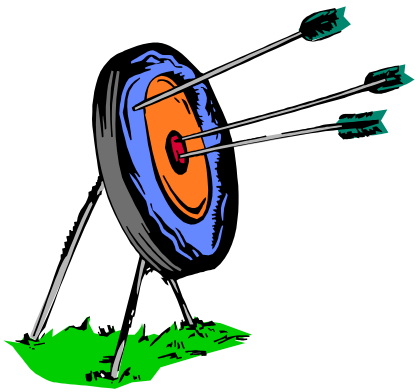
le salon de
la sécurité informatique
FRANCE
21-22 NOVEMBRE 2000
CNIT-PARIS La Défense

SÉCURISATION D'UN RÉSEAU EXPLOITÉ SOUS WINDOWS 2000

Microsoft Windows 2000

Patrick CHAMBET patrick.chambet@edelweb.fr
Jean OLIVE jean.olive@edelweb.fr
EdelWeb http://www.edelweb.fr

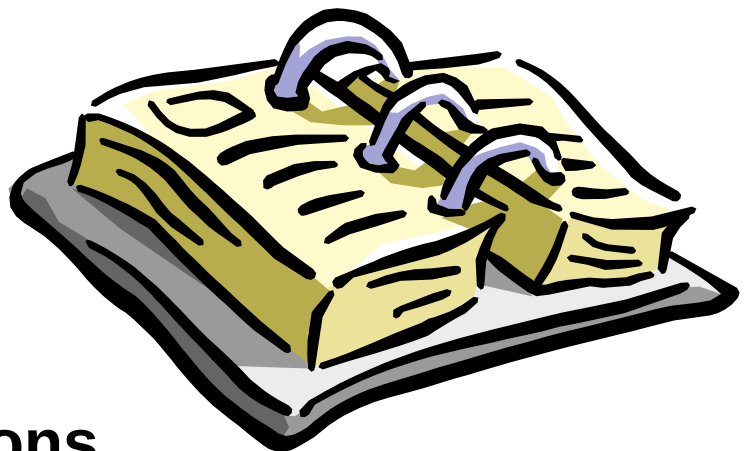
OBJECTIFS



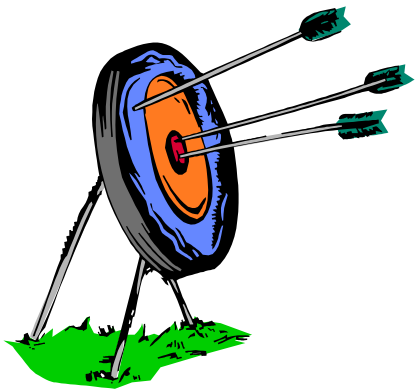
- Identifier les principaux écueils de la sécurisation d'un réseau sous Windows 2000
- Parcourir la boîte à outils de sécurité de Windows 2000
- Présenter une démarche globale
  - ✓ Pourquoi ?
  - ✓ Les grandes lignes
  - ✓ Les résultats
- Proposer / montrer quelques mesures de sécurisation

ORDRE DU JOUR

- Le pôle sécurité Windows 2000
- Les apports de Windows 2000 sur le plan de sécurité
- Les écueils
- Une démarche de sécurisation
- Les principales recommandations



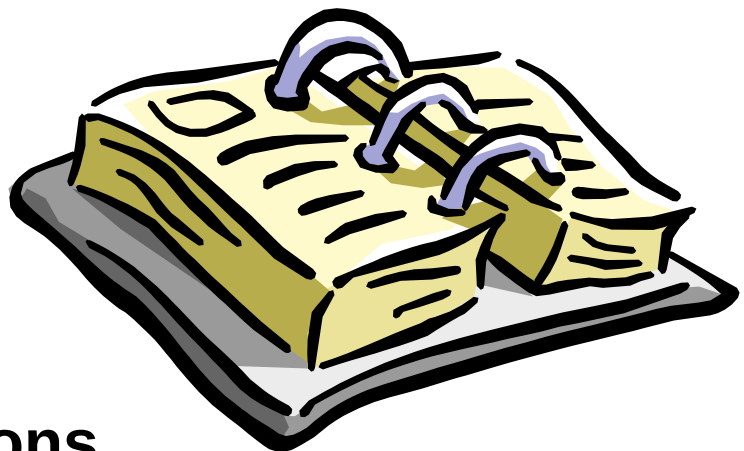
POLE SECURITE WINDOWS 2000



- La sécurité Windows 2000, pourquoi ?
- Constitution d'un pôle spécifique
  - ✓ Une équipe de 4 experts depuis 6 mois
  - ✓ Développement / études / …
- Résultats
  - ✓ Des formations sécurité Windows 2000
  - ✓ Des « EdelFiles »
  - ✓ Une méthode
  - ✓ Des revues / qualifications de vulnérabilités et des tests de parades

ORDRE DU JOUR

- Le pôle sécurité Windows 2000
- Les apports de Windows 2000 sur le plan de sécurité
- Les écueils
- Une démarche de sécurisation
- Les principales recommandations



APPORTS DE WINDOWS 2000

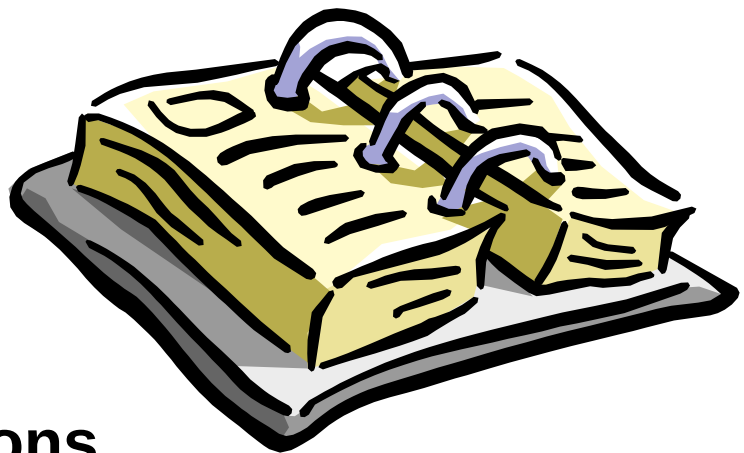
Principales lacunes de NT 4.0	Solutions de Windows 2000
Aucune protection contre le vol d'information	EFS
Options de sécurité répartis sur plusieurs outils et difficile à déployer	Stratégies de sécurité
Manque de granularité des privilèges d'administration	ACL sur les objets et leurs propriétés Unité Organisationnelle
Écrasement des DLL système par des programmes d'installation	Windows File Protection (WFP)
Lacunes	Solutions partielles
Bogues et vulnérabilités	Communes / Nouvelles / Peu de retour du terrain
Majorité des services ne fonctionnant qu'avec des privilèges étendus	Aucune solution

APPORTS DE WINDOWS 2000

- **Mais également :**
  - ✓ **Gestion centralisée des ressources et des services**
  - ✓ **Structure logique décorrélée de la structure physique**
    - ⇨ **Active Directory**
  - ✓ **Nouveaux objets**
  - ✓ **Nouveaux outils**
  - ✓ **Nouveaux protocoles**
    - **Kerberos v5**
    - **IPSEC, PPTP, …**
  - ✓ **PKI**
  - ✓ **Support des SmartCards**

ORDRE DU JOUR

- Le pôle sécurité Windows 2000
- Les apports de Windows 2000 sur le plan de sécurité
- Les écueils
- Une démarche de sécurisation
- Les principales recommandations

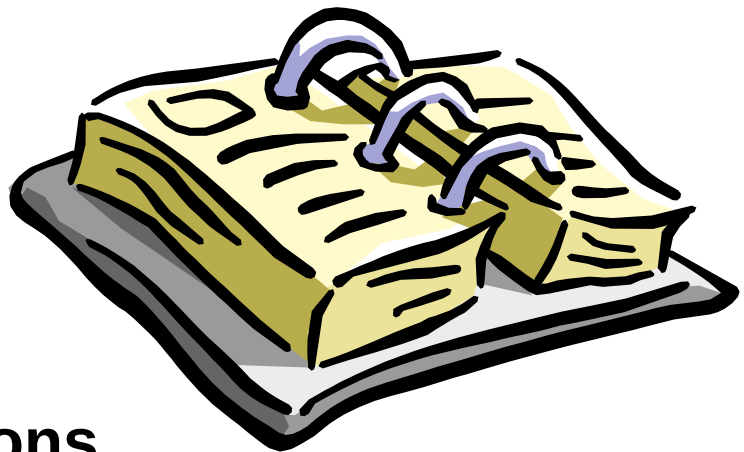


LES PRINCIPAUX ECUEILS

- **Choisir face à la richesse fonctionnelle**
  - ✓ NTLM / Kerberos / PKI
  - ✓ NTFS / EFS
  - ✓ Active Directory
  - ✓ …
- **Migration**
  - ✓ Architecture du système d'information
  - ✓ Applications
- **Eviter les vulnérabilités**
  - ✓ Système encore neuf
  - ✓ Exemples …

ORDRE DU JOUR

- Le pôle sécurité Windows 2000
- Les apports de Windows 2000 sur le plan de sécurité
- Les écueils
- Une démarche de sécurisation
- Les principales recommandations



LA DEMARCHE : POURQUOI ?

- **L'installation de Windows 2000 nécessite des choix d'architecture irréversibles**
  - ✓ Identifier les éléments structurants
  - ✓ Proposer les grandes orientations et identifier les impacts
- **Windows 2000 présente des vulnérabilités, des lacunes, des dangers**
  - ✓ Identifier et qualifier les vulnérabilités connues
  - ✓ Couvrir l'ensemble des vulnérabilités pertinentes pour l'entreprise
  - ✓ Assurer un suivi et une veille technologique permanente
- **Windows 2000 supporte des systèmes d'information**
  - ✓ Mettre en place une politique de sécurité globale du réseau de l'entreprise sous Windows 2000
  - ✓ Définir un niveau minimum de sécurité non dérogeable
  - ✓ Proposer des compléments pour répondre à des besoins renforcés

LES GRANDES LIGNES DE LA DEMARCHE

- **OBJ 1 : Couvrir les risques de sécurité du réseau cible en utilisant des éléments méthodologiques reconnus et réutilisables (CC)**
- **OBJ 2 : Adapter les mesures aux besoins**
- **OBJ 3 : Définir une organisation de la sécurité Windows 2000 cohérente et globale**

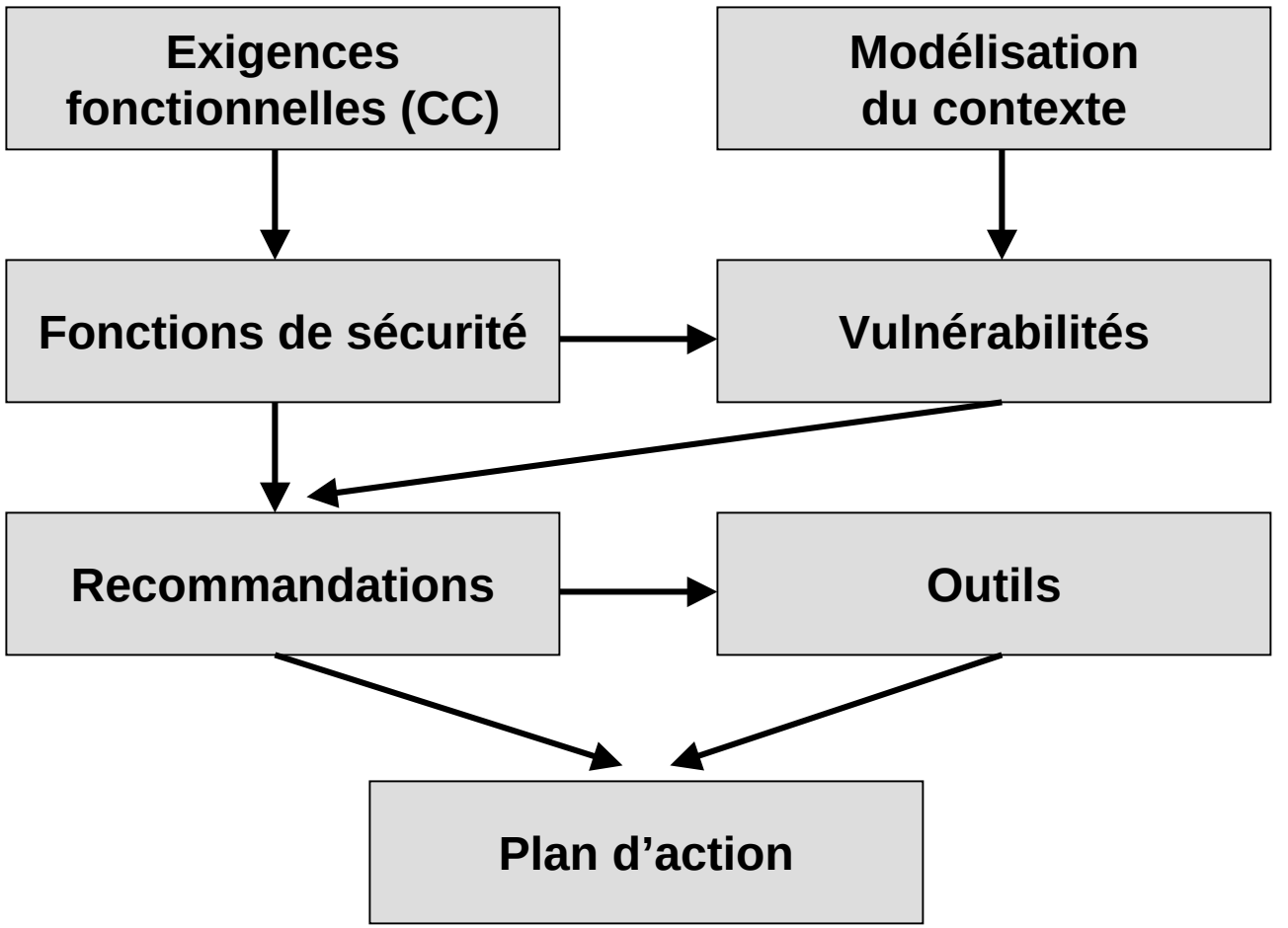
- **OBJ 4 : Disposer d'un cadre de référence pour mettre en place l'ensemble des services de sécurité**
- **OBJ 5 : Avoir un référentiel de suivi de la sécurité**

UN GUIDE DE SECURISATION

- **Les référentiels actualisés quotidiennement**
  - ✓ **La modélisation du contexte**
  - ✓ **Les exigences fonctionnelles des Critères Communs**
  - ✓ **Les fonctionnalités de sécurité de Windows 2000 et leurs consignes de mise en œuvre**
  - ✓ **Les vulnérabilités et limites des fonctions de sécurité**
  - ✓ **Les recommandations et parades**
  - ✓ **Les outils**

UN GUIDE DE SECURISATION

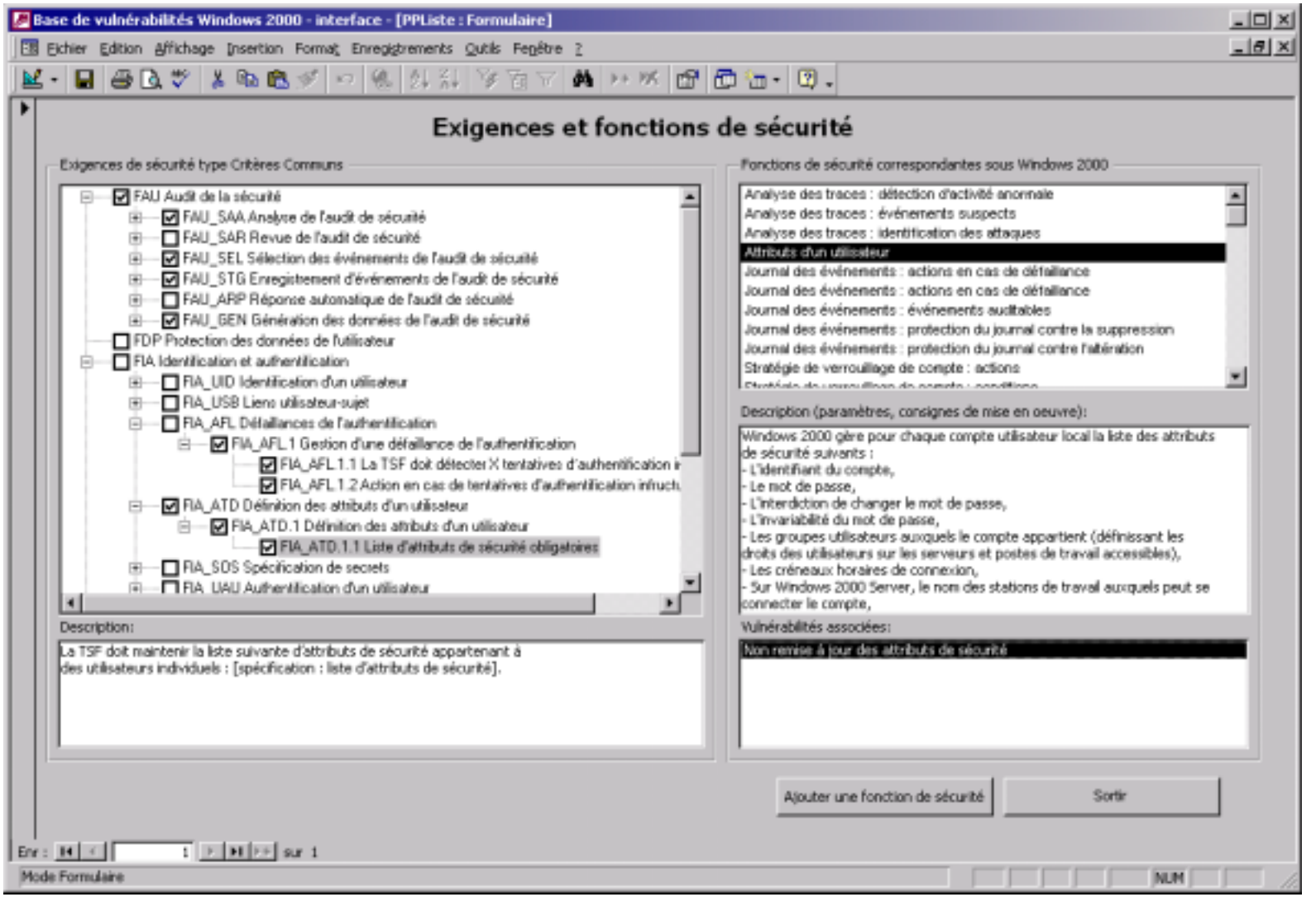
➢ La méthode:



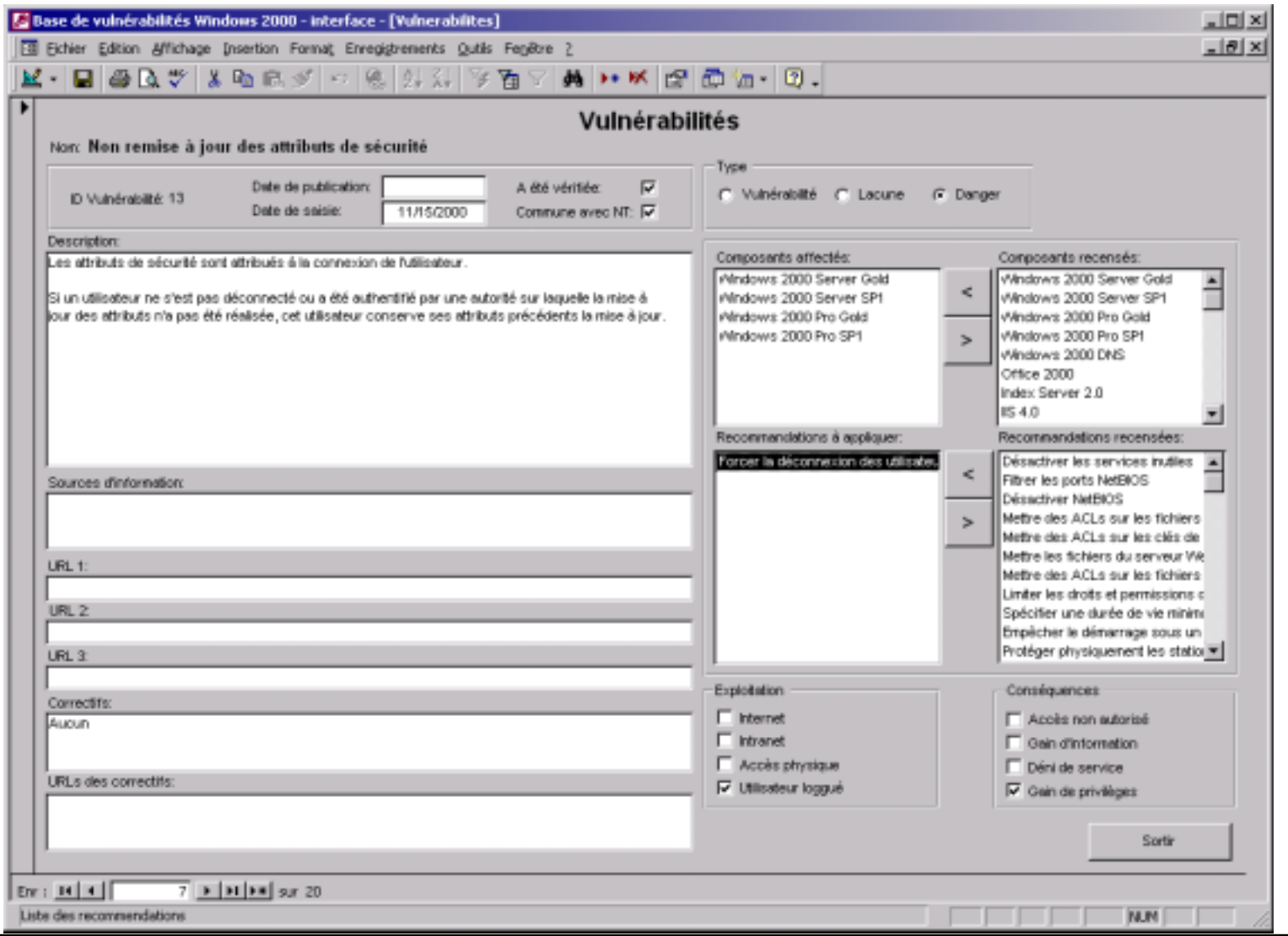
LA DEMARCHE : LES RESULTATS

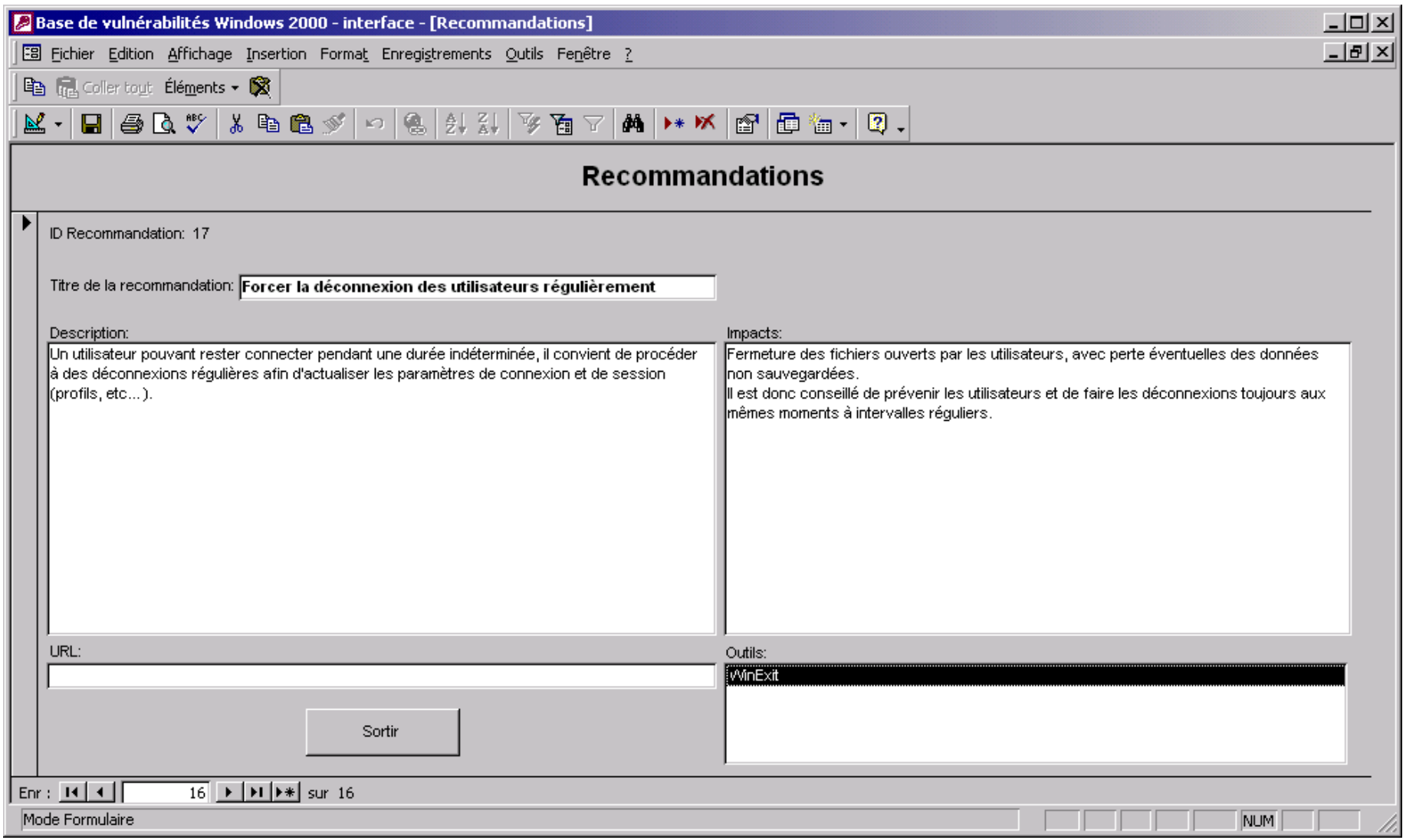
Démo

LE GUIDE DE SECURISATION DE WINDOWS 2000



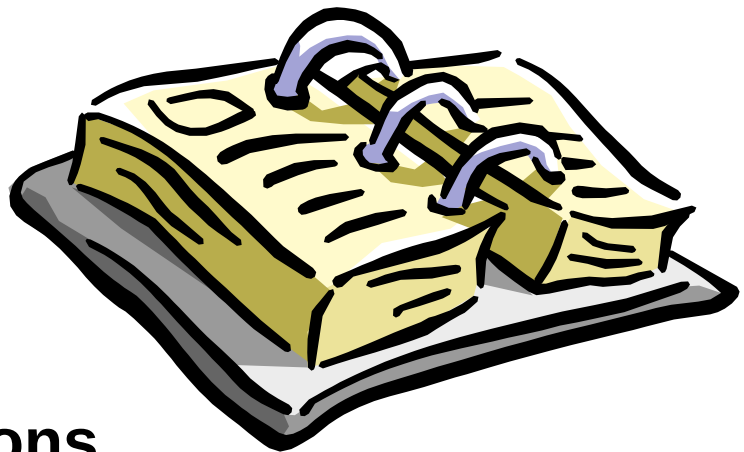
LE GUIDE DE SECURISATION DE WINDOWS 2000




Base de vulnérabilités Windows 2000 - interface - [Recommandations]
Fichier Edition Affichage Insertion Format Enregistrements Outils Fenêtre ?
Coller tout Éléments
Recommandations
ID Recommandation: 17
Titre de la recommandation: Forcer la déconnexion des utilisateurs régulièrement
Description:
Un utilisateur pouvant rester connecter pendant une durée indéterminée, il convient de procéder à des déconnexions régulières afin d'actualiser les paramètres de connexion et de session (profils, etc...).
Impacts:
Fermeture des fichiers ouverts par les utilisateurs, avec perte éventuelles des données non sauvegardées.
Il est donc conseillé de prévenir les utilisateurs et de faire les déconnexions toujours aux mêmes moments à intervalles réguliers.
URL:
Outils:
WinExit
Sortir
Enr : 16 sur 16
Mode Formulaire
NUM

ORDRE DU JOUR

- Le pôle sécurité Windows 2000
- Les apports de Windows 2000 sur le plan de sécurité
- Les écueils
- Une démarche de sécurisation
- Les principales recommandations



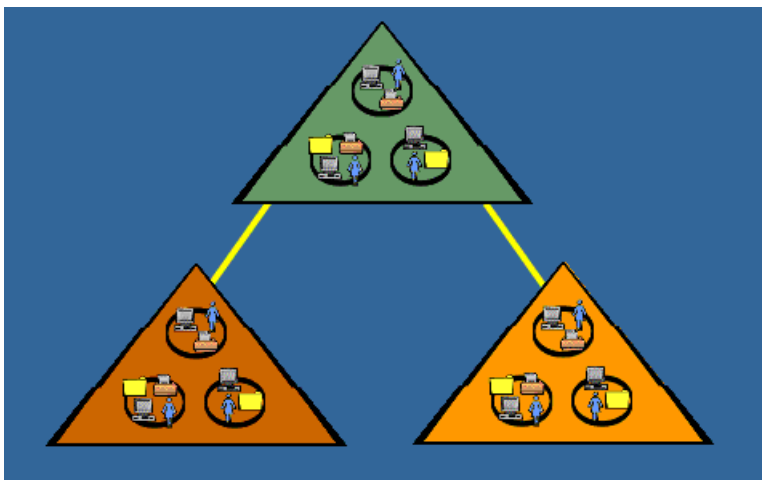
Recommandations : Architecture du réseau

- **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 si possible**
- **Supprimer les clients pré-Windows 2000**

Recommandations : Active Directory

- 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

- 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

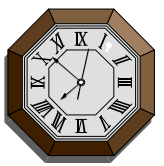
- Sécuriser les permissions aux clefs sensibles (cf checklists)
- Les permissions par défaut sont plus sécurisées que sous NT 4.0
- `RDISK /s` n'existe plus (plus de `AT` possible)
- Pour créer une Emergency Repair Disk, on utilise l'utilitaire de Backup (`NTBackup.exe`) et toujours le répertoire `\WINNT\repair`...

Recommandations: Système de fichiers

- 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 : Sécurisation des accès réseau (1)

- **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)



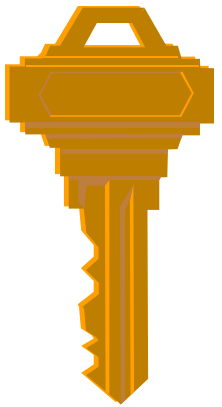
- **Services: désactiver les services inutilisés**
  - ✓ NetBIOS
  - ✓ IIS
  - ✓ RIS / TFTP
  - ✓ Windows Media Player
  - ✓ …

Recommandations : Sécurisation des accès réseau (2)

- **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`**

Recommandations: En résumé

- Déléguer l'administration
- Activer les options de sécurité dans les stratégies
- Utiliser les stratégies d'audit
- Utiliser EFS pour vraiment maîtriser l'accès aux fichiers



CONCLUSION

- **Nous obtenons un résultat concret: un niveau de sécurité élevé correspondant à vos besoins avec Windows 2000.**

- **Edelweb est prêt pour vous assister dans votre migration et dans tout projet évoluant autour de la plate-forme Windows 2000 au sein du système d'information de votre entreprise.**

QUESTIONS