Etat des lieux de la sécurité dans Windows XP

Améliorations et écueils

Nicolas RUFF

nicolas.ruff@edelweb.fr

Ordre du jour

- Authentification
- Réseau
- Stratégies de groupe
- Fichiers
- Noyau
- Support
- Autres

- Cible de la présentation : Windows XP Pro 32 bits

Authentification

- **Restrictions d'ouverture de session**
  - Les comptes locaux sans mot de passe ne peuvent pas ouvrir de session distante (ex. administrateur local)
    - Corrige la vulnérabilité « pas de mot de passe sur les partages administratifs jusqu'au premier redémarrage »
    - S'applique aussi à Remote Desktop
    - Clé « LimitBlankPasswordUse »
  - Accès anonymes : une configuration par défaut à peine plus robuste
    - EveryoneIncludesAnonymous = 0
    - RestrictAnonymous = 0
    - RestrictAnonymousSAM = 1
- **Gestion des mots de passe**
  - Intégration de l'authentification « Passport »
  - « Credential Manager »
    - Les mots de passe saisis par l'utilisateur peuvent être mémorisés
    - Répertoire %profile%\Application Data\Microsoft\Credentials\<SID>\Credentials
  - Disquette de « password recovery »
    - Permet la réinitialisation d'un compte local dont le mot de passe est perdu

Réseau (1/2)

- **ICS (Internet Connexion Sharing)**
- **ICF (Internet Connexion Firewall)**
  - Protége contre les accès entrants uniquement
  - Fonctions disponibles
    - Filtrage de port (RDP, IMAP4, IMAP3, POP3, SMTP, FTP, Telnet, HTTP, HTTPS
    - Filtrage ICMP par commande
    - Journalisation des paquets bloqués et entrants
  - Ne remplace pas les Firewalls personnels
    - Ne protège pas contre les chevaux de Troie
- **Support Wireless**
  - Support des protocoles 802.11 & 802.1X
  - Services de configuration automatique (à désactiver)
  - Avec 802.1X, support de l'authentification EAP par certificat (utilisateur ou machine)
- **Windows XP supporte les deux types de partages**
  - Partages « simplifiés » (à la 9x/ME) : contrôle d'accès par mot de passe
    - Gestion des mots de passe difficile
    - Pas de compromission de comptes de domaine si le mot de passe doit être stocké en clair dans une application ou attaqué par force brute
  - Partages NT/2K : contrôle d'accès par utilisateur

Réseau (2/2)

- **Serveur Web IIS 5.1 (option)**
  - Suite à Code Red sur Windows 2000 Server …
- **Des accès Internet permanents …**
  - Windows Product Activation (WPA)
  - Mises à jour automatiques
    - à l'installation
    - en exploitation par WindowsUpdate
  - Rapports d'erreur (système et applications)
  - Fonction « rechercher », aide en ligne, etc.
  - Fonction « cette version de Windows est-elle légale ? »
  - Applications : MSN Messenger, Windows Media
    - « Supercookie » dans Windows Media
    - Les identifiants de tous les DVD lus avec Windows Media sont envoyés chez Microsoft

Stratégies de groupe

- **Stratégies de groupe**
  - Plus de 300 nouveaux paramètres
  - Peuvent être importés dans Windows 2000 à la place des modèles existants
    - Fichiers \WINDOWS\System32\GroupPolicy\Adm*.adm
  - Options de sécurité beaucoup plus nombreuses
    - Ex. Désactiver le stockage du hash LM
  - Outil RSOP (Resultant Set Of Policy)
    - GPRESULT /Z
- **Restrictions d'exécution pour les applications**
  - Par signature digitale & contrôle d'intégrité
    - Attention : pas de vérification de cohérence entre signature et nom de fichier (« bug » déjà présent dans Windows 2000)
  - Selon la zone d'exécution (Internet, Intranet)
  - Selon le chemin d'accès à la ressource

Fichiers

- **Amélioration de la protection des exécutables**
  - « Side-by-side DLLs »
    - L'éditeur doit fournir un « manifest » au format XML des DLLs utilisées
    - Stocké dans le répertoire \WINDOWS\WinSxS
    - Ce système sera-t-il utilisé par les éditeurs ?
    - Rappel : depuis Windows 2000, si il existe un fichier « APP.EXE.LOCAL » dans le répertoire de l'application « APP », alors les DLLs sont recherchées dans le répertoire courant avant la Registry
  - « System Restore »
    - Effectue des points de sauvegarde périodique des fichiers système (~ 1 jour)
    - Répertoire « System Volume Information » sur chaque disque – inaccessible même à l'administrateur
    - Utilise environ 10% du lecteur
  - « Device Driver Rollback »
    - Il est possible de revenir à la version antérieure des drivers
    - Fichier « driver rollback.inf »
- **EFS : des améliorations fonctionnelles**
  - Chiffrement multi-utilisateurs
  - Possibilité de chiffrement des « Offline Folders »

Noyau

- **Services**
  - 3 comptes de service
    - SYSTEM (NT AUTHORITY\SYSTEM
    - SERVICE LOCAL (NT AUTHORITY\LocalService)
    - SERVICE RESEAU (NT AUTHORITY\NetworkService)
  - Ce deux derniers ont un mot de passe de 15 caractères géré par le système
    - Le hash LM n'est pas stocké
  - Privilèges
    - Changer les quotas de mémoire d'un processus
    - Générer des audit de sécurité
    - Ouvrir une session en tant que service (service réseau uniquement)
    - Remplacer un jeton de niveau processus
- **Les pages mémoire du noyau sont en lecture seule**

Support

- **Support**
  - RemoteAssistance
    - Un compte HelpAssistant « caché », membre d'aucun groupe
    - Le mot de passe de ce compte est dans « LSA Secrets »
    - En cas de demande d'assistance, un jeton d'accès est créé
      - Durée de validité indépendante de son utilisation
      - Contient adresse IP et port en clair
      - Falsifiable (nom présenté par l'utilisateur en clair)
      - Utilisable par n'importe qui
      - Contient le mot de passe HelpAssistant sous forme brouillée
    - Ce jeton doit impérativement être protégé par mot de passe !
    - Connexion dans la session de l'utilisateur par Terminal Server
    - Deux modes : visualisation / interactif
  - RemoteDesktop
    - Un Terminal Server Personnel basé sur RDP 5.1 (port TCP/3389)
    - Mêmes risques et mêmes options de configuration que Terminal Server

Autres

- **« Fast User Switching »**
  - Basé sur une technologie Terminal Server
  - Non disponible sur les machines jointes à un domaine
- **« Forgotten Password »**
  - L'utilisateur peut fournir un « indice » pour retrouver son mot de passe
  - Il est possible de créer une disquette de réinitialisation de mot de passe à usage unique
- **« Universal Plug&Play »**
  - Découverte automatique des nouveaux périphériques réseau
  - Utilise des extensions HTTP (mini serveur Web)
  - Ports TCP/2869 et UDP/1900
  - A désactiver !
- **« Raw sockets »**
  - Est-ce vraiment un problème de sécurité ?

Conclusion

- **Windows XP : de nouveaux risques réels**
  - Beaucoup de nouvelles fonctions peu sécurisées et actives par défaut
    - Ex. UPNP, Media Player 8
  - Des accès Internet fréquents et non maîtrisés par l'utilisateur

- **Windows XP : des avantages indéniables en matière de sécurité**
  - Plus « finalisé » que Windows 2000
    - Ex. EFS multi-utilisateurs
  - Nouvelles fonctions de sécurité et d'administration intéressantes
    - Ex. refus de connexion pour les comptes sans mot de passe

Annexe

- **Bibliographie**
  - Microsoft
    - http://www.microsoft.com/windowsxp/
    - http://www.microsoft.com/security/
  - Confidentialité Windows Media
    - http://www.computerbytesman.com/privacy/supercookie.htm
    - http://www.computerbytesman.com/privacy/wmp8dvd.htm
  - L'affaire Gibson et les « Raw Sockets »
    - http://grc.com/dos/intro.htm
  - WPA
    - http://www.licenturion.com/xp/
- **Outils**
  - Windows XP Powertoys
    - En cours de développement