# OSSIR – 11 mars 2002
# Génération, analyse et exploitation des traces sous Windows 2000

**Par Nicolas RUFF**

**nicolas.ruff@edelweb.fr**

# Objectifs

- **Exposer brièvement les principes de « l'audit » sous Windows NT/2000/XP**
  - Comprendre ce qu'il est possible de faire ou non
- **Mettre en place une stratégie d'audit pertinente**
  - Ne pas générer de données inexploitables
- **Etre capable d'exploiter les traces de sécurité**
  - Ne pas générer de données inexploitables
- **Connaître les limites de l'audit**
  - Mettre en œuvre des mesures complémentaires

➢ ***L'audit est vu ici comme la fonction de génération et d'exploitation des traces de sécurité***

# L’audit : pourquoi ?

- **Elément fondamental de toute politique de sécurité**
- **Pourquoi ?**
  - Détection - en temps réel (si les outils utilisés le permette) - d’événements d’origine malveillante
  - Investigation a posteriori (explication et recherche de l’origine)

  Mais aussi :
  - Dépannage
  - Constitution de preuves (ex. sur injonction judiciaire)

- **Comment ?**
  - Des principes présentés ci-après
  - Chaque réseau est un cas particulier !

- **Cibles de l’audit**
  - Contrôleurs de domaine
    - La cible de sécurité principale, car le DC gère les comptes, les groupes et l’authentification
  - Serveurs
    - Chaque serveur applicatif doit être traité à part (événements et journaux spécifiques)
  - Postes de travail
    - La télécollecte et le volume de données est problématique

***Dans la suite de cette présentation, la cible est le journal sécurité sur le DC***

# 1. Fonctionnement de l'audit (1/3)

- **Règles de la stratégie d'audit**
  - L'audit peut être activé/désactivé globalement
  - Eléments individuels de la stratégie
    - Gestion des comptes
    - Accès au service d'annuaire [Active Directory]
    - Accès aux objets*
    - Suivi de processus
    - Connexion [stocké au lieu de connexion]
    - Connexion aux comptes [stocké au lieu d'authentification]
    - Système
    - Modifications de stratégie [audit, IPSEC, Kerberos, EFS, QoS, domaine]
    - Utilisation des privilèges

    ** L'audit doit ensuite être activé sur chaque objet*
  - La stratégie d'audit est stockée sous la clé HKEY_LOCAL_MACHINE\Security\Policy\Poladtev
- **Plusieurs journaux (répartis)**
  - Par défaut : Applications, Sécurité, Système
  - Mais aussi : DNS, Directory Service, Réplication de fichiers

# 1. Fonctionnement de l’audit (2/3)

- **Service d’audit**
  - Le service de journalisation est inclus dans SERVICES.EXE
  - Il s’appelle EventLog et s’exécute sous le compte SYSTEM
  - Il ne peut être ni arrêté, ni désactivé
- **Chaque source d’événement doit au préalable s’enregistrer dans la LSA**
  - API : ADVAPI32!ReportEvent() et ADVAPI32!RegisterEventSource()
- **Tous les paramètres du service sont dans la clé HKLM\SYSTEM\CurrentControlSet\Services\Eventlog***

# 1. Fonctionnement de l'audit (3/3)

- **Fichiers de traces : stockage**
  - Ils sont stockés par défaut dans %SystemRoot%\System32\config
    - Les déplacer sur une autre partition
  - Taille par défaut faible (512 Ko)
    - Dimensionner en fonction du réseau et de l'outil d'archivage (conseillé : entre 10 et 100 Mo)
  - Définir la stratégie de rotation du journal
  - Stockage au format binaire .EVT
    - Date, heure, source, catégorie, type, ID, utilisateur, ordinateur + paramètres optionnels
    - Format « brut » (ex. les utilisateurs sont référencés par SID)
- **Fichiers de traces**
  - « Event Message File » : chaîne descriptive de l'événement avec paramètres %1, %2, etc. Un paramètre %%nnnn est substitué dans le « Parameter Message File »
  - « Category Message File » : description des « catégories » (journal sécurité uniquement)
  - « Parameter Message File » : table de constantes à substituer dans la description (ex. champs de bits)
- **Conclusion : les journaux doivent être affichés sur le système qui les a générés**

# 2. Mettre en place une stratégie (1/5)

- **Principes**
  - Utiliser des comptes nominatifs
    - Bannir « administrateur » (et « invité ») !
  - Tous les utilisateurs ont des comptes de domaine
  - Stratégie proposée
    - (AA) [SE] Système
    - (BB) [SE] Connexion
    - (CC) [SE] Accès aux objets*
    - (DD) [SE] Utilisation des privilèges
    - (EE) [--] Suivi de processus
    - (FF) [SE] Modifications de stratégie
    - (GG) [SE] Gestion des comptes
    - (HH) [--] Accès au service d'annuaire
    - (JJ) [SE] Connexion aux comptes

    ** L'audit doit ensuite être activé sur chaque objet (fichier ou clé de base de registre)*

# 2. Mettre en place une stratégie (2/5)

## Evénements courants à stocker

- Authentification
  - [BB] 528 : logon (local ou par Terminal Server)
  - [BB] 529-537, 539 : échec du logon (cause précisée)
  - [BB] 538 : logoff
    - Très nombreux
    - En authentification NTLM : nom du compte
    - En authentification Kerberos : aucune information exploitable
  - [BB] 540 : logon réseau (enregistré sur ce DC)
    - Très nombreux
    - En authentification NTLM : nom du compte + nom NetBIOS de la station
    - En authentification Kerberos : aucune information exploitable

# 2. Mettre en place une stratégie (3/5)

- Authentification (suite)
  - [GG] 644 : compte verrouillé
  - [JJ] 680 : connexion (authentifiée par ce DC)
    - Très nombreux
    - En authentification NTLM : nom du compte et nom NetBIOS de la station
    - En authentification Kerberos : événement non généré !
  - [JJ] 681 : échec de connexion
  - [BB] 682, 683 : reconnexion/déconnexion de compte
- Gestion des tickets Kerberos (67x)
  - [JJ] 672 : connexion de compte
    - Contient : utilisateur, adresse IP
  - [JJ] 673 : allocation de ticket de service
    - Très nombreux
    - Inexploitables
  - [JJ] 677 : échec d'allocation de ticket de service
    - Très nombreux dans un réseau mixte (Windows 2000, Windows NT4, SAMBA)
    - Inexploitables

# 2. Mettre en place une stratégie (4/5)

- **Evénements rares et à surveiller**
  - [AA] 517 : purge du journal
  - [FF] 608, 609 : ajout/suppression de droits
  - [FF] 610, 611, 620 : ajout/suppression/modification de relations d'approbation
  - [FF] 612, 617, 618, 619, 643 : modifications de stratégie
  - [GG] 624-630 : manipulations de comptes utilisateur
  - [GG] 632, 633 : ajout/suppression d'un membre dans un groupe global
  - [GG] 645-647 : manipulations de comptes machine
  - [GG] 660, 661 : ajout/suppression d'un membre dans un groupe de sécurité universel

# 2. Mettre en place une stratégie (5/5)

- **Evénements inexploitables**
  - Types
    - Accès à l'annuaire
    - Suivi de processus
    - 541-547, 613-616 : IKE et IPSEC
    - 560-566 : audit sur les objets
    - 576 : privilèges associés à la session
  - Causes
    - Problème de volumétrie
    - Manque d'informations dans l'événement
    - Trop techniques (ex. n° de handle au lieu du nom de fichier)
- **Pollution des journaux**
  - Connexions récurrentes
    - Agents de monitoring (ex. PATROL)
    - Connexion de comptes machine

# 3. Lire les journaux

- **Exporter les journaux toutes les heures ou tous les jours**
- **Importer le résultat dans une base SQL**
- **Consolider les données de tous les DC d'un même domaine**
  - Supprimer les doublons
- **Filtrer le bruit (avant ou après importation)**
  - Connexion de comptes machines ou d'agents
  - Evénements inexploitables
    - 560-566 : audit sur les objets
    - 541-547, 613-616 : IKE et IPSEC
    - 673, 677 : tickets de service Kerberos
- **Utiliser des outils de reporting**
  - Comptes-rendus hebdomadaires
  - Alertes « en temps réel »
- **Archiver la base mensuellement**
- **Purger les événements communs**
  - Connexions
- **Conserver accessibles les événements rares**
  - Création de comptes, modification de groupes

# 4. Les limites de l'audit

- **Bruit**
  - Volume de données
    - 5000 postes ⇨ 100 Mo par jour ⇨ environ 20% de bruit
  - Il est impossible de restreindre l'audit en fonction de la source (sauf audit sur les objets)
  - Connexion de comptes machine ou d'agents automatisés
- **Fiabilité des informations**
  - Le journal peut être effacé par un administrateur
  - Des événements individuels peuvent être effacés par un administrateur (outil WinZapper)
  - Les paramètres enregistrés sont fournis par les applications – problème de fiabilité (ex. noms NetBIOS) et lacunes
- **Certains événements sont inexploitables**
  - Accès aux objets
  - Accès à l'annuaire
  - Suivi de processus
- **Exploitation des journaux**
  - Le déploiement d'une stratégie d'audit sur un parc génère un problème de volumétrie et de télécollecte
  - Il existe d'autres journaux que les journaux système (fichiers .LOG et .TXT générés par les applications)
  - L'utilisation de comptes génériques ne permet pas le mapping avec un utilisateur réel (ex. compte SYSTEM)
  - Chaque entrée d'audit possède ses propres paramètres

# Annexe

## Bibliographie

- Liste des événements « sécurité » sous Windows 2000 : Q299475, Q301677
- Localisation de la stratégie d'audit : Q246120

## Outils

- Kit de Ressources Techniques : DUMPEL
- Aelita / EventAdmin
- BMC / Patrol
- CyberSafe / LogAnalyst
- DorianSoft / Event Archiver & Event Analyst
- TNT Software / Event Log Monitor
- RippleTech / LogCaster
- eSecurity / eSentinel