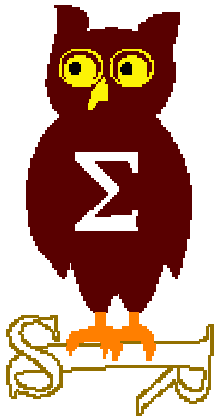
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 8 octobre 2001



EdelWeb

Revue des dernières vulnérabilités de Windows 2000

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités

- Avis de sécurité Microsoft depuis le 10/09/2001 :
  - MS01-048 : Déni de service RPC (NT4 uniquement)
  - MS01-049 : Déni de service sur OWA par une requête malformée
- Code Blue / Code Green
  - Vers anti-« Code Red »
- Virus W32/Nimda
  - Nombreuses méthodes de propagation
    - Virus de messagerie
    - Partages réseau
    - Ver IIS
    - Navigation sur site Web compromis
    - Recherche les backdoors Code Red
  - Pas de charge destructive
- Virus W32/Vote

EdelWeb

Rédaction d'un guide de sécurisation Windows 2000

Groupe Sécurité Windows

Préambule (1/2)

EdelWeb

- Validation de l'objectif et de la démarche
- Calendrier
- Modalités de travail

Préambule (2/2)

EdelWeb

- Guides de référence
  - « Hardening Windows 2000 »
  - NSA
- Présentation
  - Risque(s) couvert(s)
  - Action(s) à entreprendre
  - Impact(s)
- Rôles
  - Poste de travail
  - Serveur de fichier / d'impression
  - Contrôleur de domaine

Plan du guide (1/2)

- **Plan du guide**
  - Recommandations générales
    - Installation
    - Sécurité physique
    - Modes dégradés
    - Administration de la sécurité et suivi des correctifs
  - Base de registre
    - Gestion des droits
    - Clés sensibles
  - Système de fichiers
    - Gestion des droits
    - Audit
    - Fichiers et commandes sensibles
    - Sauvegarde et restauration

Plan du guide (2/2)

- Stratégies de sécurité
  - Comptes
  - Droits
  - Audit
- Services démarrés
- Accès réseau
  - Authentification
  - Accès anonymes
  - Configuration des protocoles (NetBIOS, TCP/IP, Autres)
- Options diverses
  - Verrouillage de session
  - Options de sécurité
- Active Directory (DC uniquement)
  - Sécurité de l'annuaire
  - Délégation d'administration
  - Stratégies de groupe

Annexes optionnelles

EdelWeb

- **Fonctions de sécurité**
  - EFS
  - IPSEC
  - Terminal Serveur (en mode administration)
- **Serveurs particuliers**
  - DNS
  - Accès distants
  - DHCP
  - WINS
  - RIS
  - Certificate Server
- **Applications courantes**
  - IIS 5
  - Exchange 2000

Partie 1 : généralités (1/2)

- **Installation**
  - Ne pas faire de mise à jour depuis Windows NT4 et/ou FAT
    - Sinon appliquer le modèle « Setup Security » (SCE)
  - Installer sur un système de fichiers NTFS
  - Ne pas faire de multi-boot
  - Isoler la machine du réseau lors de l'installation
    - Risque(s) : partages administratifs, intrusion avant application des correctifs
- **Sécurité physique**
  - Démarrer uniquement sur disque dur
  - Désactiver les fonctions APM (clavier / réseau)
  - Protéger la configuration du BIOS par mot de passe
  - Contrôler les accès physiques (serveurs uniquement)

Partie 1 : généralités (2/2)

EdelWeb

- **Modes dégradés**
  - Installer la Recovery Console (serveurs uniquement)
  - Protéger le mode « Restauration des services d'annuaire » par mot de passe (serveurs uniquement)
- **Administration de la sécurité**
  - S'abonner à la liste de diffusion des alertes Microsoft
  - Évaluer le besoin et l'impact des correctifs (dans un environnement hors production)
  - Nommer au moins deux administrateurs par système
  - Les administrateurs doivent disposer d'un compte utilisateur non privilégié et utiliser au maximum la fonction RunAs
  - Exploiter les journaux d'audit
  - *La délégation d'administration est traitée dans le chapitre « Active Directory »*

Questions / réponses

EdelWeb

- Thèmes proposés pour la prochaine réunion :
  - Suite de la présentation IP par HSC
  - Authentification forte (biométrie – produit KeyWare)
- Date :
  12 novembre 2001
- Questions / réponses