Active Directory
NT 4.0	2000		Impossible
2000	NT 4.0		Authentification Kerberos ou NTLM Réplication NTLM avec les BDC Application des OU et des GP sur les clients 2000
2000 (mode mixte)			Réplication multimaîtres
2000 (mode natif)			Groupes de sécurité universels et imbrication des groupes



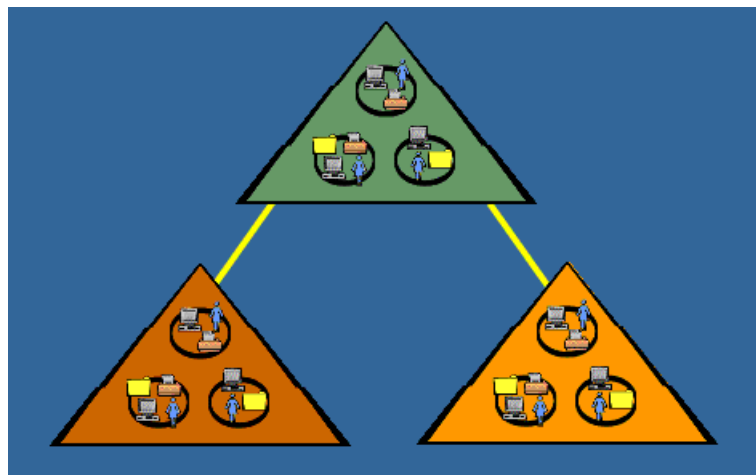
**Le maintien d'un parc de clients de générations antérieures (Win 9x/ME et NT 4.0) ne permet pas d'obtenir un niveau de sécurité suffisant.**

# Recommandations : Active Directory



© EdelWeb 2000

- Accorder les autorisations d'accès aux groupes
- Accorder des autorisations aux OU le plus possible
- Utiliser l'héritage pour les stratégies de groupes
- Surveiller les membres du groupe Enterprise Administrators
- Attention à la définition des droits sur les attributs
- Attention à la réplication
  - Volume
  - Sécurité des échanges

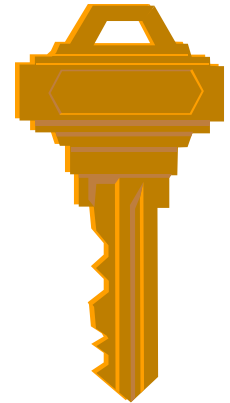


# Recommandations : Gestion des utilisateurs



© EdelWeb 2000

- **Stratégie «A G DL P» (idem NT 4.0):**
  - (A G) Affecter des utilisateurs à des groupes globaux
  - (DL) Inclure des groupes globaux dans des groupes locaux au domaine
  - (P) Accorder les permissions aux groupes locaux
- **Nouvelles recommandations:**
  - Utiliser les groupes et les OU (plutôt que les utilisateurs individuels)
  - Utiliser les groupes de distribution autant que possible
  - Définir des droits explicites (autoriser *ou* refuser)
  - Limiter l'appartenance individuelle aux groupes universels
  - Utiliser les stratégies de groupe
  - Attention à l'héritage des permissions
  - Attention à l'ordre d'application des permissions



# Recommandations :

## Base de registre



© EdelWeb 2000

- **Sécuriser les permissions aux clefs sensibles (cf checklists)**
- **Les permissions par défaut sont plus sécurisées que sous NT 4.0**
- **RDISK /s n'existe plus (plus de AT possible)**
- **Pour créer une Emergency Repair Disk, on utilise l'utilitaire de Backup (NTBackup.exe) et toujours le répertoire `\WINNT\repair...`**

# Recommandations: Système de fichiers



© EdelWeb 2000

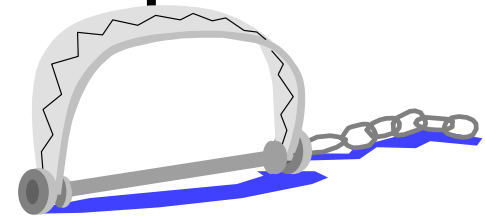
- **Ne pas utiliser le système FAT**
- **Utiliser NTFS 5**
- **Utiliser EFS**
  - **Supprimer l'agent de récupération local**
  - **Exporter le certificat de l'agent de récupération d'entreprise**
  - **EFS ne remplace pas les permissions d'accès**
  - **EFS ne protège pas contre la destruction**
  - **Une copie applicative n'est pas cryptée**
- **Attention à l'héritage des permissions**

# Recommandations: Permissions (1)



© EdelWeb 2000

- Utiliser les permissions avancées pour interdire explicitement la suppression
- Utiliser l'héritage des permissions du répertoire parent
- Vulnérabilité:
  - La permission « Supprimer » n'est pas retirée lorsque aucune permission n'est accordée sur un fichier



Démo



# Recommandations: Permissions (2)



© EdelWeb 2000

- **Paramétrer correctement les permissions sur les fichiers de la racine du disque ainsi que de \WINNT et de ses sous-répertoires (cf checklists)**
- **Vulnérabilité:**
  - **Le cryptage de Autoexec.bat empêche tout logon sur le serveur**

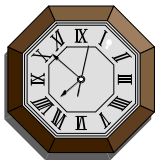


# Recommandations : Sécurisation des accès réseau (1)



© EdelWeb 2000

- **Authentification**
  - Désactiver le logon en clair (clients SAMBA)
  - Désactiver LM
  - Utiliser au minimum NTLM v2
  - Désactiver les protocoles inutiles (NetBEUI, ...)
  - Les horloges des serveurs doivent être synchronisées à 5 minutes près (authentification Kerberos)
- **Services: désactiver les services inutilisés**
  - NetBIOS
  - IIS
  - RIS / TFTP
  - Windows Media Player
  - ...



# Recommandations :

## Sécurisation des accès réseau (2)



© EdelWeb 2000

- **Supprimer NTLM sur un réseau en mode natif (homogène Windows 2000)**
- **IPSEC**
  - Les versions export utilisent DES lorsque 3DES est demandé
  - Ceci peut entraîner des problèmes d'interopérabilité
  - **Correctif : High Encryption Pack:**  
<http://www.microsoft.com/windows2000/downloads/.../recommended/encryption/default.asp>

Démo





## **Objectif : limiter le recours au compte administrateur local.**

- **Chaque machine Windows 2000 du domaine peut être gérée à distance:**
  - Journaux
  - Informations système
  - Partages
  - Périphériques
  - Utilisateurs et groupes locaux
  - Stockage (partitions, défragmentation)
  - Services
- **Fonctions d'installation**
  - Packages MSI et MST
  - Publication d'applications dans Active Directory
  - Assignation d'applications
- **Certaines applications (IE, ...) peuvent être paramétrées par les GPO**
- **Fonction "RunAs"**
- **Windows Terminal Server: prise de contrôle des clients à distance**



- **Surveiller les groupes**
  - DnsAdmins
  - DnsUpdateProxy
  
- **Vulnérabilité**
  - Windows 2000 accepte des réponses DNS de serveurs non sollicités
  - **Correctif :**  
`\HKLM\SYSTEM\CurrentControlSet\Services\...`  
`...\DNSCache\Parameters\QueryIPMatching = 1`

# Recommandations: IIS 5.0



© EdelWeb 2000

- **Utiliser les outils de configuration de la sécurité:**
  - IIS 5.0 Hotfix Checking Tool
  - IIS 5.0 Security Configuration Tool
- **Limiter le nombre de Gestionnaires de site Web dans IIS**
- **Vulnérabilité:**
  - **Mots de passe des comptes IUSR\_MachineName et IWAM\_MachineName visibles en clair dans la métabase d'IIS 4.0 et 5.0**



**Démo**

# Recommandations: Index Server 2.0



© EdelWeb 2000

- Démarré par défaut
- Restreindre les types de fichiers à indexer (.htm, .txt et .doc seulement par exemple)
- Restreindre les répertoires à indexer
- Vulnérabilité:
  - Tout fichier indexé d'un serveur Web peut devenir visible après une recherche effectuée judicieusement

# Outils: Microsoft Management Console (MMC)



© EdelWeb 2000

- **Fonctionnalités**
  - Interface d'administration unique pour tous les outils
  - Hautement configurable
    - Composants logiciels disponibles
    - Champ d'application de ces composants
    - Possibilités de modification de la configuration ou non
    - Mode auteur / mode utilisateur
  - Extensible par des « snap-ins »
  - Une configuration peut être stockée dans un fichier .msc
- **Usages**
  - Administration du système
  - Création de consoles personnalisées pour des administrateurs délégués

**Démo**



# Outils: Security Configuration Tool Set (SCTS)



© EdelWeb 2000

- «Snap-in» pour la MMC
- Apparu avec le SP4 de NT 4.0
- Permet de:
  - Définir
  - Appliquer
  - Vérifier l'application d'un modèle de sécurité
  - Personnalisé
  - Prédéfini
- Sont couverts :
  - Les stratégies de sécurité
  - Les droits des utilisateurs
  - La composition des groupes
  - Les ACL des objets
  - Les services système

**Démo**





- **Outil de nettoyage de disque (cleanmgr)**
  - Supprime les fichiers temporaires
  - Vide la corbeille
  - Enlève les composants inutilisés
- `C:\Documents and Settings\User`
  - Profils
  - Dossier TEMP
  - Documents récents
  - Corbeille
  - Certificats
- **Commande RunAs**
  - Permet de lancer un process dans un autre contexte de sécurité



# Recommandations: En résumé



© EdelWeb 2000

- **Administration**
  - Déléguer
  - Surveiller le compte Administrateur d'Entreprise
  - Renommer le compte Administrateur local
- Activer les options de sécurité dans les stratégies
- Utiliser les stratégies d'audit
- Utiliser EFS pour vraiment maîtriser l'accès aux fichiers
- Utiliser le SCTS (avec planification: AT)



# Conclusion



© EdelWeb 2000

- **Windows 2000 représente un saut important en matière de sécurité**
- **La sécurité a été prise en compte très en amont**
- **Mais encore peu de retours d'expérience de déploiement à grande échelle**





- **Microsoft :**

- **Windows 2000**

- <http://www.microsoft.com/windows2000/>

- **Sécurité**

- <http://www.microsoft.com/security/>

- **Knowledge Base**

- <http://search.support.microsoft.com/kb/>

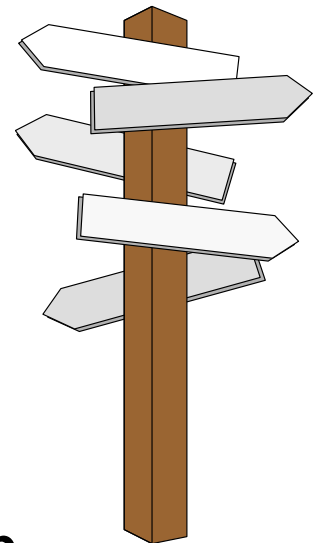
- **Security bulletins**

- <http://www.microsoft.com/technet/security/current.asp>

- **Mises à jour**

- <http://www.microsoft.com/windows2000/downloads/critical>

- <http://www.microsoft.com/windows2000/downloads/recommended>





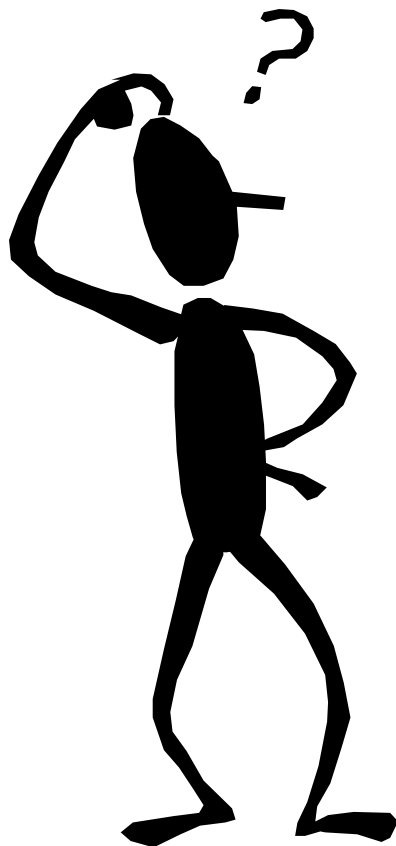
- **Bugtraq, NTBugtraq, Security Focus**
  - <http://www.securityfocus.com/>
- **SANS (System Administration, Networking and Security)**
  - <http://www.sans.org/>
- **Windows 2000 Magazine Security News**
  - <http://www.ntsecurity.net/>
- **Security Portal**
  - <http://www.securityportal.com/>



# Questions



© EdelWeb 2000





# Jusqu'où sécuriserez-vous aujourd'hui ?

