Configuration de sécurité de base de Windows 2000 et Windows XP

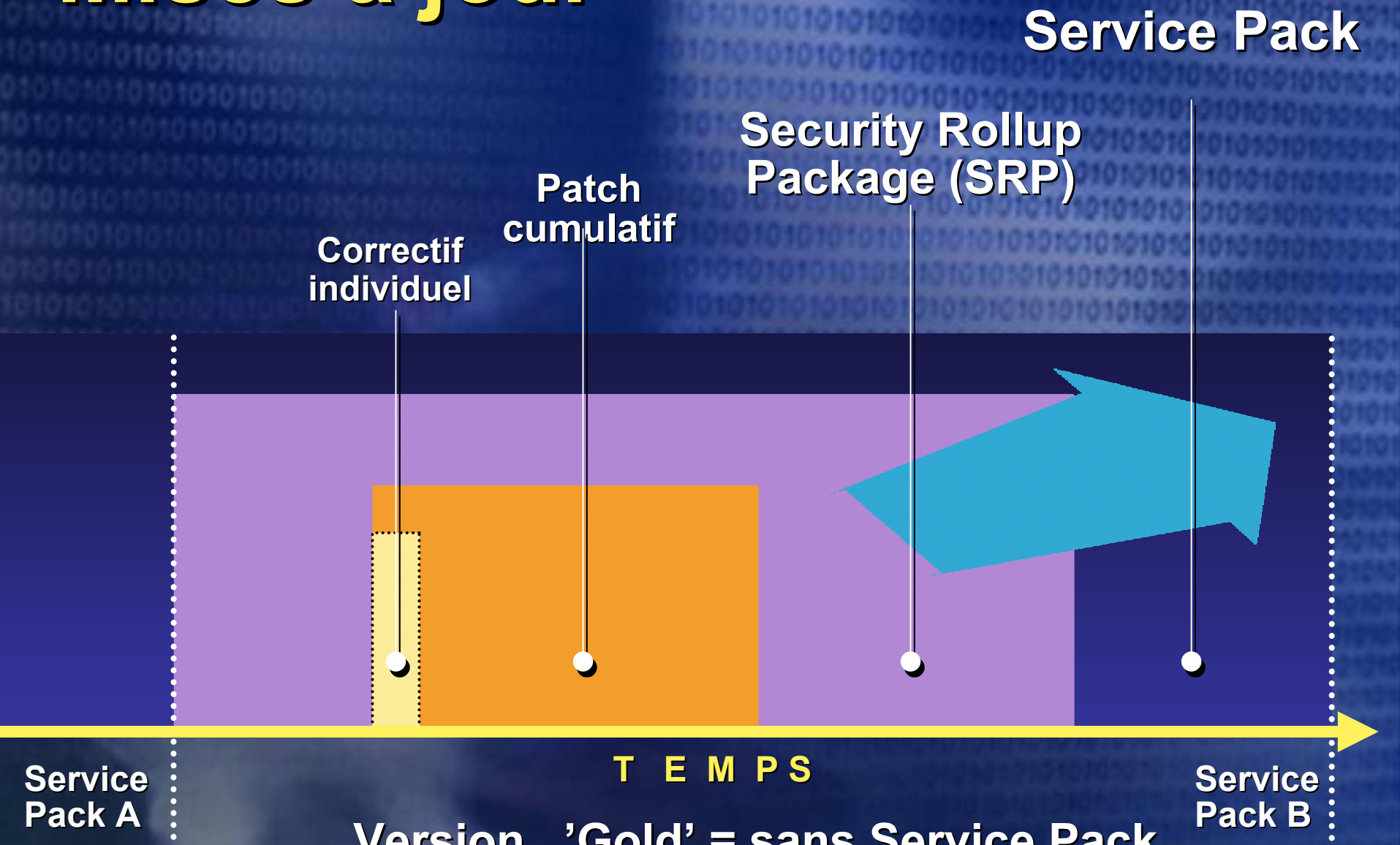
Cyril Voisin
Microsoft France

http://www.microsoft.com/security

Introduction

- Trustworthy Computing
- Programme de sécurité *Strategic Technology Protection Program (Get Secure, Stay Secure)*
- Sécurité =
  - Personnes
  - Processus
  - Technologies
- Sécurité de base
  - Logiciels avec toutes les mises à jour de sécurité
  - Configuration adéquate
  - Attitude

Mises à jour



Version ’Gold’ = sans Service Pack

Possibilité d’installation intégrée

hfnetchk

- Outil en ligne de commande d'inventaire des correctifs de sécurité manquants
  - pour Windows NT 4, Windows 2000, IIS4/5, Windows XP, IE 5.01+ et SQL Server 7/2000
- Fonctionnement
  - Importe la liste des correctifs de sécurité (base XML)
    - Brute : http://www.microsoft.com/technet/security/search/mssecure.xml
    - Compressée : http://download.microsoft.com/download/xml/security/1.0/NT5/EN-US/mssecure.cab
  - Vérifie que les clés de registre ont été installées
  - Vérifie pour chaque correctif que tous les fichiers sont présents
  - Vérifie le numéro de version de chaque fichier et les sommes de vérification
- Pour chaque correctif manquant, indique le bulletin de sécurité et la fiche technique correspondants
  - ex: MS01-044 et Q301625
- Pour aller plus loin :
  - http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/hfnetchk.asp
  - Q303215 et Q305385
  - Exemple de batch d'utilisation dans le Security Operations Guide

qchain

- Permet l'installation de plusieurs correctifs à la fois avec un seul redémarrage (limite l'indisponibilité des machines)
- Fonctionnement
  - Lancer les installations des correctifs nécessitant un redémarrage avec l'option empêchant le redémarrage (-z)
  - Lancer qchain
  - Redémarrer
- Inutile pour Windows XP qui inclut déjà un mécanisme de gestion des versions de mises à jour simultanées
- http://support.microsoft.com/support/kb/articles/Q296/8/61.asp

Notification de mise à jour critique

- Recherche automatique de correctifs de sécurité importants sur Windows Update
- Possibilité de notifier ou de télécharger et installer
- Disponible en téléchargement pour Windows 2000 (fourni avec Windows XP)

- Pour recevoir les bulletins directement par messagerie dès leur publication (en anglais) : souscrivez au service de notification d'alertes de sécurité par messagerie en envoyant un message quelconque à securbas@microsoft.com

Autres outils de sécurité

- Snap-in Modèles de sécurité
- Snap-in Configuration et analyse de la sécurité
- Extension Paramètres de sécurité dans l'éditeur de stratégie de groupe
- Outil de ligne de commande secedit.exe

- En français, snap-in = composant logiciel enfichable

Stratégies de groupe

- Spécifient des options pour des machines et utilisateurs gérés
- Ceci inclut des paramètres de clés de registres, des paramètres de sécurité, etc…
- Assignées grâce à Active Directory (ou locales mais plus limitées)
- Ordre d'application : Locale, Site, Domaine, OU
- Les réglages machines l'emportent sur les réglages utilisateurs

Paramètrage commun

Pour le détail des paramètres à appliquer, consulter le Security ToolKit

- Tous les disques en NTFS
- Mot de passe fort pour l'Administrateur
- Désactivation des services inutiles
- Désactiver ou supprimer les comptes inutiles
- Protéger les fichiers et les répertoires
- Vérifier que le compte Invité est désactivé
- Protéger le registre contre l'accès anonyme
- Limiter l'accès aux informations publiques sur l'autorité de sécurité locale (LSA)
  - Restrict Anonymous = 2
  - attention aux contrôleurs de domaine

Paramétrage commun

- Stratégie de mot de passe forts (`passfilt.dll`)
- Stratégie de verrouillage de compte
- Configurer le compte Administrateur
- Supprimer les partages de fichiers inutiles
- Permissions sur les partages
- Antivirus et mises à jour (non fourni)
- Parefeu (intégré dans XP)
- Service Pack et correctifs ultérieurs
- SYSKEY de niveau supérieur
- Mettre à jour Internet Explorer
- Activer l'audit (considérer l'utilisation d'un IDS)

Modèles de stratégies de groupe

- A adapter au cas par cas
- Dans l'OS
  - securews.inf
  - secureDC.inf
  - hisecws.inf
  - hisecDC.inf, …
- En téléchargement
  - hisecweb.inf
- Dans le Security Operations Guide
  - baseline.inf
  - baselineDC.inf
  - File and Print Incremental.inf
  - IIS incremental.inf
  - Infrastructure Incremental.inf

Windows 2000 Server

- Installation silencieuse avec IIS désactivé (voir unattend.txt dans le Security ToolKit)

```
[Components]
    fp_extensions=Off iis_common=Off
    iisdbg = off
    iis_doc=Off
    iis_ftp=Off
    iis_htmla=Off
    iis_inetmgr=Off
    iis_nntp=Off
    iis_nntp_docs=Off
    iis_pwmgr=Off
    iis_smtp=Off
    iis_smtp_docs=Off
    iis_www_vdir_msadc=Off iis_www_vdir_printers=Off
    iis_www_vdir_scripts=Off
    iis_www_vdir_terminalservices=Off
    iis_www=Off
```

- NoLMHash : pour ne pas stocker les hashes au format LAN Manager
- Après l'ajout d'un nouveau service, ne pas oublier d'installer les mises à jour de sécurité nécessaires

IIS 5

- Réduction de la surface d'attaque
  - Supprimer les exemples d'applications
    - IISSamples
    - IISHelp
    - MSADC
  - Supprimer le répertoire virtuel IISADMPWD
    - Si serveur mis à jour depuis IIS4/NT4
  - Supprimer les mappages de scripts inutilisés
    - .htr, .idc, .stm, .shtm, .shtml, .printer, .htw, .ida, .idq
  - Au niveau de l'OS, désactiver NetBIOS (onglet WINS des paramètres TCP/IP avancés)

IIS 5

- Durcissement de la configuration
  - Permissions sur les répertoires virtuels.
    - Exemple :
      - Tous types de fichiers : contrôle total (F) pour Administrateurs et Système
      - Contenu statique (pages, images): lecture (R) pour Tout le monde
      - Scripts, CGI, include : exécution (X) pour Tout le monde
    - Astuce : créer un répertoire par type de fichiers et y appliquer les permissions
    - Remplacer les permissions sur `C:\inetpub\ftproot` (serveur FTP) et `C:\inetpub\mailroot` (serveur SMTP) ou déplacer ces répertoires sur un volume différent de celui d'IIS ou utiliser les quotas
  - Permissions sur les fichiers de journaux IIS (`%systemroot%\system32\LogFiles`)
    - Administrateurs et Système : contrôle total (F)
    - Tout le monde : lecture, écriture, création

IIS 5

- Activation de la journalisation
  - Adresse IP du client
  - Nom d'utilisateur
  - Méthode
  - Ressource URI
  - État HTTP
  - État Win32
  - Agent utilisateur
  - (Adresse IP du serveur)
  - (Port du serveur)
- Contenu sur une partition différente que celle du système
- Authentification

IIS 5

- Modèle de sécurité `hisecweb.inf` (http://download.microsoft.com/download/win2000srv/SCM/1.0/NT5/EN-US/hisecweb.exe)
  - Copier le modèle dans `%windir%\security\templates`.
  - Ouvrir le snap-in Modèles de sécurité, et regarder les réglages
  - Ouvrir le Snap-in Configuration et analyse de la sécurité, et charger le modèle.
  - Choisir Analyser la machine maintenant dans le menu contextuel.
  - Le travail s'exécute.
  - Regarder le résultat, et mettre à jour le modèle si nécessaire.
  - Une fois que le modèle vous convient, choisir, choisir Configurer la machine maintenant dans le menu contextuel.
- Filtrage IPSec pour déterminer les connections autorisées et les machines sources
- Liste des autorités de confiance racines (*root CA*)

IIS 5

- N'exécuter que du code digne de confiance
  - Vérifiez le code de vos applications maison et éditeurs ! (cf Writing Secure Code)
    - Pages ASP, filtres ISAPI
    - Ex : Attention aux entrées dans les formulaires ou Querystring (Injection SQL par ex.); valider les entrées, utiliser des expressions régulières, chercher si tout est accepté plutôt que la présence de quelque chose à rejeter
    - Ex : `dumpbin /imports MyISAPI.dll | find "RevertToSelf"`
  - Désenregistrement des composants COM inutiles
- Désactiver l'accès aux répertoires parents (..\)
- Désactiver l'adresse IP dans l'entête Content-Location (Q218180)

IIS Lockdown et URLScan

- Asssistant de verrouillage simplifiant la sécurisation d'IIS en :
  - Durcissant la configuration
  - Éliminant les services inutiles
  - Mettant des permissions sur les commandes système
- Rôles de serveur : plusieurs modèles sont fournis pour les applications Microsoft dépendant d'IIS:
  - Exchange Server 5.5 et 2000, Commerce Server, BizTalk,SharePoint Portal Server, FrontPage Server Extensions, SharePoint Team Server…

IIS Lockdown et URLScan

- Possibilité de supprimer ou de désactiver les services d'IIS comme HTTP, FTP, SMTP et NNTP
- Installation par script possible (fichier de réponses)
- Téléchargement
  - http://www.microsoft.com/technet/security/tools/locktool.asp
- URLscan
  - Analyse toutes les requêtes arrivant sur le serveur IIS (filtre ISAPI)
  - En fonction du paramétrage, les requêtes jugées dangereuses sont rejetées systématiquement
    - voir `%windir%\system32\inetsrv\urlscan\urlscan.ini`
    - Verbe, extension, encodage d'URL, caractères non ASCII, séquence de caractères particulières, entête
- URLScan est intégré à IIS lockdown 2.1, avec des modèles personnalisés pour chaque rôle de serveur

Windows 2000 Pro / XP Pro

- Déploiement de correctifs possible par SMS (exemples de scripts fournis dans le Security Toolkit)
- Outils d'évaluation de machines de référence ou de machines individuelles :
  - Windows Update
    - Permet le téléchargement par visite du site des mises à jour critiques manquantes (attention à prendre en compte un possible temps de latence)
    - http://windowsupdate.microsoft.com
  - Personal Security Advisor
    - Outil Web pour évaluer la configuration de la machine qui s'y connecte
    - http://www.microsoft.com/technet/mpsa/start.asp
- Firewall personnel (XP seulement)
  - À activer sur chacune des connexion réseau à protéger

Personal Security Advisor

- L'analyse du poste porte sur les points suivants :
  - Correctifs de sécurité
  - Mots de passe
  - Configuration d'IE et d'Outlook Express
  - Configuration des Macros Office
  - Pour chaque faille de sécurité détectée MPSA fournit une explication et la méthode pour corriger cette faiblesse
- Liste des points contrôlés : voir annexe

Code hostile

- Stratégies de restriction logicielle (Windows XP seulement)
  - Permet d'indiquer explicitement ce qui peut être exécuté / ce qui ne peut pas l'être
  - Indication de
    - Chemin (ex : `%windir%\system32\dllcache`, répertoire des attachements du logiciel de messagerie) et types de fichiers (extensions)
    - Hash (SHA-1 et MD5)
    - Certificat (Scripts et package Windows Installer, pas pour les .dll et .exe)
    - Zone Internet (package Windows Installer)
  - Ne remplace pas un logiciel antivirus !

Outils actuellement en beta

- Baseline Security Advisor
  - Outil pour l'évaluation de machines sur un réseau (correctifs manquants, éléments de paramétrage)
  - Semblable à Personal Security Advisor mais support des serveurs et utilisable à distance
- Windows Update Corporate Edition
  - Serveur Windows Update d'Intranet
  - Choix des correctifs à publier par les administrateurs
  - Client Windows Update paramétrable par stratégie de groupe (Automatic Update)

Références

- *Security Operations Guide for Windows 2000 Server*
  http://www.microsoft.com/technet/security/prodtech/windows2000serv/staysecure/default.asp
- **Documentation du Security Tool Kit :**
  http://www.microsoft.com/technet/security/tools/stkintro.asp
  - http://www.microsoft.com/technet/security/tools/w2ksvrcl.asp
  - http://www.microsoft.com/technet/security/tools/iis5chk.asp
- *Designing Secure Web-Based Applications for Microsoft Windows 2000*
  MS Press, ISBN: 0735609950
- *Writing Secure Code*
  MS Press, ISBN 0-7356-1588-8
  http://www.microsoft.com/mspress/books/5612.asp

Questions ?

Annexes

Installation intégrée

- Directement en Service Pack + Security Rollup Package + mises à jour de sécurité ultérieures (*slipstreaming*)
- Voir le Guide d'installation et de déploiement du Service Pack de Microsoft® Windows® 2000
  - Copie des fichiers d'installation normaux (`xcopy D:\i386 E:\Win2000\i386 /e`)
  - Extraction des fichiers d'install (`W2ksp2.exe /x`) dans un répertoire (`c:\rep` par ex.)
  - Application à la source d'installation (`c:\rep\i386\Update\Update.exe -s:E:\Win2000`)
- Q311401 : SRP1 pour Windows 2000 SP2

Résultat de HFNetChk

```
* WINDOWS 2000 ADVANCED SERVER SP2

Patch NOT Found MS00-077          Q299796
Patch NOT Found MS00-079          Q276471
Patch NOT Found MS01-007          Q285851
Patch NOT Found MS01-013          Q285156
Patch NOT Found MS01-052          Q307454

* Internet Information Services 5.0

Patch NOT Found MS01-025          Q296185
Patch NOT Found MS01-044          Q301625

* Internet Explorer 5.01 SP2

Patch NOT Found MS01-027          Q295106
Patch NOT Found MS01-051          Q306121
```

Article Technique

Bulletin de sécurité

Script qchain (exemple)

```
@echo off
setlocal
set CHEMINMAJ=C:\MAJ
%CHEMINMAJ%\Q123456_w2k_sp3_x86_fr.exe -z -m
%CHEMINMAJ%\Qxyzabc_w2k_sp3_x86_fr.exe -z -m
%CHEMINMAJ%\qchain.exe
```

Editeur de sécurité (secedit)

- Outil pour la plupart des tâches d'administration de la sécurité
- Peut être utilisé pour analyser la configuration de sécurité d'une machine donnée par rapport à un référentiel
- Les options en ligne de commande permettent de créer des scripts qui comprennent des options de configuration ou d'analyse de la sécurité

Editeur de sécurité

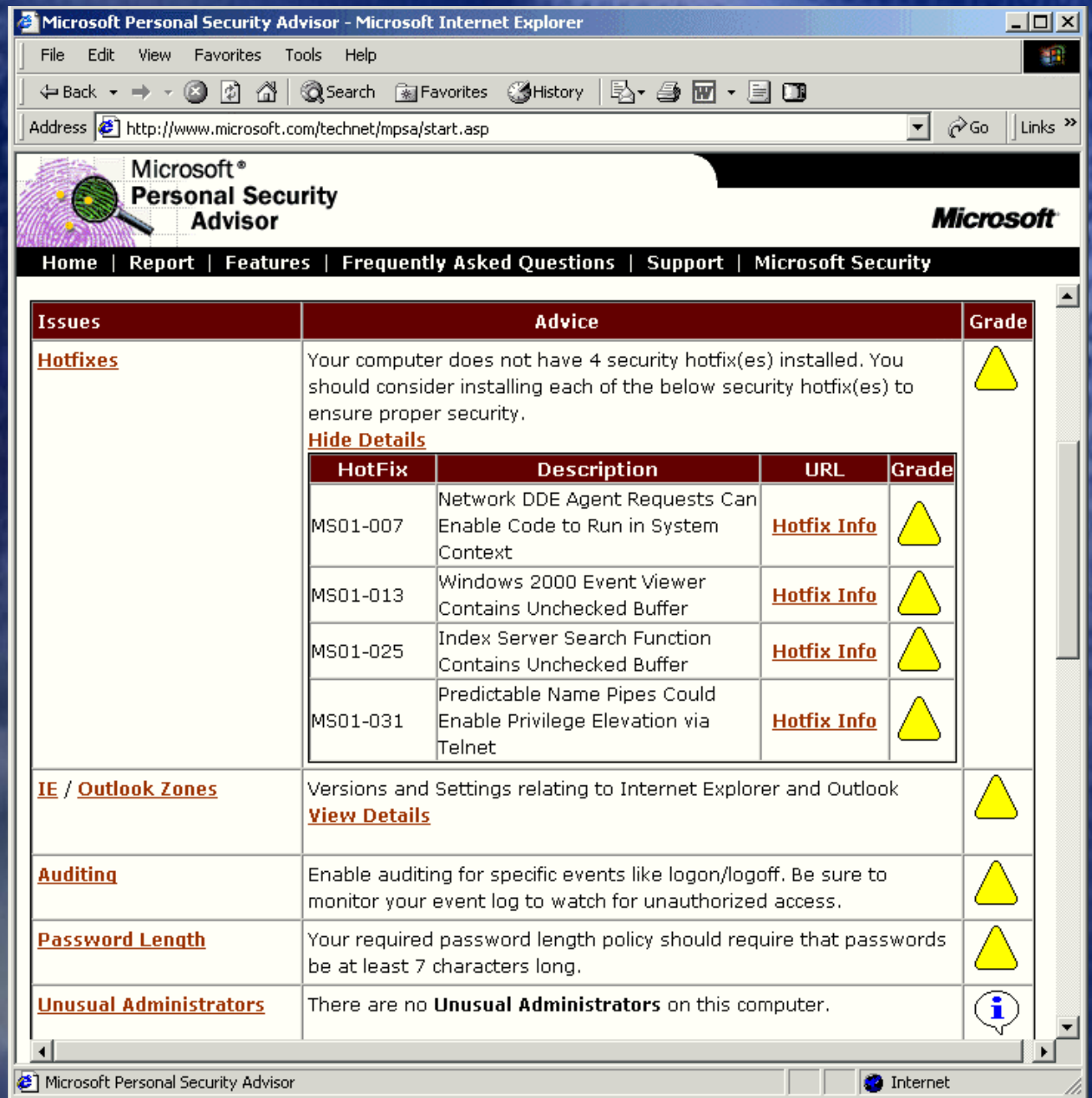
- Permet de configurer et d'analyser les paramètres suivants :
  - Account Policies
  - Local Policies
  - Event Logs
  - Restricted Groups (admin, backup)
  - System Services
  - System Registry
  - File System Store
- Exemple pour configurer la sécurité du système de fichiers :
  - Aller dans `%systemroot%\security\database`
  - Taper `secedit /configure /db MySecure.sdb /areas FILESTORE /log %systemroot%\security\logs\MySecure.log /verbose`
  - Puis `%systemroot%\security\logs\MySecure.log`

Personal Security Advisor

Liste des points contrôlés :

. Mots de passe
. Service Packs et correctifs
. Auditing Windows 2000 Events
. Secured File Systems
. Accès Anonymes
. Comptes Administrateurs inhabituels
. Zones de Sécurité Internet Explorer
. Longueur du mot de passe Windows 2000 / NT
. Comptes de Services
. RASMAN
. Auditing Windows NT Events
. Auto Logon
. Dossiers partagés
. Outlook Security Zone
. Macro Virus dans Office

Microsoft Personal Security Advisor



Serveurs Windows .NET

- Surface d'attaque réduite
  - Installation par défaut plus sécurisée (IIS non installé par ex.)
  - IIS verrouillé à l'installation (fichiers statiques)
- Code source (PREfix! Et PREfast! : outils d'analyse automatisés enrichis régulièrement des dernières découvertes; cf *Buffer Overuns*)
- Nouveaux comptes avec des niveaux de privilège moins élevés
- Notion de rôles

- Pas seulement des fonctionnalités de sécurité mais des fonctionnalités sécurisées

Autres outils

- Filever
  - En local …

```
I:\Program Files\Support Tools>filever
    %systemroot%\system32\lsass.exe
--a-- W32i   DLL ENU   5.0.2195.2964 shp
    33,552 05-04-2001 lsass.exe
```

  - Ou à distance, avec un nom UNC …

```
I:\Program Files\Support Tools>filever
    \\mcla002ad\d$\winnt\system32\lsass.exe
--a-- W32i   DLL ENU   5.0.2195.4301 shp
    33,552 09-06-2001 lsass.exe
```