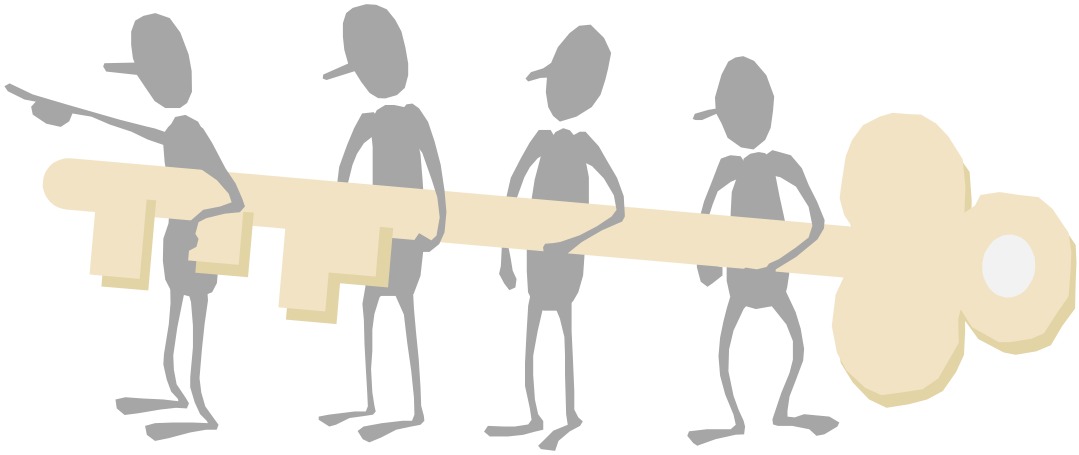
12 septembre 2003

Sécurité de Windows NT

Généralités, mise en œuvre.



SOMMAIRE

1. INTRODUCTION 1

2. MECANISMES DE SECURITE DE WINDOWS NT 2

2.1. ARCHITECTURE DE SECURITE DE WINDOWS NT 3
2.1.1. Composants du système de sécurité 3
2.1.2. Jetons d'accès 5
2.1.3. Les Security Identifiers (SID) 6
2.1.4. Descripteurs de Sécurité 8
2.1.5. DACLs Non-standards 10
2.1.6. Les niveaux d'impersonnation 10
2.2. PROCESSUS D'OUVERTURE DE SESSION SOUS WINDOWS NT 4.0 11
2.2.1. Procédure d'ouverture de session détaillée 12
2.2.2. Connexion dans un domaine 14
2.3. PROCESSUS D'OUVERTURE DE SESSION SOUS WINDOWS 2000 17
2.4. MECANISME DE STOCKAGE DES MOTS DE PASSE 18
2.4.1. Structure Lan Manager (LM hash) 18
2.4.2. Structure native Windows NT (NT hash) 20
2.4.3. Autres emplacements de stockage des mots de passe 20
2.4.4. Stockage des mots de passe par les anciens clients Windows 21
2.5. MECANISME D'AUTHENTIFICATION SUR LE RESEAU 22
2.5.1. Authentification Lan Manager 22
2.5.2. Authentification Native Windows NT 23
2.5.3. Variante d'authentification HTTP Microsoft 23
2.6. LE SYSTEME DE FICHIERS NTFS 25
2.6.1. Fonctionnement interne de NTFS 25
2.6.2. Les ACLs 27
2.6.3. Les « Data-Streams » 28
2.6.4. Partages et permissions de partage 29
2.6.5. Les ACLs de Windows 2000 30
2.6.6. Encrypted File System (EFS) 31
2.7. LA BASE DES REGISTRES 34
2.7.1. Généralités 34
2.7.2. Structure de la base des registres 34
2.7.3. Fichiers de la base de registre 36
2.7.4. Sécurité de la base des registres 36

3. GESTION DE LA SECURITE SOUS WINDOWS NT 38

3.1. DOMAINES WINDOWS NT 38
3.1.1. Qu'est ce qu'un domaine ? 38
3.1.2. Approbations de domaines 39
3.1.3. Architectures possibles 40
3.1.3.1. Modèle à Domaine Unique 40
3.1.3.2. Modèle à Domaine Maître 40
3.1.3.3. Modèle à Domaines Maître Multiples 41
3.1.3.4. Modèle à Domaines de Confiance Réciproques 41
3.2. ARCHITECTURE DE WINDOWS 2000 : FORETS, ARBRES ET UOS 43
3.2.1. Gestion centralisée des ressources et services / Active Directory 43
3.2.2. Introduction à l'Active Directory 45
3.2.3. Structure Logique de l'Active Directory 45
3.2.3.1. Objets 45

3.2.3.2. Unités d'organisation 45
3.2.3.3. Domaines 46
3.2.3.4. Arbres et Forêts 47
3.2.4. Relations d'approbation 47
3.3. GESTION DES UTILISATEURS 49
3.3.1. Droits des utilisateurs 49
3.3.2. Groupes globaux et locaux 49
3.3.3. Stratégies de compte 50
3.3.4. Profils utilisateurs 50
3.3.5. Stratégies Système (Poledit.exe) 51
3.3.6. Windows 2000 et les Stratégies de Groupes (GPO) 52
3.3.7. Scripts d'ouverture de session 52
3.4. JOURNALISATION DES EVENEMENTS 53

4. LES OUTILS D'AIDE A L'ADMINISTRATION DE LA SECURITE 55

4.1. PREAMBULE 55
4.2. AUDITER SON SYSTEME D'INFORMATION 55
4.2.1. Produits ISS 55
4.2.2. LANguard Network Scanner 56
4.2.3. NetBIOS Auditing Tool (NAT) 57
4.2.4. Cybercop Scanner / Ballista 59
4.2.5. Kane Security Analyst 59
4.2.6. Satan 60
4.2.7. Etherpeek 60
4.2.8. Sniffer Basic / Sniffer Pro 61
4.2.9. Ethereal 61
4.2.10. Port Scanning 61
4.3. DETECTION D'INTRUSION 62
4.3.1. Détection comportementale 62
4.3.2. Détection par scénario 62
4.3.3. Autres types de détection 62
4.4. COMBLER LES FAILLES 63
4.4.1. Services Packs et Hot Fixes 63
4.4.2. SecEdit 63
4.4.3. Security Config Wizard 63
4.4.4. LSA Pro 64
4.5. OUTILS DIVERS 64
4.5.1. Le NT Resource Kit 64
4.5.2. John the ripper 65
4.5.3. L0phtcrack 65
4.6. ANTIVIRUS 66

5. SECURISER WINDOWS NT 67

5.1. RAPPEL SUR LE NIVEAU DE SECURITE C2 67
5.2. CHOIX D'UNE ARCHITECTURE 68
5.2.1. Choix de l'architecture réseau 68
5.2.2. Choix des matériels 68
5.2.3. Sauvegardes 69
5.3. INSTALLATION DE WINDOWS NT 70
5.3.1. Protection physique des machines : 70
5.3.2. Configuration Matérielle des Machines 70
5.3.3. Choix du Système de Fichiers 70
5.3.4. Configuration du réseau 71
5.4. CORRECTIONS DES VULNERABILITES MAJEURES ET MINEURES 72
5.4.1. Ou trouver les Services Pack et Hot-fixes 72
5.4.2. Comment installer ces correctifs ? 72
5.5. ACTIONS SUR LA BASE DES REGISTRES 73
5.6. PROTECTION ET PARAMETRAGE DU SYSTEME 74
5.6.1. Mettre en place une stratégie de droits 74
5.6.2. Supprimer les sous-systèmes POSIX et OS/2 74
5.6.3. Désactiver le sous-système WOW 75
5.6.4. Régler le seuil d'alerte de l'occupation du disque dur 75

5.6.5. Effacer le fichier de mémoire virtuelle ... *75*
5.6.6. Gérer les plantages ... *76*
5.6.7. Protéger l'accès à la clé Aedebug ... *76*
5.6.8. Limiter l'accès à la base des objets NT ... *77*
5.6.9. Limiter l'utilisation du service Planning ... *77*
5.6.10. Gérer les extensions associées à certains programmes ... *78*
5.6.11. Désactiver la fonction AutoRun des CD-Rom ... *78*
5.6.12. Forcer l'ouverture de session pour l'arrêt du système ... *78*
5.7. PROTECTION DES MOTS DE PASSE ... 79
5.7.1. Mettre en place une stratégie de compte ... *79*
5.7.2. Obliger les utilisateurs à choisir des mots de passe complexes ... *80*
5.7.3. Alerter l'utilisateur du prochain changement de mot de passe ... *81*
5.7.4. Désactiver l'authentification Lan Manager ... *81*
5.7.5. Interdire le transit de mot de passe en clair ... *81*
5.7.6. Sécuriser l'accès au fichier SAM._ ... *82*
5.7.7. Chiffrement de la SAM avec Syskey ... *82*
5.7.8. Limiter le cache d'authentification des stations ... *82*
5.7.9. Contrôler les Notification Packages ... *83*
5.8. CONFIGURATION DE L'AUDIT ... 84
5.8.1. Mettre en place une stratégie d'audit ... *84*
5.8.2. Régler les paramètres des journaux ... *84*
5.8.3. Limiter l'accès aux journaux d'audit ... *85*
5.8.4. Limiter le droit de gérer le journal d'audit et de sécurité ... *85*
5.8.5. Activer l'audit des objets système ... *85*
5.8.6. Arrêter le système quand le journal d'audit est saturé ... *86*
5.8.7. Afficher une bannière d'ouverture de session ... *86*
5.8.8. Auditer l'utilisation des privilèges de sauvegarde et de restauration ... *86*
5.8.9. Enregistrer les erreurs de l'analyseur de performances ... *87*
5.9. PROTECTION DES COMPTES ... 88
5.9.1. Désactiver le compte Invité ... *88*
5.9.2. Gérer les comptes utilisateurs ... *88*
5.9.3. Renommer le compte Administrateur ... *89*
5.9.4. Choisir un mot de passe pour l'administrateur ... *89*
5.9.5. Rendre le compte Administrateur verrouillable ... *90*
5.9.6. Limiter les membres du groupes Administrateurs ... *90*
5.9.7. Cacher le nom du dernier utilisateur connecté ... *90*
5.9.8. Interdir l'ouverture de session automatique ... *91*
5.10. PROTECTION DE LA BASE DE REGISTRE ... 92
5.10.1. Contrôler les accès distants à la base de registre ... *92*
5.10.2. Modifier les permissions sur les clés de la base de registre ... *92*
5.10.3. Désactiver les outils d'édition de la base de registre ... *93*
5.11. PROTECTION DES PERIPHERIQUES ... 94
5.11.1. Empêcher l'ajout d'imprimante ... *94*
5.11.2. Contrôler l'accès aux périphériques amovibles ... *94*
5.12. PROTECTION DES SERVICES RESEAU ... 95
5.12.1. Limiter la connexion anonyme ... *95*
5.12.2. Activer la signature SMB ... *95*
5.12.3. Désactiver les partages administratifs ... *96*
5.12.4. Masquer une station ou un serveur ... *97*
5.12.5. Interdire l'utilisation de DCOM ... *97*
5.13. PROTECTION DU SYSTEME DE FICHIERS ... 98
5.13.1. Généralités ... *98*
5.13.1.1. Sécurisation par modification des permissions standards ... 99
5.14. AUTRES REGLAGES ... 101
5.14.1. Disquettes de réparation d'urgence ... *101*
5.14.2. Mot de passe pour le lancement de services ... *101*
5.15. MAINTIENT EN CONDITION DE LA SECURITE D'UN SYSTEME ... 102

6. ANNEXES ... 104

6.1. PERMISSIONS PAR DEFAUT LORS DE L'INSTALLATION DU SYSTEME ... 105
6.1.1. Windows NT Workstation : ... *105*
6.1.2. Windows NT Server : ... *109*

6.2. PERMISSIONS PRECONISEES POUR UNE CONFIGURATION C2 DU SYSTEME 114
6.3. PRINCIPALES VULNERABILITES DE WINDOWS NT 117
6.3.1. GetAdmin 117
6.3.2. Ping Of Death II 117
6.3.3. L'attaque Out Of Band (OOB) 117
6.3.4. L'attaque SMB Downgrade 117
6.3.5. SYN Flooding 117
6.3.6. Land Attack 118
6.3.7. Teardrop 118
6.3.8. KnownDLLs 118
6.3.9. Aedebug 118
6.3.10. Attaques « Man in the Middle » 119
6.4. BEST OF INSECURITY - CE QU'IL NE FAUT PAS FAIRE 120
6.5. DESCRIPTIONS DES DROITS WINDOWS NT STANDARDS ET AVANCES 122
6.5.1. Droits standards 122
6.5.2. Droits avancés 124
6.6. SOURCES D'INFORMATION 126
6.6.1. Sources CELAR 126
6.6.2. Livres 126
6.6.3. Internet 128
6.7. GLOSSAIRE 130
6.8. L'EDITEUR DE STRATEGIE SYSTEME (POLEDIT.EXE) 132
6.8.1. Principe de fonctionnement 132
6.8.2. Les fichiers ADM 132
6.8.2.1. Sections des fichiers ADM 132
6.8.2.2. Catégories 133
6.8.2.3. Keynames 134
6.8.2.4. Policies 134
6.8.2.5. Options de Policy 134
6.8.2.6. Autres mots-clefs 135
6.8.3. Création et application d'une stratégie système 136

Historique des évolutions

Versions	Date	Evolutions
1.0	15/07/1999	- Création du document - Finalisation Août 1999
1.1	16/11/1999	- Correctifs mineurs - Mise à jour des liens Internet et des références bibliographiques. - Mise à jour sur les Services Pack et Hot Fixes.
1.2	Avril 2000	- Correctifs mineurs - Précisions sur le processus d'ouverture de session - Mécanismes de sécurité internes (SID, RID, SD, Jetons…) - Précisions sur le système de fichiers NTFS - Windows 2000
1.2.1	Octobre 2000	- Correctifs Windows 2000 + correctifs mineurs
1.2.2	Juin-Juillet 2001	- Ajout de l'annexe sur l'éditeur de stratégies système
2.0	Octobre 2002 - Mars 2003	- Refonte complète du document et mise en conformité du plan selon les propositions de David Boucart (CFBS)

1. Introduction

Windows NT est un système d'exploitation multitâche auquel est intégré une interface graphique et permettant la mise de machines en réseaux. A cet effet, deux versions du système d'exploitation existent : Windows NT Server et Windows NT Workstation. Le code des deux versions est identiques, seule la configuration de certaines informations de la base des registres diffère, ainsi que disponibilité de certains outils d'administration dans la version Serveur.

Windows NT a été développé depuis 1989 par Microsoft. Initialement prévu pour fonctionner avec un processeur Risc i860 et pour être compatible avec OS/2, rapidement le système s'orienta vers les processeurs Intel x86 et vers une compatibilité avec Windows. La première démonstration de NT eut lieu au Comdex en octobre 1991, puis les premières versions bêta virent le jour au printemps 1992 avant le lancement de Windows NT 3.1 en juillet 1993. La suite Office fut disponible en août 1994, immédiatement suivie d'une évolution majeure de NT qui devint NT 3.5.

L'étape suivante a été la sortie de Windows NT 3.51 en mai 1995 qui offrait la compatibilité avec Windows 3.11 et en reprenait l'interface graphique. La version actuelle, Windows NT 4.0, sortit en août 1996, et reprenait l'interface graphique de Windows 95. Enfin, la première version bêta de Windows NT 5.0 fut adressée aux développeurs en septembre 1997.

Plus récemment, Microsoft annonçait la disparition de Windows NT 5.0 au profit de Windows 2000, censé fusionner les développements conjoints de Windows 98 et de Windows NT. Windows 2000 est officiellement sorti le 17 février 2000, et est actuellement commercialisé par Microsoft.

Dans un futur proche, Microsoft poursuit l'évolution de son offre de systèmes d'exploitation avec l'arrivée de Windows .NET, remplaçant annoncé de Windows 2000 Serveur. A cette date, seule une version Beta (Release Candidate 2) de Windows .NET est actuellement disponible, les postes sous Windows XP devant remplacer dans cette nouvelle architecture les postes clients de type NT 4.0 Workstation ou Windows 2000 Professionnel.

Le système Windows NT a été développé dès le départ avec le souci d'offrir des fonctions et mécanismes de sécurité à ses utilisateurs. Cependant, la configuration fournie par défaut lors de l'installation d'un système Windows NT 4.0 (installation de base en Service Pack 1) reste trop laxiste quant à la sécurité du système.

Ce support de cours décrit ces fonctions et mécanismes en tentant de couvrir à la fois les technologies Windows NT 4.0 et Windows 2000, similaires par de nombreux aspects, et donne des pistes sur les moyens de parvenir à une sécurité optimale.

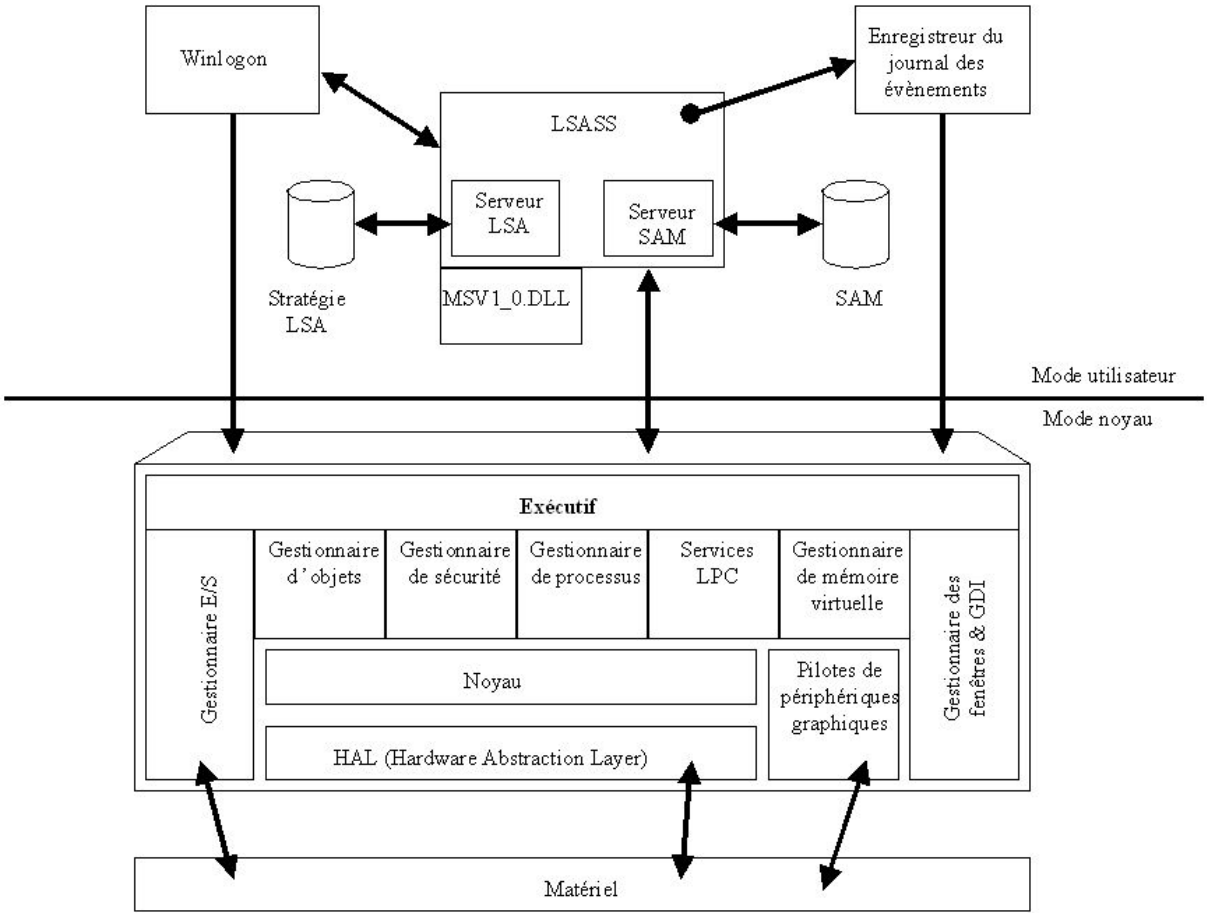
2. Mécanismes de sécurité de Windows NT

Ce chapitre traite des principaux mécanismes **internes** utilisés dans la sécurité de Windows NT Server et Workstation.

Notons que les mécanismes présentés dans ce chapitre sont rigoureusement identiques à ceux implémentés dans les plate-formes Windows 2000. Seules quelques différences notables, en particulier dans l'architecture générale du système et l'implémentation de certaines fonctions, existent dans la nouvelle mouture du système d'exploitation de Microsoft. Ces différences seront présentées tout au long de ce chapitre.

2.1. Architecture de sécurité de Windows NT

Le noyau de Windows NT est architecturé suivant le schéma présenté ci-dessous :



Un des modules fondamentaux de l'exécutif est le gestionnaire d'objet. En effet, le concept de base utilisé dans Windows NT est l'objet. Les différents types d'objet gérés par le système sont :

- les événements (événement système, interruption…),
- les fichiers (fichier réel sur disque ou fichier virtuel correspondant à un périphérique),
- jeton d'accès (identification d'un utilisateur),
- port LPC[1] (utilisé pour la communication inter processus),
- processus,
- sémaphore,
- thread,
- timer.

Le système d'exploitation a la charge de créer et détruire ces objets et, pour ce qui nous intéresse, de gérer des « Security Descriptor » pour chacun d'entre eux : ceux-ci indiquent qui a le droit de faire quoi sur ces objets.

2.1.1. Composants du système de sécurité

La sécurité de Windows NT est intégrée au système d'exploitation au sein d'une structure complexe comprenant divers éléments. Le sous-système de sécurité fonctionne pour sa plus

[1] Local Procedure Call

grande part en mode Utilisateur (User Mode), il arrive cependant que certaines parties de ce sous-système soient lancées en mode Noyau (Kernel Mode) principalement pour vérifier les jetons d'accès des utilisateurs et pour l'audit du système.

Ce sous-système de sécurité a pour but de contrôler les accès aux ressources Windows NT. Celui-ci offre les services suivants :

- Un processus pour authentifier les utilisateurs reposant sur une base de données des utilisateurs,
- Une méthode pour permettre au propriétaire d'un objet de créer des listes à contrôle d'accès discrétionnaires (DACLs) afin de déterminer les types d'accès autorisés sur cet objet,
- La possibilité de surveiller et enregistrer les activités des utilisateurs au cours d'une session,
- Un espace mémoire protégé afin de s'assurer que les accès mémoire sont protégés contre un accès non autorisé.

Ce qui suit est une liste des différents composants qui entrent en jeu dans l'implémentation de la sécurité sous Windows NT :

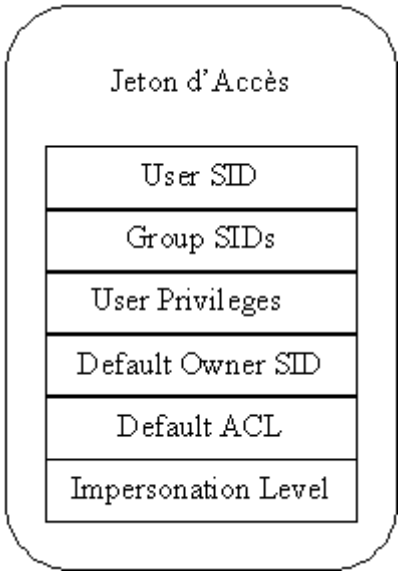
- **Logon Process**, Processus d'ouverture de Session. Processus en mode utilisateur exécutant WINLOGON.EXE qui est chargé de capturer les informations de login pour les fournir au LSA, et de créer le processus initial dans la session utilisateur.
- **Network Logon Service**, Service d'ouverture de session en réseau (NETLOGON). Service en mode utilisateur à l'intérieur du processus SERVICES.EXE, et qui répond aux demandes d'ouverture de session en réseau. L'ouverture de session réseau est traitée comme une ouverture de session locale, en envoyant les données au LSASS pour vérification
- **SRM (Security Reference Database)**, ou Moniteur de Référence de Sécurité. Composant de l'exécutif Windows NT (NTOSKRNL.EXE), chargé d'effectuer les vérifications de sécurité concernant l'accès aux objets, en manipulant des privilèges (droits des utilisateurs), et en générant des messages d'audit. Ces messages sont stockés dans le fichier SECEVENT.EVT situé sous `%SYSTEMROOT%\SYSTEM32\CONFIG`.
- **LSA, Local Security Authority server**, Serveur d'autorité de la sécurité locale. Processus en mode utilisateur exécutant l'image LSASS.EXE qui est responsable de la stratégie locale de sécurité du système, de l'authentification des utilisateurs, de la gestion de leurs privilèges, de la politique de gestion des mots de passe et de l'envoi de messages d'audit de sécurité au journal des événements. La LSA communique directement avec le Security Reference Monitor (SRM) via des "pipes non nommés" sécurisés (au travers de LPCs) pour les aspects de vérification et de manipulation des privilèges utilisateurs et pour l'envoi d'événements de sécurité à auditer
- **LSA Policy Database**, Base de données de la stratégie LSA. Base de données qui contient les paramètres de la LSA. Cette base de données est placée dans le registre sous HKEY_LOCAL_MACHINE\Security. L'accès à cette base est protégé par une DACL interdisant sa manipulation par de simples utilisateurs.
- **SAM Server, Security Account Manager Server**. Serveur du gestionnaire de la SAM, ensemble de fonctions permettant de gérer la SAM. Le SAM s'exécute dans le contexte du processus LSASS.EXE.
- **SAM database, Base de données SAM**. Base de données qui contient la liste des utilisateurs et des groupes pour une machine ou pour un domaine. Située dans le registre sous la clef HKEY_LOCAL_MACHINE\SAM. L'accès à cette base est protégé par une DACL interdisant sa manipulation par de simples utilisateurs.

- **Default Authentication Package**, Package d'authentification par défaut. DLL nommée MSV1_0.DLL s'exécutant dans le contexte de LSASS, et qui implémente le mécanisme d'authentification de Windows NT. Cette DLL est chargé de vérifier les informations de login dans la SAM et retourne le résultat au processus de Logon.

2.1.2. Jetons d'accès

Une fois qu'un utilisateur a été authentifié au sein de sa session, celui-ci se voit remettre un jeton d'accès. Ce jeton est utilisé pour toute la durée de la session est n'est libéré que lorsque l'utilisateur ferme sa session. Il est utilisé pour représenter l'utilisateur dans toutes les demandes d'accès aux ressources du système.

La figure suivante précise le contenu d'un jeton d'accès :



Notons que ce jeton contient un certain nombre d'informations additionnelles sur l'utilisateur, et utilisées par le sous-système de sécurité de Windows NT.

La table suivante précise les rôles de chacune de ces informations :

Composants du jeton d'accès	Description
User Security Identifier	Représentation numérique du compte utilisateur pour identifier l'utilisateur sur le système. Exemple : S-1-5-21-1548958964-189547354-1147859600-500
Group Security Identifier(s)	Représentation numérique des groupes (locaux et globaux) auxquels appartient l'utilisateur. Exemple : S-1-1-0 (groupe "Tout le monde")
User Privileges	Les droits qu'un utilisateur possède. Exemple : SeRemoteShutdownPrivilege (droit d'éteindre une machine à distance)
Default Owner SID	Utilisé par le sous-système de sécurité si aucune sécurité n'a été précisée pour certaines API du sous-système Win32 au cours de la création du jeton. Exemple : S-1-5-21-1548958964-189547354-1147859600-500
Default Discretionary ACL	Utilisé par le sous-système de sécurité si aucune sécurité n'a été précisée pour certaines API du sous-système Win32 au cours de la création du jeton. Exemples : Accès 0x0000FFFF Autorisé pour "ADMINISTRATEURS" Accès 0X001F0000 Dénié pour "TOUT LE MONDE"
Impersonation Level	Fixe le niveau d'impersonation pour le jeton d'accès, et détermine les informations qu'un autre processus dispose pour le compte d'un client Exemple : SecurityImpersonation

2.1.3. Les Security Identifiers (SID)

Les Identificateurs de Sécurité (Security Identifiers - SID) sont des représentations binaires d'une machine, d'un utilisateur ou d'un groupe et qui sont utilisés pour identifier ces comptes par le sous-système de sécurité de Windows NT pour les mécanismes d'identification, de contrôle d'accès et d'audit du système. Le SID "primaire" ou "local" d'une machine est généré au moment de l'installation de Windows NT et est créé en utilisant un algorithme de hachage basé sur des nombres de 32 bits dérivés du nom de la machine, du temps écoulé pendant l'exécution du thread utilisé pour créer le compte, et de l'heure du système.

La structure d'un SID définit les Identificateurs sous la forme d'un unique "Top Authority", ou "Identifier Authority", et d'une liste de "Sub Authorities", ou "Relatives Identifiers" (RIDs). L'Identifier Authority représente l'origine du SID, suivie de N Sub Authorities qui représentent des informations supplémentaires sur les origines du SID.

L'exemple qui suit correspond au SID (en mode texte) du compte local (BUILTIN) Administrateur pour une machine Windows NT Workstation.

S-1-5-21-1548958964-189547354-1147859600-500

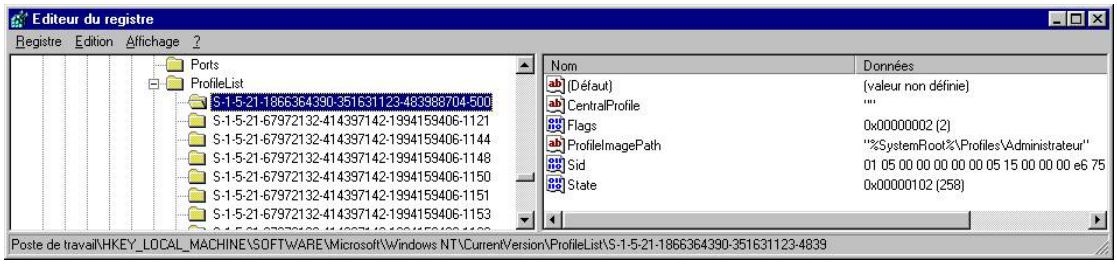
La structure d'un SID (en mode de représentation texte) est de la forme :

S – R – I – S1 – S2 – S3 – S4 – S5 (A)

- S est un marquant précisant que les chiffres représentent un SID
- R est le niveau de révision du SID (1 dans notre exemple)
- I est l'Identifier Authority (5 dans notre exemple)
- S1 représente la première Sub Authority (21 dans notre exemple)
- S2 représente la seconde Sub Authority (1548958964 dans notre exemple)
- S3 représente la troisième Sub Authority (189547354 dans notre exemple)
- S4 représente la quatrième Sub Authority (1147859600 dans notre exemple)
- S5 (A) est la cinquième Sub Authority (généralement le RID du compte utilisateur - ici 500)

Quand un nouveau compte est créé, Le SID de la machine est concaténé avec une extension numérique représentant le nouveau compte. Windows NT réserve les nombres entre 0 et 999 pour les comptes et les groupes système, les nombres supérieurs à 1000 sont alors utilisés pour les nouveaux comptes et groupes utilisateurs.

Pour visualiser les représentations en mode texte des SIDs des utilisateurs utilisés sur un système, on peut utiliser un éditeur de registre et visualiser ces SIDs sous la clef HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList. En cliquant sur les sous-clefs du SID, on peut voir à quel compte tel SID appartient.



Certains SIDs sont réservés à des comptes (systèmes, groupes, machines…) connus. Parmi ceux-ci, on peut citer :

S-1-1-0	:	Groupe "Tout le monde".
S-1-3-0	:	Créateur Propriétaire.
S-1-5-1	:	Dialup.
S-1-5-2	:	Network.
S-1-5-3	:	Batch.
S-1-5-4	:	Interactive.
S-1-5-5-XXXX-YYYY	:	Logon ID.
S-1-5-6	:	Service.
S-1-5-7	:	Anonymous.
S-1-5-8	:	Proxy.
S-1-5-18	:	System.
S-1-5-32-XXXX	:	Built-in domain Group.
S-1-5-32-544	:	Local Administrator Group (Groupe Local Administrateurs).
S-1-5-32-545	:	Local Users Group (Groupe Local Utilisateurs).
S-1-5-32-546	:	Guest Group (Groupe Invité).
S-1-5-32-547	:	Local Power Users Group (Groupe Local Utilisateurs avec pouvoir).
S-1-5-32-548	:	Account Operators Group (Groupe Opérateurs de comptes).
S-1-5-32-549	:	System Operators Group (Groupe Opérateurs du système).
S-1-5-32-550	:	Print Operators Group (Groupe Opérateurs d'Impression).
S-1-5-32-551	:	Local Backup Operators Group (Groupe Local Opérateurs de sauvegarde).
S-1-5-32-552	:	Local Replicators Group (Groupe Local Réplicateur).
S-1-5-21-XXXX-YYYY-ZZZZ	:	Machine ID.

S-1-5-21-WWWW-XXXX-YYYY-ZZZZ : User ID.
S-1-5-21-WWWW-XXXX-YYYY-500 : Compte Administrateur

2.1.4. Descripteurs de Sécurité

Des descripteurs de sécurité (Security Descriptors - SD) sont assignés à tous les objets sécurisables de Windows NT, lors de leur création. Ces descripteurs sont utilisés, en interne du système d'exploitation, afin de déterminer les permissions qu'un utilisateur dispose sur ces objets.

Les objets sécurisables du système sont les suivants :

- Fichiers
- Répertoires
- Mappings de fichiers
- Pipes
- Mailslots
- Processus
- Threads
- Jetons d'accès
- Machines Windows
- Bureaux
- Clefs de registre
- Objets Services
- Périphériques
- Objets de Synchronisation (événements, mutexs, sémaphores)
- Objets en mode Utilisateurs
- Objets en mode Noyau

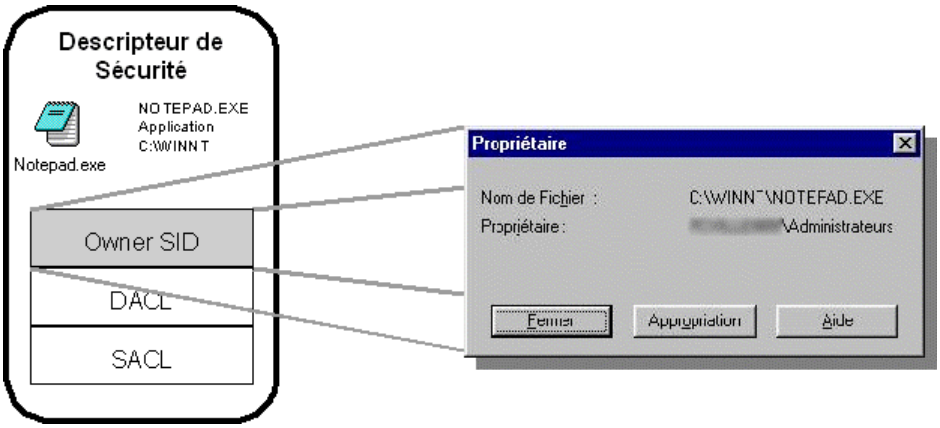
Un descripteur de sécurité contrôle donc qui a accès à un objet, il comporte les attributs suivants :

Attributs d'un Descripteur de Sécurité	**Description**
SID du propriétaire (Owner SID)	Le descripteur de sécurité du propriétaire de l'objet.
SID du groupe	Identificateur de sécurité du groupe principal pour l'objet (**utilisé uniquement par le sous système POSIX**)
Discretionary ACL (DACL)	Le DACL détermine quels utilisateurs et/ou groupes ont accès à cet objet ainsi que le type d'accès autorisé.
System ACL (SACL)	Le SACL est utilisé pour déterminer ce qui doit être audité sur cet objet.

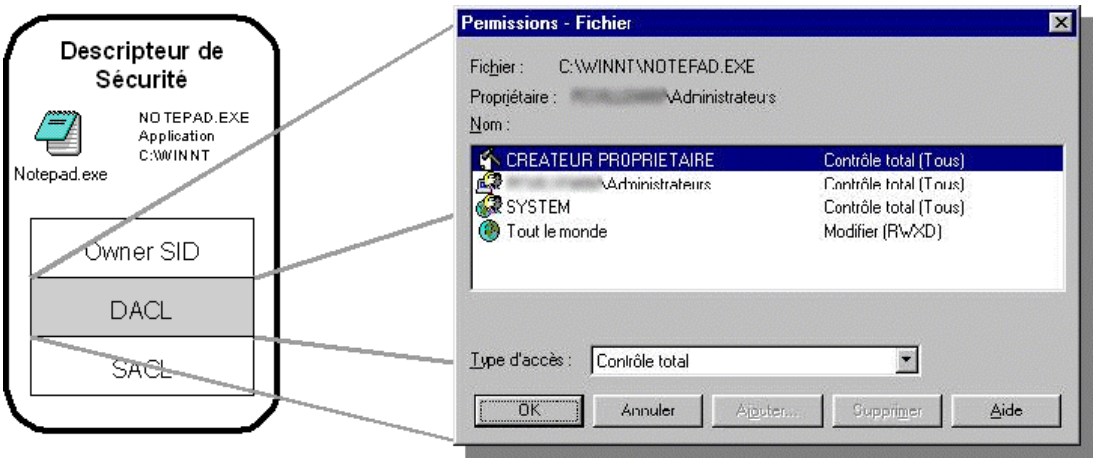
Quand un utilisateur ou un processus requiert un accès à un objet sécurisé, le processus requérant présente d'abord son jeton d'accès au SRM qui vérifie alors les permissions sur cet objet en interrogeant le Security Descriptor de l'objet. Si les permissions positionnées ne permettent pas l'accès à cet objet ou si l'utilisateur (ou le processus) appelant ne dispose pas d'un privilège lui donnant accès à cet objet, la requête est rejetée. Dans le cas contraire, la requête est acceptée et éventuellement auditée si le SACL le précise

L'exemple qui suit donne les différents éléments pour le programme NOTEPAD.EXE. Ces trois fenêtres sont accessibles en cliquant sur le bouton droit de la souris sur le fichier correspondant et en sélectionnant l'option "Propriétés" ; l'onglet "Sécurité" propose 3 boutons, correspondant chacun aux trois figures qui suivent.

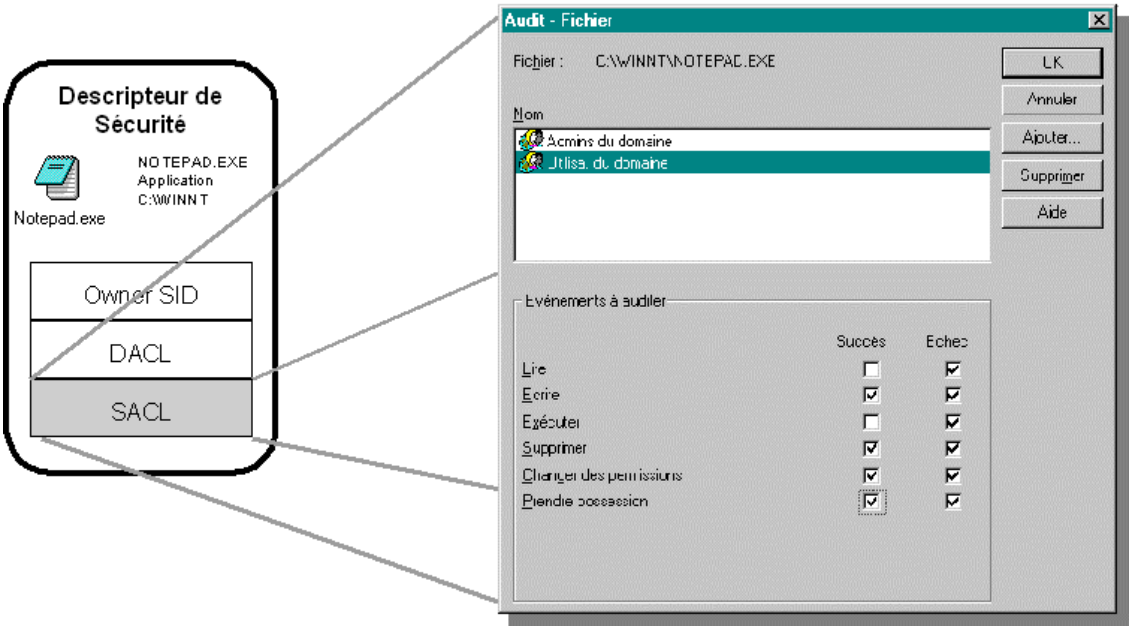
SID du propriétaire



DACL :



SACL :



2.1.5. DACLs Non-standards

Dans certains cas, il est possible de trouver des DACLs non-standards sur des objets du système. Ces DACLs sont les suivantes :

- **DACL Vide** : Il s'agit simplement d'une ACL vide, c'est à dire sans aucune entrée. Ceci implique que le groupe "Tout le monde" n'a pas accès à l'objet.

- **DACL Nulle** : Loin d'être une ACL Vide, cette ACL donne accès à l'objet au groupe "Tout le Monde", y compris pour les sessions Nulles et Anonymes.

- **DACLs manquantes** : Il s'agit habituellement d'une erreur lors de la création de l'objet, mais il peut s'agir d'un événement intentionnel (Cheval de Troyes par exemple) ; l'objet est créé **sans** DACL, permettant ainsi l'accès au groupe "Tout le monde"

2.1.6. Les niveaux d'impersonnation

Lorsqu'un utilisateur accède à un programme, celui-ci s'exécute dans le contexte de sécurité de l'utilisateur. La combinaison du jeton d'accès et du programme lancé s'appelle un "Sujet". Souvent, un même "Sujet" peut être amené à appeler d'autres processus pour réaliser sa tâche, comme un processus serveur.

Il peut parfois être utile qu'un processus serveur utilise le contexte de sécurité de l'utilisateur ayant fait appel à lui, plutôt que son propre contexte de sécurité, tout simplement parce qu'un processus serveur peut disposer de privilèges moindres ou supérieurs que ceux de l'utilisateur ayant fait appel à lui. Si le procédé d'impersonnation n'existait pas, les requêtes à des serveurs dépendraient directement du contexte de sécurité dans lequel a été lancé le processus serveur.

Ainsi, dans le cas d'une requête d'accès à un fichier, le processus serveur de fichiers peut disposer de privilèges systèmes. Si l'appel a lieu dans le contexte de sécurité du serveur de fichier, l'utilisateur pourra donc avoir accès à TOUT le système de fichiers, outrepassant ainsi les permissions restrictives qui auraient pu être positionnées sur les fichiers. Le mécanisme d'impersonnation permet de contourner la difficulté en effectuant la requête dans le contexte de sécurité de l'utilisateur et donc en obligeant le serveur à réagir comme s'il était lui-même l'utilisateur ayant réalisé la requête.

Les différents niveaux d'impersonnation sont les suivants :

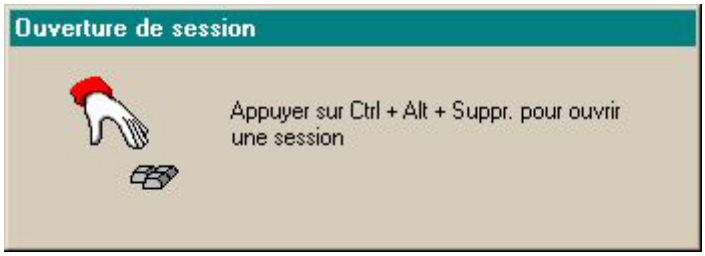
Niveau d'Impersonnation	Description
SecurityAnonymous	Le processus serveur ne peut identifier le client. Pas de possibilité d'Impersonnation
SecurityIdentification	Le processus serveur ne peut qu'identifier le client (et donc accéder à son jeton d'accès) mais ne peut pas réaliser d'impersonnation. Utile pour déterminer au niveau du serveur si un utilisateur a le droit d'effectuer telle ou telle requête : c'est alors le processus serveur qui gère les permissions et non le système d'exploitation.
SecurityImpersonation	Le processus serveur peut identifier le client (et donc accéder à son jeton d'accès) et peut réaliser une Impersonnation en local. Il ne peut pas réaliser d'impersonnation pour un client distant.
SecurityDelegation	Non disponible actuellement (sauf sous Windows 2000). Le processus serveur peut identifier le client (et donc accéder à son jeton d'accès) et peut réaliser une Impersonnation pour un client local **et** distant.

2.2. Processus d'ouverture de session sous Windows NT 4.0

Le but de l'ouverture de session est de fournir à l'utilisateur un jeton d'accès qui contiendra les droits et les SID locaux et globaux relatifs à cet utilisateur.

Toute la conception du mécanisme d'ouverture de session sous Windows NT repose sur une architecture client / serveur. Simplement dans le cas d'une ouverture de session en local, le serveur est exécuté sur la même machine que le client.

Chaque utilisateur doit procéder à une ouverture de session Windows NT afin d'utiliser les ressources de cette machine ou du réseau sur laquelle elle est installée**. Ce processus de Logon est obligatoire**. Une fois ce processus réalisé, un jeton d'accès est généré, qui contient des informations de sécurité spécifique à l'utilisateur concerné, entre autres : identificateur de sécurité (SID), identificateur de groupes, droits et permissions utilisateur. L'utilisateur, ainsi que tout processus lancé par celui-ci, est alors identifié par ce jeton.



2.2.1. Procédure d'ouverture de session détaillée

Au cours du démarrage de Windows NT, le processus WINLOGON est lancé et crée un environnement contrôlé d'ouverture de session. Les 4 étapes décrites par la suite sont celles qui sont effectuées avant une quelconque interaction avec l'utilisateur.

1. WINLOGON crée une fenêtre sécurisée ayant un accès exclusif au système et ouvre trois environnements de travail séparés ("application", "écran de veille" et "environnement du Winlogon"). Le processus Winlogon tourne alors en mode exclusif ; dès cet instant, tout processus en mode utilisateur est mis en attente, jusqu'à ce que la procédure soit menée à son terme ou annulée. Le fait que les applications en mode utilisateurs soient interrompues au cours du processus a une raison de sécurité : à cause de cette interruption, les chevaux de Troie relatifs au logon sont stoppés, ainsi que d'éventuels « key loggers » - programmes enregistrant les frappes claviers.

2. WINLOGON ouvre ensuite une connexion LPC vers la Local Security Authority (LSA) du système local. Cette connexion, établie par le biais de l'API *LsaRegisterLogonProcess*, est un canal sécurisé au travers duquel les informations d'authentification seront passé au package d'authentification (par défaut MSV1_0) à fins de validation.

3. WINLOGON interroge alors le package d'authentification et obtient alors un numéro de processus pour le package installé, numéro qui lui servira pour le passage des informations d'authentification.

4. Après avoir enregistré les informations d'environnement récupérées durant les précédentes phases, la Security Attention Sequence (SAS - par défaut la combinaison de touches CTRL-ALT-DEL) est activée et l'environnement de travail est verrouillé.

Une fois activée, un utilisateur peut dès lors utiliser la combinaison de touches du SAS. Ce SAS génère une interruption qui est envoyée au système ; le système réagit alors en amorçant la séquence de Logon. Dès qu'un utilisateur active le SAS, plus aucun processus ne peut alors accéder à l'environnement de travail. A ce point de la procédure, l'interface graphique d'ouverture de session est lancée et permet alors à l'utilisateur de saisir les informations relatives à l'authentification (couple login/password et type de connexion - distante ou locale).

WINLOGON récupère alors ces informations et les transmet en clair, via la fonction *LSALogonUser*, auprès de la LSA (LSASS.EXE) en même temps que le numéro de processus du package d'authentification (MSV1_0). Le LSA envoie alors les données d'authentification en clair au MSV1_0 pour vérification.

Ce package est séparé en deux moitiés (dites "hautes" et "basses"), la partie "haute" chiffre le mot de passe aux formats Lan Manager (grâce à une "One Way Function" ou OWF) et Windows NT (par un MD4). Le login de l'utilisateur n'est pas chiffré. Pour plus d'informations sur le procédé de chiffrement des mots de passe, se référer au § 2.4 (Mécanisme de stockage des mots de passe).

Le MSV1_0 vérifie alors le type d'ouverture de session demandée (locale, distante ou service). Si le type est "*local*" ou "*service*", le MSV1_0 envoie alors les informations chiffrées à sa partie basse. Si le type est "*distant*" (cas de la connexion dans un domaine), ces informations sont transmises directement au processus NETLOGON local à la machine qui sera chargé de la communication avec le serveur d'authentification distant.

Dans les deux cas, le MSV1_0 récupère et vérifie les données d'authentification avec le contenu de la base SAM correspondante (locale ou distante) afin de déterminer si ces informations sont valides et si l'utilisateur a le droit d'ouvrir une session du type demandé. Le compte est scruté régulièrement par la suite afin de vérifier dans le temps que de nouvelles restrictions ne s'appliquent.

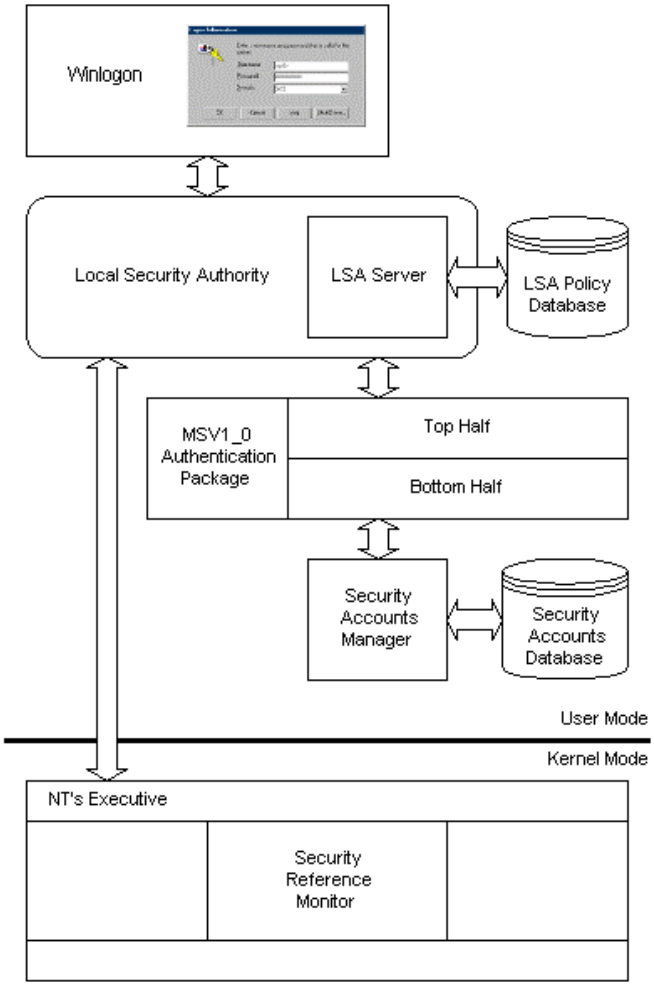
En cas de validation, le package d'authentification poursuit son action et collecte les informations concernant le compte utilisateur parmi lesquelles :

1. L'identificateur de sécurité de l'utilisateur (SID)
2. Les SIDs de chaque groupe auquel appartient l'utilisateur,
3. Le SID du propriétaire par défaut,
4. Le DACL (Discretionnary Access Control List) par défaut

Une fois ces opérations effectuées, le MSV1_0 passe ces informations à l'exécutif de Windows NT pour la création d'un jeton d'accès. Selon que la demande d'ouverture de session est locale ou distante, l'exécutif créera soit un jeton Primaire (ouverture de session locale) soit un jeton dit "d'impersonnation" (ouverture de session distante). Ce jeton est alors renvoyé au MSV1_0 afin d'initier la session utilisateur.

Enfin, le processus WINLOGON crée une tâche, qui lance un nouveau Shell et lance le GUI. Toutes les autres tâches démarrées ensuite hériteront du jeton créé.

La figure suivante résume les différentes étapes de l'ouverture de session :



Ce jeton ne sert pas seulement à valider les accès aux objets du système**, il est également utilisé pour identifier les actions de l'utilisateur dans les journaux d'événement et pour accéder aux ressources réseau.**

Nota : les composants qui gèrent la partie graphique du processus de Logon sont situés dans une librairie du système appelée MSGINA.DLL (GINA pour Graphical Identification aNd

Authentication). Rien n'empêche les développeurs de remplacer cette librairie par une de leur propre conception, pour peu que l'on respecte les APIs du système d'exploitation ; en particulier, il est possible, en modifiant cette DLL, de changer la combinaison de touches du SAS.

Il est possible, dans une certaine mesure, de modifier le comportement du processus WINLOGON en modifiant la base des registres sous la clef HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon. Sans aller jusqu'à modifier « à la main » la base des registres, on peut réaliser les mêmes opérations avec le programme POLEDIT.EXE (Policy Editor).

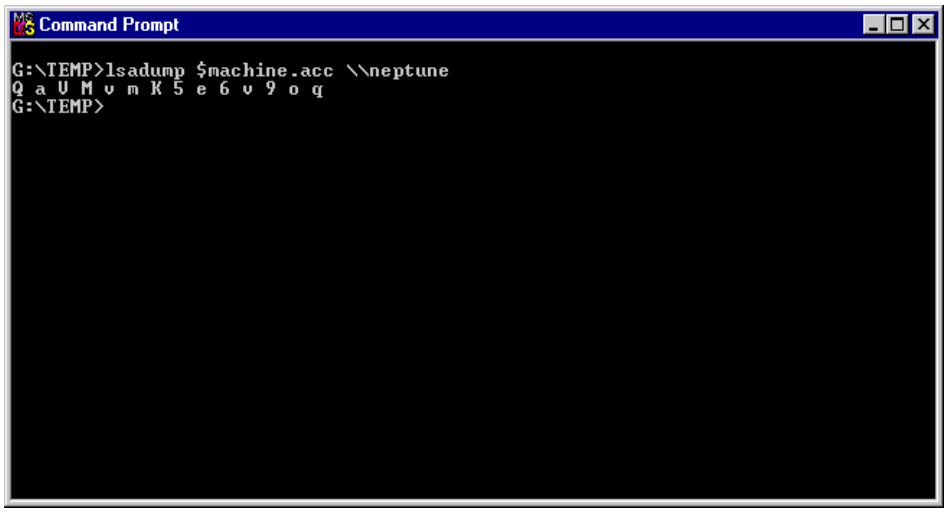
2.2.2. Connexion dans un domaine

Si une machine Windows NT fait partie d'un domaine, il ne suffit pas d'être authentifié sur la machine locale, il est également nécessaire de l'être sur l 'ensemble du domaine. Dans ce cas de figure, le processus WINLOGON appelle le processus NETLOGON pour gérer la communication avec le serveur distant mais la procédure d'ouverture de session dans un domaine reste strictement identique à celle d'une ouverture de session locale.

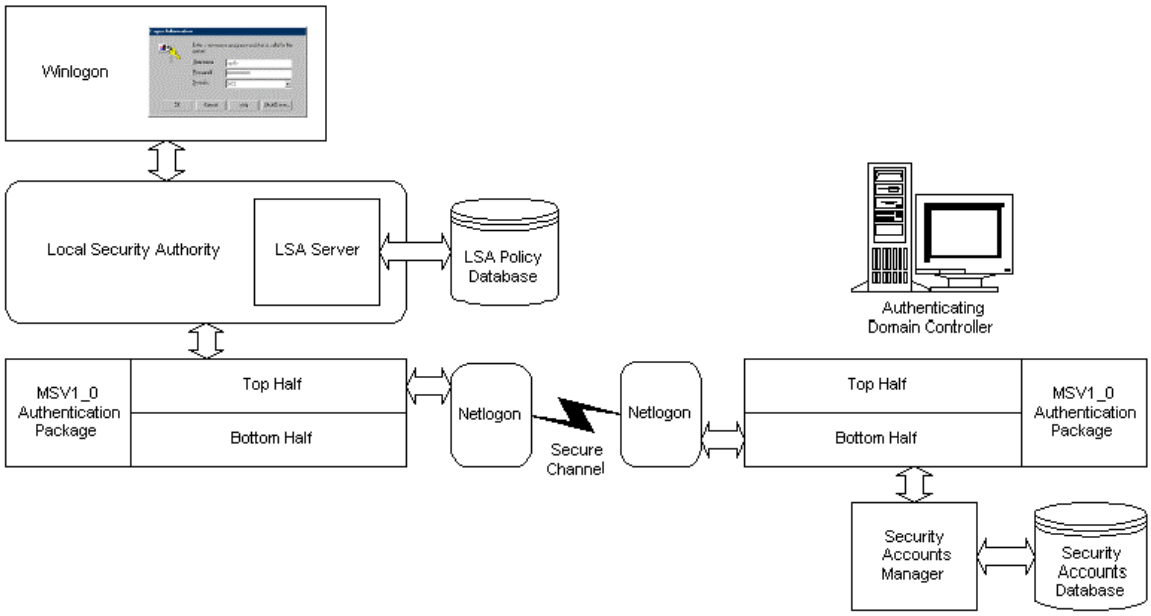
Le processus NETLOGON a alors la charge de contacter un serveur de domaine pour lui passer les données d'authentification.

Une fois que le serveur de domaine est trouvé, NETLOGON doit alors vérifier si la machine locale est membre de ce domaine. Il réalise ceci en tentant d'établir un canal de communication sécurisé avec le serveur de domaine. Cette communication est réalisée en utilisant un mot de passe spécifique. Ce mot de passe est généré aléatoirement par un serveur de domaine pour chaque machine membre du domaine puis transmis aux machines concernées lors de l'entrée dans le domaine. Il est changé par le serveur de domaine tous les sept jours, et retransmis aux machines concernées par un canal sécurisé par le mot de passe précédent.

Enfin, le mot de passe est stocké dans la sous-clef $MACHINE.ACC, située dans HKEY_LOCAL_MACHINE\ SECURITY\Policy\LSA\Secrets. Le mot de passe n'est pas accessible (ni même visible) dans l'état à l'aide des éditeurs de registre standard (regedit ou regedt32). On peut cependant en lister le contenu à l'aide d'un outil du domaine public appelé LSADump, pour peu de disposer de privilèges administrateur sur la machine visée



C'est à travers de ce canal sécurisé que seront transmises les informations d'authentification entre le client et le serveur.



Le mécanisme d'authentification au travers du réseau, via le canal sécurisé, est décrit plus précisément au § 2.5 -

Mécanisme d'authentification sur le réseau

2.3. Processus d'ouverture de session sous Windows 2000

Windows 2000 offre la gestion native de protocoles jusqu'ici non supportés par Windows NT (sauf à utiliser des développements de tierce partie). Pour l'essentiel, on peut noter le support de Kerberos V5 pour l'accès sécurisé aux ressources (authentification), ainsi que des fonctionnalités IPSEC.

Kerberos :

Le protocole Kerberos fut créé à l'origine au sein du MIT en 1983 par les ingénieurs travaillant sur le Projet Athena. Kerberos V5 est désormais un standard de l'IETF (Internet Engineering Task Force) dont les spécifications sont décrites par la RFC[1] 1510. Selon Microsoft, l'implémentation de Kerberos V5 suit les recommandations de cette RFC, et les mécanismes et les formats utilisés pour le passage des jetons de sécurité suivent la RFC 1964.

Dans les faits, et selon la documentation Microsoft, la GSS-API[2] définie dans la RFC 1964 n'est utilisée que dans le cas où l'un des deux cotés, client ou serveur, n'est pas un système Windows 2000. Dans le cas contraire, c'est la SSPI[3] , mécanisme propriétaire de Microsoft semblable à la GSS-API, qui est utilisée. La SSPI n'est qu'une implémentation particulière de la RFC 1964 dans laquelle Microsoft utilise des champs inutilisés du protocole pour passer des informations spécifiques à Windows 2000 ; de fait, les formats utilisés par la SSPI n'étant pas documentés (la SSPI est présentée comme un boite noire, regroupant des API communes), il apparaît délicat de faire fonctionner ensemble un système Windows 2000 avec un autre système compatible Kerberos V5, tout en bénéficiant de l'ensemble des fonctionnalités offertes par l'utilisation de Kerberos dans Windows 2000.

Ceci étant, on trouve sur l'Internet l'ensemble des méthodes nécessaires :

1. pour faire tourner une machine Unix en tant que Serveur Kerberos pour une architecture Windows 2000,

2. pour utiliser un serveur Windows 2000 en tant que serveur Kerberso dans une architecture Kerberos classique

Cette implémentation particulière de la RFC 1964 a d'ailleurs provoqué l'ire de la communauté Internet et en particulier de l'IETF qui, bien évidemment, n'a pas été consulté.

Dans son principe, Kerberos est un mécanisme d'authentification mutuel entre clients et serveurs ; un client réalise une authentification mutuelle sur un serveur Kerberos afin d'obtenir un jeton d'accès pour une ressource. Ce jeton d'accès, à validité limitée dans le temps, sert alors de moyen d'authentification pour accéder à la ressource considérée.

Dans les années qui ont précédé l'arrivée de Windows 2000, l'authentification dans le monde Windows NT était assurée par un mécanisme propriétaire appelé NTLM. Ce mécanisme a montré ses limites en termes de performances et d'efficacité et c'est donc vers Kerberos V5 que s'est tourné Microsoft pour le mécanisme d'authentification par défaut de Windows 2000. Cependant, Windows 2000 continue à assurer une compatibilité avec Windows NT puisqu'il est capable de réaliser des authentifications NTLM dans le cas de communications avec des machines Windows NT.

Pour ce qui concerne l'ouverture de session sous Windows 2000, le comportement par défaut lorsque l'on tente de s'authentifier depuis une machine Windows 2000 Pro sur un serveur Windows 2000 est d'utiliser le protocole d'authentification Kerberos.

[1] Request For comment
[2] Generic Security Service Application Program Interface
[3] Security Support Provider Interface

2.4. Mécanisme de stockage des mots de passe

Le système d'exploitation Windows NT stocke les mots de passe des utilisateurs dans une base de données spécifique appelée SAM. La base SAM contient tous les noms des utilisateurs référencés sur la machine, leur mot de passe sous sa forme chiffrée, les groupes auxquels ils appartiennent, ainsi que la description des groupes.

Cette base SAM est protégée par le mécanisme de contrôle d'accès fourni par le système d'exploitation. Elle est accessible, pour peu de disposer des droits suffisants, soit directement par la lecture des fichiers SAM (situés dans `%Systemroot%\system32\config\SAM`), soit par interrogation de la base des registres.

La structure des données utilisateurs en SAM dispose de deux champs disponibles pour stocker les mots de passe :

1. le premier de ces champs permet le stockage du mot de passe au format Lan Manager (pour d'historiques raisons de compatibilité Win95 et Win3.11, qui ne peuvent s'authentifier qu'avec ce mécanisme),

2. le second champ permet de stocker le mot de passe selon le format natif de Windows NT.

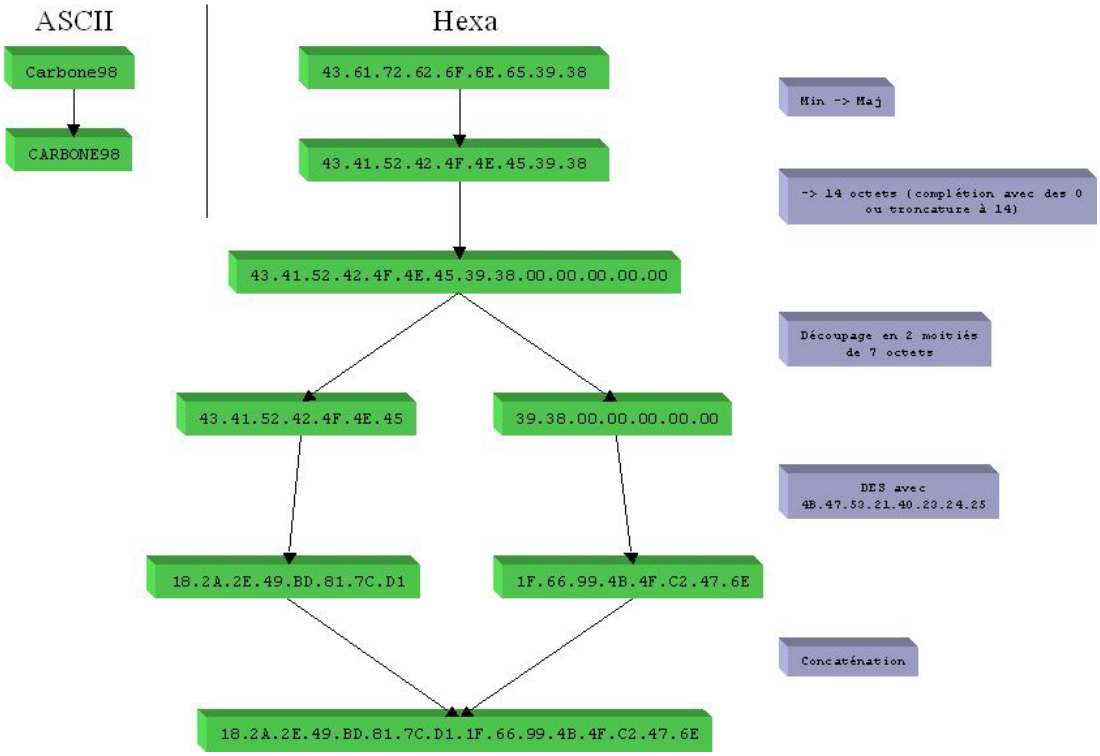
Dans les deux cas, **le mot de passe n'est pas stocké en clair**, mais sous sa forme chiffrée. La différence entre ces deux mécanismes est l'algorithme de chiffrement utilisé.

2.4.1. Structure Lan Manager (LM hash)

L'algorithme de chiffrement du « LANMAN password » est le suivant :

- Passer le mot de passe en clair en majuscule.
- Si le mot de passe en clair est plus grand que 14 caractères, alors le tronquer à 14 caractères, sinon le compléter avec des 0.
- Former deux clefs de chiffrement K1 et K2 avec les deux moitiés (7 octets) du mot de passe résultant du point précédent.

Chiffrer la « magic value » 4B.47.53.21.40.23.24.25h avec K1 et K2 avec l'algorithme de chiffrement DES. Le résultat du chiffrement d'avec K1 forme les 8 octets de poids faible du « LANMAN password ». Le résultat du chiffrement avec K2 forme les 8 octets de poids fort.



Création d'un Hash Lan Manager

Exemple reprenant la Figure ci-dessus :

Avec le mot de passe suivant « Carbone98» ;

1/ Carbone98 → CARBONE98 (passage en majuscules)

2/ CARBONE98 → `43.41.52.42.4F.4E.45.39.38.00.00.00.00.00` (complétion avec des zéros)

3/ `43.41.52.42.4F.4E.45.39.38.00.00.00.00.00` → `43.41.52.42.4F.4E.45` + `39.38.00.00.00.00.00`
(découpage en deux parties de 7 octets chacune)

4/ `43.41.52.42.4F.4E.45` → `18.2A.2E.49.BD.81.7C.D1` et
`39.38.00.00.00.00.00` → `1F.66.99.4B.4F.C2.47.6E`
(chiffrement de la « magic value » avec K1 et K2)

5/ Finalement, le LM hash sera
`18.2A.2E.49.BD.81.7C.D1.1F.66.99.4B.4F.C2.47.6E`

Ainsi, découvrir un mot de passe stocké sous la forme LM Hash revient à découvrir 2 mots de passe d'une taille de 7 caractères maximum (insensibles majuscules / minuscules).

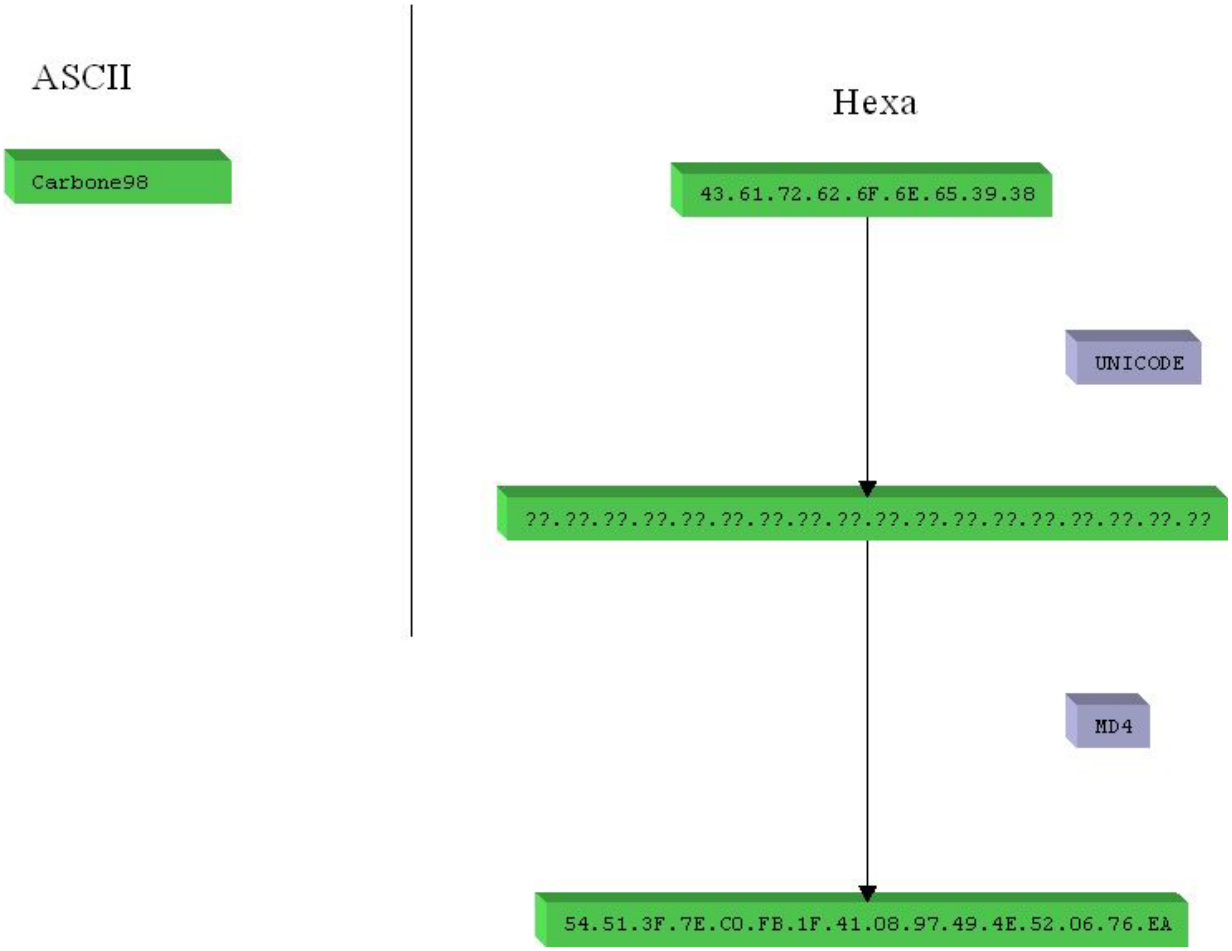
D'autre part, dans la mesure où il n'existe pas de mécanisme de « salage », **deux mots de passe identiques auront le même cryptogramme LM Hash**.

Il est également facile de déterminer si un mot de passe a une taille inférieure à 8 caractères. En effet, la seconde partie du LM Hash sera alors toujours 0xAAD3B435B51404EE (résultat du chiffrement de 0x4B47532140232425 avec 0x00000000000000).

2.4.2. Structure native Windows NT (NT hash)

L'algorithme de chiffrement du « NT password » est le suivant :

- Le mot de passe est convertit au format UNICODE.
- Un MD4 (algorithme de hachage permettant de calculer une empreinte d'un motif binaire) est appliqué sur le mot de passe résultant pour former les 16 octets du « NT password ».



Création d'un Hash Windows NT

D'autre part, dans la mesure où il n'existe pas de mécanisme de « salage », deux mots de passe identiques auront le même cryptogramme NT Hash.

2.4.3. Autres emplacements de stockage des mots de passe

Sous Windows NT, outre la base SAM, les mots de passe peuvent être stockés à d'autres endroits du système.

Ainsi, chaque client Windows NT dispose d'**un cache d'authentification** (c'est ce qui permet à un utilisateur de se connecter quand même, hors réseau, quand un contrôleur de domaine n'est pas joignable).

Cette structure de cache placée dans la base des registres conserve une copie des dix dernières authentifications (hashes Lan Manager et NT). Ce cache est protégé logiquement contre une lecture par les utilisateurs simples, il peut cependant être accessible par un « dump » direct du disque dur.

D'autre part, une copie de la SAM (située sous `%systemroot%\repair`) est également disponible (à conditions d'avoir au préalable généré une disquette de réparation d'urgence) et est utilisée par le système en cas de problèmes matériels. Cette copie est protégée logiquement contre une lecture par les utilisateurs ne disposant pas de privilèges.

Plus généralement, une copie de la SAM peut être stockée sur les disquettes de réparation d'urgence (ainsi que sur des bandes de sauvegarde quand on sauvegarde un disque système) : il convient donc de protéger physiquement ces supports amovibles.

2.4.4. Stockage des mots de passe par les anciens clients Windows

L'ouverture de session sous les stations Windows 3.11 for Workgroups et Windows 95/98 utilise un fichier d'extension PWL dans lequel les mots de passe sont enregistrés. Bien que le fichier soit crypté, l'algorithme utilisé n'est pas résistant. Ce fichier permet de mémoriser tous les mots de passe saisis par l'utilisateur au cours de la session, de façon à automatiser par la suite ces mêmes connexions.

Il faut EVITER de se connecter en administrateur sur le domaine à partir d'une station Windows intégrée dans un domaine.

Il est possible (et recommandé) de désactiver la mise en cache des mots de passe.

Windows for Workgroups

Dans le fichier SYSTEM.INI, ajoutez :

[Network]
passwordcaching=no

Windows 95

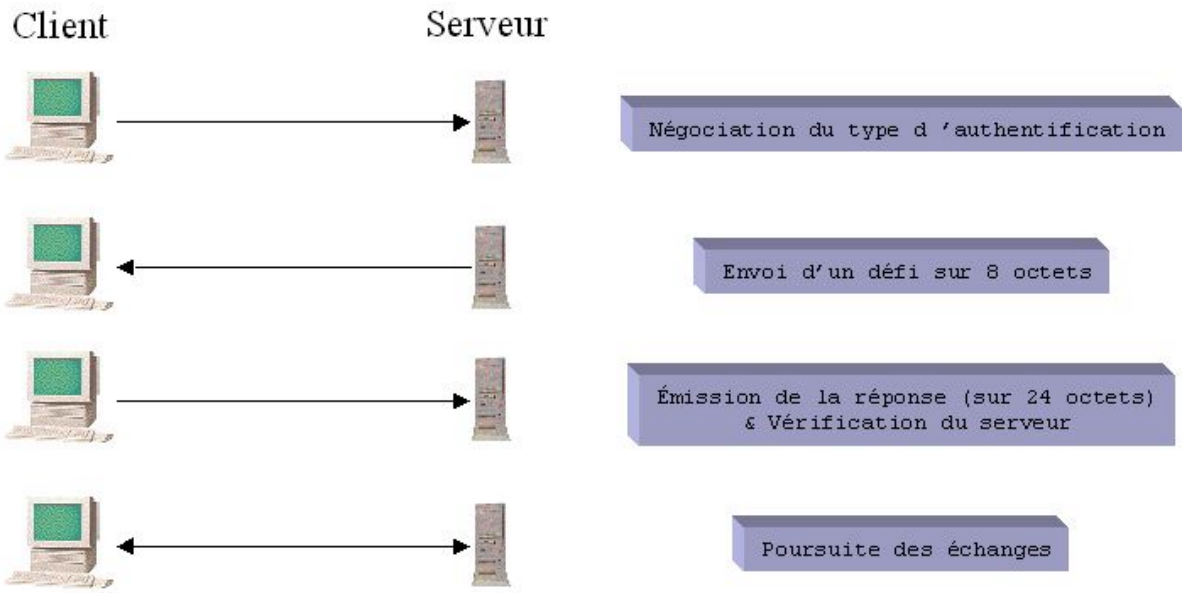
Modifier la base de registre de chacune des stations :

Ruche **HKEY_LOCAL_MACHINE\SYSTEM**
Clé **SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Policies\ Network**
Nom **DisablePwdCaching**
Type **Chaîne**
Valeur **1** (Désactivation de la mise en cache des mots de passe)

2.5. Mécanisme d'authentification sur le réseau

D'une façon générale, le principe d'authentification entre un client et un serveur NT est le suivant :

- Etablissement d'une session NetBIOS entre le serveur et le client
- Négociation du type d'authentification disponible sur le client
- Le serveur envoie un défi sur 8 octets
- Le client calcule sa réponse et l'envoie au serveur
- Le serveur calcule la réponse correcte (Lan Man et NT) et compare son résultat avec celui du client.
- Si son résultat NT n'est pas correct, il vérifie son résultat Lan Man avec celui fourni par le client (pour compatibilité Windows 3.11 et Windows 95/98)
- Le serveur valide l'authentification puis poursuit les échanges.



Mécanisme d'authentification Windows NT

2.5.1. Authentification Lan Manager

Le protocole d'authentification entre un client et un serveur sur un réseau Windows NT, en suivant le schéma d'authentification Lan Manager, est le suivant :

1/ Supposons que l'utilisateur à authentifier dispose d'un LM Hash de valeur 0x182A2E49BD817CD11F66994B4FC2476E (ce qui est le LM Hash du mot de passe « Carbone98 »).

2/ Le serveur envoie un défi de 8 octets à l'utilisateur.

3/ L'utilisateur prend son LM Hash (0x182A2E49BD817CD11F66994B4FC2476E), et ajoute 5 octets de valeur nulle à celui-ci (le LM Hash devient alors 0x182A2E49BD817CD11F66994B4FC2476E0000000000)

4/ La chaîne 0x182A2E49BD817CD11F66994B4FC2476E0000000000 est scindée alors en trois groupes de 7 octets :

182A2E49BD817C + D11F66994B4FC2 + 476E0000000000

5/ Chacune de ces chaînes est ensuite modifiée pour former une clef DES de parité paire de 8 octets (on prend chaque bloc de 7 bits auquel on rajoute un bit de parité paire)

6/ Nous avons donc maintenant 3 clefs DES de 8 octets (clef1, clef2 et clef3)

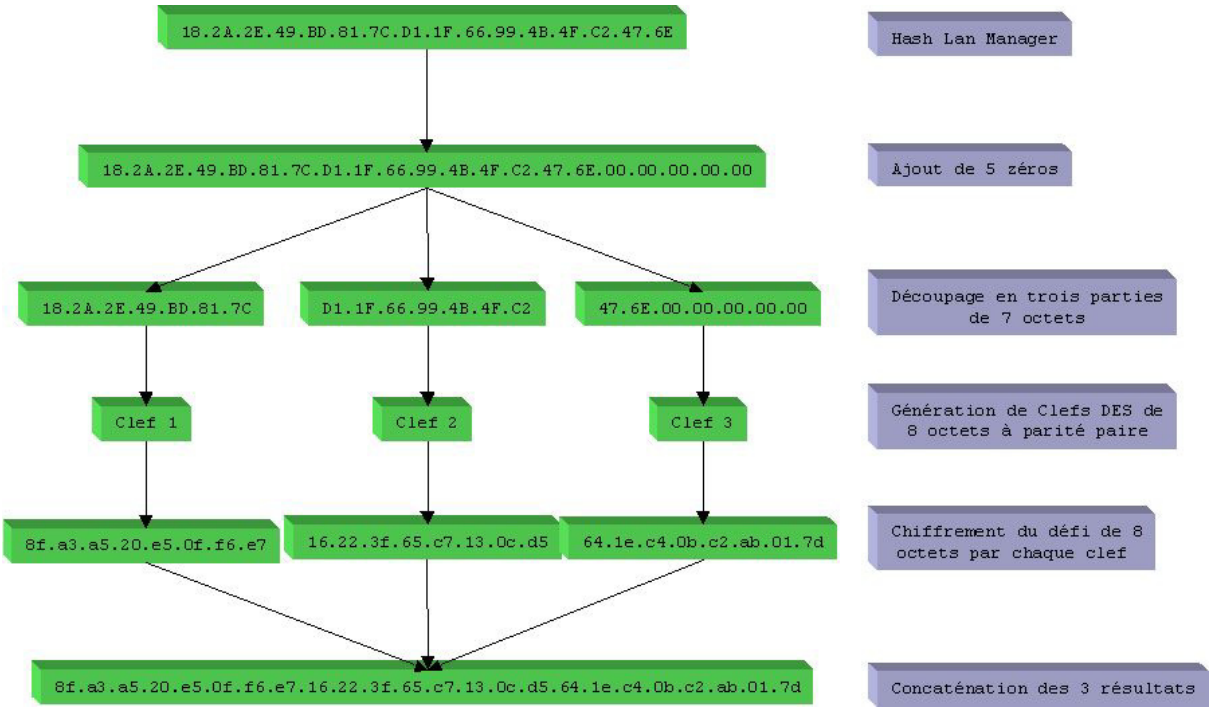
7/ clef1 est utilisée pour chiffrer le défi.
Le résultat est 0x8fa3a520e50ff6e7.

8/ clef2 est utilisée pour chiffrer le défi.
Le résultat est 0x16223f65c7130cd5.

9/ clef3 est utilisée pour chiffrer le défi.
Le résultat est 0x641ec40bc2ab017d.

10/ Ces trois valeurs sont concaténées et envoyées au serveur sous la forme d'une réponse de 24 octets (0x8fa3a520e50ff6e716223f65c7130cd5641ec40bc2ab017d)

11/ De son coté, le serveur a réalisé la même opération : il n'a plus qu'à comparer le résultat de son calcul avec celui renvoyé par l'utilisateur ; en cas de résultat identique, l'utilisateur est authentifié au sein de sa session.



Mécanisme de Défi/Réponse Lan Manager

2.5.2. Authentification Native Windows NT

Lors d'une authentification NT pure, le défi est chiffré avec comme clef le Hash Windows NT, puis cette réponse de 24 octets est émise auprès du serveur.

2.5.3. Variante d'authentification HTTP Microsoft

Lorsqu'un serveur est équipé du service Internet Information Service (IIS) de Microsoft, il est possible de demander aux clients d'effectuer une authentification pour tout ou partie des requêtes. Deux options sont possibles : la première consiste à demander au client une authentification de

base (dans ce cas, le couple login/password passe en clair sur le réseau), la seconde est une variante de l'authentification LanManager/NT (type d'authentification NTLM) qui permet de positionner des permissions d'accès aux répertoires sur les utilisateurs et/ou les groupes déclarés sur le serveur.

Pour la seconde solution, une ouverture de session HTTP a lieu entre le client et le serveur, durant laquelle le serveur envoie une requête de défi/réponse auprès du client ; le défi sur 8 octets est alors encodé au format MIME64 au sein d'une trame HTTP. Le client renvoie alors une réponse HTTP de la forme :

GET filepath	La commande GET classique du protocole HTTP
Accept	liste des types MIME supportés par le client
Referer	L'URL sur laquelle se trouve actuellement le client
Accept-Language	la langue du client (ex : « en » pour l'anglais)
UA-pixels	Taille de l'écran du client
UA-color	Nombre de couleurs supportées par le client
UA-OS	Système d'exploitation du client (ex : « Windows NT »)
UA-CPU	Type de processeur du client (ex : « x86 » pour un Intel)
User-Agent	Le navigateur utilisé (ex : « Mozilla » pour Netscape)
Host	Le nom du serveur Web
Connection	Le type de connexion
Authorization	Le type d'authentification et les données d'authentification

Dans ce cas, le champ « Authorization » est rempli avec la valeur « NTLM », suivi de son nom de login, du nom de sa machine, du nom de son domaine, puis des 48 octets de la réponse au défi. Compte tenu du fait que le protocole HTTP ne supporte que des caractères codés sur 7 bits et que la réponse au défi NTLM est codée sur 8 bits significatifs, la réponse au défi est ici encodée au format MIME64.

Seules les différentes versions de Internet Explorer sont capables de s'authentifier de cette manière auprès d'un serveur IIS.

Le comportement par défaut d'un Windows NT Workstation avec Internet Explorer comme navigateur est d'envoyer la réponse au défi sous les deux formes connues Lan Manager et NTLM. A noter que ce mécanisme est mis en œuvre **systématiquement et à l'insu de l'utilisateur,** si le serveur le demande et si le client dispose d'un client Internet Explorer.

A partir de la version 4 de Internet Explorer, il est possible de paramètrer le client pour ne pas envoyer systématiquement la variante d'authentification HTTP (Paramètres / Internet, Onglet Sécurité). Depuis cette version il s'agit d'ailleurs du comportement par défaut du navigateur Internet de Microsoft.

2.6. Le système de fichiers NTFS

Le système de gestion de fichiers natif de Windows NT est NTFS (New Technology File System), largement inspiré des développements précédents pour OS/2 (HPFS - High Performance File System). Ce système de fichier permet de gérer des listes de contrôle d'accès afin de déterminer qui a accès aux objets du système de fichiers.

2.6.1. Fonctionnement interne de NTFS

Par rapport au système FAT, les volumes NTFS disposent en plus des fonctionnalités suivantes :

- Capacité à gérer des partitions de plus de 2Go
- Support des noms longs et des caractères Majuscules/Minuscules
- Positionnement de listes à contrôle d'accès sur les objets gérés par le système de gestions de fichiers,
- Audits des différents accès aux objets,
- Procédé d'accès aux objets gérés par des mécanismes transactionnels et permettant d'assurer des fonctions d'intégrité, et de tolérances aux pannes de niveau élémentaire (mécanismes de journaux avant / journaux après)
- Possibilité de gérer du mirorring entre disques, et des agrégats de partitions par bandes.
- Procédé de défragmentation "à la volée".

Tolérance aux pannes

NTFS utilise un mécanisme transactionnel pour les accès aux objets dont il a la responsabilité. Lorsqu'une donnée est accédée, le sous-système de disques vérifie les informations relatives aux fichiers accédés dans une table appelée Master File Table (MFT).

Cette table, qui est un fichier caché du système, nommé $MFT et situé à la racine du disque, contient toutes les informations concernant les données stockées sur le disque, dont :

- des informations utilisées pour monter le système de fichier,
- la liste des mauvais clusters,
- les attributs de chaque fichier

Lors d'une requête d'accès à un fichier, la MFT est interrogée pour vérifier l'existence du fichier et, en cas de succès, les attributs de sécurité (SIDs) sont chargés et comparés au jeton d'accès du processus appelant.

Lorsque le fichier est ouvert, une entrée est créée par le Log File Service (LFS) et stockée sur le disque dans le fichier caché $LogFile. Ce fichier est utilisé par le LFS pour enregistrer les modifications réalisées sur le fichier. Ce qui est enregistré dans ce fichier ne concerne cependant **que les modifications sur le système de fichiers** (emplacement sur le disque des blocs modifiés par exemple) et non pas les modifications sur le fichier. Dans la mesure ou c'est un mécanisme transactionnel qui est utilisé pour l'écriture sur le disque, les données sont écrites au sein d'une transaction ininterruptible ce qui permet, en cas de plantage d'une entrée / sortie sur le disque de revenir à une situation antérieure sans difficulté. L'écriture est programmée à intervalles réguliers par un mécanisme de "write back", toute modification d'un fichier étant d'abord réalisée en mémoire avant d'être effective. Grâce à ce mécanisme, les altérations de données qui auraient pu

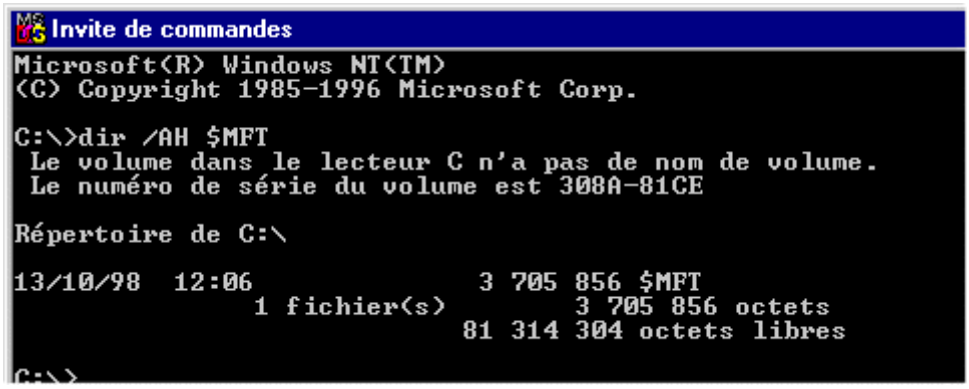
avoir lieu en mémoire peuvent être éventuellement réparées par consultation du fichier $LogFile par le système.

Les fichiers cachés de Windows NT

On a vu que NTFS gérait au moins deux fichiers cachés ($MFT et $LogFile). Ces attributs "cachés" des fichiers vont plus loin que le simple bit H hérités des systèmes FAT, puisqu'il est effectivement impossible de visualiser ces fichiers en utilisant les APIs utilisateurs standards de Windows NT. Il existe d'autres fichiers cachés, et portant le nom de fichiers de MetaData ("metadata files") dont voici la liste :

Nom du fichier	Description
$MFT	**Master File Table** : stocke toutes les informations sur toutes les données stockées sur le disque (y compris les autres fichiers Metadata)
$MFTMirr	**MFT Mirror File** : contient les 16 premiers enregistrements de la MFT et est stocké en milieu de volume. Ce fichier est utilisé pour réparer des dommages à la MFT.
$LogFile	Ce fichier critique est utilisé par le Log File Service pour gérer les modifications aux fichiers et répertoires sur la structure du système de fichiers NTFS. Utilisée en cas de crash du système.
$Volume	Ce fichier contient la version de NTFS utilisée et le nom du volume.
$AttrDef	**Attribute Definition File** : contient des informations sur les types d'attributs acceptables permis pour l'utilisation du volume, comme le fait que le disque soit ou non recouvrable en cas de panne.
$Bitmap	Ce fichier contient, pour chaque cluster, une information indiquant si celui-ci est utilisé ou occupé. L'information est stockée sous la forme d'un tableau de bits.
$Boot	Ce fichier contient des informations de bootstrap pour accéder au volume NTFS.
$BadClus	En cas de détection de mauvais clusters, ceux ci sont référencés dans ce ficher afin de ne plus être utilisés ultérieurement. Si un mauvais cluster est détecté, NTFS positionne un bit dans le fichier $Volume afin de provoquer un CHKDSK au prochain redémarrage en vue de l'éventuel réparation des clusters.
$Quota	Un fichier inutilisé sous Windows NT 4.0, et susceptible sous Windows 2000 de contenir des informations sur les quotas de disque des utilisateurs.
$UpCase	Ce fichier est utilisé pour mapper les lettres majuscules avec les lettres minuscules pour l'accès aux fichiers et répertoires

Il n'est pas possible d'ouvrir ces fichiers avec un quelconque éditeur, par contre on peut visualiser leur existence et leur taille par la simple frappe de la commande "`DIR /AH NomdeFichier`" à la racine du disque (C:\).

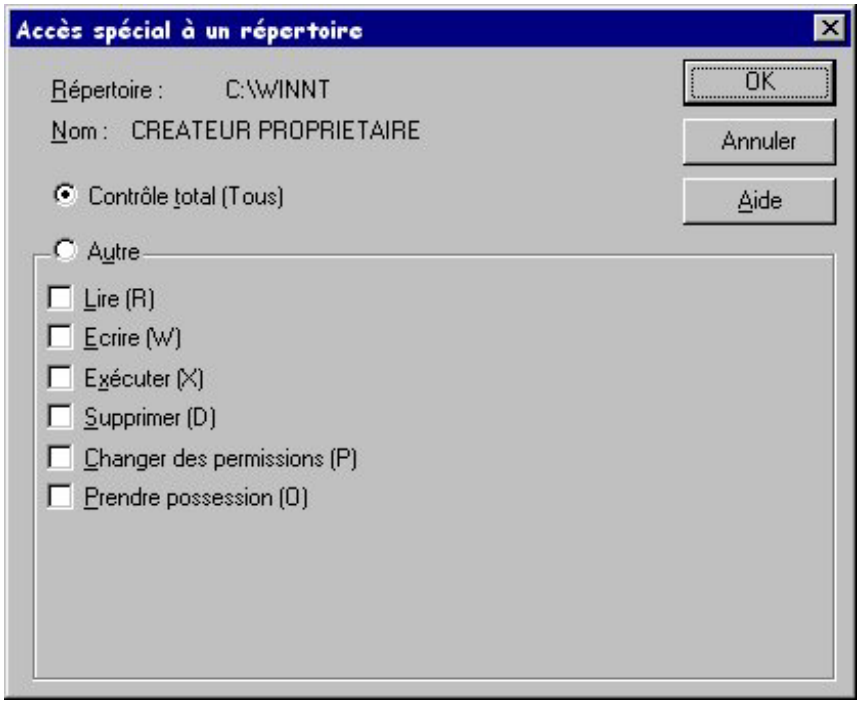


2.6.2. Les ACLs

Les ACLs sont des listes d'utilisateurs et de groupes qui disposent de permissions pour accéder ou agir sur les objets du système de fichiers. Chaque objet Windows NT dispose d'un descripteur de sécurité (voir § 2.1.4 - Descripteurs de Sécurité) dans lequel sont stockées les ACLs.

Chaque permission listée ci dessous peut être associée à un utilisateur ou à un groupe. Les permissions accordables sous NTFS sont les suivantes :

R	Répertoire :	permet de lister le contenu d'un répertoire
	Fichier :	permet de lire le contenu d'un fichier
W	Répertoire :	permet d'ajouter des fichiers et de créer des sous-répertoires
	Fichier :	permet de modifier le contenu d'un fichier
X	Répertoire :	permet de traverser un répertoire (cd)
	Fichier :	permet d'exécuter un fichier si c'est un programme
D	Répertoire :	permet d'effacer répertoire et sous-répertoire
	Fichier :	permet d'effacer un fichier
P	Répertoire :	permet de modifier les permissions d'un répertoire
	Fichier :	permet de modifier les permissions d'un fichier
O	Répertoire :	permet de s'approprier un répertoire
	Fichier :	permet de s'approprier un fichier



Windows NT fournit en outre une liste de permissions standards, prédéfinies, parmi lesquelles :

Nom	*Répertoire*	*Fichier*
Aucun Accès	Aucun	Aucun
Lister	RX	Non spécifié
Lire	RX	RX
Ajouter	WX	Non spécifié
Ajouter et lire	RWX	RX
Modifier	RWXD	RWXD
Contrôle total	RWXDPO	RWXDPO

Le positionnement des ACLs sur des objets du système suit une logique cumulative : les permissions accordées grâce à ces ACLs sont cumulées au profit des utilisateur et des groupes, à l'exception de la permission "Aucun Accès". Ainsi, si un utilisateur UserA dispose sur un objet de la permission RX, que ce même utilisateur appartient au groupe GroupeA et que ce groupe dispose de la permission WX sur cet objet, alors l'utilisateur UserA disposera au final des permissions RWX sur cet objet, résultants des permissions cumulées de UserA et de GroupeA.

Note importante : la permission « Aucun Accès » a priorité sur les autres permissions, aussi la chose à ne pas faire est d'attribuer cette permission au groupe « Tout le monde » (plus personne n'aura donc accès à cet objet, y compris les Administrateurs).

2.6.3. Les « Data-Streams »

La structure interne du système de fichier NTFS permet de gérer des « streams » (littéralement : des « Flux »). Un fichier est généralement constitué d'une seule Stream dite « de données » (data-stream) dans laquelle on retrouve le contenu des fichiers. Cependant, il est possible d'ajouter des « data-streams » additionnelles à un fichier NTFS afin d'y stocker des informations diverses. C'est grâce à ce mécanisme que Windows NT peut par exemple gérer des partages AppleShare pour les clients Macintosh : le système stocke dans des data-streams additionnelles les informations que les Macintosh utilisent sous forme de ressources - associations entre le fichier et l'applicatif à lancer pour l'ouvrir, icônes associées, etc.

Ces data-stream sont « invisibles », la seule façon de les lister est d'utiliser un programme spécifique du domaine public (LADS par exemple).

Pour créer une data-stream additionnelle dans un fichier TOTO.TXT, il suffit d'ouvrir ce fichier avec un programme sachant gérer les data-streams comme NOTEPAD.EXE, et en précisant le nom de la data-stream à la suite du nom de fichier, séparé par le caractère « : ». Exemple : la commande « `NOTEPAD.EXE TOTO.TXT:STREAM1` », créera (ou ouvrira si la data-stream existe) une data-stream STREAM1 dans le fichier TOTO.TXT. Note : on peut ajouter autant de data-streams que l'on veut dans un fichier, et de la taille que l'on veut, **sans que la taille apparente du fichier ne soit affectée.**

Lors d'une copie de fichier, ces data-streams additionnelles ne sont copiées que si le volume de destination est bien au format NTFS et qu'on utilise la pile protocolaire Windows NT (copie par copier / coller sous l'explorateur par exemple), elles ne sont pas copiées lors d'un transfert FTP ou HTTP.

2.6.4. Partages et permissions de partage

Windows NT permet de gérer des volumes partagés sur un réseau et de positionner des permissions d'accès sur ces partages.

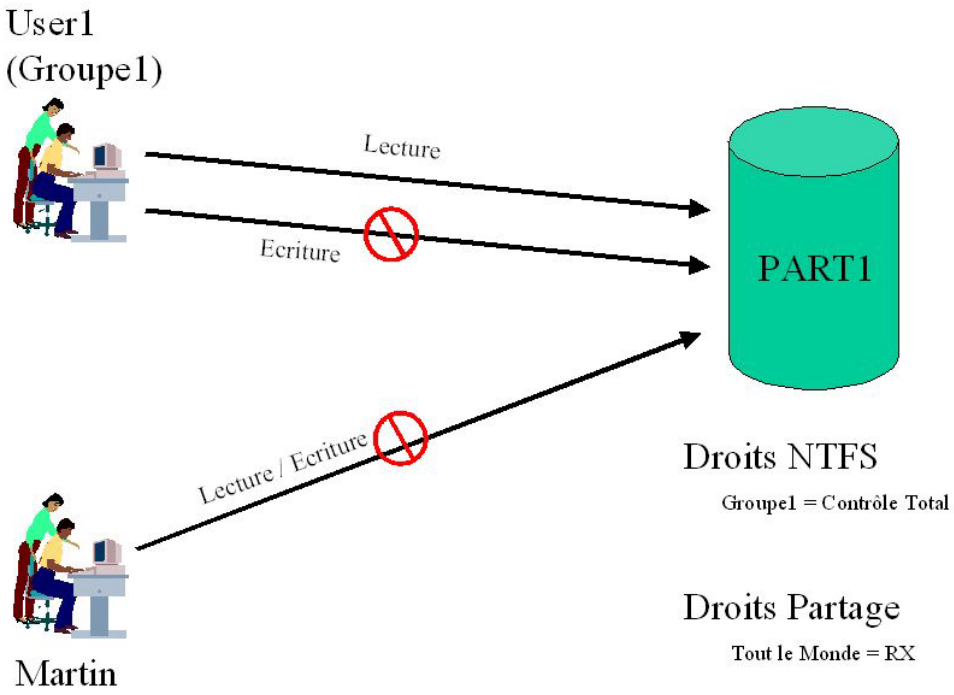
A la création d'un partage, on peut définir des permissions à deux niveaux distincts : **permissions sur le partage** lui-même et **permissions NTFS** sur le contenu du partage.

Les permissions sur le partage sont similaires aux permissions que l'on peut positionner sur les répertoires NTFS, à ceci près que ces permissions ne concernent que la façon dont le partage sera vu sur le réseau. Les permissions NTFS sont les permissions que l'on peut positionner sur les répertoires et fichiers.

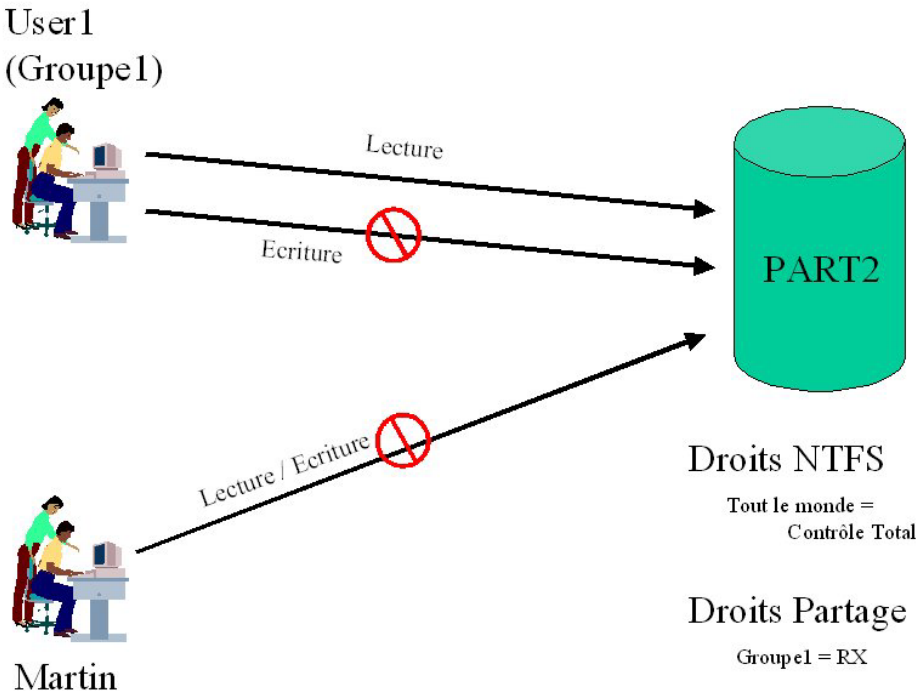
Lorsque les deux mécanismes sont mis en œuvre, les permissions sur le partage donnent les permissions maximales applicables sur le répertoire partagé à travers le réseau.

Les exemples qui suivent donnent deux techniques différentes pour autoriser l'accès à un partage à un groupe d'utilisateur en lecture / exécution (permissions RX).

Exemple 1 : on définit un partage PART1 sur un répertoire avec la permission NTFS « Groupe1 » = « Contrôle Total », et la permission de partage « Tout le monde » = « RX ». L'utilisateur distant « User1 », appartenant au groupe « Groupe1 » n'a pas accès en Ecriture au partage, malgré la permission NFTS lui attribuant le contrôle total sur le répertoire. Cependant, les utilisateurs du groupe « Groupe1 » accédant au répertoire en local (donc hors connexion réseau) y auront accès en Contrôle Total.



Exemple 2 : on définit un partage PART2 sur un répertoire avec la permission NTFS « Tout le monde » = « Contrôle Total », et la permission de partage « Groupe1 » = « RX ». L'utilisateur distant « User1 », appartenant au groupe « Groupe1 » n'aura de la même façon accès au répertoire PART2 qu'en lecture / exécution, du fait des restrictions sur les permissions du partage.



Il est également possible d'interdire la visualisation des partages via le voisinage réseau, en ajoutant à la fin du nom de partage le caractère $. C'est par exemple le cas du partage Admin$, qui est le partage administratif actif par défaut sur toutes les machines Windows NT et qui pointe généralement sur le répertoire « C:\Winnt » (il pointe en fait sur le répertoire indiqué par la variable `%systemroot%`).

2.6.5. Les ACLs de Windows 2000

Sous Windows 2000, quelques différences existent avec Windows NT 4.0 dans les propriétés de sécurité des objets du système de fichier. Ces "nouvelles" fonctionalités ont en fait été présentes dès l'arrivée du Service Pack 4 de Windows NT 4.0, puisque ce Service Pack mettait à jour le système de fichier NTFS de façon transparente pour l'utilisateur / administrateur.

Simplement l'interface utilisateur de Windows NT ne permettait pas leur manipulation, sauf à installer l'utilitaire SecEdit, présent sur le CD-Rom du Service Pack 4 distribué par Microsoft.

Sous Windows 2000, ces nouvelles fonctionnalités sont natives et, parmi celles-ci, on trouve :

- La possibilité de propager les permissions à des objets enfant (héritage implicite)
- La possibilité d'interdire l'héritage des permissions

Ce mécanisme d'héritage est rigoureusement identique à la notion d'héritage dans le monde de la programmation objet ; un objet parent (un répertoire par exemple), disposant d'un liste à contrôle d'accès, propagera ces permissions aux objets enfants et ce de manière automatique. Ainsi, en cas de modification des permissions de l'objet parent, les objets enfant se verront automatiquement appliqués ces modifications tout en conservant leurs propres permissions.

Exemple :

Un répertoire PERE dispose de l'ACL suivante pour les fichiers :

Tout le monde = Lire (RX)

Tout fichier ou répertoire ENFANT créé sous ce répertoire se verra alors attribuer l'ACL du répertoire PERE.

Supposons alors que l'on ajoute une entrée à l'ACL du fichier ENFANT :

Utilisateur Martin = Ecrire

L'ACL du fichier ENFANT sera donc :

Tout le monde = Lire (RX)
Utilisateur Martin = Ecrire

Si l'administrateur modifie l'ACL du répertoire PERE ainsi :

Tout le monde = Lire (RX)
Groupe GESTIONNAIRES = Modifier

Sans qu'il soit nécessaire de faire quoi que ce soit, le fichier ENFANT disposera alors de l'ACL suivante :

Tout le monde = Lire (RX)
Utilisateur Martin = Ecrire
Groupe GESTIONNAIRES = Modifier

Si, par contre, le fichier ENFANT était situé dans un répertoire FILS du répertoire PERE et que ce répertoire FILS ait été paramétré pour le blocage de l'héritage des permissions, alors aucun des fichiers du répertoire FILS n'héritera de la nouvelle ACL tandis que tous les autres répertoire et fichiers fils de PERE disposeront de leur nouvelleACL.

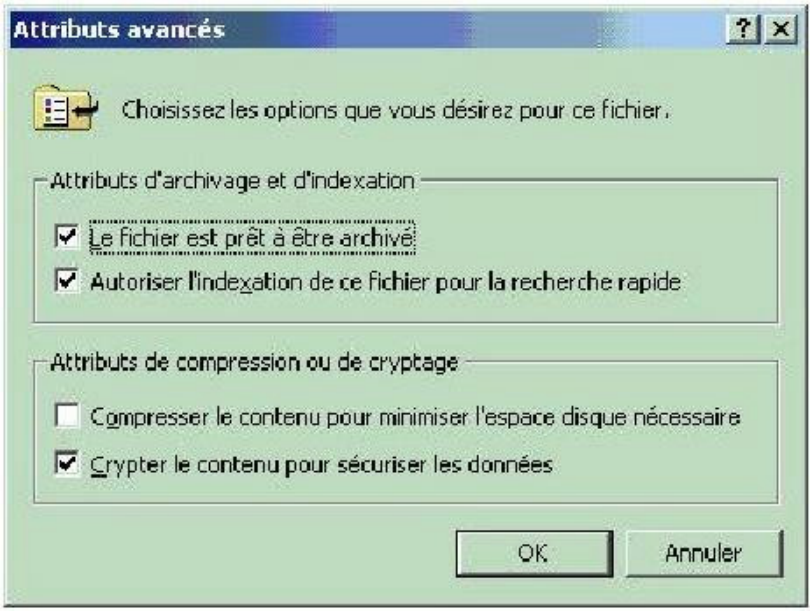
2.6.6. Encrypted File System (EFS)

Sous Windows NT, le système de fichier utilisé (NTFS - New Technology File System) permettait de gérer des permissions sur les objets gérés par celui-ci (répertoires, fichiers).

Cependant les permissions positionnées sur ces objets pouvaient être outrepassées par un accès physique au média de stockage. Ainsi de nombreux utilitaires ont vu leur apparition, permettant depuis une disquette de démarrage MS-DOS ou Linux d'accéder directement au disque dur sans être contraint par les éventuelles permissions positionnées sur le système de gestion de fichiers.

Avec Windows 2000 apparaît la notion de système de fichier chiffré ou EFS (Encrypted File System). Il s'agit d'une simple sur-couche transparente à NTFS, utilisant les nouvelles fonctionnalités apparues avec NTFS V2 qui devient de facto le standard de système de gestion de fichiers sous Windows 2000[1].

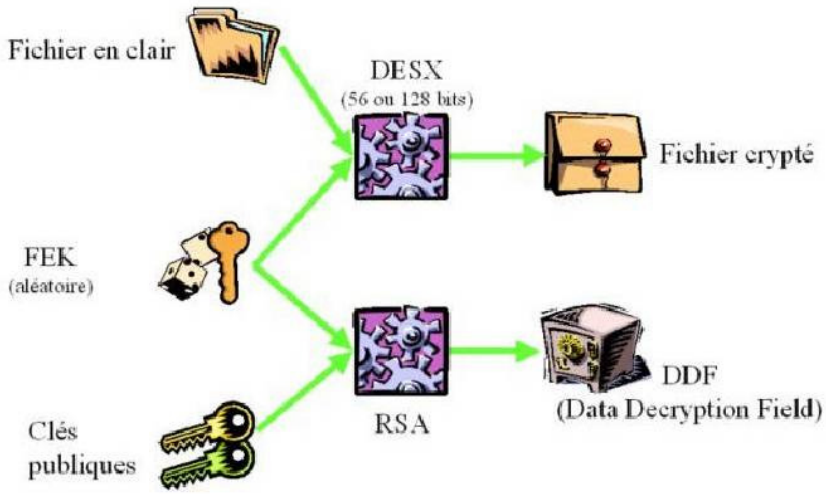
[1] Windows 2000 continue à gérer les partitions de type FAT, y compris les partitions FAT32 ce qui est une nouveauté, mais l'ensemble des fonctionnalités de sécurité n'est utilisable qu'à la condition d'utiliser le système de gestion de fichiers NTFS.



Le chiffrement peut intervenir au niveau d'un fichier ou d'une arborescence. En outre, chaque fichier est chiffré à l'aide d'une clef différente tirée aléatoirement. Le mécanisme de chiffrement de fichiers permet de plus la capacité de récupération de fichiers chiffrés par un administrateur.

Le mécanisme de chiffrement utilisé est le suivant :

- Une clef (FEK - File Encryption Key) de 128 bits est tirée aléatoirement par le système.
- Cette FEK sert à chiffrer, par un algorithme DESX, le fichier considéré
- Cette FEK est alors chiffrée par un algorithme de chiffrement à clef publique ; la FEK est chiffrée à l'aide de la clef publique de l'utilisateur (donc connue de tous) et le résultat est stocké dans NTFS sous un champ particulier associé au fichier (champ DDF - Data Decryption Field).
- Pour déchiffrer le fichier, l'utilisateur utilise une clef privée (connue de lui seul) associé à son compte, afin de déchiffrer le champ DDF
- La FEK récupérée dans ce champ permet alors de déchiffrer le fichier
- En outre, un mécanisme permet à un administrateur système de déchiffrer un fichier par un utilisateur.



Dans les faits, il est possible de chiffrer un fichier en faisant en sorte que plusieurs utilisateurs puissent le déchiffrer. Il suffit pour cela de générer autant de DDF qu'il existe d'utilisateurs capables de déchiffrer le fichier.

En plus des champs DDF, un ou plusieurs champs dits DRF (Data Recovery Field) sont ajoutés au fichier, permettant à des agents de récupération (paramétrables par l'administrateur) de déchiffrer le FEK du fichier, rendant ainsi possible la récupération par l'administrateur d'un fichier chiffré. Par défaut, l'administrateur du système est un agent de récupération.

2.7. La base des registres

2.7.1. Généralités

La base des registres fournit, sous Windows 9x et NT, une base de données unique dans laquelle sont stockées toutes les informations de configuration, au sein d'une structure hiérarchique. Avant Windows 95 et dans le monde Windows, la seule façon de configurer des applications et les fonctions du système d'exploitation était d'utiliser des fichiers de configuration (les fameux .INI dans le meilleur des cas, d'autres fichiers plus exotiques dans d'autres cas).

Dans les environnements Windows 9x et NT, la base des registres remplace définitivement ce fonctionnement à base de fichiers de configuration, du moins pour les applications 32 bits. Chaque clef dans le registre est similaire, dans son fonctionnement, aux en-têtes *entre crochetés* des fichiers .INI.

Les problèmes liés à l'utilisation de ces fichiers .INI étaient nombreux. Entre autre, il était impossible d'utiliser ces fichiers pour y stocker autre chose que du texte pur, ce qui peut être gênant quand on doit stocker des valeurs de type hexadécimales ou binaires (on doit alors avoir recours à une forme de codage de ces valeurs), de plus la structure de ces fichiers interdisait la possibilité de hiérarchiser leur contenu.

Une clef de registre peut donc contenir un ensemble de types de valeurs autres que du texte pur, et il est possible d'utiliser des sous-clefs (donc de hiérarchiser le contenu de la base).

Pour visualiser le contenu de la base des registres on peut utiliser les deux utilitaires fournis avec le système d'exploitation ; regedit.exe et regedt32.exe. Seul le second programme, d'ailleurs absent dans Windows 9x, permet de positionner des ACLs sur des clefs de registre.

2.7.2. Structure de la base des registres

Sous Windows NT, la base des registres est divisée en 5 structures distinctes :

HKEY_CURRENT_USER

Cette clef contient les informations de configuration liées à l'utilisateur en cours de session. Les préférences d'écran, l'état du bureau, les volumes montées etc. sont stockés dans cette clef. Dans les faits, cette clef n'est qu'un alias, initialisé à l'ouverture de session, vers une ruche de la clef HKEY_USERS.

HKEY_USERS

Cette clef contient les informations de configuration liées aux utilisateurs du système. Les ruches de cette clef correspondent aux profils utilisateurs que l'on trouve dans le répertoire `%systemroot%\profiles` (plus précisément, le fichier Ntuser.dat (ou Ntuser.man) situé dans chaque profil utilisateur).

HKEY_LOCAL_MACHINE

Cette clef contient les informations de configuration spécifique à la machine, indépendamment de l'utilisateur en cours de session. Ces informations sont stockées dans le répertoire `%systemroot%\system32\config`[1] comme une série de fichiers systèmes, à l'exception de la clef volatile « hardware ».

De par les informations qui s'y trouvent, cette clef est probablement la plus importante et la plus sensible de toute la base des registres. Elle contient cinq sous-clefs :

[1] %systemroot% est une variable d'environnement dont le contenu pointe vers le répertoire d'installation du système, généralement C:\Winnt

Hardware : base de données décrivant le matériel présent sur l'ordinateur, la manière dont les pilotes de périphérique doivent utiliser le matériel etc. une grande partie des données situées dans cette sous-clef est régénérée à chaque démarrage par le système d'exploitation.

SAM : Security Account Manager, contient toutes les informations relatives aux utilisateurs et aux groupes déclarés sur la machine.

Security : base de données contenant la politique de sécurité locale à la machine, comme les droits spécifiques des utilisateurs. Le contenu de cette clef n'est utilisé que par le sous-système de sécurité du système d'exploitation.

Software: Cette clef contient des informations sur les logiciels installés ainsi que des informations de configuration du système d'exploitation.

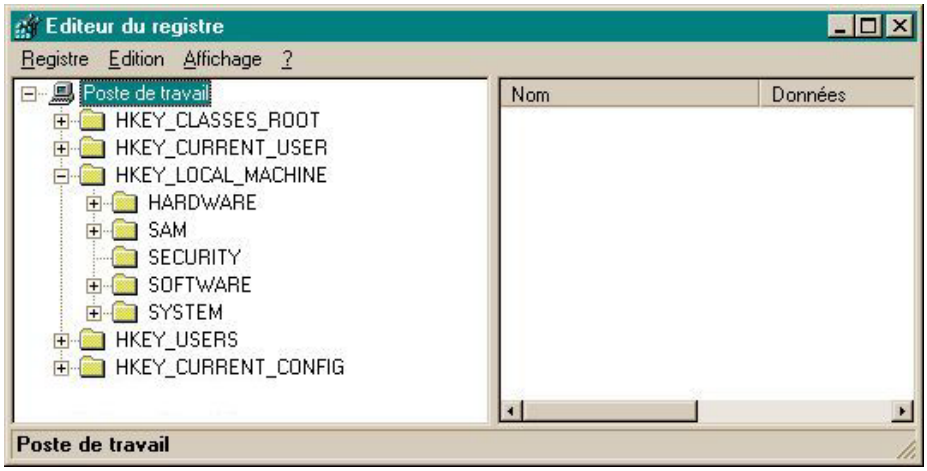
System: Base de données contrôlant le démarrage de Windows NT, le chargement des pilotes de périphérique et le comportement du système d'exploitation.

HKEY_CLASSES_ROOT

Les informations stockées ici sont utilisées par le système d'exploitation pour savoir quelle application lancer quand un fichier est ouvert par lien OLE (double click sur un fichier par exemple), et pour stocker les informations concernant les liens et les encapsulations entre objets. C'est en fait un alias vers une sous-clef de HKEY_LOCAL_MACHINE\Software

HKEY_CURRENT_CONFIG

Les informations stockées dans cette clef sont utilisées pour déterminer quels logiciels et pilotes de périphérique doivent être chargés, ou pour la résolution d'écran à utiliser. Cette clef contient des sous-clefs System et Software qui conservent des traces des précédentes configurations.



Chaque branche peut contenir un certain nombre de clés et de sous clés. Chaque clé/sous-clé contient un certain nombre de valeurs constituées de trois éléments :

- Un **nom**, exemple Wallpaper
- Un **type**, exemple REG_SZ (chaîne de caractère)
- Une **valeur courante** ou **contenu** exemple "c:\winnt\lanma256.bmp"

2.7.3. Fichiers de la base de registre

Les fichiers contenant les informations de la base de registre sont stockés dans le répertoire `%SYSTEMROOT%/SYSTEM32/CONFIG`. Ce sont :

- **SAM** pour la branche **HKEY_LOCAL_MACHINE\SAM**
- **SECURITY** pour la branche **HKEY_LOCAL_MACHINE\Security**
- **SOFTWARE** pour la branche **HKEY_LOCAL_MACHINE\Software**
- **SYSTEM** pour les branches **HKEY_LOCAL_MACHINE\System** & **HKEY_CURRENT_CONFIG**
- **DEFAULT** pour la branche **HKEY_USERS\.DEFAULT**
- **Ntuser.dat** pour la branche **HKEY_CURRENT_USER** (ce fichier est stocké dans le répertoire `%SYSTEMROOT%\PROFILES\%USERNAME%`).

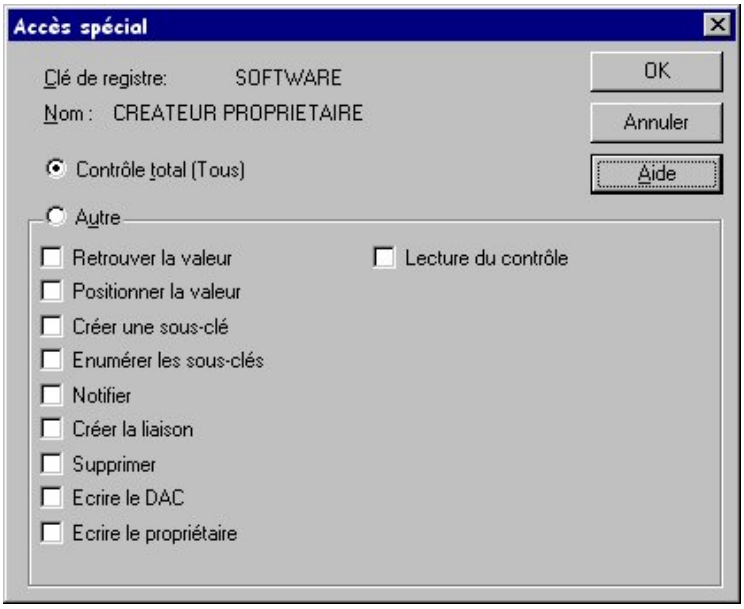
Ces fichiers sont aussi appelés **RUCHES** et sont accompagnés de compagnons d'extensions différentes :

- **system.alt** qui contient une copie de sauvegarde de **HKEY_LOCAL_MACHINE\System**.
- **.log** - le journal des modifications apportées sur le fichier initial.
- **.sav** - une copie du fichier initial après la configuration en mode texte.

2.7.4. Sécurité de la base des registres

Compte tenu du rôle capital que joue la base des registres au sein de la configuration du système d'exploitation, il est possible de positionner des ACLs (Access Control List, ou permissions) sur tout ou partie de la base des registres. Ainsi, la ruche HKEY_LOCAL_MACHINE\SAM est elle protégée contre une lecture par les utilisateurs et pour cause : cette structure ne contient rien de moins que les cryptogrammes représentant les mots de passe chiffrés des utilisateurs. On verra que même les Administrateurs n'ont pas accès à cette structure, bien qu'ils aient la possibilité de la déprotéger.

D'autres clefs, toutes aussi sensibles que la SAM, sont également protégées par défaut au cours de l'installation d'un système Windows NT. Notons que cette protection par ACLs ne peut être réalisée efficacement qu'à la condition sine qua non d'utiliser le système de fichier NTFS sur le disque accueillant le système d'exploitation. Le positionnement d'ACLs sur des clefs de la base des registres peut se faire en utilisant l'utilitaire regedt32.exe.



Les ACLs que l'on peut positionner sur les objets de la base des registres sont les suivantes :

Retrouver la valeur : droit de lire une entrée à partir d'une clef de registre.

Positionner la valeur : droit de définir les entrées dans une clef de registre.

Créer une sous-clef : droit de créer une sous-clef sur une clef de registre.

Enumérer les sous-clefs : droit de lister les sous-clefs d'une clef de registre.

Notifier : droit d'auditer les événements de notification.

Créer la liaison : droit de créer une liaison symbolique dans une clef (alias).

Supprimer : droit de supprimer la clef sélectionnée.

Ecrire le DAC : droit de positionner des ACLs sur une clef.

Ecrire le propriétaire : droit d'affecter un propriétaire à une clef.

Lecture du contrôle : droit de lister les informations de sécurité (ACLs) d'une clef.

3. Gestion de la sécurité sous Windows NT

Ce chapitre traite ici des **mécanismes de haut niveau** et des **outils**, disponibles en standard avec le système d'exploitation Microsoft Windows NT Server et Workstation, permettant d'administrer au mieux les fonctions de sécurité du système d'exploitation.

3.1. Domaines Windows NT

3.1.1. Qu'est ce qu'un domaine ?

Un domaine Windows NT est un ensemble de machines partageant des ressources communes ; ces ressources peuvent être des comptes utilisateurs, des partages de fichiers, des imprimantes, certains périphériques (lecteurs de bandes, CD-Roms, scanners), etc.

Un domaine Windows NT est articulé autour d'une machine **Windows NT Server** qui joue le rôle de **contrôleur principal de domaine (PDC),** il peut être éventuellement secondé par un ou plusieurs **contrôleurs secondaires de domaines (BDC).**

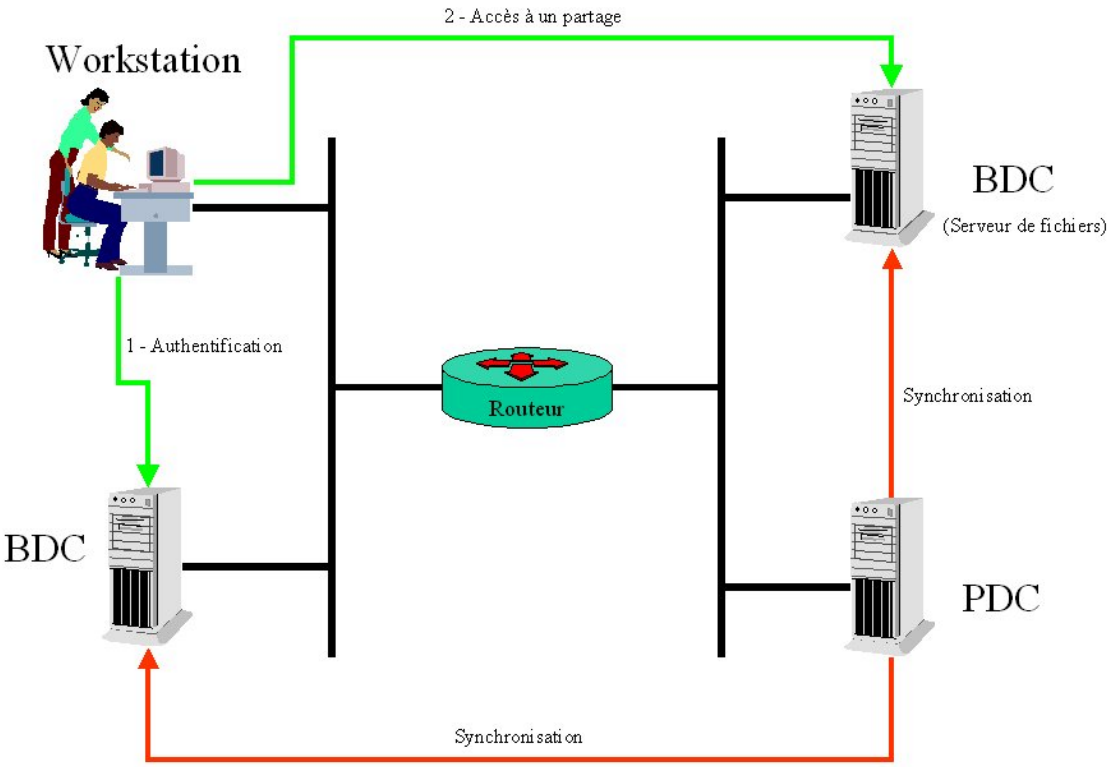
Les contrôleurs de domaines **valident les ouvertures de session** des clients **et contrôlent l'accès aux ressources** des serveurs. Dans un domaine Windows NT, toute machine peut jouer le rôle d'un serveur de ressources, mais en général, ce rôle est plutôt dévolu aux machines Windows NT Server, pour des raisons de performance, de sécurité et de limitations sur le nombre de connexions concurrentielles sous Windows NT Workstation..

Les rôles d'un PDC dans un domaine sont de :

- Gérer la base centralisée des comptes utilisateurs,
- Valider les ouvertures de session des utilisateurs,
- Fournir éventuellement des profils utilisateurs centralisés,
- Contrôler les accès des utilisateurs aux ressources du domaine.

Chaque BDC dispose d'une copie de la SAM. Cette copie est mise à jour régulièrement par un mécanisme de synchronisation. Ses rôles sont de :

- Soulager le PDC (un utilisateur est validé par le DC le plus proche)
- Pouvoir remplacer le PDC si ce dernier a un problème.



3.1.2. Approbations de domaines

Dans certains cas, il peut être utile de séparer un grand nombre de machines en des domaines différents. La communication entre les machines de ces domaines est alors assurée par un mécanisme **d'approbation de domaine**, qui peut être mono ou bidirectionnel.

Les raisons de cette séparation sont multiples ; segments éloignés reliés par des liaisons lentes, éclatement des responsabilités de l'administration d'un réseau (on peut par exemple décider qu'un domaine A gère des utilisateurs et qu'un domaine B gère des ressources)…

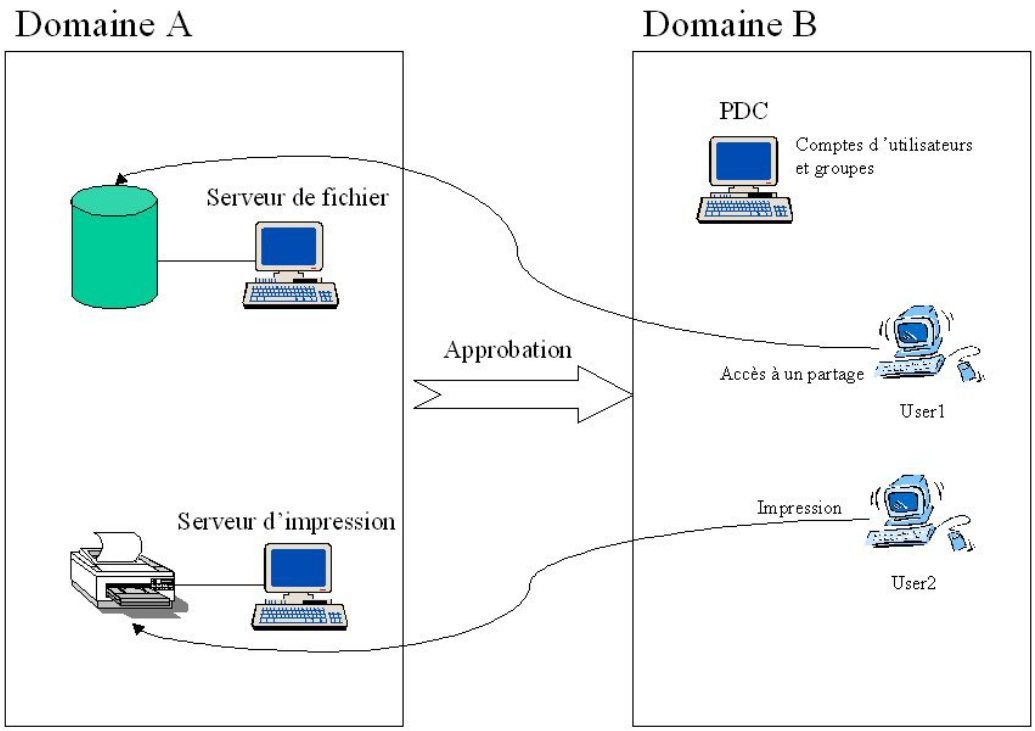
Ainsi, un utilisateur déclaré dans un domaine peut accéder à des ressources partagées dans un autre domaine. Dans ce cas, soit on utilise des mécanismes basiques comme l'utilisation d'un compte Invité ou le positionnement de permissions pour le groupe « Tout le monde », soit on met en œuvre le mécanisme d'approbation de domaines.

Cette dernière possibilité est cependant la plus efficace, car elle permet de gérer plus finement les permissions des utilisateurs.

Pour établir une relation d'approbation entre deux domaines, il faut passer par l'utilitaire « Gestionnaire des utilisateurs du domaine », menu « Stratégies ». Par nature, les relations d'approbation ne sont ni symétriques ni transitives, cependant il est possible de mettre en œuvre une relation d'approbation bidirectionnelle en faisant en sorte que deux domaines s'approuvent mutuellement. En outre, un domaine ne peut en approuver un autre que si l'administrateur du futur domaine approuvé autorise que d'autres domaines approuvent le sien.

Ainsi, si le domaine A approuve le domaine B :

- Les utilisateurs du domaine B pourront s'y connecter depuis n'importe quelle machine de A et de B,
- Les administrateurs de A pourront positionner des permissions sur les ressources du domaine A pour les utilisateurs du domaine B.



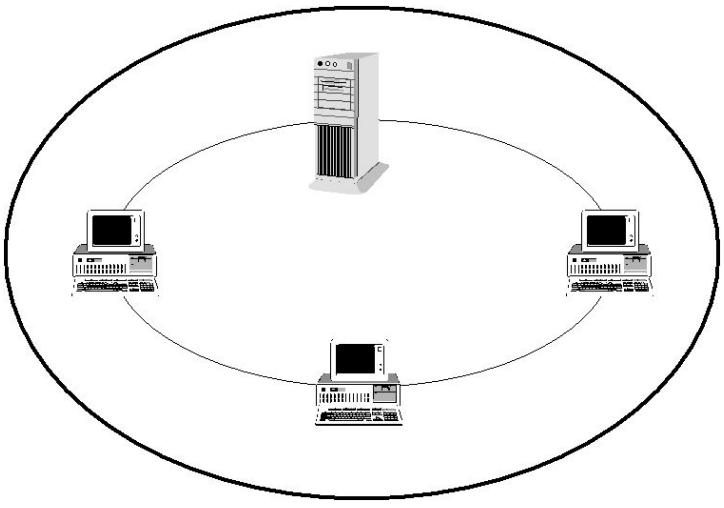
Approbation de B par A

3.1.3. Architectures possibles

Dans le cas de l'utilisation de domaine(s) Windows NT, on peut distinguer 4 cas de figure possibles.

3.1.3.1. Modèle à Domaine Unique

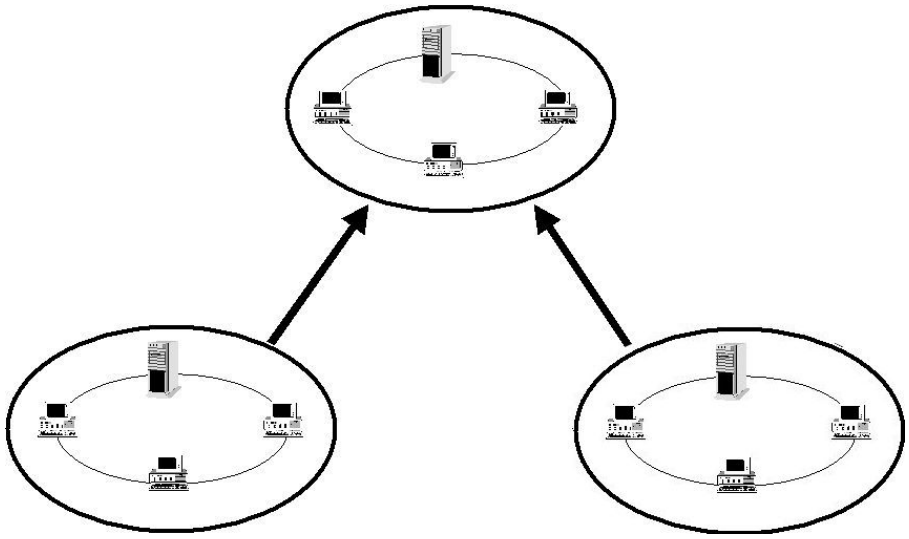
Dans ce modèle, on utilise un unique Domaine Windows NT, géré par un unique PDC, sans relations d'approbation.



Utilisation : on utilise ce modèle lorsque le réseau est peu étendu et que l'administration est centralisée autour d'une équipe unique.

3.1.3.2. Modèle à Domaine Maître

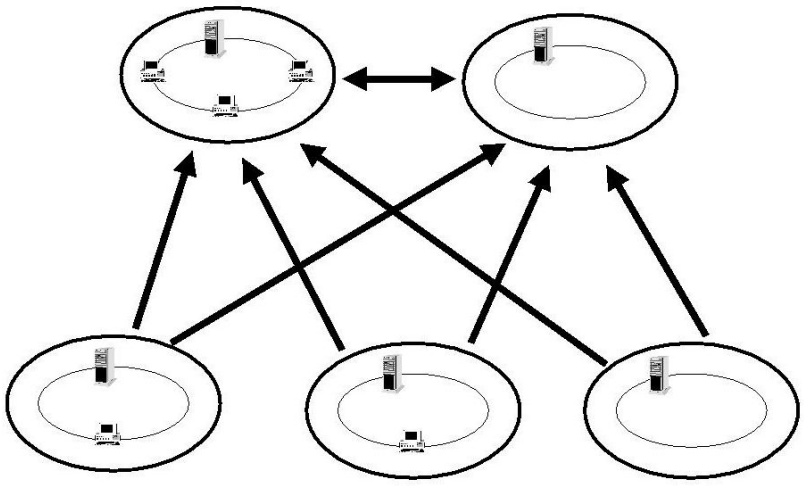
Dans ce modèle, on utilise un domaine dit « Maître », qui gère un certain nombre de ressources communes aux autres domaines. Ce domaine Maître est alors approuvé par les autres domaines.



Utilisation : Ce modèle peut être utilisé dans le cadre d'une centralisation des droits d'administration communs, ou dans le cas d'un réseau étendu. Le domaine maître maintient des ressources de sécurité pour tous les autres domaines, les autres domaines étant utilisés comme des domaines de ressources et éventuellement d'utilisateurs. Cette configuration permet de gérer jusqu'à 15000 utilisateurs. Il existe une relation d'approbation entre chaque domaine et le domaine maître.

3.1.3.3. Modèle à Domaines Maître Multiples

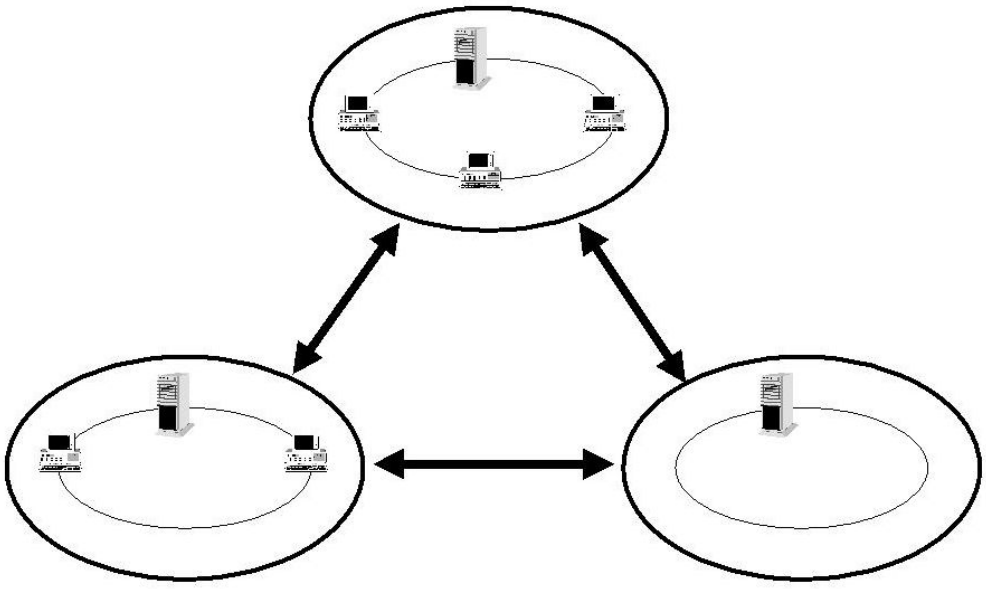
Ce modèle est similaire au modèle à domaine Maître, à la différence près que l'on utilise plusieurs domaines Maîtres s'approuvant mutuellement. L'administration est plus complexe de par le fait qu'il est parfois nécessaire de créer chaque compte utilisateur dans chaque domaine maître.



Utilisation : même utilisation que dans le modèle à domaine Maître, mais en choisissant un cloisonnement des différentes ressources communes accessibles (par exemple, deux domaines d'utilisateurs différents mais accédant à des ressources communes).

3.1.3.4. Modèle à Domaines de Confiance Réciproques

Ce modèle repose sur N domaines différents, avec une approbation réciproque des domaines.



Utilisation : cas particulier d'une administration ou l'on souhaite une certaine autonomie des différents réseaux, et dans le cas où chaque domaine fournirait des ressources aux autres.

3.2. Architecture de Windows 2000 : Forêts, Arbres et Uos

L'une des principales évolutions du système d'exploitation Windows 2000 par rapport à son prédécesseur consiste dans la définition d'une architecture de système d'information, dans laquelle vont s'intégrer les postes Windows 2000, radicalement différente de celle que nous étions habitués à manipuler avec windows NT 4.0.

Cependant, cette évolution s'est effectuée relativement en douceur dans la mesure où Microsoft à repris les grands concepts existants pour les améliorer et les compléter.

La socle sur lequel repose cette évolution d'architecture s'appelle l'Active Directory, qui représente la même révolution que pouvait représenter l'arrivée de la base de registres avec Windows 9x et NT.

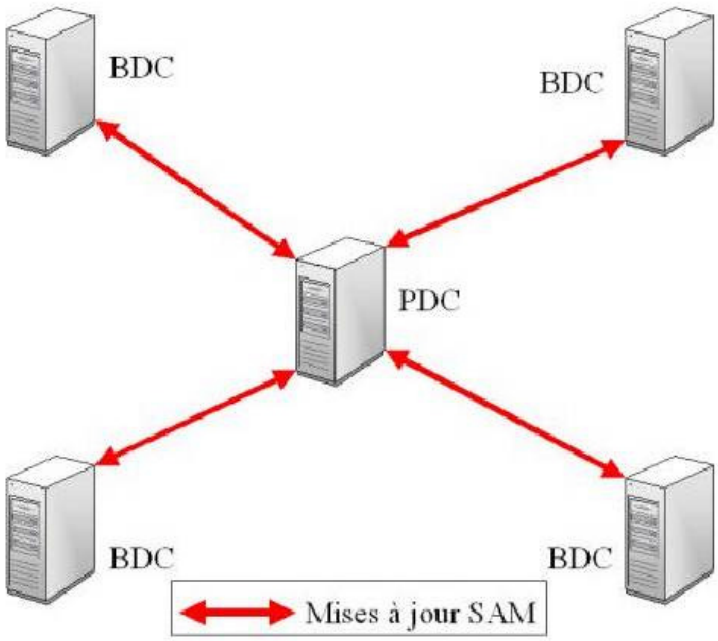
3.2.1. Gestion centralisée des ressources et services / Active Directory

Sous Windows NT, il était possible de regrouper des ressources communes au sein d'une structure appelée "Domaine Windows NT". Le principe de base de ce regroupement était de centraliser sur des serveurs un certain nombre d'informations pour les rendre accessibles à l'ensemble des machines reliées à un domaine. Ainsi, la notion de domaine Windows NT impliquait la maintenance et la mise à jour d'une base centralisée des utilisateurs sur un ou plusieurs serveurs.

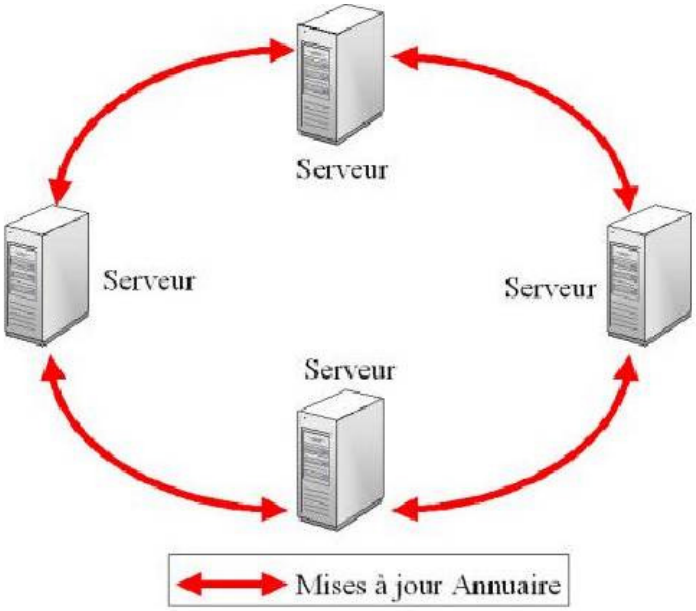
Ce principe a été retenu sous Windows 2000, mais la base s'est enrichie de nouveaux objets et permet en outre d'en gérer un plus grand nombre ; sous Windows NT la base SAM des utilisateurs était limitée à 40000 entrées, sous Windows 2000 la base d'annuaire autorise plusieurs millions d'entrées.

Du fait de l'extension du principe d'annuaire centralisé sous Windows 2000, la gestion de cet annuaire a été regroupée autour de "Active Directory", système de base d'annuaire hiérarchique centralisée sur des serveurs.

En fait la notion de "centralisation" sous Windows 2000 n'est pas tout à fait exacte stricto sensu. En effet, sous Windows NT la base était centralisée sur un serveur (le serveur principal de domaine ou PDC - Principal Domain Controler) éventuellement épaulé par d'autres serveurs (serveurs secondaires ou BDC -Backup Domain Controler), la relation entre PDC et BDC étant réalisé sur un mode maître-esclave ; chaque modification est rapportée au PDC qui a la charge de répercuter ces modifications sur l'ensemble des BDC.



Sous Windows 2000, la base d'annuaire "Active Directory" est répartie sur l'ensemble des serveurs et chaque serveur possède un rôle équivalent aux autres serveurs. Alors que, sous Windows NT, l'organisation logique des serveurs était architecturée autour d'une organisation en étoile, l'organisation logique des serveurs Windows 2000 est architecturée autour d'une organisation en anneau ; chaque modification d'annuaire sur un serveur est répercutée auprès des serveurs contigus, de proche en proche.



Sous Windows 2000, donc, apparaît la notion d'Active Directory. Active Directory est un service d'annuaire, hiérarchique, et disponible uniquement dans la version serveur de Windows 2000. Son rôle essentiel est de fournir un service réseau qui identifie toutes les ressources d'un réseau et rend ces dernières accessibles aux utilisateurs et aux applications. Ces ressources sont définies dans des entités typées appelées "objets". Un objet peut consister en des données utilisateurs, des imprimantes, des serveurs, des stations de travail, des groupes etc.

Notons que Active Directory reste un annuaire propriétaire, même si il peut s'interfacer avec des services standardisés (LDAP ou Novell NDS par exemple).

De plus, il est ici utile de préciser que Active Directory repose pour son fonctionnement sur le service de nommage DNS, ce qui peut apparaître curieux dans la mesure ou l'on a affaire à un service d'annuaire qui repose sur un autre service d'annuaire (dans son fonctionnement, DNS est un service d'annuaire).

3.2.2. Introduction à l'Active Directory

Active Directory (AD) reste la plus grande évolution qu'ai connu le système d'exploitation Microsoft. Cette évolution est comparable au passage sous Windows 3.11 des fichiers de paramétrage de type .INI à la notion de base de registre de Windows 9x et NT.

Active Directory reste avant tout une base d'annuaire dont le rôle est de regrouper tous les objets réseau au sein d'une structure hiérarchique. Dans son principe, Active Directory est une base distribuée ; tous les serveurs d'un même domaine Windows 2000 disposent d'une réplique de cette base.

L'AD permet alors :

- De centraliser la gestion de la forêt (y compris dans ses aspects sécurité),
- D'assurer l'authentification des utilisateurs (les données relatives à ceux-ci sont stockés dans l'AD, en particulier leurs mots de passe[1])
- D'autoriser la mise en place d'ACLs sur chaque objet stocké dans l'AD,
- De stocker toutes les informations de gestion d'une forêt (Stratégies de sécurité, utilisateurs, groupes, profils, certificats…)

3.2.3. Structure Logique de l'Active Directory

La structure logique de Active Directory est composée de forêts, d'arbres, de domaines, d'unités d'organisation et d'objets.

3.2.3.1. Objets

Un objet, dans Active Directory, peut être un compte d'utilisateur, une imprimante, un compte d'ordinateur, un dossier partagé publié, un groupe…

Chaque objet est composé d'un ensemble **d'attributs**, qui sont représentatifs de l'objet. Tous les attributs d'un objet sont définis dans ce qui est appelé le **Schéma** ; le schéma est modifiable pour permettre à certains objets de se voir affectés d'autres attributs.

Un ensemble d'objets disposant des mêmes attributs est connu sous le nom de **classe**.

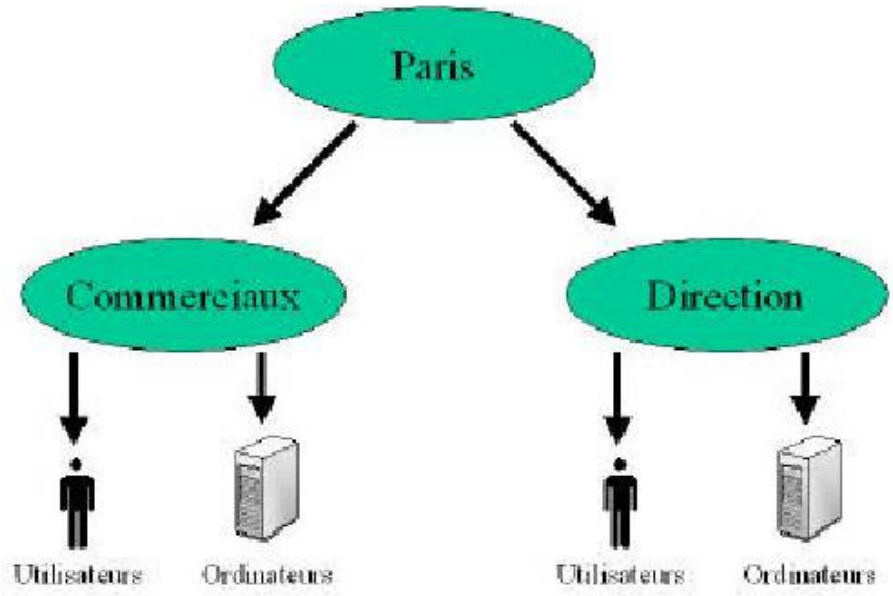
3.2.3.2. Unités d'organisation

Une Unité d'Organisation (OU) est un conteneur utilisé pour organiser les objets d'un domaine en groupe d'administration. Elle contient des objets tels que des comptes utilisateurs, des groupes, des ordinateurs, des imprimantes, des applications, des partages de fichiers etc.

Les Unités d'organisation peuvent être structurées de façon hiérarchique.

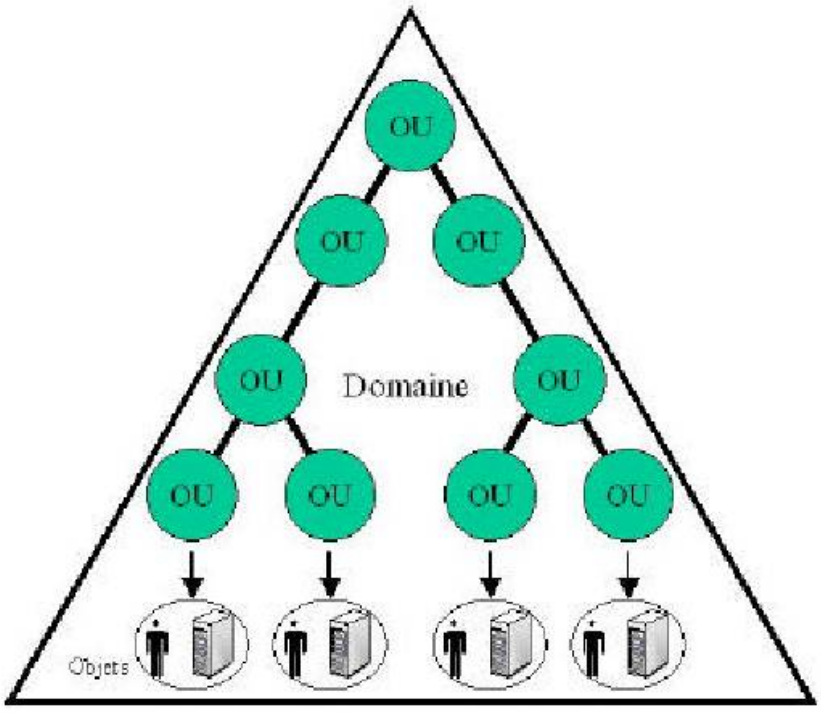
[1] Lorsque l'on installe l'AD sur une machine Windows 2000, l'ensemble des donées de la SAM est transférée dans l'AD. La SAM existe toujours mais elle comprend plus que deux entrées relatives à l'Administrateur et au compte Invité

L'exemple proposé ici précise une organisation d'OU dans laquelle on définit une OU "Paris" contenant deux OU "Commerciaux" et "Direction" :



3.2.3.3. Domaines

Un domaine est un regroupement logique de plusieurs OU organisés de façon hiérarchique et d'objets.

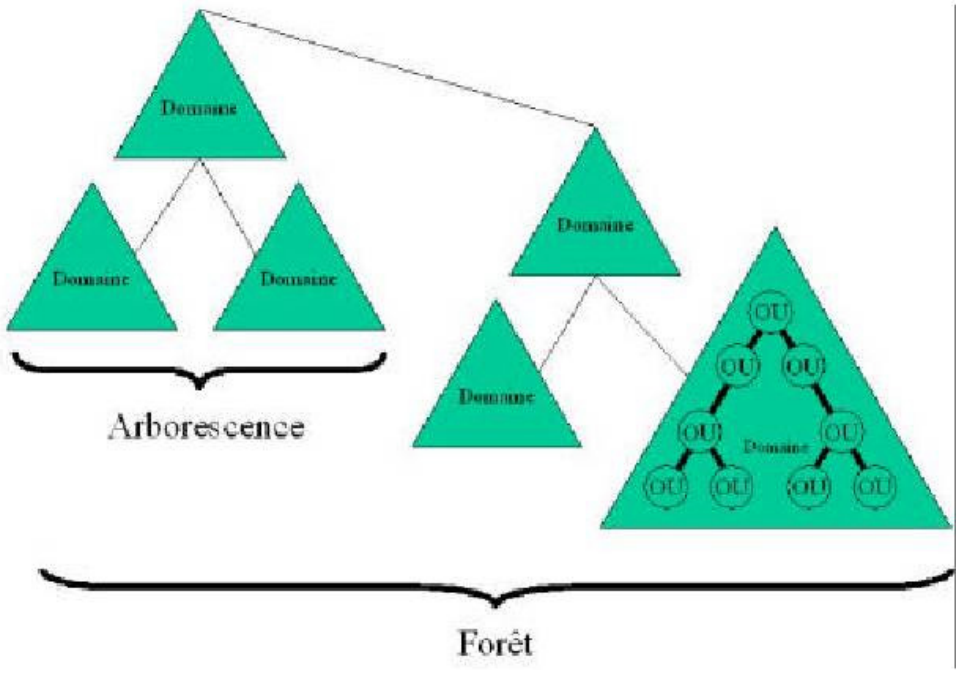


Un domaine est une limite de sécurité ; l'accès aux objets du domaine est géré par des listes à contrôles d'accès (ACLs). Toutes les stratégies et paramètres de sécurité (comme les autorisations administratives, les stratégies de sécurité et les listes à contrôle d'accès) ne passent pas d'un domaine à l'autre. L'administrateur du domaine possède des droits absolus pour définir les stratégies uniquement dans le domaine en question.

3.2.3.4. Arbres et Forêts

Une arborescence, ou arbre, est un regroupement ou une organisation hiérarchisée d'un ou de plusieurs domaines Windows 2000.

Une forêt est un regroupement ou une organisation hiérarchisée d'une ou de plusieurs arborescences.



L'arborescence et la forêt sont toutes deux des espaces de noms. Un espace de noms étant une zone limitée dans laquelle un nom peut être résolu. Il existe deux type d'espace de noms :

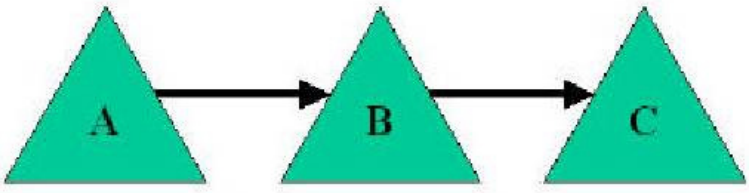
- **Espace de noms contigu**. Le nom de l'objet enfant dans une hiérarchie d'objet contient toujours le nom du domaine parent. Une arborescence est un espace de nom contigu.

- **Espace de noms disjoint**. Les noms d'un objet parent et d'un enfant de ce même objet parent ne sont pas directement liés entre eux. Une forêt est un espace de noms disjoint.

3.2.4. Relations d'approbation

Une relation d'approbation est un lien entre deux domaines qui fait en sorte que le domaine d'approbation prend en compte les authentifications d'ouverture de session du domaine approuvé.

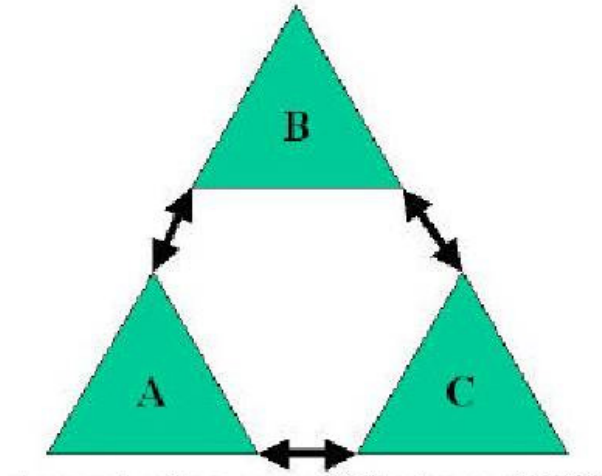
Sous Windows NT 4.0, la notion de relation d'approbation existait déjà mais ces relations étaient de type unidirectionnelles et non transitives. Ainsi, dans le cas de trois domaines A, B et C Windows NT 4.0, si A approuve B qui approuve C il est faux de dire que A approuve C (non transitivité des relation d'approbation) ou que B approuve A (approbation unidirectionnelle).



Approbation sous Windows NT 4.0

Windows 2000 est capable d'assurer la gestion de ce type de relations d'approbation si le système est dans un environnement Windows NT 4.0, mais le fonctionnement normal des approbations entre Serveurs Windows 2000 est celui de relations d'approbations transitives bidirectionnelles. Ainsi, dans le cas de trois domaines A, B et C Windows 2000, où les relations entre ces domaines sont de type Parent-Enfants, ou si ces domaines sont ceux de premier niveau d'une forêt, alors ;

- A approuve B, qui approuve A,
- B approuve C, qui approuve B,
- A approuve C, qui approuve A.



Approbation sous Windows 2000

Les relations d'approbation existant entre les domaines d'une arborescence sont établies et gérées automatiquement. Lorsque l'on crée un domaine enfant, une relation d'approbation transitive bidirectionnelle est automatiquement établie avec le domaine parent, ce qui définit une relation d'approbation avec tous les autres domaines de l'arborescence.

Ce mécanisme d'approbation transitive bidirectionnelle est une conséquence directe de l'utilisation de Kerberos comme mécanisme natif d'authentification.

3.3. Gestion des utilisateurs

3.3.1. Droits des utilisateurs

Les utilisateurs peuvent être gérés sous Windows NT par un utilitaire fourni avec le système d'exploitation. Cet utilitaire varie selon que l'on désire gérer des utilisateurs locaux à une machine (**Gestionnaire des utilisateurs**) ou des utilisateurs dans un domaine Windows NT (**Gestionnaire des utilisateurs pour le domaine**), mais son utilisation reste identique.

C'est avec cet utilitaire que l'on peut gérer les **droits étendus** sur un domaine ou une machine ; ce sont des droits particuliers, indépendants des permissions NTFS, et qui sont accordables à tout utilisateur d'un domaine ou d'une machine. On peut ainsi accorder ou révoquer à un utilisateur, par exemple le droit de charger et décharger des pilotes de périphérique, le droit d'autoriser une ouverture de session ou le droit de déboguer les programmes.

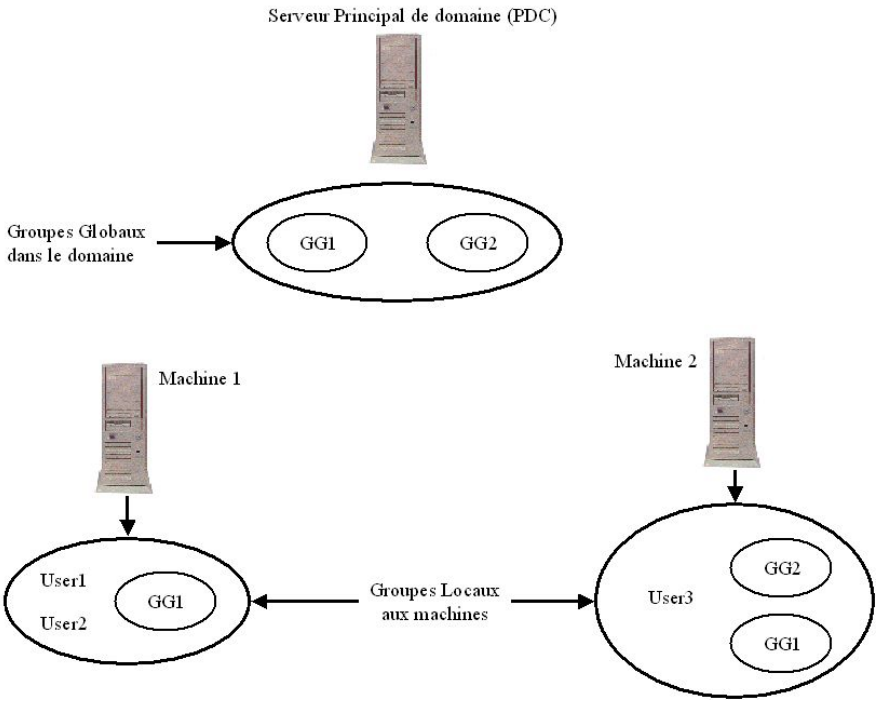
3.3.2. Groupes globaux et locaux

Afin de pouvoir regrouper efficacement les utilisateurs présentant les mêmes besoins, le système Windows NT offre la notion de groupes. Un groupe est d'un des deux types suivant :

- **groupe global** qui est constitué de plusieurs comptes d'utilisateur d'un domaine. Un groupe global n'a de signification que pour un domaine. « Global » signifie que le groupe peut recevoir des droits et des permissions pour utiliser des ressources de plusieurs domaines (portée globale).

- **groupe local** qui est constitué de comptes d'utilisateurs et de groupes d'un ou plusieurs domaines. Les utilisateurs et groupes globaux n'appartenant pas au domaine ne peuvent être ajoutés que si leur domaine est approuvé. « Local » signifie que les droits et permissions accordés ne sont valables que pour une machine (portée locale).

Dans une utilisation standard, les groupes globaux servent à définir des ensembles de personnes et n'ont pas de droits et de permissions directement associées. Ils sont ensuite ajoutés à des groupes locaux, qui eux définissent les droits et permissions relatifs au domaine concerné.



3.3.3. Stratégies de compte

Le même utilitaire permettant de gérer les utilisateurs permet également de préciser la stratégie de gestion des comptes utilisateurs : il est ainsi possible de donner une durée de validité à un mot de passe, de conserver un historique des n derniers mots de passe (afin d'éviter la saisie d'un mot de passe déjà utilisé par le même utilisateur), de définir un verrouillage des comptes après N tentatives de connexion infructueuses, etc.

3.3.4. Profils utilisateurs

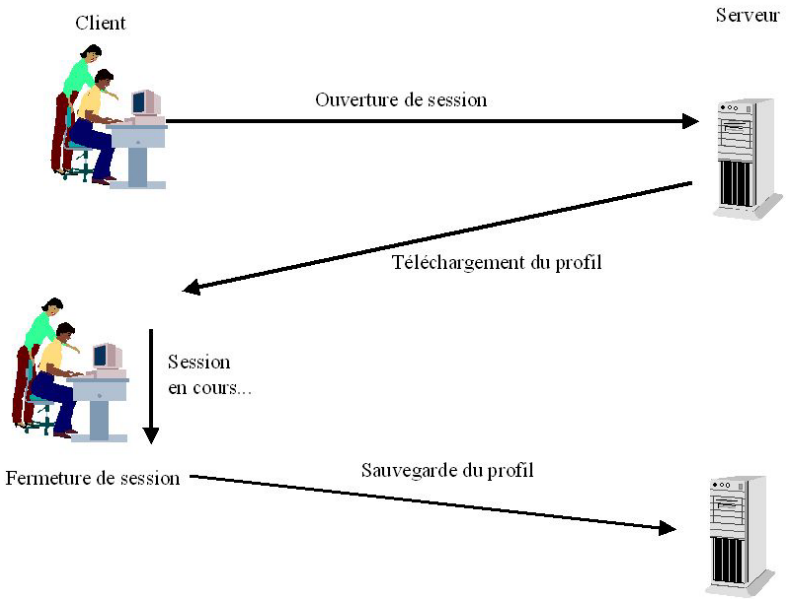
Afin que chaque utilisateur puisse conserver ses propres paramètres de configuration (fond d'écran, couleurs par défaut…), Windows NT utilise pour chaque utilisateur la notion de Profil. Un profil est constitué d'un fichier Ntuser.dat ou Ntuser.man et d'une arborescence qui contient l'ensemble des paramètres utilisateurs. Ces profils sont stockés sur la machine locale dans le répertoire `%systemroot%\Profiles\%username%`.[1]

Un profil utilisateur contient tous les paramètres réglables par l'utilisateur pour son environnement de travail (tels que le choix de la couleur des fenêtres, les paramètres d'affichages, les connexions réseau …) plus des réglages qui peuvent lui être imposés par l'administrateur.

Un profil doit être d'un des types suivants :

- **un profil local** qui est stocké sur une machine en particulier et qui n'est accessible à l'utilisateur que lorsqu'il ouvre une session sur cette machine,
- **un profil errant** qui est stocké sur le serveur et qui permet à l'utilisateur de se connecter sur n'importe quelle machine en retrouvant ses préférences,
- **un profil obligatoire** qui est un profil errant pré-configuré et que l'utilisateur ne peut pas changer.

Dans le cas des profils errants, ceux-ci sont téléchargés depuis le serveur sur la machine locale (sous %systemroot%\Profiles\%username%) lors de l'ouverture de session d'un utilisateur, puis sont sauvegardés sur le serveur à la fermeture de session.



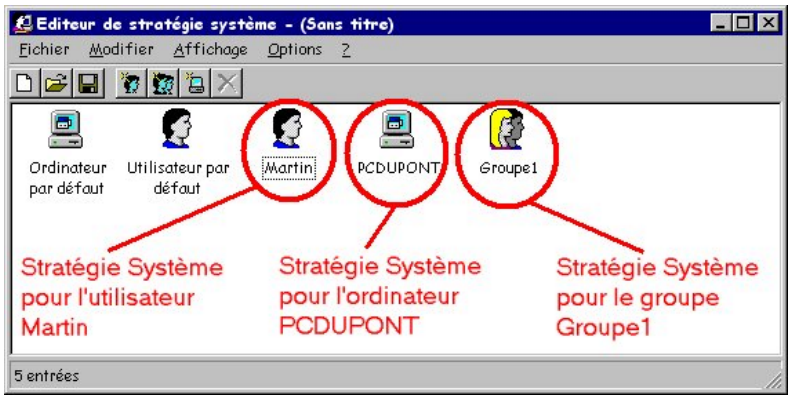
Dans le cas d'un profil obligatoire, c'est le fichier Ntuser.dat, renommé en Ntuser.man (.man pour Mandatory), qui est utilisé et l'utilisateur n'aura alors plus la possibilité de modifier son propre profil.

[1] %username% est une variable d'environnement, initialisée à la connexion d'un utilisateur et valable durant toute la session, et contenant le nom de login de l'utilisateur

3.3.5. Stratégies Système (Poledit.exe)

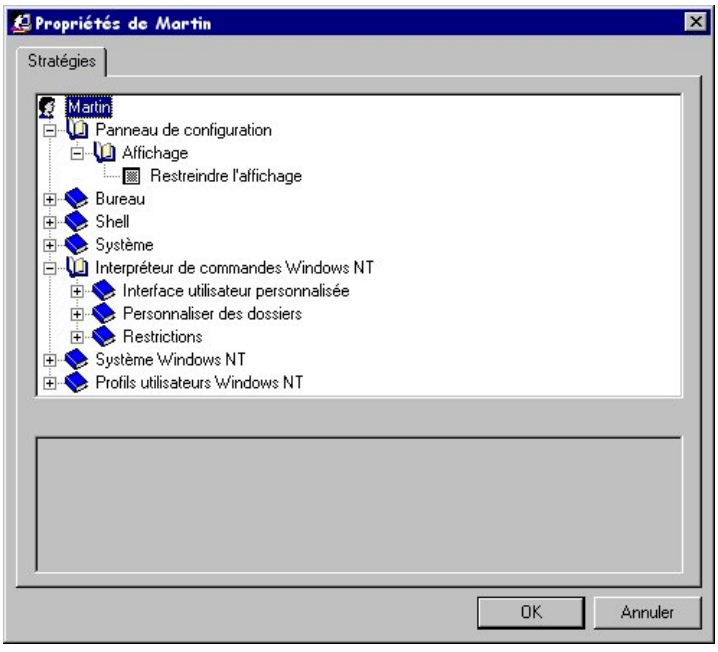
On peut restreindre l'utilisation qu'un utilisateur fait d'une machine en utilisant un outil fourni avec le système d'exploitation et qui se nomme « Editeur de stratégie système » (programme poledit.exe).

Cet utilitaire peut être utilisé pour définir l'environnement utilisateur (quelles applications sont disponibles, ce qui apparaît sur le bureau de chaque utilisateur…) dans ce que l'on appelle une « System Policy » ou Stratégie Système. L'éditeur de Stratégie Système génère un fichier qui consiste en un jeu de paramètres du registre (fichier .POL) : chaque utilisateur peut alors disposer d'un profil différent, en fonction de ses prérogatives et de l'utilisation qui est faite de la machine sur laquelle l'utilisateur se connecte. On peut définir des Stratégies pour un Utilisateur, un Groupe ou pour une Machine.



Les fichiers de Stratégie système sont à stocker dans le répertoire partagé NETLOGON du contrôleur de domaine.

Quand un utilisateur se connecte sur une machine Windows NT, le profil utilisateur est chargé depuis un répertoire partagé sur le serveur et est alors appliqué pendant le temps que dure l'ouverture de session. On peut définir des stratégies Système pour une machine, pour un utilisateur ou pour un groupe donné. Le système vérifie à l'ouverture de session quelle Stratégie on doit appliquer en fonction du nom de l'utilisateur, des groupes auxquels il appartient et de la machine depuis laquelle il se connecte. Le contenu exact du paramétrage d'une Stratégie Système est défini au sein d'un fichier .ADM ; le système fournit des fichiers .ADM par défaut, mais il est possible de créer soit même des fichiers .ADM spécifiques afin d'affiner ce qu'on souhaite paramétrer.



Exemple de Stratégie Système pour l'utilisateur Martin

Pour plus d'informations sur l'éditeur de Stratégie Système, se reporter au document Microsoft « Windows NT® Server - Guide to Microsoft® Windows NT® 4.0 Profiles and Policies » disponible en ligne sur le serveur Internet de Microsoft à la section « White Papers ».

On trouvera également en annexe de ce document un chapitre consacré plus particulièrement à l'éditeur de stratégie système

3.3.6. Windows 2000 et les Stratégies de Groupes (GPO)

Avec windows 2000 est apparue la notion de stratégie de groupes (GPO - Group Policy Object) connue sous une autre forme sous Windows NT, avec l'éditeur de stratégies système (Poledit.exe). Les stratégies systèmes permettaient d'associer à un Ordinateur, un Groupe ou un Utilisateur, un jeu de paramètres de la base des registres permettant de restreindre l'utilisation du système. Lors de l'ouverture de session, la stratégie système était chargée depuis un contrôleur de domaine et appliquée tout le temps que durait la session utilisateur.

Dans Windows 2000 la Stratégie de Groupe représente alors une généralisation de la notion de Stratégie Système de Windows NT.

L'étendue des fonctionnalités de Stratégie de Groupe reste cependant plus vaste que ce qui se faisait sous Windows NT ; par exemple il est désormais possible de gérer des scripts de fermetures de session (sous Windows NT seuls les scripts d'ouverture de session étaient disponibles), d'autre part les Stratégies de Groupes permettent de gérer des événements au démarrage et à l'arrêt des ordinateurs (alors que les stratégies systèmes n'influaient que sur l'ouverture de session).

Sous Windows 2000, les objets GPO sont stockés dans Active Directory et ce n'est plus Poledit (l'éditeur de stratégies) qui est utilisé pour les gérer mais un "snap-in" de la MMC. De plus, alors que les stratégies systèmes étaient affectées à des groupes ou à des ordinateurs, les Stratégies de Groupes sont affectées à des conteneurs Active Directory. Enfin, sous Windows 2000, ces stratégies peuvent être modifiées à chaud, puisqu'elles sont automatiquement rafraîchies toutes les 90 minutes.

Des Stratégies de Groupes peuvent être appliquées sur différents niveaux. L'ordre d'application des différentes stratégies est réalisé selon une méthode hiérarchique, comme suit :

- Les stratégies au niveau du site sont d'abord appliquées,
- Puis ensuite celles au niveau du domaine,
- Et enfin celles au niveau de OU (Organisation Unit).

Il y a cumul des stratégies tant qu'aucun conflit n'intervient. S'il y a conflit, c'est alors la stratégie la plus prête de l'utilisateur qui est alors appliquée (donc celle qui se trouve au niveau de la dernière UO d'appartenace de l'utilisateur). Dans le cas ou plusieurs stratégies sont définies pour le même conteneur, les stratégies sont alors lues dans l'ordre de la liste, du bas vers le haut.

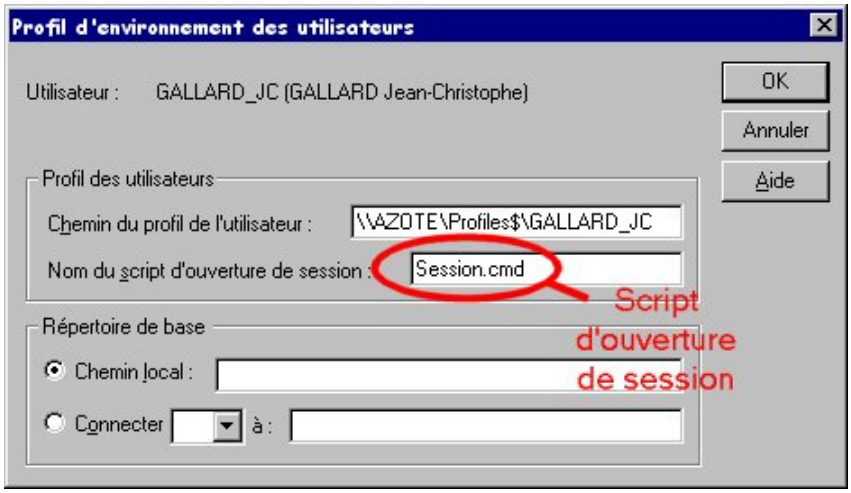
Une différence de taille apparaît lorsque l'on compare les GPO Windows 2000 avec les Stratégies système de NT 4.0 : alors que sous Poledit, les Stratégies étaient applicables à des utilisateurs et / ou des groupes, **les GPO ne s'appliquent qu'aux Unités Organisationnelles**.

Ce point qui semble compliquer la tâche d'administration ne fait dans les faits que la simplifier. En effet, lorsque l'on change un utilisateur ou un ordinateur d'unité organisationnelle, la stratégie de groupe de cette UO lui est directement appliquée sans qu'une modification des stratégies n'intervienne. En outre, il n'est plus nécessaire de créer spécifiquement des groupes pour les stratégies systèmes.

3.3.7. Scripts d'ouverture de session

Il est également possible d'utiliser des scripts de connexion. Il s'agit de fichiers Scripts (.BAT, .CMD…) ou de programmes (.EXE, .COM) qui sont lancés automatiquement lors de l'ouverture de session par un utilisateur.

Pour attribuer un script d'ouverture de session à un utilisateur, aller dans le « Gestionnaire des utilisateurs », choisir un utilisateur, cliquer sur le bouton « Profils » et frapper le nom du script qu'on désire voir lancer à chaque ouverture de session.

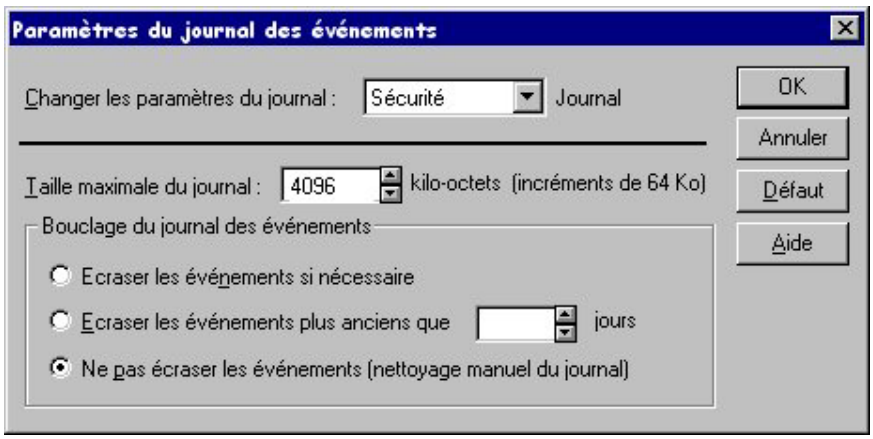


Les scripts d'ouverture de session doivent être placés dans le répertoire partagé NETLOGON des serveurs de domaine

3.4. Journalisation des événements

Sous Windows NT, il n'existe que trois types de journaux d'audit qui sont les journaux **« Application », « Système » et « Sécurité ».** Le niveau de journalisation est laissé à la discrétion des applicatifs, seul le journal de sécurité est paramétrable afin de ne filtrer que certains événements (option « Stratégie d'audit » du « Gestionnaire des utilisateurs »).

On peut cependant paramétrer les journaux sur leur taille maximale, sur la stratégie à adopter en cas de saturation et sur la durée de validité des informations y figurant (Option « Paramètres du journal » de « l'Observateur d'événements »).


Paramètres du journal des événements
Changer les paramètres du journal :
Sécurité
Journal
OK
Annuler
Défaut
Aide
Taille maximale du journal :
4096
kilo-octets (incréments de 64 Ko)
Bouclage du journal des événements
Ecraser les événements si nécessaire
Ecraser les événements plus anciens que
jours
Ne pas écraser les événements (nettoyage manuel du journal)

4. Les outils d'aide à l'administration de la sécurité

4.1. Préambule

Sécuriser un système Windows NT est une opération parfois fastidieuse mais réalisable assez facilement si l'on suit quelques règles de bon sens. Connaître le niveau de sécurité d'un système déjà en place est par contre plus délicat. Cependant, le système d'exploitation de Microsoft, malgré la multitude d'utilitaires disponibles en standard, peut s'avérer insuffisant pour ces manipulations. Il existe malgré tout un certain nombre d'utilitaires permettant de gérer la sécurité de son site.

Les chapitres qui suivent donnent quelques indications sur des outils, commerciaux ou du domaine public, qui peuvent être mis en œuvre afin d'obtenir une idée générale de la sécurité de son réseau et de le protéger. La liste n'est pas exhaustive, les outils proposés dans les pages qui suivent donnent simplement des indications sur les produits les plus courants.

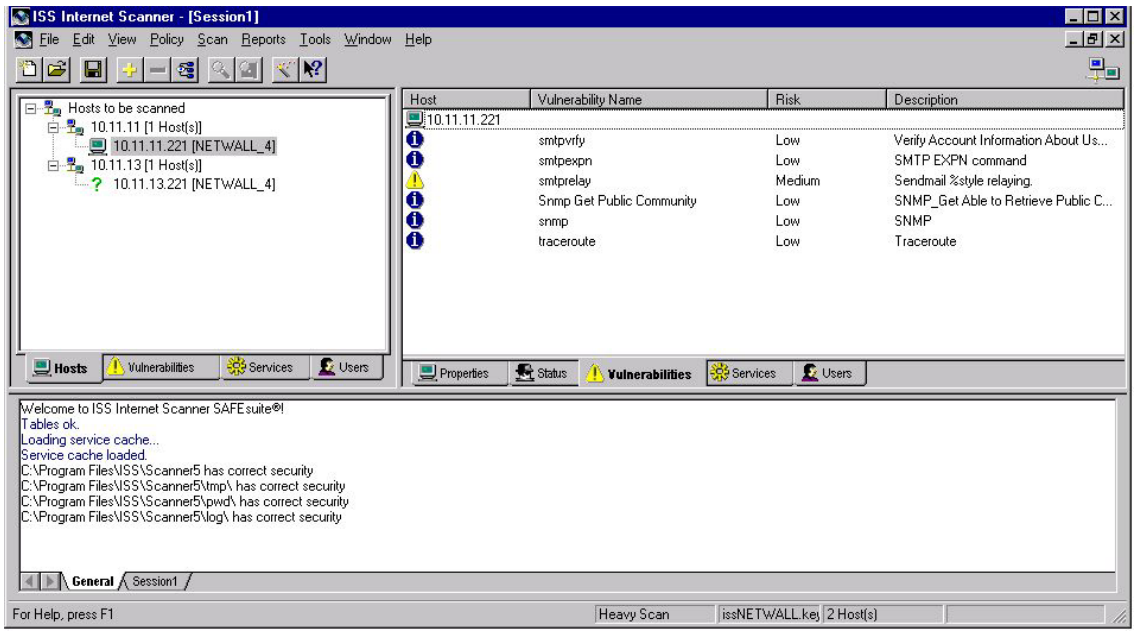
4.2. Auditer son système d'information

4.2.1. Produits ISS

La société ISS (Internet Security Systems) propose depuis quelques temps des outils d'audit de la sécurité informatique. Son produit phare, leader dans le domaine, est sans aucun doute **Internet Scanner**. Ce produit permet d'obtenir une vision générale de la sécurité de ses systèmes informatiques **du point de vue du réseau**.

L'outil fonctionne sur le réseau, depuis une machine NT ou Unix sur laquelle il est installé, et va scanner un réseau pour y découvrir les machines présentes, puis, pour chaque machine, il teste les ports de services utilisés (les services « serveurs » présents) et tente d'y découvrir des vulnérabilités connues.

Extrêmement complet et remis à jours très régulièrement, c'est probablement le meilleur outil d'audit disponible sur le marché. Il permet en outre de générer automatiquement des rapports d'audit dans divers formats.



Cependant, **la complexité du produit et des tests qu'il réalise en fait un outil à ne pas mettre entre toutes les mains** ; il nécessite une **bonne maîtrise des couches TCP/IP et de la sécurité**

informatique en général. Ce produit est d'ailleurs massivement utilisé par les cabinets d'audit spécialisés en SSI (y compris au sein du ministère de la défense). Notons également que son coût prohibitif en fait un outil difficilement utilisable localement pour un réseau informatique de faible importance.

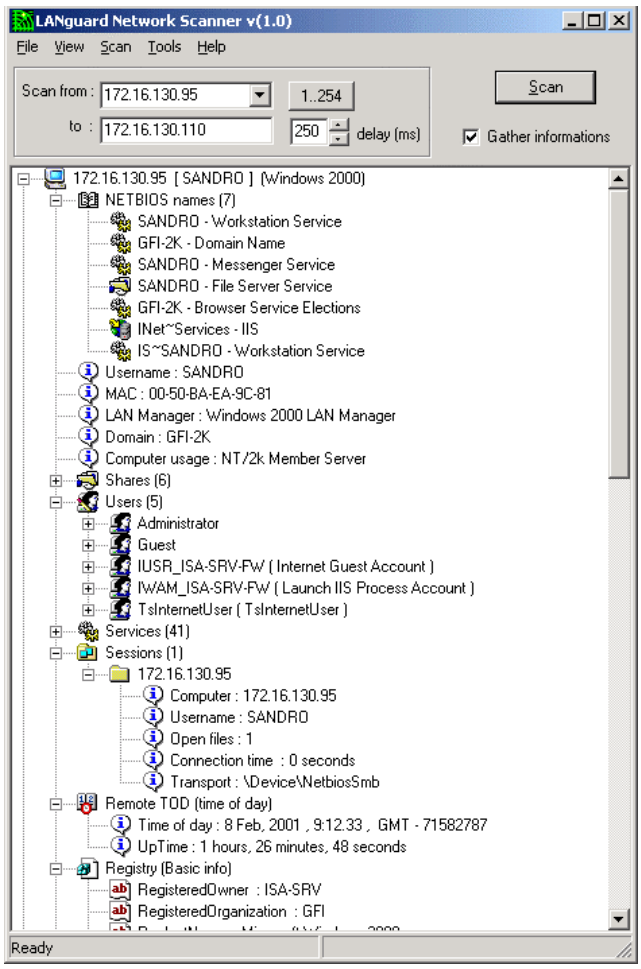
Un autre outil fourni par cette même société est **Security System Scanner**. Cet utilitaire permet d'auditer un système informatique (Unix à l'origine, Windows NT est désormais supporté) de l'intérieur de la machine, il s'installe en local sur la machine cible puis vérifie la configuration interne du système d'exploitation et remonte des alertes en cas de découvertes de vulnérabilités ou de mauvaises configurations.

4.2.2. LANguard Network Scanner

http://www.languard.com

LANguard Network Scanner est un outil freeware capable d'auditer la sécurité d'un réseau. Il permet de :

- scanner un réseau à l'aide de requête UDP sur chaque adresse IP.
- lister la table des noms NETBIOS de chaque système détecté
- récupèrer les noms NETBIOS des machines, les noms des utilisateurs connectés et les adresses MAC
- identifier les systèmes à l'aide de requête SMB (Windows 9x/NT/2000/Unix).
- lister tous les partages (y compris les imprimantes et les partages administratifs cachés)
- identifier les mots de passes sur les partages de Windows 9x.
- tester la résistance des mots de passe des systèmes Windows 9x/NT/2000 à partir d'un dictionnaire.
- identifier les service TCP/IP standards (http, ftp, telnet, smtp...)
- lister les utilisateurs, les services des systèmes Windows NT et 2000.
- récupèrer les informations de la base de registre
- scanner les ports TCP/UDP avec enregistrement des bannières)
- détecter les agents SNMP



4.2.3. NetBIOS Auditing Tool (NAT)

NAT est à la fois un outil de balayage des ressources partagées et de crackage de mots de passe. Il tente d'effectuer des connexions à partir de listes de noms d'utilisateurs et de mots de passe. Beaucoup de systèmes Windows NT étant bien souvent peu protégés, cette méthode peut s'avérer efficace.

Neon Surge et Rhino9 ont développé une interface graphique pour NAT.

Voici le résultat d'un scan de NAT :

```
[*]--- Reading usernames from userlist.txt
[*]--- Reading passwords from passlist.txt

[*]--- Checking host: 0.0.0.0
[*]--- Obtaining list of remote NetBIOS names

[*]--- Attempting to connect with name: *
[*]--- Unable to connect

[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to connect with protocol: MICROSOFT NETWORKS 1.03
[*]--- Server time is Tue Oct 14 11:33:46 1997
[*]--- Timezone is UTC-4.0
[*]--- Remote server wants us to encrypt, telling it not to

[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to establish session
```

```
[*]--- Was not able to establish session with no password
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password:
`ADMINISTRATOR'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `GUEST'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `ROOT'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `ADMIN'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `PASSWORD'
[*]--- CONNECTED: Username: `ADMINISTRATOR' Password: `PASSWORD'

[*]--- Obtained server information:

Server=[AENEMA] User=[] Workgroup=[STATICA] Domain=[]

[*]--- Obtained listing of shares:


Sharename      Type      Comment
---------      ----      -------
ADMIN$         Disk:     Remote Admin
C$             Disk:     Default share
D$             Disk:     Default share
E$             Disk:     Default share
HPLaser4       Printer:  HP LaserJet 4Si
IPC$           IPC:      Remote IPC
NETLOGON       Disk:     Logon server share
print$         Disk:     Printer Drivers

[*]--- This machine has a browse list:

Server               Comment
---------            -------
AENEMA

[*]--- Attempting to access share: \\*SMBSERVER\
[*]--- Unable to access

[*]--- Attempting to access share: \\*SMBSERVER\ADMIN$
[*]--- WARNING: Able to access share: \\*SMBSERVER\ADMIN$
[*]--- Checking write access in: \\*SMBSERVER\ADMIN$
[*]--- WARNING: Directory is writeable: \\*SMBSERVER\ADMIN$
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\ADMIN$

[*]--- Attempting to access share: \\*SMBSERVER\C$
[*]--- WARNING: Able to access share: \\*SMBSERVER\C$
[*]--- Checking write access in: \\*SMBSERVER\C$
[*]--- WARNING: Directory is writeable: \\*SMBSERVER\C$
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\C$

[*]--- Attempting to access share: \\*SMBSERVER\D$
[*]--- WARNING: Able to access share: \\*SMBSERVER\D$
[*]--- Checking write access in: \\*SMBSERVER\D$
[*]--- WARNING: Directory is writeable: \\*SMBSERVER\D$
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\D$

[*]--- Attempting to access share: \\*SMBSERVER\E$
[*]--- WARNING: Able to access share: \\*SMBSERVER\E$
[*]--- Checking write access in: \\*SMBSERVER\E$
[*]--- WARNING: Directory is writeable: \\*SMBSERVER\E$
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\E$

[*]--- Attempting to access share: \\*SMBSERVER\NETLOGON
[*]--- WARNING: Able to access share: \\*SMBSERVER\NETLOGON
[*]--- Checking write access in: \\*SMBSERVER\NETLOGON
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\NETLOGON

[*]--- Attempting to access share: \\*SMBSERVER\print$
[*]--- WARNING: Able to access share: \\*SMBSERVER\print$
[*]--- Checking write access in: \\*SMBSERVER\print$
[*]--- WARNING: Directory is writeable: \\*SMBSERVER\print$
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\print$
```

```
[*]--- Attempting to access share: \\*SMBSERVER\ROOT
[*]--- Unable to access

[*]--- Attempting to access share: \\*SMBSERVER\WINNT$
[*]--- Unable to access
```

4.2.4. Cybercop Scanner / Ballista

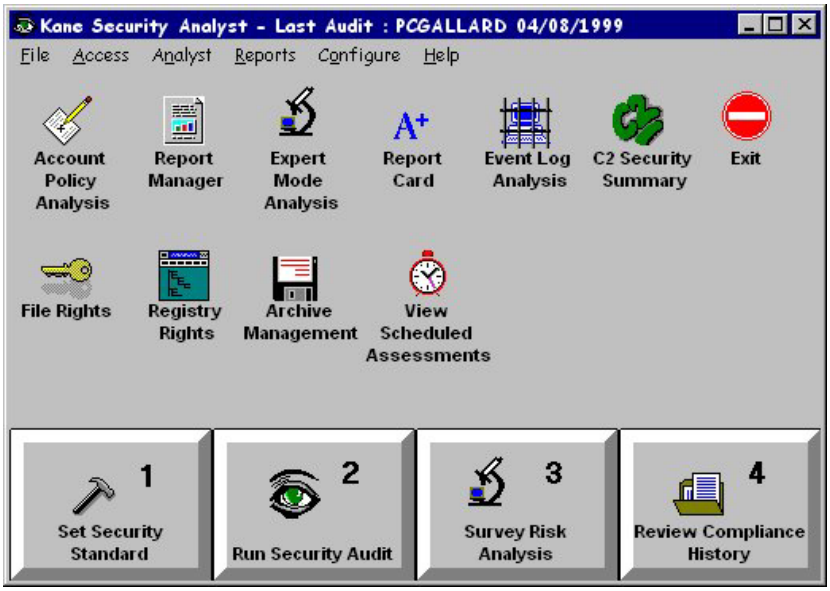
Concurrent direct de ISS, Cybercop Scanner est un produit plus récent, issu d'un développement spécifique pour le ministère de la défense canadien (Ballista). Le principe de fonctionnement est similaire au produit d'ISS, mais cet utilitaire, dans sa version actuelle, souffre d'un manque de professionnalisme évident dans son développement.

Moins cher et moins complexe à mettre en œuvre, il est plus recommandé pour une utilisation sur un réseau de faible importance.

4.2.5. Kane Security Analyst

Produit par **SecurityDynamics**, cet outil permet de scanner des machines Windows NT en fonction d'une politique de sécurité donnée, et de remonter des alertes en cas de violation de celle-ci.

L'outil est très puissant mais assez difficile à mettre en œuvre puisqu'il nécessite une bonne maîtrise des problèmes de sécurité sous Windows NT. Il peut cependant représenter un bon compromis coût / efficacité, dans la mesure où son coût est nettement inférieur aux produits ISS. Cependant**, cet outil ne vérifie pas la présence de vulnérabilités connues** comme peut le faire ISS, et ne prend en compte que des machines Windows NT.



La même société distribue également un second produit appelé **Kane Security Monitor**, dont le principe de fonctionnement en client / serveur permet d'auditer, à distance, certains événements de sécurité sur des machines Windows NT. Dans son fonctionnement, il s'apparente plus à un

produit de détection d'intrusion qu'à un véritable outil d'audit. Il nécessite l'installation préalable de services spécifiques sur les machines cibles.

4.2.6. Satan

Satan a été développé par Dan Farmer, un ex-ingénieur de Sun, expert en sécurité informatique (ex, car ce développement lui a valu son licenciement), puis versé immédiatement dans le domaine public. Premier outil d'audit vraiment cohérent jamais développé, les premiers développements datent de 1991. Satan ne fonctionne que depuis une machine Unix.

Ce produit n'est cité ici que pour son caractère historique, car son ancienneté fait de lui un produit bien obsolète.

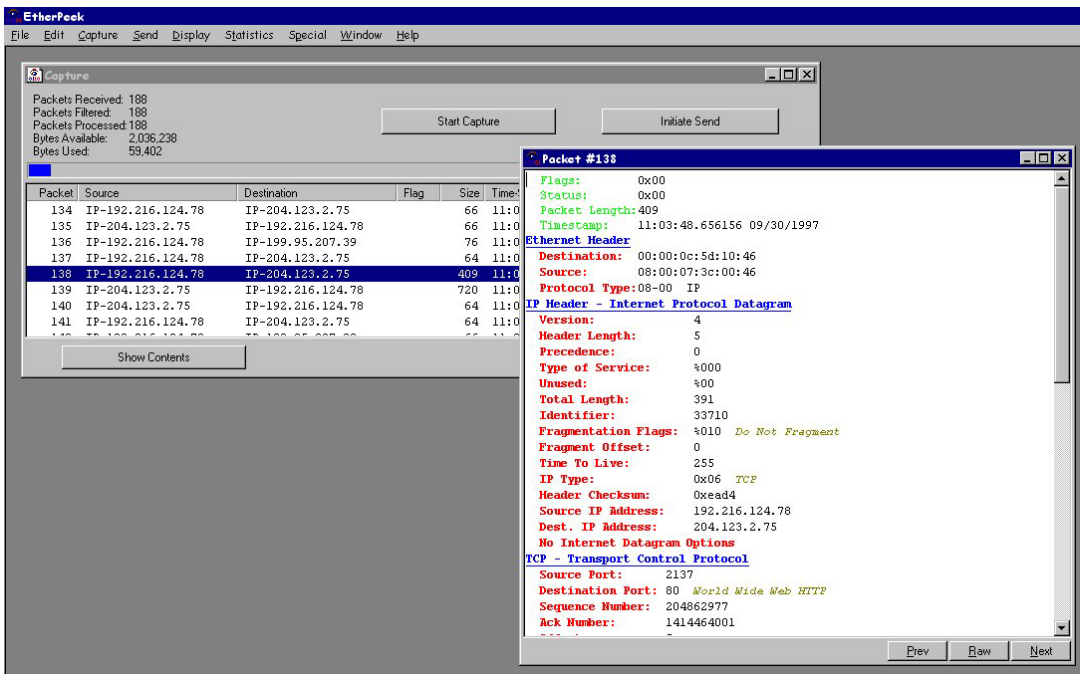
C'est donc un produit assez ancien qui n'a jamais été remis à jour depuis sa version 1.1.1 (qui date déjà de 1994). Son codage est un modèle de ce qu'il ne faut pas faire : un mélange hétéroclite de code Perl, de Shell script et d'un peu de code C recompilé à la volée, le tout peu commenté.

Contrairement à d'autres scanners du commerce, **il n'est pas bridé** ce qui permet de scanner tout l'Internet si on le désire. Son interface est typiquement UNIX, c'est à dire ; paramétrage par fichiers de configuration, sortie des résultats dans des fichiers (texte ou HTML) et dans un format difficilement exploitable (il faut faire un gros effort de traduction pour comprendre ce qu'il remonte comme information). Coté efficacité, on peut dire que, compte tenu de son âge avancé**, il n'est pas à utiliser car sa base de vulnérabilité est beaucoup trop ancienne**.

Important : certaines versions de Satan, téléchargeables sur l'Internet, ont été « plombées » par son auteur. Lorsque ces versions de Satan découvrent une vulnérabilité grave sur une machine (permettant de rentrer en tant que « root »), Satan introduit une BackDoor dans le système (le Daemon de messagerie - sendmail -, en ajoutant des règles dans le fichier de configuration 'sendmail.cf'). C'est Dan Farmer lui-même qui a dévoilé le problème en 1996.

4.2.7. Etherpeek

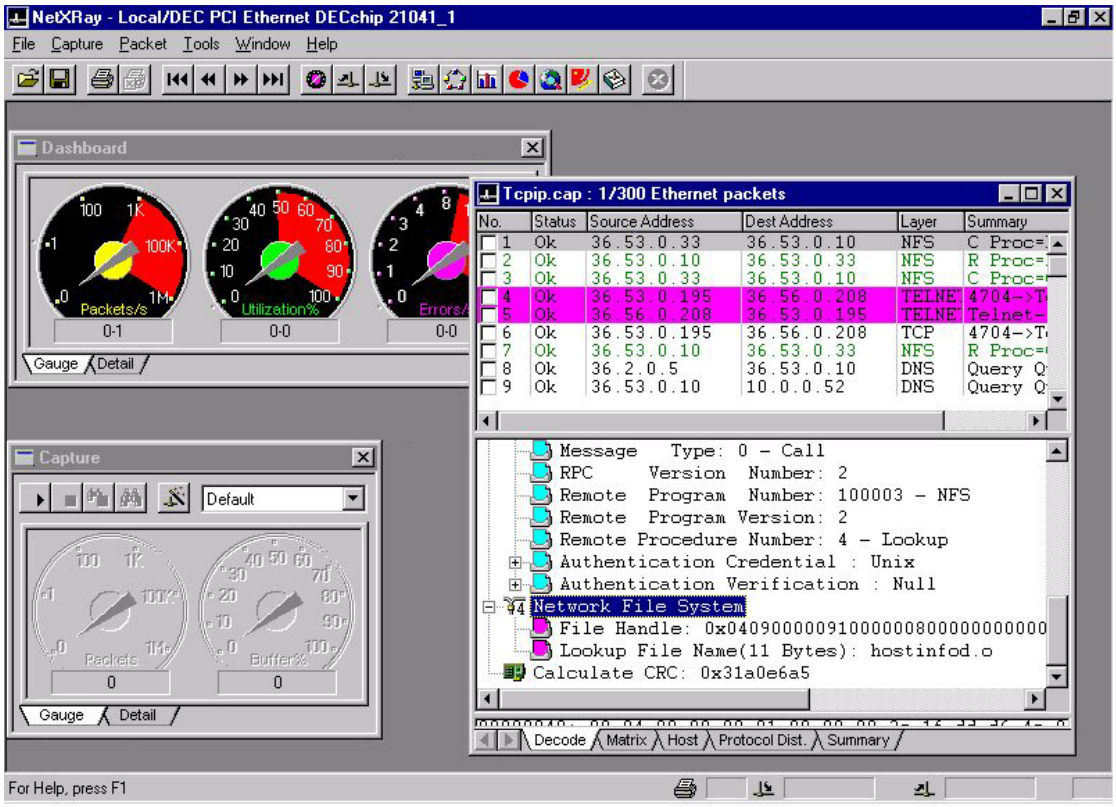
Ce produit n'est pas exactement un produit d'audit, son rôle est de permettre la capture de trames sur un réseau Ethernet. Il est doté d'une interface permettant de décoder les paquets émis et sait gérer la grande majorité des protocoles existants.



L'outil peut être très utile pour déterminer les machines qui se parlent et les protocoles utilisés sur son réseau.

4.2.8. Sniffer Basic / Sniffer Pro

Ces deux produits sont similaires dans leur fonctionnement à Etherpeek. L'effort a été mis sur les aspects « sonde réseau » et « décodage de paquets », ce qui en fait un outil idéal pour avoir une idée de la charge de son réseau et des protocoles qui y transitent.



Point important s'agissant de Windows NT, ils savent parfaitement décoder les paquets émis par des stations Windows (protocole SMB, ou CIFS). Cependant, le module de recherche de chaînes dans les paquets est un peu sommaire et le module de génération de paquets reste très basique.

La version « Basic » a disparu au profit de la version « Pro »

4.2.9. Ethereal

Freeware, Windows.
Gerald Combs
http://www.ethereal.com/.
Installer la version 0.8.20.

Ethereal est un analyseur de trames réseau fonctionnant sous Windows et Unix. Il supporte en natif de très nombreux protocoles. C'est un produit similaire à Etherpeek et Sniffer Pro mais en libre utilisation.

4.2.10. Port Scanning

Il existe également un grand nombre d'outils permettant de réaliser du « Port Scanning ». Ces outils se contentent d'effectuer un scan sur une ou plusieurs machines afin de remonter comme information les ports de services actifs.

On peut citer ici un bon produit, complet, gratuit, et sous Windows NT : SuperScan.

4.3. Détection d'intrusion

Un des problèmes majeur qui se posent à un administrateur système est celui de la détection d'intrusion : comment déceler qu'une attaque est en train d'être menée sur son système d'information ?

Certains outils permettent de réaliser cette fonction. On peut cependant distinguer deux techniques principales pour réaliser cette fonction, chacune ayant ses avantages et ses inconvénients ; la **détection comportementale** et la **détection par scénario**.

4.3.1. Détection comportementale

Le principe est de gérer, pour chaque utilisateur ou pour chaque machine (voire pour le réseau lui-même), un profil d'utilisation mis à jour à chaque action sur le système d'information. On passe donc d'abord par une phase d'apprentissage durant laquelle l'outil examine le comportement standard d'un utilisateur (ou d'une machine, ou d'un réseau). Une fois ce comportement stocké dans la mémoire du détecteur d'intrusion, tout écart majeur par rapport à ce comportement de référence génère une alerte qui est remonté auprès des administrateurs.

Ce mécanisme est très efficace à condition que le comportement moyen d'un utilisateur ne varie pas trop d'un jour à l'autre. Il peut être toutefois mis en défaut de plusieurs manières.

Ainsi, un utilisateur qui adopte un comportement normal mais qui dévie lentement vers un comportement plus agressif passera au travers des mailles du filet (l'outil considérera que ce comportement agressif est un comportement normal).

De même, lorsque l'utilisation du système d'information change du jour au lendemain le nombre de fausses alertes devient très important. La NSA américaine a fait les frais de ce changement de comportement lors de la guerre du Golfe : le comportement de ses utilisateurs a changé du tout au tout dès lors que les premières frappes militaires ont commencé en janvier 1991, à tel point que l'outil de détection d'intrusion a du être déconnecté pour éviter de remonter 150 Mo d'alertes en une journée.

4.3.2. Détection par scénario

Le principe de détection par scénario consiste à déterminer un certain nombre de scénarios d'attaque et de remonter des alertes à chaque fois qu'un tel scénario est rencontré. On peut ainsi décider de remonter une alerte lorsqu'une machine teste séquentiellement tous les ports de service d'une autre machine, ou lorsqu'un utilisateur lance 10 fois par minute la commande « ps » sous un système Unix.

Cette technique est assez efficace pour contrer la plupart des attaques, elle se heurte toutefois aux problèmes suivants : des scénarii d'attaque inconnus ne seront pas détectés, et, connaissant les types de scénarii gérés par l'outil, il est assez facile de monter un nouveau scénario d'attaque qui passera entre les mailles du filet.

La grande majorité des outils de détection d'intrusion actuellement disponibles fonctionne sur ce principe de détection par scénario.

A titre d'exemple, on peut citer un outil assez ancien sous Unix, « Gabriel », qui détecte les scans en provenance de l'outil Satan, et RealSecure de la société ISS (version Unix et NT) qui fonctionne sur ce même principe.

4.3.3. Autres types de détection

D'autres types de mécanismes de détection d'intrusion existent, mais leur développement est pour l'instant limité aux laboratoires de recherche. Pour information, on peut citer le produit Gassata

(pour Unix), développé à l'école Supélec de Rennes, qui gère un curieux mécanisme de détection d'intrusion par analyse de traces, basé sur un algorithme génétique…

4.4. Combler les failles

4.4.1. Services Packs et Hot Fixes

Suite aux nombreux bugs découverts au fil de l'eau par les utilisateurs de Windows NT, Microsoft fournit des révisions de son système d'exploitation, sous la forme de « **Service Packs** » et de « **Hot Fixes** ».

Services Pack et Hot Fixes permettent de faire évoluer un système Windows NT et de **corriger certains problèmes de dysfonctionnement ou de sécurité**. Le hot-fix est **une correction mineure** qui se limite à un point ou service particulier. Le Service Pack **est une mise à jour majeure** du système d'exploitation qui prend en compte tous les hot fixes et services pack précédents.

S'agissant de remplacement d'exécutables et/ou de librairies buggés par d'autres (non, ou moins buggés), il est impératif de **suivre les préconisations de Microsoft quant à l'ordre d'application** des Hot Fixes.

4.4.2. SecEdit

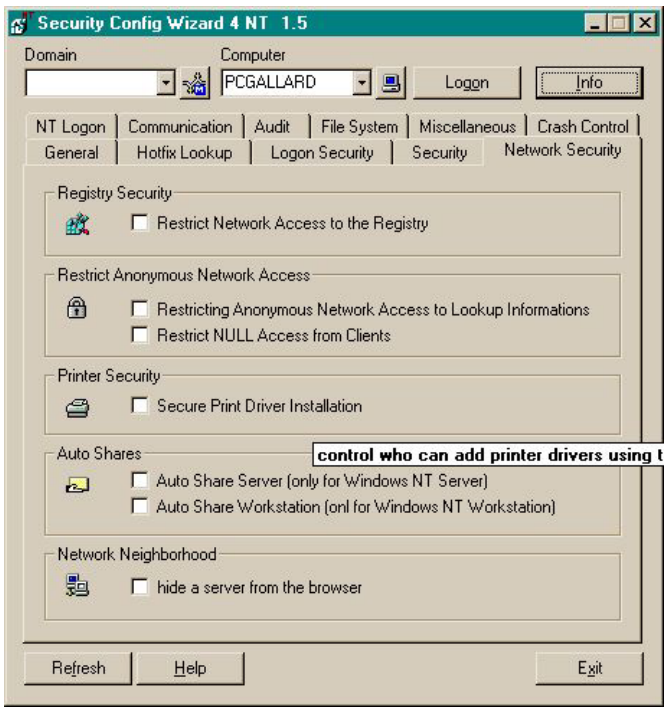
Présent dans le CD-Rom du Service Pack 4 (mais à installer **en plus** du SP4), SecEdit constitue l'outil de base de la sécurisation du système d'exploitation sous Windows 2000.

SecEdit se présente sous la forme d'une extension spécifique de la MMC (Microsoft Management Console). Cet outil permet de postionner des options de sécurité par modification de paramètres dans la base de registre, mais surtout permet de modifier les ACLs standard à la fois sur le système de fichier et sur la base de registre.

Notons que l'installation de SecEdit sous Windows NT 4.0 **active** les nouvelles fonctionnalités du système de fichiers NTFS présentes dès le Service Pack 4, mais inemployés jusqu'à l'arrivée de Windows 2000 ; dès lors, on peut remarquer une modification de l'interface de saisie / modification des ACLs sur le système de fichiers.

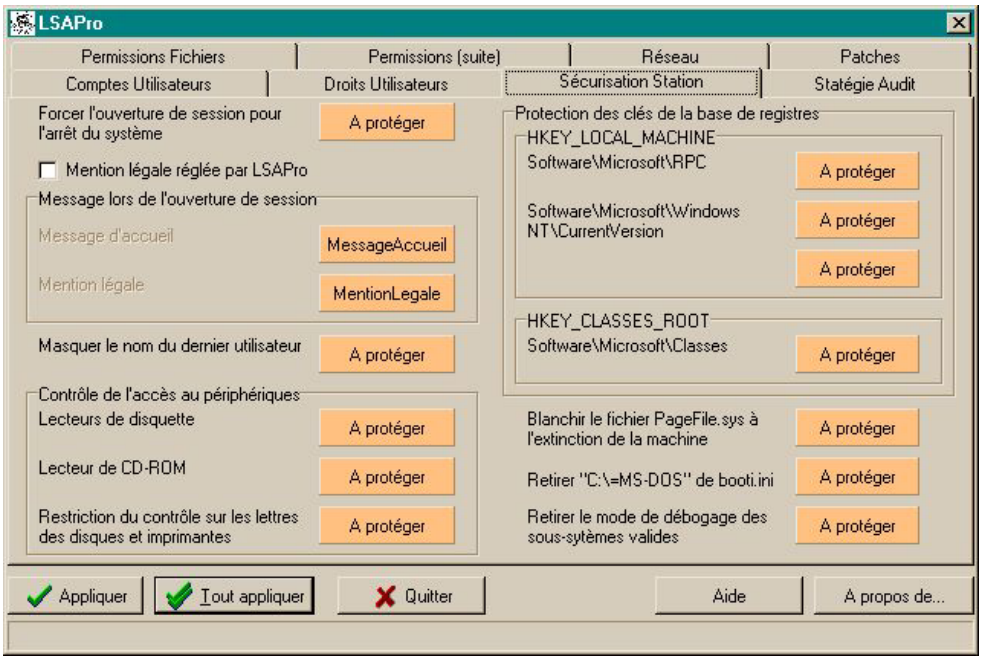
4.4.3. Security Config Wizard

Produit du domaine public, Security Config Wizard est un utilitaire qui permet de sécuriser une machine Windows NT en local et à travers un réseau. L'outil est remarquablement complet et offre une interface graphique qui en fait un outil très simple à mettre en œuvre. La sécurisation intervient sur la base des registres, le système de fichiers et la politique de sécurité.



4.4.4. LSA Pro

Développé au sein de l'équipe BASILIC du CELAR / CASSI, LSAPro est un outil d'aide à la sécurisation de postes Windows NT. Les premiers développements datent de 1997, l'outil a été créé dans le but d'automatiser les recommandations émises par le CELAR sur la sécurité du système Windows NT. Le développement de l'outil a définitevement été abandonné suite à la distribution de SecEdit par Microsoft.



Il nécessite cependant une bonne connaissance des mécanismes de sécurité de Windows NT pour être mis en œuvre de façon optimale.

4.5. Outils divers

4.5.1. Le NT Resource Kit

Microsoft fournit, outre son système d'exploitation, une collection de programmes pour Windows NT au sein d'un package appelé le NT Resource Kit. On trouvera dans cette collection un bon nombre d'utilitaires comblant des manques de Windows NT. La plupart de ces utilitaires se présentent sous la forme de commandes MS-DOS acceptant des paramètres. D'autres outils un peu plus complexes disposent d'une interface graphique. C'est une véritable mine d'information pour les Administrateurs de systèmes Windows NT.

4.5.2. John the ripper

Largement inspiré de Crack (outil de craquage de mots de passe Unix), John the ripper est un craqueur de mot de passe multi-plateformes ; les sources sont disponibles pour une dizaine de systèmes d'exploitation. A noter que les primitives de chiffrement DES ont été entièrement réécrites et optimisées pour les processeurs à base MMX et K6 : cependant ses performances sont inférieures de moitié pour le craquage exhaustif de mots de passe Windows NT par rapport à l0phtcrack (voir plus loin - selon les machines et les OS, le ratio va de 2 à 3).

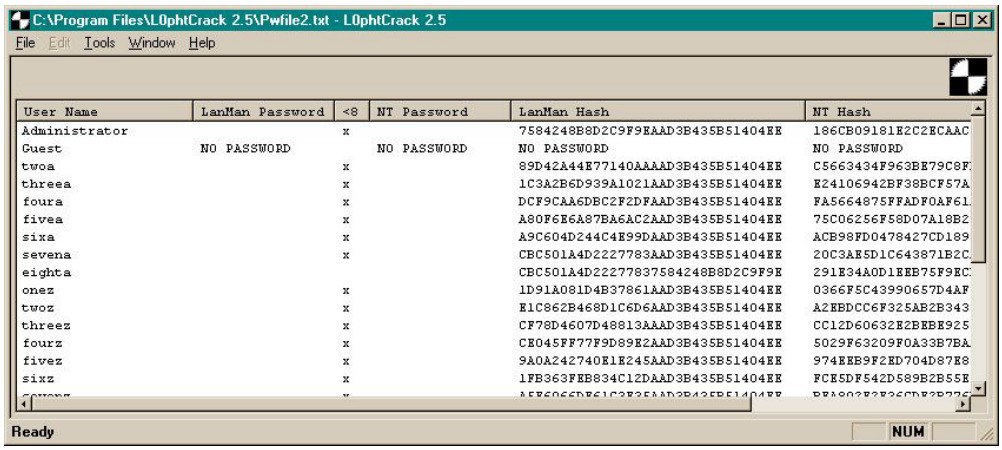
Il permet de réaliser des attaques exhaustives et par dictionnaire de la même façon que le Crack Unix, en utilisant éventuellement des règles de compositions de mots de passe. Son principal avantage est qu'il permet d'attaquer à la fois les fichiers de mots de passe Unix et Windows NT (pour ce dernier en utilisant préalablement l'utilitaire pwdump - version 1 ou 2 - pour récupérer la table SAM d'un serveur).

Entièrement paramétrable, mais livré sans aucune interface graphique (les paramètres sont saisis dans des fichiers de configuration au format texte), cet utilitaire est gratuit.

A la date de rédaction de ce document, la dernière version du logiciel était la 1.6.

4.5.3. L0phtcrack

Société créée par un ancien groupe de hackers américains, l0pht a développé un outil de craquage de mots de passe pour Windows NT. Il permet de réaliser des attaques exhaustives et par dictionnaires, cependant, l'attaque par dictionnaire ne permet pas d'ajouter des règles de composition de mots de passe comme avec le Crack Unix. La seule option possible est ici d'utiliser tous les mots d'un dictionnaire et de rajouter à la fin, pour chacun d'eux, un ou plusieurs caractères choisis (attaque mixte dictionnaire - exhaustif).



La version 2.5x permet de récupérer un fichier de mots de passe par :

- « dump » de la table SAM d'un système Windows NT (pour peu de disposer de privilèges d'administration),
- lecture du fichier sam._, image de la SAM générée par RDISK (utilitaire de disquette de réparation) qui est contenu dans le dossier %systemroot%\repair et sur la disquette de réparation,

- écoute du réseau afin d'y capturer des trames d'authentification en vue d'un crack ultérieur.

Le résultat peut être soumis à une attaque exhaustive ou par dictionnaire. Ces mêmes versions permettent de réaliser environ 700.000 essais par seconde sur un Pentium II à 333 Mhz.

L'outil est disponible en téléchargement sur le site Web de L0pht, en version d'évaluation 15 jours. Il est entièrement graphique. La version non-limitée est payante (environ 15 US$). Cet outil a, en outre, récemment évolué et la version 3 est enfin disponible.

4.6. Antivirus

Il n'est pas question ici de préconiser l'emploi de tel ou tel antivirus disponible sur le marché. Du point de vue de l'efficacité de détection, les produits disponibles se valent à peu près tous (à de rares exceptions près). Cependant, il s'avère pratiquement indispensable de protéger son système d'information contre les attaques de virus.

Le choix d'un antivirus se fera en fonction de l'utilisation qui est faite du système d'information, on peut cependant préconiser un certain nombre de règles à respecter, parmi lesquelles :

- Disposer d'un antivirus dont le moteur et les bases de définition de virus sont récents,
- Avoir un contrat avec son fournisseur afin de s'assurer des mises à jour régulières tout au long de la vie du système d'information,
- Corollaire du point précédent ; s'assurer de la pérennité de son fournisseur,
- Pour la mise à jour de son antivirus, opter de préférence pour un mécanisme qui évite de devoir passer sur tous les postes. A ce titre, on peut distinguer deux types de technologies : la première est une **mise à jour automatique depuis un serveur** (c'est le serveur qui va mettre à jour ses postes clients - Sweep par exemple), la seconde est **une mise à jour sur requête expresse de l'utilisateur** (c'est le client qui déclenche la mise à jour - Norton Antivirus par exemple). Il est toutefois bon de rappeler que dans le cas de la seconde solution, par expérience, les utilisateurs ne pensent presque jamais à mettre leur antivirus à jour.
- Prévoir un « sas » antivirus en libre service afin de décontaminer les fichiers en provenance d'autres réseaux,
- En cas d'utilisation d'une messagerie, penser à vérifier que son antivirus est capable d'analyser les pièces jointes des messages,
- Penser également à vérifier que son antivirus est configuré pour analyser les fichiers compressés les plus courants (ZIP, GZ, ARJ, etc.)

5. Sécuriser Windows NT

5.1. Rappel sur le niveau de sécurité C2

Le gouvernement américain a écrit une série de manuels sur la sécurité informatique au cours des précédentes années. Cette série, appelée « Rainbow Series » (nom dû aux couleurs des couvertures des différents manuels) fut publiée dès le mois de décembre 1985 avec le « Orange Book » et donne une liste de critères d'évaluation pour la sécurité informatique. D'autres manuels furent publiés ultérieurement comme le « Red Book », qui donne une interprétation de l' « Orange Book » pour les systèmes en réseau, ou le «Blue Book » qui donne une interprétation de l' « Orange Book » pour les sous-systèmes.

Le Livre Orange donne 4 niveaux de sécurité, ou classes, allant de D (protection minimale) à A (protection vérifiée). La classe C comporte les niveaux C1 (sécurité discrétionnaire) et C2 (accès contrôlé). Chaque niveau statue sur les protections à mettre en œuvre pour le niveau considéré et dans chacune des options suivantes : Politique de sécurité, Imputabilité, Assurance, et Documentation. Le niveau D ne requiert aucun critère d'évaluation et est généralement destiné aux systèmes évalués et qui ont échoué au cours de l'évaluation. **Le niveau C2 est le niveau minimal accepté par l'administration américaine pour ses systèmes**.

Microsoft, en vue d'accéder au niveau de sécurité C2, a donc ajouté un certain nombre de fonctions de sécurité au cours du développement de Windows NT, destinées à faire passer le cap de l'évaluation C2 et parmi lesquelles on trouve pèle mêle ; imputabilité des actions des utilisateurs, accès authentifié aux ressources, audit des événements de sécurité, listes à contrôle d'accès, protection de l'espace mémoire, etc.

Notons que ce niveau de sécurité C2 n'est pas suffisant en tant que tel pour assurer une sécurité maximale, il s'agit uniquement d'un niveau minimal de sécurité lié à l'utilisation de certains mécanismes et à la présence de documentation sur ces fonctions au niveau de l'utilisateur final. De plus, la certification C2, au sens de l'Orange Book, d'un système informatique n'est accordée par le gouvernement américain qu'à la condition que celui-ci soit utilisé **hors réseau**.

5.2. Choix d'une architecture

5.2.1. Choix de l'architecture réseau

Le choix de l'architecture réseau est ici capital car c'est à ce niveau que seront prises des décisions qui impacteront directement l'utilisation de son système d'information. Il convient donc de faire le bon choix dès le départ, changer d'architecture en cours d'utilisation ayant des coûts, parfois prohibitifs, en matière d'administration.

Pour le choix de l'infrastructure réseau, on fera essentiellement attention à l'aspect performance : on évitera ainsi d'utiliser une liaison à faible débit pour interconnecter un serveur de fichiers qui sera très sollicité. Cependant, on pourra également envisager **l'utilisation de certains mécanismes de sécurité, au niveau réseau**, afin d'assurer un complément de sécurité dans les couches basses du réseau : brouillage de trames, hubs intelligents, routeurs filtrants, commutateurs Ethernet, firewalls, etc.

Les systèmes Windows NT en réseau supporte deux modes d'architecture :

- l'architecture "Workgroups", hérité des systèmes Microsoft antérieurs, Windows 95 et Windows 3.11.
- l'architecture "Domaine", spécifique à Windows NT.

Pour des raisons de centralisation des informations de sécurité, il est préférable d'opter pour une gestion de son système d'information à base de domaine(s) Windows NT. Se reporter quant à leur utilisation au chapitre § 3.1.3 - Architectures possibles.

Du point de vue de l'architecture, il est important de **tenter de répartir différemment les données et les services en fonction de leur type**. On évite de cette manière d'être dépendant d'une seule machine ou d'un seul disque pour le fonctionnement de son système.

Ainsi, on pourra stocker les données partagées sur un serveur de fichiers sur un espace disque différent de celui du système d'exploitation. De même, et essentiellement pour des raisons de performances, on évitera d'utiliser le même serveur pour réaliser des opérations aussi différentes que « Serveur Web », « Serveur Principal de domaine », « Serveur de Messagerie », « Serveur de fichier », « Serveur DNS ou WINS » etc.

Dans la mesure du possible**, ne jamais laisser un serveur principal de domaine sans serveur secondaire**, car, en cas de panne du premier, plus personne ne pourra continuer à se connecter au réseau.

5.2.2. Choix des matériels

Le choix de son matériel a un impact relativement faible sur la sécurité globale de son système d'information. La règle qui s'impose ici est essentiellement de tailler son ou ses serveurs en fonction de l'utilisation qui en sera faite. Sans être exhaustif, on peut cependant citer les points importants suivants :

- Pour un serveur de fichiers, la mémoire vive disponible a peu d'importance (sauf si l'on prévoit de très nombreuses connexions), par contre la capacité disque doit être largement suffisante pour parer aux évolutions du système et en particulier si l'on souhaite mettre en place des volumes privés destinés aux utilisateurs,

- Afin d'éviter une sursaturation des disques, on peut songer à mettre à place un mécanisme de Quotas, qui limite l'espace disque allouable pour un partage. Windows NT 4.0 ne gère pas ce type de mécanisme de façon native, il est nécessaire de faire l'achat d'un produit spécifique (Quota Manager par exemple).

- Il peut être également utile de s'équiper de systèmes de tolérance aux pannes (RAID 5, double alimentation, UPS, clustering etc.) pour un serveur sensible (serveur de fichiers, serveur principal de domaine…),

- Un serveur d'impression sous Windows NT nécessite peu d'espace disque, mais est assez gourmand en ressources mémoire. Il est donc important d'avoir une mémoire vive importante pour ce type d'activité (64 Mo est un minimum),

- Certains applicatifs serveurs sont extrêmement gourmands en mémoire vive. C'est par exemple le cas pour Microsoft Exchange (serveur de messagerie) et pour Lotus Notes (serveur de tout !). Pour ces applications, il est nécessaire de s'équiper d'au moins 128 Mo de RAM, voire de 256 Mo pour un bon confort d'utilisation. De même, éviter d'utiliser le même serveur pour héberger ces deux applicatifs concurrents.

- La plus value qu'offre un système multiprocesseurs pour un serveur Windows NT n'est à priori pas évidente. Elle peut cependant être utile dans le cas d'un serveur d'applications ou d'une machine destinée à de l'infographie (utilisation particulièrement exigeante en ressources CPU). Encore faut-il gérer la répartition de charge sur les processeurs de façon optimale…

5.2.3. Sauvegardes

Dans le cadre de l'utilisation d'un système d'information orienté client / serveur (serveur principal de domaine, serveur de fichiers…) il est fortement recommandé d'implémenter une ou plusieurs solutions de sauvegardes. La ou les solutions retenues devront permettre la sauvegarde de **l'intégralité de l'espace disque** que l'on désire sauvegarder (même si on n'en utilise que 10%).

Eviter de n'effectuer que des sauvegardes totales. Privilégier les solutions à base de sauvegardes incrémentales dans la semaine et de sauvegardes totales le week-end. Conserver les bandes dans un espace protégé, de préférence résistant au feu, et physiquement éloigné des serveurs.

La durée de conservation de ces bandes dépendra de l'utilisation du système d'information, mais on peut recommander une conservation des sauvegardes totales pendant 6 mois à 1an.

Enfin, **penser à la suite de la première sauvegarde à vérifier que l'on peut restaurer sans problème ses fichiers sauvegardés** (i.e. vérifier que l'opération de sauvegarde / restauration fonctionne).

5.3. Installation de Windows NT

Un certain nombre d'opérations doivent être réalisées avant ou lors de l'installation d'un système Windows NT, ce afin d'assurer une sécurité minimale. Les paragraphes qui suivent précisent les options recommandées à mettre en œuvre.

5.3.1. Protection physique des machines :

Les serveurs, et en particulier les contrôleurs de domaine, contiennent par nature des informations sensibles. A ce titre, ceux-ci doivent pouvoir bénéficier d'une protection physique afin d'éviter que n'importe qui puisse y avoir accès. **Il ne doit pas être possible pour un utilisateur normal de pouvoir accéder physiquement aux éléments matériels d'un serveur**.

Toute personne qui aurait accès physiquement au serveur pourrait, à partir d'un autre système d'exploitation (MS-DOS ou Linux), utiliser des outils capable d'accéder aux volumes NTFS, sans connaître les mots de passe (NTFSDOS,..). Certains outils peuvent également modifier le mot de passe du compte Administrateur (ntpasswd).

Ainsi, dans la mesure du possible, les serveurs doivent être situés dans un environnement protégé (salle à accès contrôlé par exemple) et / ou disposer de dispositifs interdisant leur manipulation de manière simple (verrous, boulonnage au sol, chaîne antivol...). Tous les grands constructeurs proposent des serveurs offrant des options de sécurité physique de ce type

5.3.2. Configuration Matérielle des Machines

Un certain nombre de précautions, applicables à tous les systèmes d'exploitation d'ailleurs, sont recommandées :

- Désactiver les composants matériels non utilisés. Certains composants matériels peuvent permettre de contourner la politique de sécurité mise en place, tel les ports séries (modems), les ports parallèles (lecteurs ZIP), les lecteurs de disquettes. S'il n'est pas possible de les retirer physiquement, il est souvent possible de les désactiver dans le BIOS de la machine.

- Protéger l'accès au BIOS (Basic Input Output System) avec un mot de passe :le BIOS est présent sur toute machine de type PC, généralement stocké dans une puce réinscriptible de la carte mère. Il contient les fonctions système de base et le paramétrage fin de la carte mère. Le minimum consiste ici à protéger l'accès à ces paramètres par un mot de passe connu des seuls administrateurs, et ce afin d'éviter une modification non voulue du BIOS.

- Interdire le démarrage de la machine à partir d'un média autre que le disque dur. Le BIOS permet généralement de préciser le média de démarrage.

- Verrouiller les disques durs amovibles ou ne pas en utiliser Il serait alors possible de retirer les disques afin de lire les partitions NTFS à partir d'une autre configuration Windows NT, ou même Windows 95/98 ou Linux.

5.3.3. Choix du Système de Fichiers

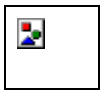
L'installation de Windows NT doit se faire de préférence sur une partition NTFS sans aucun autre système d'exploitation.

En général, il est conseillé :

- **De ne pas installer d'autres systèmes d'exploitation à l'aide d'un multi-boot**. Le multi-boot permet de faire cohabiter plusieurs systèmes d'exploitation sur une même machine, en sélectionnant le système d'exploitation que l'on désire utiliser au démarrage de la machine.

Ceci permettrait d'accèder au système de fichier NTFS en contournant les persmissions positionnées.

- **De n'utiliser que le système de fichier NTFS** :



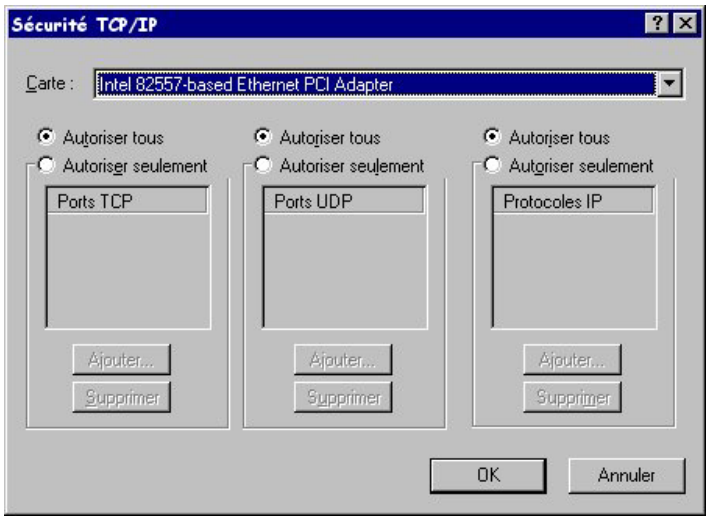
  - Si l'on doit sécuriser une machine déjà installée et qui dispose d'un disque système en FAT, il faut avant tout lancer sous une invite de commande MS-DOS l'utilitaire **convert** (commande `CONVERT lecteur: /FS:NTFS /V`) afin de convertir le système FAT en système NTFS, puis rebooter la machine, la conversion s'effectue alors au redémarrage de la machine. Il faut ensuite utiliser le programme **fixacls.exe** fournit avec le NT Ressource Kit afin de positionner les permissions par défaut sur les fichiers du système d'exploitation, sinon tout le disque est en "Contrôle Total" pour "Tout le monde".

- **De ne pas dupliquer des installations**. Chaque installation de Windows NT génère un SID, unique, qui est utilisé par les mécanismes d'authentification. En copiant une installation type, certains mécanismes de sécurité peuvent être contournés. Certains logiciels de duplication de disques peuvent résoudre ce problème.

5.3.4. Configuration du réseau

Lors de l'installation des services réseau, il est recommandé de **n'utiliser QUE la couche TCP/IP** comme gestionnaire de réseau. Eviter d'installer « Netbios over TCP » ainsi que toute autre couche réseau (IPX/SPX, Protocole AppleTalk…) s'il n'existe pas de besoin spécifique. Dans la mesure du possible **n'installer que des services qui sont indispensables**.

Il est également possible de restreindre l'utilisation des ports de service atteignables sur une machine Windows NT. L'opération s'effectue depuis le panneau de configuration, icône Réseau, option TCP/IP, en cliquant la boîte « Activer la sécurité ». Elle nécessite de parfaitement connaître les ports de services TCP et UDP qui seront utilisés sur la machine.



Si une machine Windows NT est utilisée comme routeur disposant d'une interface reliée à un réseau extérieur non sûr, il est alors préférable de *casser* le lien entre la pile Netbios et l'interface réseau considérée (Onglet *Liaisons* du panneau de configuration réseau). Ainsi, cette machine ne répondra plus aux requêtes Netbios sur l'interface externe.

5.4. Corrections des vulnérabilités majeures et mineures

Avant toute sécurisation ultérieure d'une machine Windows NT, il est nécessaire de combler les principales vulnérabilités connues. Microsoft fournit à cet effet des « Service Packs » et « Hot Fixes » destinés à combler des bugs référencés mais aussi des vulnérabilités (voir § 4.4.1 - Services Packs et Hot Fixes).

A la date de rédaction de ce document, le service pack courant de NT4 est le SP6.

Avant tout chargement d'un Service Pack, il est conseillé de réaliser une sauvegarde du disque système et de créer une disquette de réparation d'urgence. Lors de l'installation, cocher la case « Créer un répertoire de désinstallation » afin de pouvoir revenir en arrière en cas de problèmes.

5.4.1. Ou trouver les Services Pack et Hot-fixes

Les hot-fixes NT 4 français peuvent être téléchargés depuis le site ftp de Microsoft à l'adresse :

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/frn/nt40 .

Le service pack 3 est aussi disponible depuis cette adresse, cependant les services pack 4, 5 et 6 doivent être obtenus à partir du site Internet de Microsoft :

http://support.microsoft.com/support/ntserver/content/servicepacks/default.asp

ou

http://www.microsoft.com/support/winnt/default.htm

5.4.2. Comment installer ces correctifs ?

Un Hot-fix est une archive auto-extractible qui remplace des fichiers « défectueux **». Il est impératif de respecter l'ordre d'application des hot-fixes préconisé par Microsoft. A noter certains hot-fixes (i.e. : Post SP5) doivent aussi être appliqués sur des Service Pack antérieurs** (i.e. : SP3), si l'administrateur n'a pas souhaité passer le poste au Service Pack suivant.

Les hot-fixes sont généralement accompagnés d'un ou plusieurs fichiers Qxxxxxx.txt précisant le cadre d'application du hot-fix et les corrections qu'il implémente. Il est souhaitable de consulter ces fichiers qui peuvent contenir des instructions supplémentaires à réaliser (ex : modification de la base de registre) pour terminer la correction.

Note : à la date de rédaction de ce document, l'ordre des Hot-fixes n'a de sens que pour le Service Pack 3, les Service Pack 4, 5 et 6 n'ont pas de Hot-fixes se recouvrant.

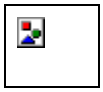
Concernant les Hot-Fixes post Service Pack 6, ceux-ci sont désormais intégrés depuis le 20 juillet 2001 à un correctif plus général appelé "**Post Windows NT 4.0 Service Pack 6a Security Rollup Package**", ou "**SRP**", décrit dans l'article de Microsoft Q299444.

Ce SRP inclut tous les correctifs Post Service Pack 6a pour Windows NT 4.0 (Server et Workstation) et est disponible en téléchargement sur le site de Microsoft (le correctif pèse tout de même quelques 13 Mo !).

Notons que **ce correctif inclut également l'ensemble des correctifs relatifs au service IIS** (Internet Information Service) de Microsoft.

5.5. Actions sur la base des registres

Après avoir procédé aux opérations précédentes sur les machines, on peut pousser la phase de sécurisation plus loin, en modifiant certaines entrées de la base des registres.



Cependant **il est rappelé qu'une manipulation erronée de la base des registres peut, dans certains cas, s'avérer catastrophique et nécessiter une réinstallation complète du système**. Il est donc recommandé de porter une attention toute particulière à ce type d'opération délicate.

Certaines manipulations de la base des registres peuvent entraîner des dysfonctionnements ultérieurs, liés soit à une utilisation particulière du système d'information, soit à la présence d'applicatifs nécessitant une non-protection de certaines parties de la base des registres.

DANS LE DOUTE, NE PAS APPLIQUER DE MODIFICATIONS A LA BASE DES REGISTRES.

Pour les modifications relatives au paramétrage de la base de registre, la suite du document présente de façon synthétique les diverses recommandation et paramétrages type que l'on peut trouver dans la literrature spécialisé. Il peut également être utilie de se référer aux guide de recommandations Windows NT et 2000 fournis avec ce document.

Il existe cependant un certain nombre d'outils permettant de réaliser les modifications décrites ci-dessous de façon automatique. Se reporter au chapitre § 4.4 pour la description de certains d'entre eux.

5.6. Protection et paramétrage du système

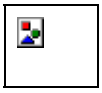
5.6.1. Mettre en place une stratégie de droits

Droits des utilisateurs :

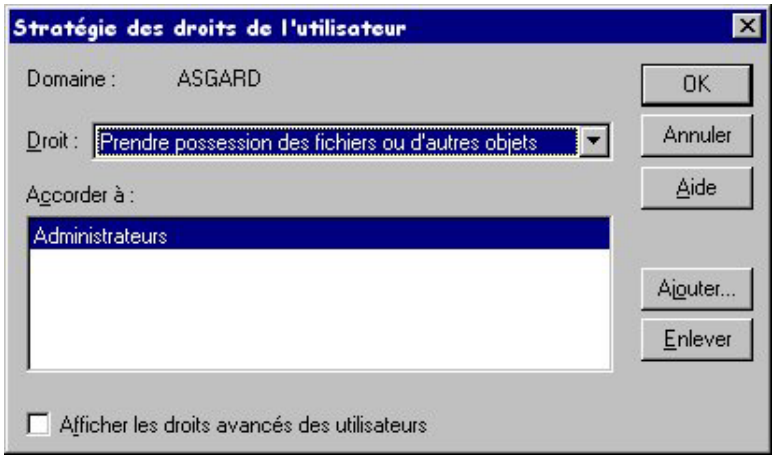
Arrêter le système	Seulement « Administrateurs » (éventuellement les Utilisateurs)
Augmenter la priorité de planification	Seulement « Administrateurs »
Déboguer les programmes	Retirer toutes les entrées
Modifier l'heure système	Seulement « Administrateurs »
Optimiser un processus	Seulement « Administrateurs »
Ouvrir une session localement	Seulement « Administrateurs », « Opérateurs de sauvegarde » et « Utilisateurs » (**sur un serveur, retirer « Utilisateurs » si ce n'est pas déjà fait**)
Accéder depuis le réseau	Seulement « Administrateurs », « Opérateurs de sauvegarde » et « Utilisateurs »
Forcer l'arrêt à partir d'un serveur distant	Seulement « Administrateurs »

S'assurer des configurations suivantes (installées par défaut mais à respecter) :

Agir en tant que partie du système d'exploitation	Retirer toutes les entrées
Créer un objet-jeton	Retirer toutes les entrées
Prendre possession des fichiers et autres objets	Seulement « Administrateurs »
Remplacer un jeton niveau de processus	Retirer toutes les entrées
Restaurer / Sauvegarder des fichiers ou répertoires	Seulement « Administrateurs » et « Opérateurs de sauvegarde »
Verrouiller des pages mémoire	Retirer toutes les entrées



Pour les autres droits non listés, personne ne doit les posséder, sauf besoin spécifique.



5.6.2. Supprimer les sous-systèmes POSIX et OS/2

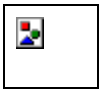
Les sous-systèmes OS/2 et POSIX pourraient permettre de contourner certaines sécurités du système.

Modifier la base de registre :

Ruche HKEY_LOCAL_MACHINE\SYSTEM

Clé System\CurrentControlSet\Control\Session Manager\SubSystems
Nom Debug, Os2, Posix
Type REG_MULTI_SZ
Valeur Supprimer les trois clés

Dans le répertoire %SYSTEMROOT%\System32, supprimer les fichiers : OS2SS.EXE, OS2SRV.EXE, OS2.EXE, PSXSS.EXE, POSIX.EXE, PSXDLL.EXE



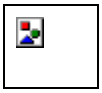
Certains utilitaires peuvent utiliser ces sous-systèmes (notamment des utilitaires de type Unix fournis avec le NT Ressource Kit). Pour pouvoir continuer à utiliser ces utilitaires, ne pas supprimer ces sous-systèmes.

5.6.3. Désactiver le sous-système WOW

Le sous-systèmes WOW permet l'exécution de programmes DOS et Windows 16 bits. Il est possible de le désactiver lorsqu'aucune application 16 bits n'est utilisée.

Modifier la base de registre :

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Control\Wow
Action Supprimer la clé



Dans le répertoire %SYSTEMROOT%\System32, supprimer les fichiers : NTVDM.EXE, KRNL386.EXE

Aucune application 16 bits ne pourra fonctionner sur le système.

5.6.4. Régler le seuil d'alerte de l'occupation du disque dur

Il est possible de préciser un seuil d'alerte d'occupation du disque dur. Par défaut, la valeur est réglée sur 10. Ainsi, s'il reste moins de 10% d'espace disque, une alarme (Event ID 2013) est générée dans le journal.

Régler l'entrée suivante dans la base de registre :

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Services\LanmanServer\Parameters
Nom DiskSpaceThreshold
Type REG_DWORD
Valeur 10 (valeur par défaut)
0 à 99

5.6.5. Effacer le fichier de mémoire virtuelle

Certaines données transitent sur le disque dans le fichier de mémoire virtuelle de la machine (pagefile.sys). Si des données sensibles sont manipulées sur la station, on recommande l'effacement automatique de ce fichier à l'arrêt du système afin de garantir la confidentialité des informations.

Cet effacement n'est réalisé QU'AU MOMENT D'UN ARRÊT (PROPRE) DE LA MACHINE.

Modifier l'entrée suivante dans la base de registre.

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Control\Session Manager\Memory
Nom ClearPageFileAtShutdown
Type REG_DWORD
Valeur 1

5.6.6. Gérer les plantages

Plusieurs clés de la base de registre permettent de préciser le comportement de Windows NT en cas de plantage. Les plantages doivent être pris en compte, qu'ils soient provoqués par une attaque de type Deni de service ou qu'ils soient la conséquence d'un "bug".

La plupart des modifications suivnates peuvent aussi être réalisées à partir du Panneau de Configuration Système.

Activer le démarrage automatique après plantage.

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Control\CrashControl
Nom AutoReboot
Type REG_DWORD
Valeur 1

Préciser si un fichier de débugage doit être créé.

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Control\CrashControl
Nom CrashDumpEnabled
Type REG_DWORD
Valeur 1

Préciser le chemin où créer le fichier.

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Control\CrashControl
Nom DumpFile
Type REG_EXPAND_SZ
Valeur %SystemRoot%\Memory.dmp

Générer un évènement dans le journal système

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Control\CrashControl
Nom LogEvent
Type REG_DWORD
Valeur 1

Ne pas écraser un fichier de débogage existant et créer un nouveau fichier.

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Control\CrashControl
Nom Overwrite
Type REG_DWORD
Valeur 1

5.6.7. Protéger l'accès à la clé Aedebug

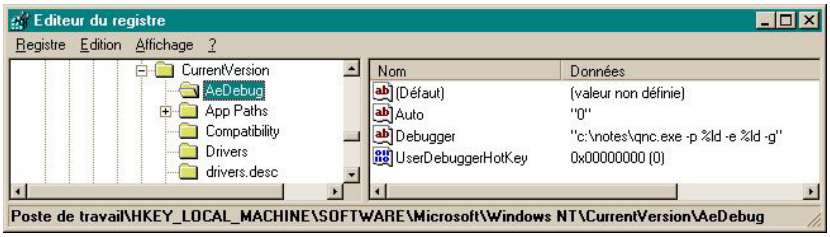
La clef Aedebug contient une chaîne de caractères qui, normalement, correspond à un programme et ses paramètres. Par défaut, ce programme est Dr Watson. Il s'agit en fait du programme à lancer en cas de plantage d'un applicatif. Ce programme est lancé avec les privilèges SYSTEM ce qui signifie que le processus lancé a le contrôle total sur la machine.

Il esp possible de modifier le contenu de cette clef (sur une installation de base elle n'est pas protégée par défaut), afin de lancer un applicatif parasite (le gestionnaire des utilisateurs par exemple) ; cet applicatif, lancé dans l'environnement de l'utilisateur qui a fait planter un programme, aura donc les privilèges SYSTEM (on peut ainsi ajouter un utilisateur dans le groupe des Administrateurs).

Le correctif à apporter ici est de positionner les permissions à Lecture pour "Tout le Monde" sur cette clef.

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé Software\Microsoft\WindowsNT\CurrentVersion\Aedebug\Debugger
Action Positionner les permissions en Lecture Seule pour "Tout le Monde"

Certains applicatifs risquent de refuser de fonctionner normalement par la suite (Lotus Notes par exemple peut, dans certaines configurations, poser problème).



5.6.8. Limiter l'accès à la base des objets NT

Cette clé permet de positionner des ACLs avec des droits corrects sur certains objets de NT.

Elle permet, en particulier, de parer la faille connue sous le nom de "KnownDll" qui permet d'obtenir des droits systèmes.

Modifier l'entrée suivante dans la base de registre.

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Control\Session Manager
Nom ProtectionMode
Type REG_DWORD
Valeur 1

5.6.9. Limiter l'utilisation du service Planning

Le service Planning permet de lancer des jobs programmés sur une machine avec la commande AT. Ces jobs se lancent avec des privilèges système et la clé gérant ce service n'est par défaut pas protégée (ce qui permet à un utilisateur de lancer un cheval de Troie).

Vérifier que la clef ci contre n'est accessible en écriture que par les administrateurs.

Ruche HKEY_LOCAL_MACHINE
Clé System\CurrentControlSet\Services\Schedule

Par défaut, seuls les administrateurs ont le droit d'utiliser la commande AT. Toutefois, il est possible de donner ce droit aux opérateurs de serveurs à l'aide de la clé ci-contre.

Vérifier la valeur de cette clé.

Ruche HKEY_LOCAL_MACHINE
Clé System\CurrentControlSet\Control\LSA
Nom SubmitControl

Type REG_DWORD
Valeur 1 (les opérateurs de serveurs peuvent programmer des jobs)
0 (seuls les administrateurs peuvent programmer des jobs)

5.6.10. Gérer les extensions associées à certains programmes

Certaines applications autorisent l'association d'extensions de fichiers (par exemple.doc pour Word). Certaines parmi celles-ci sont dangereuses, telle l'extension .reg associée à l'éditeur de registre.

En modifiant la base des registres, on peut empêcher l'exécution de regedit.exe lors de la manipulation des fichiers .reg.

Ruche HKEY_LOCAL_MACHINE
Clé Software\Classes\regfile\shell\Open\command
Nom de la clé
Type REG_SZ
Valeur Remplacer la valeur regedit %1 par notepad %1

Ruche HKEY_LOCAL_MACHINE
Clé SOFTWARE\Classes\regedit\shell\Open\command
Nom de la clé
Type REG_SZ
Valeur Remplacer la valeur regedit %1 par notepad %1

Changer les permissions de ces deux clefs pour interdire l'écriture par les non-administrateurs. Voir Modifier les permissions sur les clés de la base des registres .

5.6.11. Désactiver la fonction AutoRun des CD-Rom

A l'insertion d'un CD-ROM dans son lecteur, il est possible d'activer automatiquement un programme présent sur celui-ci.

Pour désactiver cette fonction, il faut positionner la clef ci dessous.

Ruche HKEY_LOCAL_MACHINE
Clé System\CurrentControlSet\Services\Cdrom
Nom Autorun
Type REG_DWORD
Valeur 1 (pour activer)
0 (pour désactiver)

5.6.12. Forcer l'ouverture de session pour l'arrêt du système

Il est possible de contrôler qui peut forcer l'arrêt du système. Deux approches possibles : soit on accorde cette permission à tout le monde, soit on force les personnes à ouvrir une session pour arrêter le système.

Ruche HKEY_LOCAL_MACHINE
Clé Software\ Microsoft\WindowsNT\CurrentVersion\Winlogon
Nom ShutdownWithoutLogon
Type REG_SZ
Valeur 1 (pour autoriser l'arrêt par tout le monde)
0 (pour forcer l'ouverture de session)

Si l'arrêt "brutal" à partir de l'interrupteur est possible, il est préférable d'autoriser tout le monde à arrêter la machine sans ouvrir de session.

5.7. Protection des mots de passe

5.7.1. Mettre en place une stratégie de compte

Par défaut Windows NT ne met pas en oeuvre une politique de mot de passe très résistante. Il est donc nécessaire de commencer par appliquer une stratégie de compte. Cette stratégie permet de régler la durée de validité des mots de passe, leur longueur minimale, et les mécanismes de verrouillge de compte.

Exécuter le Gestionnaire des Utilisateurs puis sélectionner le menu Stratégies, Stratégie de compte. Régler les paramètres suivants :

Restrictions sur les mots de passe :

- Durée maximale d'un mot de passe : 40 jours pour des réseaux sensibles, 2 à 3 mois pour des réseaux moyennement sensibles, plus d'un an si le réseau bénéficie d'une sécurité réseau maximale (VLAN, reconnaissance d'adresse MAC, etc.)
- Durée minimale du mot de passe : autoriser les modifications immédiatement,
- Longueur minimale du mot de passe : au moins 7 caractères (avec sensibilisation des gens sur le choix d'un bon mot de passe, i.e. composé de lettres, chiffres et symboles de ponctuation),
- Unicité du mot de passe : se souvenir des 5 derniers mots de passe.

(Nota : Pour les comptes utilisateurs avec les privilèges d'Administrateur, le mot de passe devrait être d'au moins 10 caractères, l'idéal étant un mot de passe de 14 caractères)

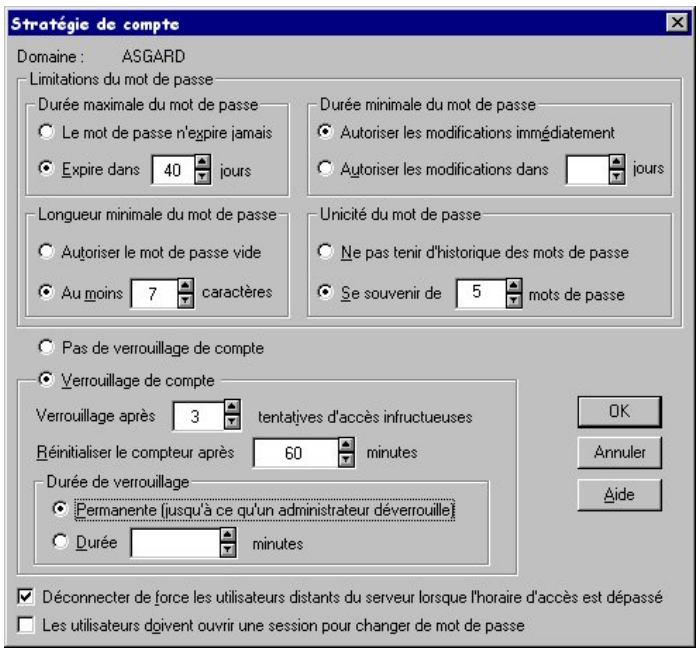
Verrouillage de compte :

- Verrouillage : après 3 ou 4 tentatives d'accès infructueuses[1],
- Réinitialisation : réinitialiser le compte après 60 mn,
- Durée de verrouillage : permanente (jusqu'à ce qu'un Administrateur la déverrouille).

Changement de mot de passe :

Les utilisateurs doivent ouvrir une session pour changer leur mot de passe : décocher la boite (en cas d'expiration du mot de passe, un utilisateur ne pourrait plus se connecter).

[1] Activer le verrouillage de compte apporte à la fois de la sécurité et de la non-sécurité. Sécurité parce qu'on se prémunit contre une attaque exhaustive sur les mots de passe des comptes, et non-sécurité parce qu'un attaquant peut alors verrouiller tous les comptes utilisateurs facilement. Le bon choix revient à l'administrateur du système en fonction de l'utilisation qui est faite du système d'information.



5.7.2. Obliger les utilisateurs à choisir des mots de passe complexes

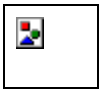
Passfilt

Le Service Pack 2 a apporté un outil capable d'améliorer la résistance des mots de passe. Passfilt est une DLL installée dans le répertoire `%SYSTEMROOT\system32`. Passfilt met en oeuvre une politique qui exige que les mots de passe comprennent au moins six caractères, ne contiennent pas le nom de login ou tout ou partie du nom de l'utilisateur et comprennent obligatoirement des caractères parmi au moins trois des catégories suivantes :

Lettres majuscules (A, B, C, ... Z)
Lettres minuscules (a, b, c, ... z)
Chiffres arabes (0,1, 2, ... 9)
Symboles (@, #, !, &, etc.)

Ajouter l'entrée suivante dans la base de registre et vérifier que le fichier PASSFILT.DLL et la clef ci contre sont en "lecture seule" pour les utilisateurs .

Ruche	HKEY_LOCAL_MACHINE\SYSTEM
Clé	System\CurrentControlSet\Control\LSA
Nom	Notification Packages
Type	REG_MULTI_SZ
Valeur	Ajouter Passfilt dans la liste



Passfilt présente deux limitations. La première est que la longueur minimale du mot de passe est codée en dur. La seconde tient au fait que Passfilt ne répond qu'aux requêtes de changement de mot de passe des utilisateurs. Un administrateur peut toujours définir des mots de passe triviaux à partir du Gestionnaire des Utilisateurs.

Passprob

Le logiciel Passprob est un outil fourni dans le kit de ressources NT qui permet d'activer une politique telle que les mots de passe doivent présenter une combinaison de majuscules et de minuscules ou contenir des chiffres ou des symboles.

```
PASSPROB /COMPLEX
```

Passprob complète la stratégie de compte, en particulier en ce qui concerne la longueur minimale des mots de passe. Il est en ce point plus intéressant que Passfilt.

5.7.3. Alerter l'utilisateur du prochain changement de mot de passe

La clef ci-contre permet de contrôler le nombre de jours avant l'expiration du mot de passe d'un utilisateur durant lesquels une boite d'avertissement est affichée. Si la clef n'existe pas, la valeur utilisée par défaut est 14.

Vous pouvez modifier ce nombre de jours "n" :

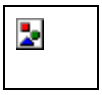
Ruche	HKEY_LOCAL_MACHINE\SYSTEM
Clé	Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
Nom	PasswordExpiryWarning
Type	REG_DWORD
Valeur	n (par défaut, n= 14)

5.7.4. Désactiver l'authentification Lan Manager

Pour ces raisons de compabilité, Windows NT accepte les authentifications Lan Manager, seules connues des systèmes Microsoft précédent. Malheureusement le mécanisme de hachage de Lan Manager est moins efficace que le mécanisme natif de Windows NT (NTML). Il est possible d'interdire l'utilisation du mécanisme d'authentification Lan Manager à partir du Service Pack 3 et uniquement si le hot-fix LM (pour le SP3) a été appliqué.

Modifier la base de registre des contrôleurs de domaine :

Ruche	HKEY_LOCAL_MACHINE\SYSTEM
Clé	System\CurrentControlSet\Control\LSA
Nom	LMCompatibilityLevel
Type	REG_DWORD
Valeur	0 (NT et LANMAN) 1 (NTLMv2 si demandé) 2 (Authentification NTLM uniquement) 3 (NTLMv2 uniquement) 4 (le contrôleur de domaine refuse l'authentification LANMAN) 5 (le contrôleur de domaine refuse l'authentification LANMAN et NTLM)



Avec les niveau 4 et 5, les clients Windows for Workgroups, Windows 9x et MS-DOS ne pourront plus se connecter sur le contrôleur de domaine. Cette modification n'est donc valable que sur les entreprises ne possédant que des systèmes Windows NT. Les disquettes d'installation des clients réseaux ne pourront plus se connecter sur le contrôleur (elles utilisent un système MS-DOS).

5.7.5. Interdire le transit de mot de passe en clair

Suite à une requête explicite d'un serveur, un mot de passe peut transiter en clair sur le réseau. On peut interdire cette fonction en supprimant la clef suivante de la base des registres.

Ruche	HKEY_LOCAL_MACHINE\SYSTEM
Clé	System\CurrentControlSet\Services\RdrParameters
Nom	EnablePlainTextPassword
Type	REG_DWORD
Valeur	0

5.7.6. Sécuriser l'accès au fichier SAM._

Le fichier SAM._ se situe dans le répertoire %SYSTEMROOT%\REPAIR et contient une copie de sauvegarde de la liste des utilisateurs et des mots de passe. Par défaut, tout le monde a le droit de lire ce fichier.

Modifier les permissions du fichier en retirant le groupe "Tout le monde". Le Service Pack 3 et ultérieur effectue cette correction de façon automatique.

5.7.7. Chiffrement de la SAM avec Syskey

Le fichier SAM contient les hashs NT et Lan Manager des mots de passe. De nombreux outils permettent maintenant de "cracker" ces mots de passe, tel Lophtcrack, John the Ripper...

Pour renforcer la protection du fichier SAM, il est possible de le sur-chiffrer à l'aide de l'outil Syskey disponible à partir du Service Pack 3. Ceci empêche la récupération des cryptogrammes des mots de passe NT depuis un fichier SAM récupéré par ailleurs (import de fichier SAM sous L0phtcrack par exemple)

Syskey propose trois méthodes pour obtenir la clé utilisée pour le chiffrement :

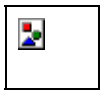
- par mot de passe saisi au démarrage du système
- par une clé stockée sur une disquette. La disquette doit être insérée au démarrage du système.
- par une clé stockée sur le disque de démarrage.

5.7.8. Limiter le cache d'authentification des stations

En cas de panne réseau, l'utilisateur ne peut plus se connecter car l'authentification s'effectue à distance sur les serveurs du domaine. Cependant, Windows NT conserve un cache d'authentification des 10 dernières connexions.

Pour permettre à l'utilisateur de continuer à travailler en local, il faut autoriser le cache d'authentification tout en limitant au maximum la possibilité pour quelqu'un d'utiliser les informations de ce cache. On ne mémorisera que le dernier utilisateur du poste afin de minimiser les informations sensibles présentes dans le cache.

Ruche	HKEY_LOCAL_MACHINE
Clé	Software\ Microsoft\ Windows NT\ Current Version\ Winlogon
Nom	CachedLogonsCount
Type	REG_SZ
Valeur	1



Cependant, suite à cette sécurisation il sera impossible, sauf pour le DERNIER utilisateur, de s'authentifier hors réseau.

La seconde clef ci-dessous permet, si elle est positionnée à 1, d'effacer automatiquement à la déconnexion d'un utilisateur son profil stocké localement sous `%systemroot%\Profiles`.

Ruche	HKEY_LOCAL_MACHINE
Clé	Software\ Microsoft\ WindowsNT\ CurrentVersion\ Winlogon
Nom	DeleteRoamingCache
Type	REG_DWORD
Valeur	0 (Situation normale) 1 (Effacement du cache des profils)

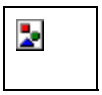
5.7.9. Contrôler les Notification Packages

Certaines DLL peuvent être installées pour gérer les mots de passe, par exemple pour les contrôler par rapport à une liste de mots de passe interdit, ou pour les synchroniser avec d'autres systèmes (Netware, ...).

Ces DLL sont appelées des "Notification Package" et leur liste apparaît dans une clé de la base de registres. Par défaut, cette clé est vide.

Les DLL spécifiées dans cette clé peuvent capturer les mots de passe dans leur version non chiffrée (Password Grabbing).

Ruche	HKEY_LOCAL_MACHINE
Clé	System\CurrentControlSet\ Control\ Lsa
Nom	Notification Packages
Type	REG_MULTI_SZ
Valeur	"Vide"



Dans le cas de l'utilisation des services Netware, la clef peut contenir une entrée pour FPNWCLNT.

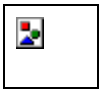
5.8. Configuration de l'Audit

5.8.1. Mettre en place une stratégie d'audit

Définir la stratégie d'audit ci-dessous. Cette stratégie représente un compromis entre la pertinence de l'audit et la quantité de données à stocker. Pour des besoins spécifiques et / ou des machines particulièrement exposées, on peut ajouter des événements à auditer.

Il s'agit ici de donner un ensemble minimal de paramètres à auditer. L'administrateur peut décider d'étendre l'audit à d'autres paramètres en fonction de ses besoins.

Il est par exemple possible d'auditer l'accès à certains fichiers, certaines clefs ou encore l'activité de la base des objets NT. Néanmoins, il faut limiter le nombre de ces éléments sous peine de rapidement saturer les journaux d'audit.

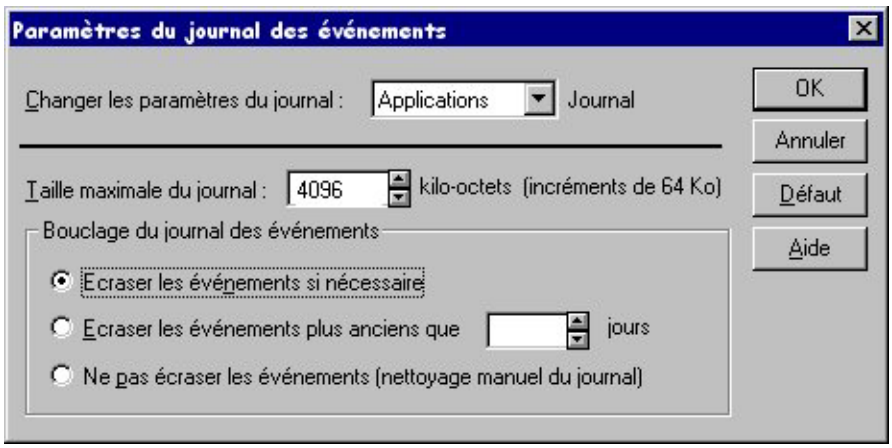


L'audit de l'ensemble des actions élémentaires d'accès aux objets du noyau NT ou aux fichiers lors des opérations de backup n'est pas recommandé car cela génère beaucoup d'événements et risque de saturer inutilement les journaux d'audit.

5.8.2. Régler les paramètres des journaux

Les journaux d'audit peuvent très rapidement se remplir. Un réglage permet de définir la politique d'effacement des anciens évènements. L'effacement automatique des anciens messages peut être utilisé pour masquer une activité.

Le réglage des paramètres pour les journaux d'audits s'effectue dans le Gestionnaire d'Evénements (menu « Journaux / Paramètres du journal »). Il **faut régler successivement les trois journaux** (système, sécurité et applications). Définir, **pour chaque journal**, les réglages visibles dans le schéma suivant.



Choisir « Ecraser les événements si nécessaire » sans quoi, après saturation du journal, plus aucun événement ne sera audité !

Cependant, si l'on choisi l'option "Ne pas écraser….", il est nécessaire d'archiver et de nettoyer régulièrement le journal d'évènements afin de ne pas interrompre l'enregistrement des messages.

5.8.3. Limiter l'accès aux journaux d'audit

Les invités et les sessions "nulles" ont la possibilité de visualiser les journaux d'évènements.

Pour leur interdire l'accès, ajouter les trois entrées suivantes dans la base des registres (une par journal).

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Services\EventLog\Security
Nom RestrictGuestAccess
Type REG_DWORD
Valeur 1

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Services\EventLog\System
Nom RestrictGuestAccess
Type REG_DWORD
Valeur 1

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Services\EventLog\Application
Nom RestrictGuestAccess
Type REG_DWORD
Valeur 1

5.8.4. Limiter le droit de gérer le journal d'audit et de sécurité

Un utilisateur disposant du droit "Gérer le journal d'audit et de sécurité", sans être membre du groupe Administrateurs, peut effacer le journal sécurité sans que l'évènement 517 (le Journal sécurité a été effacé) ne soit enregistré. Ce problème survient sur Windows NT 4.0 SP3.

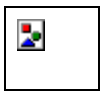
Il est préférable de ne pas accorder le privilège "Gérer le journal d'audit et de sécurité" à des utilisateurs autres que les administrateurs.

5.8.5. Activer l'audit des objets système

Ajouter l'entrée suivante dans la base de registre.

Ruche	HKEY_LOCAL_MACHINE\SYSTEM
Clé	System\CurrentControlSet\Control\Lsa
Nom	AuditBaseObjects
Type	REG_DWORD
Valeur	1

Cette clé de suffit pas à générer des audits sur les objets systèmes. Il faut aussi activer l'audit système dans la Stratégie d'Audit du Gestionnaire des Utilisateurs.



En raison du grand nombre d'évènements généré par un tel paramètrage, cette option N'EST PAS RECOMMANDEE.

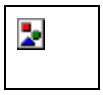
5.8.6. Arrêter le système quand le journal d'audit est saturé

La certification C2 impose l'arrêt d'un système lorsque le journal d'audit est saturé, ceci afin d'éviter que des activités illicites ne puissent être enregistrées. Le système pourra être redémarré mais seul l'administrateur pourra y avoir accès afin de vider le journal et repositionner la valeur de la clé associé. Lors de l'arrêt du système, elle est positionnée à 2.

Ajouter l'entrée suivante dans la base de registre.

Ruche	HKEY_LOCAL_MACHINE\SYSTEM
Clé	System\CurrentControlSet\Control\Lsa
Nom	CrashOnAuditFail
Type	REG_DWORD
Valeur	1

Cette précaution peut nuire à la disponibilité du système si des évènements sont générés de façon à saturer le journal.



Cette option N'EST PAS RECOMMANDEE, l'arrêt du système se traduisant dans ce cas présent par un CRASH du système (Ecran Bleu) !!!

5.8.7. Afficher une bannière d'ouverture de session

Il est possible d'afficher une bannière pour signaler explicitement que l'accès à la machine n'est autorisé qu'aux personnes habilitées. Le texte se compose d'un titre et d'un corps. Ces mentions sont plutôt du domaine juridique et ne modifient pas le niveau de sécurité technique de la machine.

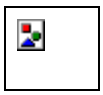
Pour le titre de la bannière, ajouter l'entrée suivante dans la base de registre.

Ruche	HKEY_LOCAL_MACHINE\SOFTWARE
Clé	Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
Nom	LegalNoticeCaption
Type	REG_SZ
Valeur	Titre à afficher

Pour le texte de la bannière, ajouter l'entrée suivante dans la base de registre.

Ruche	HKEY_LOCAL_MACHINE\SOFTWARE
Clé	Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
Nom	LegalNoticeText
Type	REG_SZ
Valeur	Texte à afficher

5.8.8. Auditer l'utilisation des privilèges de sauvegarde et de restauration



Lorsque les fichiers sont sauvegardés ou restaurés, le système vérifie pour chaque fichier si l'utilisateur qui réalise l'opération dispose des privilèges associés. En théorie, Windows NT devrait générer un événement dans le journal dans le cas où l'audit des succés d'utilisation des privilèges est activé. Ceci pourrait saturer rapidement le journal. En réalité, ces privilèges ne sont pas audités. Il est possible d'activer toutefois également cet audit, en sachant qu'**un tel paramétrage, s'il est suivi d"effet, peut rapidement saturer le journal (donc :option NON RECOMMANDEE**)

Modifier l'entrée suivante dans la base de registre.

Ruche	HKEY_LOCAL_MACHINE\SYSTEM
Clé	System\CurrentControlSet\Control\Lsa
Nom	FullPrivilegeAuditing
Type	REG_DWORD
Valeur	1

5.8.9. Enregistrer les erreurs de l'analyseur de performances

Lorsque l'analyseur de performances ne peut enregistrer une valeur ou que cette valeur est incorrecte, il peut générer un évènement dans le journal d'application.

Modifier l'entrée suivante dans la base de registre.

Ruche	HKEY_LOCAL_MACHINE\SOFTWARE
Clé	Software\Microsoft\PerfMon
Nom	ReportEventsToEventLog
Type	REG_DWORD
Valeur	1

5.9. Protection des Comptes

5.9.1. Désactiver le compte Invité

Le compte Invité permet à des utilisateurs d'accèder à un système Windows NT sans avoir besoin d'un compte utilisateur particulier. Ce compte a accès à toutes les ressources sur lesquelles le groupe Tout le monde a des permissions. Ce groupe peut disposer de permissions risquées sur le répertoire `%SYSTEMROOT%`.

Le compte Invité est désactivé par défaut sur les contrôleurs de domaine Windows NT Server et activé sur les Windows NT Workstation et sur les serveurs membres du domaine. Dans ce cas, le compte Invité peut être utilisé pour ouvrir une session localement. Sur les contrôleurs de domaine, le compte Invité ne permet l'accès qu'à travers le réseau.

Dans le gestionnaire des utilisateurs, désactiver le compte Invité sur chaque station et serveur.

5.9.2. Gérer les comptes utilisateurs

Au sujet des comptes utilisateurs:

- Ne créez que des comptes de domaine si vous êtes dans une structure en Domaine
- Ne créez pas de comptes fonctionnels. Les comptes doivent être nominatifs.

Propriétés des utilisateurs

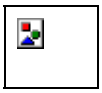
Utilisateur	8 caractères ou en fonction des besoins locaux
Nom détaillé	Libre
Description	Libre
Mot de passe	cf. Stratégie de comptes
L'utilisateur doit changer de mot de passe à la prochaine connexion	Cocher la boite à la création du compte
L'utilisateur ne peut pas changer de mot de passe	Ne pas cocher la boite
Le mot de passe n'expire jamais	Ne pas cocher la boite (sauf pour l'Administrateur local)
Compte désactivé	Ne pas cocher la boite (le compte « Invité » doit être désactivé car il ne peut pas être supprimé)
Bouton **Groupes**	PAS de comptes utilisateurs dans le groupe « Invité » et « Utilisateurs avec pouvoir «. Enlever « Invité » du groupe « Utilisateur du domaine »
Bouton **Profils**	Libre d'utilisation par l'Administrateur
Bouton **Horaires**	Activer si possible les horaires d'accès. Forcer la déconnexion des utilisateurs du serveur

5.9.3. Renommer le compte Administrateur

Le compte Administrateur de Windows NT est particulièrement connu et il n'est pas verrouillable. Il est conseillé de le renommer de façon à le rendre plus discret. Il faut éviter bien sur les noms tels que "root", "supervisor", ou pire "Administrator". Le mieux est de lui attribuer un nom d'utilisateur fictif conforme à la politique de nommage de l'entreprise.

Renommer le compte Administrateur à l'aide du Gestionnaire des Utilisateurs du domaine.

Il ne sert à rien de renommer le compte s'il est utilisé couramment devant les utilisateurs. Pour l'administration courante, vous pouvez créer un compte d'administration (membre du groupe Administrateurs du Domaine), qui aura par contre la particularité d'être verrouillable. Il sera toujours temps d'utiliser le compte d'origine pour déverrouiller le compte courant.



Renommer le compte Administrateur ne permet en aucun cas de le cacher. Il est possible de le récupérer en listant la base des comptes, en récupérant les SID, en surveillant la table NetBIOS des stations, ou tout simplement en recherchant les profils stockés sur les disques durs.

Astuce

Lorsque l'administrateur est connecté sur une station, il est possible de récupérer le nom de son compte par la commande :

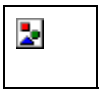
```
nbtstat -A adresse IP
```

Il peut être intéressant de créer un compte nommé Administrateur qui sera un simple utilisateur. Ce compte peut être désactivé. Il sera la cible privilégié. L'audit des échecs d'ouverture de session permettra de détecter rapidement l'attaque.

5.9.4. Choisir un mot de passe pour l'administrateur

Chaque station Windows NT dispose d'un compte Administrateur, créé à l'installation et utilisé pour la première ouverture de session. Ce compte ne peut pas être supprimé. Il n'est pas verrouillable à la suite de multiples tentatives. Aussi est-il conseillé d'utiliser un mot de passe complexe.

- Choisir un mot de passe de 14 caractères, mêlant plusieurs caractères différents, minuscules et majuscules.
- Ecrire ce mot de passe et le stocker dans un lieu physiquement protégé (coffre).
- Affecter ce mot de passe à chacun des comptes Administrateurs Locaux des stations
- Changer ce mot de passe chaque fois qu'un administrateur quitte l'équipe et en cas de divulgation



Les mots de passe des comptes locaux sont stockés sur le disque dur de la machine. Il est possible de récupérer ces fichiers et de procéder à une attaque de type "brute-forcing". Même si un mot de passe bien choisi devrait résister à ce genre d'attaque, il est préférable de ne pas utiliser le même mot de passe pour l'Administrateur local des stations et l'Administrateur des machines sensibles, tels les contrôleurs et serveurs autonomes.

5.9.5. Rendre le compte Administrateur verrouillable

Le compte Administrateur d'origine n'est pas verrouillable. Il peut donc être la cible des pirates sans aucune limitation. Ce choix a été déterminé pour éviter la perte d'accès total au serveur. Si quelqu'un parvenait à verrouiller ce compte, le serveur deviendrait inaccessible pour l'administrateur, réalisant une attaque par Deni de Service.

Passprob

Le logiciel Passprob est un outil fourni dans le kit de ressources NT qui permet de rendre le compte Administrateur verrouillable à travers une tentative de connexion par le réseau. Il reste utilisable à partir de la console du serveur et peut être ainsi déverrouillé.

```
PASSPROB /adminlockout
```

5.9.6. Limiter les membres du groupes Administrateurs

Le groupe Administrateurs de chaque station d'un domaine contient le groupe global Administrateurs du domaine, ce qui permet aux comptes administrateurs du domaine, déclarés sur les contrôleurs de domaine, d'administrer également les stations.

Il ne faut jamais inclure les comptes nominatifs des administrateurs dans le groupe Administrateurs. Dans ce cas, ils disposeraient en permanence des privilèges d'administration. Les administrateurs doivent disposer de deux comptes : un pour l'administration et un autre en qualité de simple utilisateur.

Astuce

Il peut être utile de déléguer l'administration des stations à une petite équipe, sans pour autant leur donner un compte membres des Administrateurs du domaine.. Pour cela :

- Créez un groupe global Administrateurs des Stations.
- Créez des comptes utilisateurs pour le personnel de l'équipe
- Ajoutez le groupe Administrateurs des Stations au groupe local Administrateurs de chaque station.

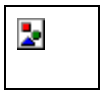
5.9.7. Cacher le nom du dernier utilisateur connecté

Lors de l'ouverture de session, le nom du dernier utilisateur connecté reste affiché. Il peut être source d'information pour un éventuel intrus.

Ajouter l'entrée suivante dans la base de registre.

Ruche	HKEY_LOCAL_MACHINE\SOFTWARE
Clé	Microsoft\Windows NT\Current Version\Winlogon
Nom	DontDisplayLastUserName

Type REG_SZ
Valeur 1



Cette protection peut aussi s'avérer être une contrainte pour les utilisateurs qui doivent saisir leur nom de login à chaque connexion.

5.9.8. Interdir l'ouverture de session automatique

Il est possible d'ouvrir une session automatiquement sur la machine en entrant des clefs supplémentaires dans la base des registres.

Il faut vérifier que les clefs suivantes n'existent pas et les détruire le cas échéant.

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
Nom AutoAdminLogon
Type REG_SZ
Valeur 1

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
Nom DefaultPassword
Type REG_SZ
Valeur Le mot de passe en clair !

5.10. Protection de la base de registre

5.10.1. Contrôler les accès distants à la base de registre

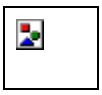
La base de registre d'un système Windows NT est consultable à distance à l'aide de l'éditeur de registre. Il est possible de limiter l'accès aux seuls administrateurs.

Les permissions de la clé winreg déterminent qui a accès à distance à la base de registre. Si la clé n'existe pas, il faut la créer.

Ruche	HKEY_LOCAL_MACHINE\SYSTEM
Clé	System\CurrentControlSet\ Control\ SecurePipeServers
Nom	winreg
Permissions	Ne laisser que Administrateurs Contrôle Total

Des machines ou des utilisateurs peuvent ne pas être affectés par cette restriction. La liste des clés autorisés se trouve dans la clé **AllowedPaths**.

Ruche	HKEY_LOCAL_MACHINE\SYSTEM
Clé	System\CurrentControlSet\ Control\ SecurePipeServers\winreg\AllowedPaths
Nom	Machine
Type	REG_MULTI_SZ
Valeur	<vide>
Nom	Users
Type	REG_MULTI_SZ
Valeur	<vide>



Certains services tels que le spooler ou le réplicateur doivent accéder à distance à certaines parties de la base des registres. **Il n'est pas recommandé de vider les clefs ci contre si l'on n'est pas sûr de ce que l'on fait**.

5.10.2. Modifier les permissions sur les clés de la base de registre

La base des registres représente un endroit particulièrement sensible car toutes les données de configuration y sont regroupées. Il convient de modifier les permissions associées à certaines clefs afin de limiter l'accès de "Tout le monde" à "Lecture seule". S'assurer de sélectionner la boite "Remplacer les permissions pour les sous-clefs".

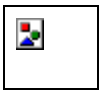
Ruche HKEY_LOCAL_MACHINE

Clé	Software\Classes (et sous-clefs)
Clé	Software\Microsoft\RPC
Clé	Software\Microsoft\Windows NT\CurrentVersion
Clé	Software\Windows 3.1MigrationStatus (et sous-clefs)
Clé	System\CurrentControlSet\Services\LanmanServer\Shares
Clé	System\CurrentControlSet\Services\UPS
Permissions	Vérifier que le groupe Tout le Monde n'a que Lecture Seule

Ruche HKEY_CLASSES_ROOT

Clé	Toutes les sous-clés
Permissions	Vérifier que le groupe Tout le Monde n'a que Lecture Seule

Ruche HKEY_USERS
Clé Default
Permissions Vérifier que le groupe Tout le Monde n'a que Lecture Seule



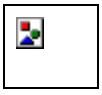
Ces clés sont des clés critiques car on peut y introduire des pointeurs vers des chevaux de Troie. Cependant, certaines applications nécessitent que ces clés soient déprotégées (comme Lotus Notes pour la clef CurrentVersion\Aedebug). Avant toute sécurisation d'une machine opérationnelle, tester cette sécurisation sur une machine de test afin de la valider.

5.10.3. Désactiver les outils d'édition de la base de registre

Il est possible de désactiver l'utilisation des outils d'édition de la base de registres (REGEDIT et REGEDT32). Ils seront exécutés mais afficheront un message d'avertissement avant de se fermer. Cette modification peut aussi être intégrée dans une stratégie de sécurité. Attention : la désactivation des outils n'empêchent pas la modification de la base de registre par l'intermédiaire d'autres outils !

Il est également possible de modifier les ACL sur les deux fichiers EXE en conséquence.

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé Software\ Microsoft\ Windows\ CurrentVersion\ Policies\ System
Nom DisableRegistryTools
Type REG_DWORD
Valeur 1



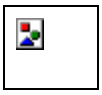
Il ne faut pas que cette modification affecte l'administrateur. Il est donc préférable de la réaliser à l'aide d'une stratégie système.

5.11. Protection des périphériques

5.11.1. Empêcher l'ajout d'imprimante

Pour que seuls les administrateurs puissent rajouter une imprimante locale, il faut positionner la clef ci-dessous. Cela empêche quelqu'un de développer un faux driver permettant de récupérer les impressions d'autres personnes.

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers
Nom AddPrintDrivers
Type REG_DWORD
Valeur 1



En modifiant cette clef, on interdit aux utilisateurs d'installer eux-mêmes une imprimante locale.

5.11.2. Contrôler l'accès aux périphériques amovibles

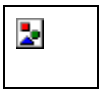
Les lecteurs de disquettes et de CD-ROM sont interdits pour une certification C2. Ne les utiliser que si le service en exprime le besoin.

Lecteurs de disquettes et CD-ROM : pour que seul l'utilisateur ayant ouvert une session localement puisse y accéder, il faut les allouer à l'ouverture de session et les libérer à la fermeture de session en modifiant les deux clefs suivantes.

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Nom AllocateFloppies
Type REG_SZ
Valeur 1 (0 par défaut)

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Nom AllocateCDRoms
Type REG_SZ
Valeur 1 (0 par défaut)

Une valeur similaire n'existe pas pour les lecteurs de bandes.



Si on applique ces modifications, il ne sera plus possible de partager un CD-ROM ou une disquette.

5.12. Protection des services réseau

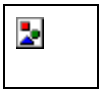
5.12.1. Limiter la connexion anonyme

La plupart des techniques de recueil d'information sur un système Windows NT sont basées sur une faille appelée la session nulle, connexion anonyme, ou encore "Red Button". Cette connexion permet de récupérer un certain nombre d'informations, tels que les partages existants, la liste des utilisateurs...

A partir du Service Pack 3, il est possible de limiter la plupart des fuites d'informations par le biais de cette session nulle.

Ajouter l'entrée suivante dans la base de registre.

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Control\LSA
Nom RestrictAnonymous
Type REG_DWORD
Valeur 1

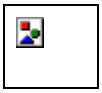


Cette clé ne bloque pas totalement la session nulle. Certaines commandes, tel sid2user, continuent de fonctionner malgré tout.

Une autre clé permet de limiter les accès en session "nulle". Elle est active par défaut, même si elle n'apparaît pas dans la base de registre.

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Services\LanmanServer\Parameters
Nom RestrictNullSessAccess
Type REG_DWORD
Valeur 1 (restriction)
0 (pas de restriction)

La clé RestrictNullSessAccess est associée aux clés NullSessionPipes et NullSessionShares qui précisent comment s'appliquent les permissions.



Lorsque cette clé est positionnée à 0, les sessions "nulles" ont accès à tous les partages avec les permissions associées au groupe "Tout le Monde".

5.12.2. Activer la signature SMB

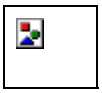
La signature SMB exige que chaque paquet échangé entre clients et serveurs Windows NT soit signé. Cette protection permet d'éviter les attaques de type "Man-in-the-Middle" et "Active message attack". Elle peut être activée sur les systèmes mis à niveau avec le Service Pack 3 ou ultérieur. Cette fonctionnalité a été en fait apporté par la nouvelle version de SMB, appelée CIFS (Common Internet File System).

Modifier la base de registre des serveurs :

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Services\LanManServer\Parameters
Nom EnableSecuritySignature
Type REG_DWORD
Valeur 1 (Activé)

Modifier la base de registre des clients NT Workstation :

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Services\Rdr\Parameters
Nom EnableSecuritySignature
Type REG_DWORD
Valeur 1 (Activé)



Cette sécurisation n'apporte pas grand chose si le réseau utilisé n'est pas interconnecté avec d'autres sites. De plus il génère un trafic plus important et un léger ralentissement des accès aux partages. En outre, la charge CPU est nettement plus importante.

Pour communiquer avec des machines autres que WindowsNT Service Pack 3 et au delà, la signature ne doit pas être utilisée : il faut alors configurer les machines NT pour autoriser la signature SMB chaque fois que possible, mais ne pas l'imposer.

Modifier la base de registre des serveurs :

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Services\LanManServer\Parameters
Nom RequireSecuritySignature
Type REG_DWORD
Valeur 1 (Activé)

Modifier la base de registre des clients NT Workstation :

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Services\Rdr\Parameters
Nom RequireSecuritySignature
Type REG_DWORD
Valeur 1 (Activé)

5.12.3. Désactiver les partages administratifs

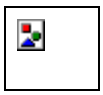
Les partages administratifs sont mis en oeuvre automatiquement au démarrage du système. Ils ne sont accessibles que par les administrateurs. Ils concernent les disques durs (C$,...) et le répertoire système (ADMIN$). Il est préconisé de les désactiver. La suppression directe ne suffit pas, le partage étant remis en place à l'initialisation.

Pour Windows NT Server, ajouter l'entrée suivante dans la base de registre.

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Services\LanmanServer\Parameters
Nom AutoShareServer
Type REG_DWORD
Valeur 0 (partages administratifs désactivés)
1 (partages administratifs activés)

Pour Windows NT Workstation, ajouter l'entrée suivante dans la base de registre.

Ruche HKEY_LOCAL_MACHINE\SYSTEM
Clé System\CurrentControlSet\Services\LanmanServer\Parameters
Nom AutoShareWks
Type REG_DWORD
Valeur 0 (partages administratifs désactivés)
1 (partages administratifs activés)



Les partages administratifs sont parfois bien pratiques pour l'administration à distance des machines.

5.12.4. Masquer une station ou un serveur

Il est possible de cacher une station ou en serveur pour qu'il ne soit pas visible dans le voisinage réseau, tout en étant accessible à partir du nom (commande NET USE).

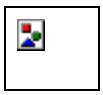
Ajouter l'entrée suivante dans la base de registre.

Ruche	HKEY_LOCAL_MACHINE\SYSTEM
Clé	System\CurrentControlSet\Services\LanmanServer\Parameters
Nom	Hidden
Type	REG_DWORD
Valeur	0 (visible) 1 (caché)

5.12.5. Interdire l'utilisation de DCOM

Le service DCOM permet d'autoriser à un utilisateur distant l'exécution d'un code DCOM sur la machine locale. DCOM n'implémente aucun mécanisme de sécurité digne de ce nom. Pour interdire ce service, changer la clef ci-contre.

Ruche	HKEY_LOCAL_MACHINE\SYSTEM
Clé	Software\Microsoft\Ole
Nom	EnableDCOM
Type	REG_SZ
Valeur	N (anciennement Y)



Il faut néanmoins être sûr qu'aucun service installé n'utilise ce mécanisme (sur une installation "par défaut" d'un système Windows NT, DCOM peut sans problème être désactivé).

5.13. Protection du système de fichiers

5.13.1. Généralités

Lors de l'installation d'un système Windows NT, des listes de contrôle d'accès sont positionnées par défaut sur le système de fichiers, à condition que le support physique soit formaté en NTFS.

Pour l'essentiel, ces ACLs sont positionnées de façon restrictive sur des répertoires et des fichiers « sensibles ». Ainsi, par exemple, les fichiers « programmes » du système (EXE, DLLs…) ne sont accessibles qu'en lecture / exécution (RX) pour les simples utilisateurs.

Cependant, ces ACLs, bien que généralement correctement positionnées par défaut, ne suffisent pas dans tous les cas à empêcher la mise en place de « cheval de Troyes » dans le système. On peut donc décider de vouloir sécuriser plus durement le système d'exploitation en ajoutant ou en modifiant les ACLs existantes.

Typiquement, une sécurisation accrue demanderait à ce que les fichiers contenant du code exécutable (EXE, DLL, VBX …) ne soient accessibles qu'en lecture / exécution (RX) pour les utilisateurs, et à ce que tous les répertoires et fichiers inutilisés soient détruits ou rendus inaccessibles.

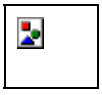
Notons qu'une telle modification peut parfois avoir des impacts imprévus sur le fonctionnement nominal du système.

Il faut ainsi toujours avoir à l'esprit :

1. que les développeurs se basent, pour le fonctionnement des applicatifs qu'ils développent, sur une installation « **normale** » (i.e. non sécurisée) d'un système Windows NT,

2. que lorsque l'on crée un sous-répertoire ou un fichier dans un répertoire, ceux-ci héritent des permissions du répertoire père,

3. et **surtout qu'un système d'information n'est jamais figé** ; des fonctions inutilisées à un instant *t* peuvent avoir une utilité dans l'avenir.



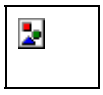
En bref, toute sécurisation additionnelle portant sur une modification des permissions NTFS doit être réalisée avec les plus grandes précautions, en sachant que lorsqu'il existe un doute sur la pertinence d'une modification il est toujours préférable de s'abstenir.

Exemples de problèmes liés à la modification des permissions NTFS standards :

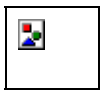
On peut ainsi décider d'interdire aux utilisateurs de créer des fichiers à la racine du système (lecteur C:) ou dans le répertoire d'installation des applicatifs (Répertoire « Program Files »). Cependant, certains applicatifs, installés préalablement ou ultérieurement, risquent de ne plus fonctionner.

C'est par exemple le cas pour Norton Antivirus Live Update, utilitaire permettant de mettre à jour son antivirus par téléchargement des bases de virus depuis un serveur. Cet applicatif crée, pendant la mise à jour des bases, un répertoire temporaire directement à la racine du système (C:) ; si C: est protégé contre un accès en écriture pour les utilisateurs, Live Update ne fonctionnera plus.

De même, si on a protégé le répertoire « Program Files » avec les permissions RX pour tout le monde, et qu'on installe Norton Antivirus par la suite, il ne sera pas possible de changer les bases de définitions de virus de Norton puisque celles-ci auront hérité des permissions du répertoire père donc de la permission RX (lecture seule !).



D'autres problèmes peuvent survenir si l'on souhaite protéger contre l'écriture des zones du système comme C:\Winnt ou C:\Winnt\System32. En effet, certains applicatifs nécessitent d'obtenir les permissions d'écriture sur ces répertoires pour pouvoir fonctionner correctement (c'est normal car la permission d'écriture est positionnée par défaut sur C:\Winnt). Protéger ces répertoires revient donc, dans certains cas, à introduire une dégradation de la qualité de service.



A ce sujet, Microsoft a par ailleurs sorti un document (Article ID Q169387) sur les permissions NTFS requises pour utiliser la suite Bureautique Office. Ces permissions sont les suivantes :

1. Les répertoires suivants doivent avoir les permissions en lecture / écriture pour les utilisateurs :

   C:\Temp
   C:\Winnt
   C:\Winnt\Forms
   C:\Winnt\System32
   C:\Program Files\Microsoft Office
   C:\Program Files\Microsoft Office\Office
   C:\Program Files\Microsoft Office\Xlstart
   C:\Program Files\Microsoft Office\Templates

2. Les fichiers suivants doivent avoir les permissions en lecture / écriture pour les utilisateurs :

   C:\Ffastun.ffa
   C:\Ffastun.ff1
   C:\Ffastun.ffo
   C:\Ffastun.ffx
   C:\Winnt\Artgalery.cag
   C:\Winnt\<LogonID>.acl[1]
   C:\Winnt\<LogonID>8.xlb
   C:\Winnt\<LogonID>.fav
   C:\Winnt\Mso97.acl
   C:\Winnt\Msoprefs.232
   C:\Winnt\Outlook.fav
   C:\Winnt\Outlook.prf
   C:\Winnt\Outlook.prt
   C:\Winnt\Forms\Frmcache.dat
   C:\Winnt\System32\Ffastlog.txt
   C:\Winnt\System32\Msforms.twd

Autre exemple : les applications Lotus (Lotus Notes par exemple), stockent dans C:\Winnt un fichier Lotus.ini ou Notes.ini contenant les préférences des utilisateurs. Si ce répertoire est protégé, Lotus Notes fonctionnera nettement moins bien !

5.13.1.1. Sécurisation par modification des permissions standards

Généralités

Les paragraphes qui suivent donnent des indications générales pour sécuriser un système par modification des permissions standard. Ces indications sont à re-boucler avec les informations contenues dans le chapitre § 5.13.1 - Généralités.

Le groupe "Tout le Monde", est le groupe par défaut des comptes Internet (IUSR_XXX) et Invité, il est également utilisé pour les ouvertures de session nulles. A la lecture des permissions par défaut

[1] <LogonID> est le nom de connexion de l'utilisateur connecté à la machine.

de Windows NT, il apparaît que ce groupe dispose parfois de privilèges excessifs sur une machine.

Ces permissions excessives peuvent être listées ainsi :

- Contrôle Total sur la racine de tous les disques NTFS
- Contrôle Total sur \WINNT
- Modifier sur \WINNT\SYSTEM32

Notons que la permission "Contrôle Total" donne la possibilité de modifier les permissions sur les fichiers et les répertoires, mais aussi celle de prendre possession de ces objets. Si la suppression de ces permissions excessive pour le groupe "Tout le Monde" n'est pas souhaité, on peut cependant remplacer ce groupe par le groupe "Utilisateurs" ou "Utilisateurs authentifiés" (Post SP3), afin de supprimer les possibilités d'accès non autorisées à des utilisateurs non-authentifiés.

Sécurisation de fichiers spécifiques

Windows NT s'appuie sur deux partitions pour démarrer : une partition de Boot, et une partition système. La plupart du temps, ces partitions sont les mêmes (C:) mais on peut très bien envisager de créer deux partitions distinctes pour ce faire.

La partition de Boot contient tous les fichiers nécessaires au démarrage du système : BOOT.INI, NTLDR, NTDETECT.COM et NTBTDD.SYS (pour les systèmes SCSI).

La partition système contient les fichiers et les répertoires hébergeant toutes les librairies et les fichiers exécutables du système. Afin de s'assurer de l'intégrité de ces fichiers, on peut supprimer toutes les permissions utilisateurs et groupes sur ceux-ci, excepté pour le groupe Administrateurs et SYSTEM.

Pour les fichiers AUTOEXEC.BAT et CONFIG.SYS, positionner la permission "Lire" pour le groupe "Tout le Monde".

Sécurisation des permissions NTFS pour une machine Windows NT Workstation

- Supprimer les permissions relatives au groupe "Tout le Monde", et les remplacer par les mêmes permissions mais pour le groupe "Utilisateurs" ou "Utilisateurs authentifiés". Si un service de publication HTTP existe sur cette machine, s'assurer que le compte IUSR_NomdeMachine a un accès en lecture à l'arborescence de publication et, surtout, qu'aucun autre accès ne lui est donné en dehors de cette arborescence
- Restreindre les permissions d'accès à "Lire" pour les répertoires contenant des fichiers exécutables. Ceci peut cependant parfois poser problème lorsque certains programmes ont besoin d'écrire des fichiers temporaires (dans quels répertoires ces programmes écrivent-ils ces fichiers temporaires ?)
- Créer des arborescences dans lesquelles les utilisateurs puissent stocker des données temporaires et / ou permanentes. Selon l'architecture choisie, ces arborescences peuvent être locales ou distantes.

Sécurisation des permissions NTFS pour une machine Windows NT Serveur

- Les accès interactifs à la console ne doivent être accessibles qu'aux administrateurs des serveurs
- Supprimer les permissions sur les fichiers et répertoires du système d'exploitation pour les groupes "Tout le Monde", "Utilisateurs" ainsi que tout autre groupe n'ayant pas à se connecter en local sur un serveur (laisser les accès à SYSTEM).

5.14. Autres réglages

5.14.1. Disquettes de réparation d'urgence

Après installation complète de la machine, et en particulier s'il s'agit d'un serveur, il est recommandé de générer des disquettes de réparation d'urgence avec l'utilitaire Rdisk.exe livré avec le système d'exploitation. Cette précaution permet de restaurer une configuration préalable suite à une mauvaise manipulation ou à un plantage fatal.

Cette disquette peut contenir une copie de la base des registres (dont la fameuse SAM) ; **elle est donc à protéger physiquement** (stockage dans un coffre par exemple). Il est également nécessaire de régénérer cette disquette à la suite de chaque modification importante du système, et après la création d'un utilisateur.

La commande à frapper pour créer une disquette de réparation d'urgence est « `rdisk` », ou « `rdisk /s` » si l'on veut sauvegarder la SAM.

D'une façon générale : **toujours créer une disquette de réparation d'urgence avant l'application d'un Service Pack et d'un Hot-Fix.**

5.14.2. Mot de passe pour le lancement de services

Certains services ont besoin de s'exécuter en tant qu'un utilisateur donné. Le mot de passe associé à cet utilisateur est alors requis pour que le service puisse se « loguer ». Or ce mot de passe est stocké chiffré dans la base des registres. Mais l'algorithme et la clef de chiffrement sont connus !

En conséquence **il n'est pas recommandé d'affecter un compte utilisateur à un service**. Cependant, si le contexte nécessite tout de même d'effectuer cette manipulation, utiliser un compte dédié.

5.15. Maintient en condition de la sécurité d'un système

Les chapitres précédents donnent des pistes à suivre pour assurer la sécurité d'un système en cours de déploiement. Il reste cependant un problème qui est celui du maintient de la sécurité d'un système, tout au long de sa vie.

Sans aller jusqu'à mettre en place une surveillance permanente de ses systèmes, il est conseillé d'auditer régulièrement son site afin de prévenir, et de détecter, d'éventuels dysfonctionnements relatifs à la sécurité (ces dysfonctionnements peuvent aller jusqu'à un piratage pur et simple de son système).

L'une des pierres angulaires nécessaire à ce type de travail reste la journalisation des événements : il est bon, même si cela est parfois fastidieux, de jeter souvent un coup d'œil sur le contenu des journaux d'événements. De même, il est conseillé de sauvegarder régulièrement ces journaux avant de les effacer ; l'avantage de ces sauvegardes est de pouvoir, si le besoin s'en fait sentir, retracer la vie d'un système d'information, et ceci est particulièrement utile après la détection d'une attaque informatique sur ses systèmes. Si l'espace disque disponible est insuffisant pour garder une trace de tous les journaux d'événements, réaliser une sauvegarde sur un CD-Rom.

A cette surveillance périodique, on peut ajouter l'utilisation de quelques outils d'analyse comme ceux décrits aux chapitres § 4.2 (Auditer son système d'information), § 4.3 (

Détection d'intrusion) et § 4.5 (Outils divers).

L'utilisation d'un outil de craquage de mots de passe permet également de sensibiliser ses utilisateurs au problème des mots de passe.

En outre, la mise en œuvre d'un mécanisme de script d'ouverture de session peut être particulièrement utile pour conserver des traces de la configuration des machines : on peut ainsi, à chaque ouverture de session, déclencher un script qui va récupérer un certain nombre d'informations relatives au poste utilisateur et les stocker dans un répertoire partagé dont les ACLs seront positionnées à RWX (pour le répertoire) et WX (pour les fichiers). Parmi les informations que l'on peut récupérer de cette manière, on peut citer :

- Configuration réseau des machines,
- Services Packs et Hot-Fixes appliqués,
- Logiciels installés,
- Versions de certains logiciels,
- Services en cours de fonctionnement,
- Liste des utilisateurs locaux des Workstations,
- Etat des variables d'environnement,
- Etc.

6. ANNEXES

6.1. Permissions par défaut lors de l'installation du système

Les tableaux qui suivent précisent les permissions NTFS par défaut, utilisées après une installation du système.

6.1.1. Windows NT Workstation :

Emplacement	Groupes	Permissions des répertoires	Permissions des fichiers
Racine du disque Système	Tout le Monde	CT	CT
C:\TEMP	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RWXD CT CT	CT RWXD CT CT
C:\WINNT (%SystemRoot%)	Tout le Monde	CT	CT
C:\WINNT	Administrateurs Tout le Monde System		CT RX CT
C:\WINNT\NOTEPAD.EXE, WIN.INI, SYSTEM.INI, CONTROL.INI, TASKMAN.EXE, SETUP.OLD, SETUPLOG.TXT, *.BMP (Sauf WINNT, WINNT256, ZAPOTEC, SOLSTICE.BMPS)	Tout le Monde		CT
C:\WINNT\CONFIG	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RWXD CT CT	CT RWXD CT CT
C:\WINNT\CONFIG*.*	Administrateurs Tout le Monde System		CT RX CT
C:\WINNT\CURSORS	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RWXD CT CT	CT RWXD CT CT
C:\WINNT\CURSORS*.*	Tout le Monde		CT
C:\WINNT\FONTS	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RWXD CT CT	CT RWXD CT CT
C:\WINNT\FONTS*.*	Administrateurs Tout le Monde System		CT RX CT
C:\WINNT\HELP	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RWXD CT CT	CT RWXD CT CT
C:\WINNT\HELP*.*	Administrateurs Tout le Monde System		CT RX* CT
C:\WINNT\HELP\EXCHNG.CNT,	Tout le Monde		CT

Emplacement	Groupes	Permissions des répertoires	Permissions des fichiers
EXCHNG.HLP, IEXPLORE.CNT, IEXPLORE.HLP, INT-MAIL.CNT, INT-MAIL.HLP, MSFS.CNT, MSFS.HLP, MSNAUTH.CNT, MSNAUTH.HLP, PINBALL.CNT, PINBALL.HLP, SCANPST.HLP, WANGIMG.CNT, WANGIMG.HLP, WANGOCX.CNT, WANGOCX.HLP, WANGOCXD.CNT, WANGOCXD.HLP, WANGSHL.CNT, WANGSHL.HLP, WORDPAD.CNT, WORDPAD.HLP			
C:\WINNT\INF	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RWXD CT CT	CT RWXD CT CT
C:\WINNT\INF*.INF	Administrateurs Tout le Monde System		CT RX CT
C:\WINNT\INF*.PNF	Tout le Monde		CT
C:\WINNT\MEDIA	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RWXD CT CT	CT RWXD CT CT
C:\WINNT\MEDIA*.MID	Administrateurs Tout le Monde System		CT RX CT
C:\WINNT\MEDIA*.RMI	Tout le Monde		CT
C:\WINNT\MEDIA*.WAV	Administrateurs Tout le Monde System		CT RX CT
C:\WINNT\PROFILES\ADMINISTRATEUR	Administrateur System Administrateurs	CT CT CT	CT CT CT
C:\WINNT\PROFILES\ALL USERS	Administrateurs Tout le Monde System	CT RX CT	CT RX CT
C:\WINNT\PROFILES\DEFAULT USERS	Administrateurs Tout le Monde System	CT RX CT	CT RX CT
C:\WINNT\REPAIR	Administrateurs Tout le Monde Créateur/Propriétaire Utilisateurs avec pouvoir System	CT RX CT RWXD CT	CT RX CT RWXD CT
C:\WINNT\REPAIR\SETUP.LOG	Tout le Monde		CT
C:\WINNT\SHELLNEW	Tout le Monde	CT	CT
C:\WINNT\SYSTEM	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RWXD CT CT	CT RWXD CT CT

Emplacement	Groupes	Permissions des répertoires	Permissions des fichiers
C:\WINNT\SYSTEM*.DLL, *.DRV & MMTASK.TSK	Tout le Monde		CT
C:\WINNT\SYSTEM\SETUP.INF	Administrateurs Tout le Monde System		CT RX CT
C:\WINNT\SYSTEM32\	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RWXD CT CT	CT RWXD CT CT
C:\WINNT\SYSTEM32*.*	Administrateurs Tout le Monde System		CT RX* CT
C:\WINNT\SYSTEM32*.PNF, *.REG, *.TRN, $WINNT$.INF, CMC.DLL, CONFIG.TMP, MAPISP32.EXE, MAPISRVR.EXE, MAPISVC.INF, MAPIU.DLL, MAPIU32.DLL, MAPIX.DLL, MAPIX32.DLL, MDISP.TLB, MDISP32.EXE, MDISP32.TLB, MINET32.DLL, ML3XEC16.EXE, MLCFG32.CPL, MMFMIG32.DLL, MSFS32.DLL, MSPST32.DLL, OEMNAD0.INF, WGPOADMN.DLL, WGPOCPL.CPL, WMSFR32.DLL, WMSUI32.DLL	Tout le Monde		CT
C:\WINNT\SYSTEM32\LOCALMON.DLL	Administrateurs Tout le Monde Créateur/Propriétaire Utilisateurs avec pouvoir		CT RX CT RWXD
C:\WINNT\SYSTEM32\CONFIG\	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RX CT CT	CT RX CT CT
C:\WINNT\SYSTEM32\CONFIG*.LOG, *.SAV, SAM, SECURITY, SYSTEM.ALT	Tout le Monde		CT
C:\WINNT\SYSTEM32\DHCP	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RX CT CT	CT RX CT CT
C:\WINNT\SYSTEM32\DRIVERS	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RX CT CT	CT RX CT CT
C:\WINNT\SYSTEM32\DRIVERS\Current NIC Drivers	Tout le Monde		CT
C:\WINNT\SYSTEM32\DRIVERS\ETC	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RX CT CT	CT RX CT CT
C:\WINNT\SYSTEM32\OS2\	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RWXD CT CT	CT RWXD CT CT

Emplacement	Groupes	Permissions des répertoires	Permissions des fichiers
C:\WINNT\SYSTEM32\OS2*.*	Administrateurs Tout le Monde System		CT RX CT
C:\WINNT\SYSTEM32\OS2\DLL	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RWXD CT CT	CT RWXD CT CT
C:\WINNT\SYSTEM32\OS2\DLL*.*	Administrateurs Tout le Monde System		CT RX CT
C:\WINNT\SYSTEM32\RAS	Administrateurs Tout le Monde Créateur/Propriétaire Utilisateurs avec pouvoir System	CT RWXD CT RWXD CT	CT RWXD CT RWXD CT
C:\WINNT\SYSTEM32\RAS*.*	Administrateurs Tout le Monde System		CT RX CT
C:\WINNT\SYSTEM32\REPL	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RX CT CT	CT RX CT CT
C:\WINNT\SYSTEM32\REPL\EXPORT	Administrateurs Tout le Monde Créateur/Propriétaire Replicateur System	CT RX CT RWXD CT	CT RX CT RWXD CT
C:\WINNT\SYSTEM32\REPL\IMPORT	Administrateurs Tout le Monde Créateur/Propriétaire Replicateur System	CT RX CT RWXD CT	CT RX CT RWXD CT
C:\WINNT\SYSTEM32\SPOOL	Administrateurs Tout le Monde Créateur/Propriétaire Utilisateurs avec pouvoir System	CT RX CT RWXD CT	CT RX CT RWXD CT
C:\WINNT\SYSTEM32\VIEWERS	Administrateurs Tout le Monde Créateur/Propriétaire System	CT RWXD CT CT	CT RWXD CT CT
C:\WINNT\SYSTEM32\VIEWERS*.*	Administrateur Tout le Monde System		CT RX CT
C:\WINNT\SYSTEM32\WINS	Tout le Monde	CT	CT

6.1.2. Windows NT Server :

Emplacement	Groupes	Permissions des répertoires	Permissions des fichiers
Racine du disque Système	Tout le Monde	CT	CT
C:\TEMP	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RWXD CT RWXD CT	CT RWXD CT RWXD CT
C:\WINNT (%SystemRoot%)	Tout le Monde	CT	CT
C:\WINNT*.*	Administrateurs Tout le Monde Opérateurs de serveur System		CT RX* RWXD CT
C:\WINNT\NOTEPAD.EXE, WIN.INI, SYSTEM.INI, CONTROL.INI, TASKMAN.EXE, SETUP.OLD, SETUPLOG.TXT, *.BMP (Sauf LANMANNT.BMP, LANMA256.BMP, ZAPOTEC.BMP, SOLSTICE.BMP)	Tout le Monde		CT
C:\WINNT\CONFIG	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RWXD CT RWXD CT	CT RWXD CT RWXD CT
C:\WINNT\CONFIG*.*	Administrateurs Tout le Monde Opérateurs de serveur System		CT RX RWXD CT
C:\WINNT\CURSORS	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RWXD CT RWXD CT	CT RWXD CT RWXD CT
C:\WINNT\CURSORS*.*	Tout le Monde		CT
C:\WINNT\FONTS	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RWXD CT RWXD CT	CT RWXD CT RWXD CT
C:\WINNT\FONTS*.*	Administrateurs Tout le Monde Opérateurs de serveur System		CT RX RWXD CT
C:\WINNT\HELP	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RWXD CT RWXD CT	CT RWXD CT RWXD CT
C:\WINNT\HELP*.*	Administrateurs Tout le Monde Opérateurs de serveur		CT RX* RWXD

Emplacement	Groupes	Permissions des répertoires	Permissions des fichiers
	System		CT
C:\WINNT\HELP\EXCHNG.CNT, EXCHNG.HLP, IEXPLORE.CNT, IEXPLORE.HLP, INT-MAIL.CNT, INT-MAIL.HLP, MSFS.CNT, MSFS.HLP, MSNAUTH.CNT, MSNAUTH.HLP, PINBALL.CNT, PINBALL.HLP, SCANPST.HLP, WANGIMG.CNT, WANGIMG.HLP, WANGOCX.CNT, WANGOCX.HLP, WANGOCXD.CNT, WANGOCXD.HLP, WANGSHL.CNT, WANGSHL.HLP, WORDPAD.CNT, WORDPAD.HLP	Tout le Monde		CT
C:\WINNT\INF	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RWXD CT RWXD CT	CT RWXD CT RWXD CT
C:\WINNT\INF*.INF	Administrateurs Tout le Monde Opérateurs de serveur System		CT RX RWXD CT
C:\WINNT\INF*.PNF	Tout le Monde		CT
C:\WINNT\MEDIA	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RWXD CT RWXD CT	CT RWXD CT RWXD CT
C:\WINNT\MEDIA*.MID	Administrateurs Tout le Monde Opérateurs de serveur System		CT RX RWXD CT
C:\WINNT\MEDIA*.RMI	Tout le Monde		CT
C:\WINNT\MEDIA*.WAV	Administrateurs Tout le Monde Opérateurs de serveur System		CT RX RWXD CT
C:\WINNT\PROFILES\ADMINISTRATEUR	Administrateur System Administrateurs	CT CT CT	CT CT CT
C:\WINNT\PROFILES\ALL USERS	Administrateurs Tout le Monde System	CT RX CT	CT RX CT
C:\WINNT\PROFILES\DEFAULT USERS	Administrateurs Tout le Monde System	CT RX CT	CT RX CT
C:\WINNT\REPAIR	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RX CT RWXD CT	CT RX CT RWXD CT

Emplacement	Groupes	Permissions des répertoires	Permissions des fichiers
C:\WINNT\REPAIR*._, DA._	Administrateurs System		CT CT
C:\WINNT\REPAIR\SETUP.LOG	Tout le Monde		CT
C:\WINNT\SHELLNEW	Tout le Monde	CT	CT
C:\WINNT\SYSTEM	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RWXD CT RWXD CT	CT RWXD CT RWXD CT
C:\WINNT\SYSTEM*.DLL, *.DRV & MMTASK.TSK	Tout le Monde		CT
C:\WINNT\SYSTEM\SETUP.INF	Administrateurs Tout le Monde Opérateurs de serveur System		CT RX RWXD CT
C:\WINNT\SYSTEM32\	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RWXD CT RWXD CT	CT RWXD CT RWXD CT
C:\WINNT\SYSTEM32*.*	Administrateurs Tout le Monde Opérateurs de serveur System		CT RX* RWXD CT
C:\WINNT\SYSTEM32*.PNF, $WINNT$.INF, CONFIG.TMP, OEMNAD0.INF	Tout le Monde		CT
C:\WINNT\SYSTEM32\LOCALMON.DLL	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur Print Operators		CT RX CT CT CT
C:\WINNT\SYSTEM32\CONFIG\	Administrateurs Tout le Monde Créateur/Propriétaire System	CT (RX) lister CT CT	CT CT CT
C:\WINNT\SYSTEM32\CONFIG*.*	Administrateurs Tout le Monde Opérateurs de serveur System		CT RX* RWXD CT
C:\WINNT\SYSTEM32\CONFIG*.LOG, *.SAV, SAM, SECURITY, SYSTEM.ALT	Tout le Monde		CT
C:\WINNT\SYSTEM32\DHCP	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RX CT CT CT	CT RX CT CT CT
C:\WINNT\SYSTEM32\DRIVERS	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RX CT CT CT	CT RX CT CT CT

Emplacement	Groupes	Permissions des répertoires	Permissions des fichiers
C:\WINNT\SYSTEM32\DRIVERS*.*	Administrateurs Tout le Monde Opérateurs de serveur System		CT RX RWXD CT
C:\WINNT\SYSTEM32\DRIVERS\Current NIC Drivers	Tout le Monde		CT
C:\WINNT\SYSTEM32\DRIVERS\ETC	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RX CT CT CT	CT RX CT CT CT
C:\WINNT\SYSTEM32\DRIVERS\ETC*.*	Administrateurs Tout le Monde Opérateurs de serveur System		CT RX RWXD CT
C:\WINNT\SYSTEM32\OS2\	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RWXD CT RWXD CT	CT RWXD CT RWXD CT
C:\WINNT\SYSTEM32\OS2*.*	Administrateurs Tout le Monde Opérateurs de serveur System		CT RX RWXD CT
C:\WINNT\SYSTEM32\OS2\DLL	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RWXD CT RWXD CT	CT RWXD CT RWXD CT
C:\WINNT\SYSTEM32\OS2\DLL*.*	Administrateurs Tout le Monde Opérateurs de serveur System		CT RX RWXD CT
C:\WINNT\SYSTEM32\RAS	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RWXD CT CT CT	CT RWXD CT CT CT
C:\WINNT\SYSTEM32\RAS*.*	Administrateurs Tout le Monde Opérateurs de serveur System		CT RX RWXD CT
C:\WINNT\SYSTEM32\RAS\ RASPHONE.PBK	Tout le Monde		CT
C:\WINNT\SYSTEM32\REPL	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System	CT RX CT CT CT	CT RX CT CT CT
C:\WINNT\SYSTEM32\REPL\EXPORT	Administrateurs Tout le Monde Créateur/Propriétaire Replicateur	CT RX CT RWXD	CT RX CT RWXD

Emplacement	Groupes	Permissions des répertoires	Permissions des fichiers
	Opérateurs de serveur System	RWXD CT	RWXD CT
C:\WINNT\SYSTEM32\REPL\IMPORT	Administrateurs Tout le Monde Créateur/Propriétaire Replicateur Opérateurs de serveur System	CT RX CT RWXD RWXD CT	CT RX CT RWXD RWXD CT
C:\WINNT\SYSTEM32\SPOOL	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur Opérateurs d'impression System	CT RX CT CT CT CT	CT RX CT CT CT CT
C:\WINNT\SYSTEM32\VIEWERS C:\WINNT\SYSTEM32\VIEWERS*.*	Administrateurs Tout le Monde Créateur/Propriétaire Opérateurs de serveur System Administrateur Tout le Monde Opérateurs de serveur System	CT RWXD CT RWXD CT	CT RWXD CT RWXD CT CT RX RWXD CT
C:\WINNT\SYSTEM32\WINS	Tout le Monde	CT	CT

6.2. Permissions préconisées pour une configuration C2 du système

Il existe un outil fourni avec NT Resource Kit de Microsoft, et appelé C2CONFIG.EXE, permettant de diagnostiquer l'état de la sécurité du système et de le comparer avec l'interprétation de Microsoft pour la sécurité C2 du système. Une des options de cet outil est de permettre de modifier les permissions NTFS par défaut, afin de le rendre compatibles avec un standard C2.

Cet outil utilise un fichier de configuration (C2NTFACL.INF), qui contient les différentes permissions qui seront positionnées avec cet outil. Le tableau qui suit précise les permissions des répertoires et des fichiers modifiés par l'outil.

Emplacement	Permissions C2
[%SystemDrive%\]	Tout le Monde - Lire BUILTIN\Administrateurs - Contrôle Total CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemDrive%*.*]	Tout le Monde - Contrôle Total
[%SystemDrive%\IO.SYS] [%SystemDrive%\MSDOS.SYS]	Tout le Monde - Modifier BUILTIN\Administrateurs - Contrôle Total SYSTEM - Contrôle Total
[%SystemDrive%\BOOT.INI] [%SystemDrive%\NTDETECT.COM] [%SystemDrive%\NTLDR.]	BUILTIN\Administrateurs - Contrôle Total SYSTEM - Contrôle Total
[%SystemDrive%\AUTOEXEC.BAT] [%SystemDrive%\CONFIG.SYS]	Tout le Monde - Lire BUILTIN\Administrateurs - Contrôle Total SYSTEM - Contrôle Total
[%SystemDrive%\TEMP\!]	Tout le Monde - Modifier BUILTIN\Administrateurs - Contrôle Total CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemDrive%\USERS\!]	Tout le Monde - Lister BUILTIN\Administrateurs - RWXD SYSTEM - Contrôle Total
[%SystemDrive%\USERS\DEFAULT\!]	Tout le Monde - RWX CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemDrive%\WIN32APP\!]	Tout le Monde - Lire BUILTIN\Administrateurs - Contrôle Total CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\!]	Tout le Monde - Modifier BUILTIN\Administrateurs - Contrôle Total CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%*.*]	Tout le Monde - Lire BUILTIN\Administrateurs - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%*.INI]	Tout le Monde - Modifier BUILTIN\Administrateurs - Contrôle Total SYSTEM - Contrôle Total

Emplacement	Permissions C2
[%SystemRoot%\LOCALMON.DLL] [%SystemRoot%\PRINTMAN.HLP]	Tout le Monde - Lire BUILTIN\Utilisateurs avec pouvoir - Modifier BUILTIN\Administrateurs - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\REPAIR\!]	BUILTIN\Administrateurs - Contrôle Total
[%SystemRoot%\SYSTEM*.*]	Tout le Monde - Lire BUILTIN\Administrateurs - Contrôle Total CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32*.*]	Tout le Monde - Lire BUILTIN\Administrateurs - Contrôle Total CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\AUTOEXEC.NT] [%SystemRoot%\SYSTEM32\CMOS.RAM] [%SystemRoot%\SYSTEM32\CONFIG.NT] [%SystemRoot%\SYSTEM32\MIDIMAP.CFG]	Tout le Monde - Modifier BUILTIN\Administrateurs - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\PASSPORT.MID]	Tout le Monde - Contrôle Total
[%SystemRoot%\SYSTEM32\CONFIG] [%SystemRoot%\SYSTEM32\CONFIG*.*]	Tout le Monde - Lister BUILTIN\Administrateurs - Contrôle Total CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\CONFIG\DEFAULT.LOG] [%SystemRoot%\SYSTEM32\CONFIG\SAM.] [%SystemRoot%\SYSTEM32\CONFIG\SAM.LOG] [%SystemRoot%\SYSTEM32\CONFIG\SECURITY.] [%SystemRoot%\SYSTEM32\CONFIG\SECURITY.LOG] [%SystemRoot%\SYSTEM32\CONFIG\SYSTEM.] [%SystemRoot%\SYSTEM32\CONFIG\SYSTEM.ALT] [%SystemRoot%\SYSTEM32\CONFIG\SYSTEM.LOG]	Tout le Monde - Contrôle Total
[%SystemRoot%\SYSTEM32\CONFIG\USERDEF.]	Tout le Monde - Lire SYSTEM - Modifier BUILTIN\Administrateurs - Contrôle Total
[%SystemRoot%\SYSTEM32\DHCP\!]	Tout le Monde - Lire BUILTIN\Utilisateurs avec pouvoir - Modifier BUILTIN\Administrateurs - Contrôle Total CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\DRIVERS\!]	Tout le Monde - Lire BUILTIN\Administrateurs - Contrôle Total CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\OS2\OSO001.009]	Tout le Monde - Lire BUILTIN\Administrateurs - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\OS2\DLL\DOSCALLS.DLL]	Tout le Monde - Lire BUILTIN\Administrateurs - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\OS2\DLL\NETAPI.DLL]	Tout le Monde - Contrôle Total
[%SystemRoot%\SYSTEM32\RAS]	Tout le Monde - Lire BUILTIN\Utilisateurs avec pouvoir - Modifier BUILTIN\Administrateurs - Contrôle Total

Emplacement	Permissions C2
	CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\RAS*.*]	Tout le Monde - Lire BUILTIN\Administrateurs - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\REPL\!]	Tout le Monde - Lire BUILTIN\Administrateurs - Contrôle Total CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\REPL\EXPORT] [%SystemRoot%\SYSTEM32\REPL\EXPORT*.*]	Tout le Monde - Modifier BUILTIN\Administrateurs - Contrôle Total CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\REPL\EXPORT\SCRIPTS] [%SystemRoot%\SYSTEM32\REPL\EXPORT\SCRIPTS*.*]	Tout le Monde - Lire BUILTIN\Réplicateur - Modifier BUILTIN\Administrateurs - Contrôle Total CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\REPL\IMPORT] [%SystemRoot%\SYSTEM32\REPL\IMPORT*.*]	Tout le Monde - Modifier BUILTIN\Administrateurs - Contrôle Total CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\REPL\IMPORT\SCRIPTS] [%SystemRoot%\SYSTEM32\REPL\IMPORT\SCRIPTS*.*]	Tout le Monde - Lire BUILTIN\Réplicateur - Modifier BUILTIN\Administrateurs - Contrôle Total CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\SPOOL\!]	Tout le Monde - Lire BUILTIN\Utilisateurs avec pouvoir - Modifier BUILTIN\Administrateurs - Contrôle Total CREATEUR PROPRIETAIRE - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\SPOOL\DRIVERS\W32X86\1]	Tout le Monde - Contrôle Total
[%SystemRoot%\SYSTEM32\SPOOL\PRTPROCS\W32X86\ WINPRINT.DLL]	Tout le Monde - Lire BUILTIN\Utilisateurs avec pouvoir - Modifier BUILTIN\Administrateurs - Contrôle Total SYSTEM - Contrôle Total
[%SystemRoot%\SYSTEM32\WINS\!]	Tout le Monde – Contrôle Total

6.3. Principales Vulnérabilités de Windows NT

Ce chapitre décrit, sans souci d'exhaustivité, des vulnérabilités courantes dans le monde Windows (9x et NT). La plupart de ces attaques reposent sur une gestion déficiente des paquets réseaux dans la pile TCP/IP de Microsoft. Toutes ces vulnérabilités peuvent être comblées par des patches (Service Pack et / ou Hot Fix) et / ou un paramétrage adéquat des machines.

6.3.1. GetAdmin

Le programme GetAdmin a été programmé en Russie par Konstantin Sobolev, il offre la possibilité, depuis un simple compte utilisateur, d'ajouter un utilisateur dans le groupe « Administrateurs ». Aucune permission particulière n'est requise pour utiliser ce programme. En Service Pack 3, il est nécessaire d'appliquer le patch GetAdmin pour combler la faille. Cependant, lorsqu'un petit programme disponible sur l'Internet (et appelé crash4.exe) est exécuté sur une machine protégée, le programme GetAdmin fonctionne ensuite sans problème. La faille a été comblée définitivement depuis le Service Pack 4.

6.3.2. Ping Of Death II

Dans la tradition de la vulnérabilité originelle « Ping Of Death » qui consistait à noyer la machine cible de gros et nombreux paquets ICMP de type « Echo Reply » (Ping), « Ping Of Death 2 » (ou Sping) envoie de multiples paquets ICMP fragmentés de 64 Ko. Le résultat est un crash de la pile TCP/IP de Windows NT (et donc de la machine).

6.3.3. L'attaque Out Of Band (OOB)

Il s'agit d'une attaque en déni de service qui affecte les machines Windows NT et Windows 95. Celle-ci est réalisée en envoyant des paquets « Out Of Band » à une connexion déjà établie. NetBios, qui écoute sur le port 139, semble le plus affecté par le problème, mais l'attaque peut cependant marcher sur un service comme DNS (dans ce cas le journal d'événement arrive à saturation avec des messages de type « select() error »).

Il semble que le système Windows NT ne sache pas gérer convenablement les messages de type OOB, ce qui a tendance à le faire paniquer et à faire apparaître le fameux « Ecran bleu de la mort ».

6.3.4. L'attaque SMB Downgrade

Lors d'une connexion à un serveur Windows NT depuis une autre machine Windows, une phase de négociation a lieu afin de déterminer le mécanisme d'authentification qui va être utilisé. Le principe de l'attaque est de créer un serveur qui demande comme unique moyen d'authentification un « clear text password », autrement dit un mot de passe en clair. Le comportement par défaut pour le client est d'obéir à la requête du serveur et d'envoyer le mot de passe de l'utilisateur en clair sur le réseau.

6.3.5. SYN Flooding

Lors d'une connexion à un serveur, le protocole TCP/IP se met en route et une phase de négociation à lieu durant laquelle est initialisée la connexion. Toute demande de connexion commence par l'envoi d'une trame de type SYN. Lorsque le serveur reçoit une telle trame, il réserve des ressources pour la future connexion, puis ré-émet une trame de type SYN-ACK (acquittement de demande de connexion).

Le comportement par défaut de Windows NT 3.51 et 4.0 est de ré-émettre jusqu'à 5 fois cette trame SYN-ACK en cas de non réponse du client, et en doublant le temps de Time-out chaque fois. La valeur initiale de Time-out étant de 3 secondes, le serveur va donc renvoyer cette trame après 3, 6, 12, 24 puis 48 secondes. Après la dernière retransmission, le serveur attend encore 96

secondes avant d'abandonner et de fermer les ressources allouées. Ainsi, en cas de réception d'une trame SYN à laquelle le client ne répond pas, il va se passer 189 secondes durant lesquelles le serveur aura alloué de la mémoire inutilement.

Le principe de l'attaque consiste à envoyer un flot continu de trames SYN, et dans laquelle l'adresse IP source est fausse (différente de l'adresse IP de l'attaquant, sans quoi ce dernier risque de planter sa propre machine !) ; aussi les trames SYN-ACK ne recevront jamais de réponse. Ainsi, l'attaquant va tenter de sursaturer la mémoire de la machine cible pendant ces 189 secondes. Normalement, la pile TCP/IP devrait n'autoriser qu'un nombre de connexions maximales simultanées sur un port donné. Il semble cependant que les premières versions de Windows NT gèrent mal ce type de demandes de connexion ce qui mène à une saturation de l'espace mémoire réservé par la pile TCP/IP (et donc généralement à un « écran bleu de la mort »)

6.3.6. Land Attack

Le principe de Land Attack est d'émettre à destination d'une machine vulnérable des paquets SYN avec des adresses source et destination identiques, et avec des ports source et destination également identiques, comme si la machine cible s'envoyait des trames à elle-même. Le résultat est un net ralentissement de la machine cible, avec parfois un plantage de la pile TCP/IP.

6.3.7. Teardrop

Cette attaque est basée sur la mauvaise gestion des fragments dans la pile TCP/IP. Le principe de cette attaque d'est d'envoyer deux paquets fragmentés à la victime. Le premier est le fragment d'offset 0 avec un « payload » de taille N, de plus le bit MF est positionné à 1. La seconde trame est le dernier fragment (MF=0) avec un offset positif <N et un « payload » <N.

La machine cible va alors tenter de réaligner les fragments, ce qui est impossible puisque le « payload » du fragment courant ne contient pas assez de données pour couvrir le réalignement. Généralement, la pile TCP/IP de la machine se plante (= « écran bleu de la mort »).

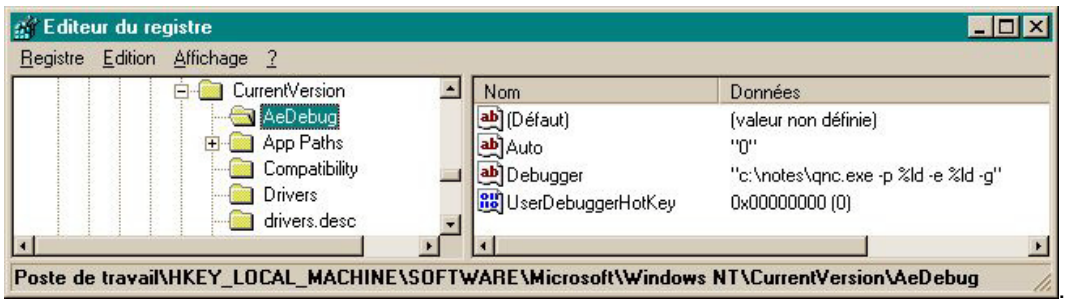
6.3.8. KnownDLLs

Cette attaque exploite une faille de protection des appels aux ressources du système, stockées dans la mémoire. Certaines de ces ressources (des librairies de fonctions dynamiques, ou DLLs) sont montées en mémoire au démarrage de la machine afin d'optimiser les temps d'accès, d'où le nom « KnownDLLs » - « DLLs connues ». Comme tout objet NT sensible, ces librairies sont protégées contre l'écriture par un utilisateur simple.

Cependant, le système gère en interne des pointeurs vers ces DLLs, et ces pointeurs, eux, ne sont pas protégés (Tout le monde = Contrôle Total). L'attaquant va donc tenter de modifier ces pointeurs afin de les faire pointer vers ses propres routines (comme dans l'environnement DOS dans lequel les virus redirigeaient les interruptions vers un code parasite).

6.3.9. Aedebug

Cette attaque repose sur un défaut de protection de la clef de registre HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Aedebug\Debugger



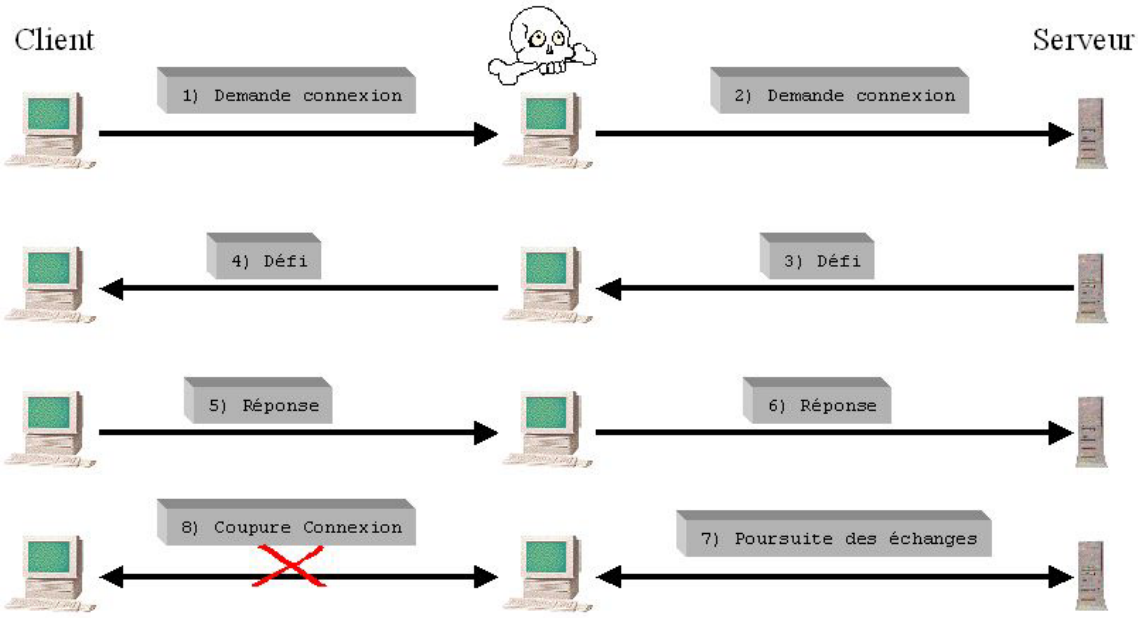
Cette clef contient une chaîne de caractères qui, normalement, correspond à un programme et ses paramètres. Par défaut, ce programme est Dr Watson. Il s'agit en fait du programme à lancer en cas de plantage d'un applicatif. Ce programme est lancé avec les privilèges SYSTEM ce qui signifie que le processus lancé a le contrôle total sur la machine.

Le principe de l'attaque est ici de modifier le contenu de cette clef (sur une installation de base elle n'est pas protégée par défaut), afin de lancer un applicatif parasite (le gestionnaire des utilisateurs par exemple) ; cet applicatif, lancé dans l'environnement de l'utilisateur qui a fait planter un programme, aura donc les privilèges SYSTEM (on peut ainsi rajouter un utilisateur dans le groupe des Administrateurs). Le correctif à apporter est ici de positionner les permissions à Lecture pour « Tout le Monde » sur cette clef, en sachant toutefois que certains applicatifs risquent de refuser de fonctionner normalement par la suite (Lotus Notes par exemple peut, dans certaines configurations, poser problème).

6.3.10. Attaques « Man in the Middle »

Les attaques de type « Man in the Middle » sont communes à tous les protocoles qui n'implémentent pas de mécanisme de signature (elles fonctionnent donc pour le protocole SMB de base, mais aussi pour les protocoles Telnet, FTP, HTTP etc.).

Le principe de l'attaque nécessite pour l'attaquant de se positionner en coupure entre un client et un serveur. Lorsque le client émet une requête auprès du serveur, la demande de connexion est interceptée par l'attaquant qui la ré-émet au serveur en changeant l'adresse source du client (il met la sienne à la place). Le serveur demande une authentification, qui est ré-émise au client par l'attaquant. Le client s'authentifie, cette authentification est alors retransmise au serveur par l'attaquant qui coupe alors la connexion entre lui et le client. Comme c'est l'attaquant qui s'est connecté au serveur (par un simple mécanisme de relayage de trames), c'est lui qui dispose désormais d'une session ouverte sur le serveur.



6.4. Best Of Insecurity - ce qu'il ne faut pas faire

On trouve assez facilement dans la littérature de précieuses recommandations sur ce qu'il est nécessaire / recommandé / obligatoire de faire, afin d'assurer un niveau de sécurité satisfaisant sur une machine Windows NT. Ce que l'on trouve plus difficilement, et c'est cette lacune que ce chapitre tenter ici de corriger, c'est une liste de choses **à ne pas faire** si l'on souhaite garantir une sécurité optimale.

La liste qui suit n'est pas exhaustive, on trouvera toujours des choix de configuration plus tordus que ceux-ci, cependant ces « erreurs » de configurations sont assez courantes et, tout en n'améliorant en rien le fonctionnement général du système elles contribuent à baisser le niveau de sécurité qu'offre une installation standard de Windows NT (comme si ça ne suffisait pas comme ça !). Notons que pour la plupart, mais sans citer lesquelles, il s'agit de situations vécues.

Ce qu'il ne faut pas faire	Pourquoi
Attribuer des droits temporaires à un utilisateur « pour voir si ca marche mieux comme ça ».	L'expérience montre qu'on oublie de repositionner les droits originaux la plupart du temps. Si on doit mener un test, le faire sur une machine de test
Mettre un mot de passe vide à un utilisateur que l'on vient de créer.	Entre le moment ou on fait ça et le moment ou l'utilisateur se connecte, un attaquant peut utiliser ce compte.
Sur un répertoire ou un fichier, mettre « Aucun accès » comme permission pour « Tout le monde ».	« Tout le monde », ca veut dire « Tout le monde » donc même les administrateurs, les opérateurs de sauvegarde etc. même si on positionne « Contrôle total » pour ceux-ci…
Créer un compte de service. En clair : aller dans « Panneau de configuration / Services », choisir un service puis cliquer sur Démarrage, cocher la boite « compte utilisateur », choisir un compte d'administrateur puis saisir le mot de passe de ce compte et valider (but de la manœuvre : faire tourner un service avec les droits de l'Administrateur)	Deux raisons : 1) le mot de passe ainsi saisi est stocké dans le registre de la machine locale PRESQUE EN CLAIR ! 2) Si vous changer le mot de passe du compte utilisé, le service refusera de fonctionner puisqu'il aura gardé l'ancien mot de passe dans la base des registres.
Réaliser une protection récursive du disque système à partir de la racine (ou de Winnt par exemple) en spécifiant « Tout le monde » = Lire (RX)	Non seulement vous empêcherez les utilisateurs de pouvoir écrire sur ce disque ce qui est fâcheux (plus de profils, plus de fichier de swap, plus de cache Internet, plus de préférences…), mais en plus vous ouvrez l'accès en lecture à des zones réservées du système (dont la SAM !)
Formater son disque système en FAT, parce que (au choix) : 1) ça marche mieux que NTFS 2) je connais mieux la FAT 3) je ne peux plus utiliser mon défragmenteur (ou Norton Utilities pour Windows 9x)	Sans NTFS, pas de protection du système d'exploitation. Revient à utiliser un Windows 95. De plus, NTFS gère en interne un mécanisme de défragmentation automatique.
Ne pas mettre de mot de passe à l'Administrateur Local d'une machine versée dans un domaine, ou verser le compte de domaine d'un utilisateur dans le groupe Administrateur Local de sa machine (raison invoquée : il faut que l'utilisateur ait certains droits sur sa propre machine)	Pour l'utilisateur, c'est l'occasion rêvée de mettre un cheval de Troie sur sa propre machine avant d'appeler l'Administrateur du domaine pour la dépanner.
Appliquer le Service Pack 4 mais pas le Hot Fix msv1-fix alors qu'on a des clients en Windows 3.11.	Bravo ! Vous venez d'introduire une vulnérabilité dans le système. Les comptes de vos clients 3.11 sont désormais accessibles sans mot de passe depuis une machine Windows NT

Ce qu'il ne faut pas faire	Pourquoi
Ne pas suivre les préconisations de Microsoft concernant l'ordre d'application des Hot Fixes.	Vous risquez d'annuler l'effet des Hot Fixes les plus récents.
Donner des noms de machines identiques dans deux domaines différents mais avec une relation d'approbation entre ces domaines (mono ou bidirectionnelle)	A priori, rien ne vous interdit de faire ça, mais certains applicatifs gèrent TRES MAL ce genre de configuration – dont Lotus cc:Mail – et se plantent suite à un conflit de nom de machine)
Appliquer à la lettre l'intégralité du guide recommandation fourni par le CASSI.	Le guide préconise une configuration **optimale** pour la sécurité de Windows NT. Cependant, certaines options de configuration nécessitent une charge d'administration ultérieure importante, voire prohibitive.
Sécuriser une machine sans avoir au préalable vérifié sur une machine de tests le fonctionnement optimal des applicatifs présent.	Certaines options de configuration peuvent empêcher des applicatifs de fonctionner normalement : TOUJOURS tester une sécurisation avant de l'appliquer dans un contexte opérationnel.

6.5. Descriptions des droits Windows NT Standards et Avancés

Ce qui suit est une rapide description des droits positionnables pour les utilisateurs et les groupes à partir de la console d'administration des utilisateurs de Windows NT 4.0

6.5.1. Droits standards

Accéder à cet ordinateur depuis le réseau
(SeNetworkLogonRight)

Ce droit permet à un utilisateur d'accéder au système depuis un réseau. Lorsque ce droit est donné sur un contrôleur de domaine à un utilisateur d'un domaine Windows NT, celui-ci lui peut accéder à tous les autres contrôleurs du même domaine. Lorsque ce droit est accordé sur une machine Windows NT (Workstation ou Serveur) à un utilisateur local d'une machine, celui ci ne peut accéder qu'à la machine sur laquelle est positionnée ce droit.

Ajouter des stations de travail au domaine
(SeMachineAccountPrivilege)

Ce droit permet à un utilisateur d'ajouter des Workstation dans un domaine. Par défaut, seuls les Administrateurs du Domaine et les Opérateurs de comptes disposent de ce privilège qui ne peut leur être révoqué. Ils peuvent en outre donner ce droit à d'autres utilisateurs.

Sauvegarder des fichiers et des répertoires
(SeBackupPrivilege)

Ce droit permet à un utilisateur d'outrepasser les permissions NTFS d'un volume afin de réaliser une sauvegarde des données. Lorsque ce droit est donné sur un contrôleur de domaine à un utilisateur d'un domaine Windows NT, celui-ci lui est valide pour tous les autres contrôleurs du même domaine. Lorsque ce droit est accordé sur une machine Windows NT (Workstation ou Serveur) à un utilisateur local d'une machine, celui-ci n'est valide que pour la machine sur laquelle est positionnée ce droit.

Modifier l'heure système
(SeSystemTimePrivilege)

Ce droit permet à un utilisateur de modifier l'heure et la date du système. Lorsque ce droit est donné sur un contrôleur de domaine à un utilisateur d'un domaine Windows NT, celui-ci lui est valide pour tous les autres contrôleurs du même domaine. Lorsque ce droit est accordé sur une machine Windows NT (Workstation ou Serveur) à un utilisateur local d'une machine, celui-ci n'est valide que pour la machine sur laquelle est positionnée ce droit.

Forcer l'arrêt à partir d'un système distant
(SeRemoteShutdownPrivilege)

Ce droit est utilisé pour permettre à un Administrateur ou un utilisateur de forcer le redémarrage d'un système à distance. Ce droit n'est pas utilisé sous Windows NT 4.0.

Charger et décharger des pilotes de périphériques
(SeLoadDriverPrivilege)

Ce droit permet à un utilisateur de charger et de décharger des pilotes de périphériques comme une interface réseau ou un contrôleur SCSI. Lorsque ce droit est donné sur un contrôleur de domaine à un utilisateur d'un domaine Windows NT, celui-ci lui est valide pour tous les autres contrôleurs du même domaine. Lorsque ce droit est accordé sur une machine Windows NT (Workstation ou Serveur) à un utilisateur local d'une machine, celui-ci n'est valide que pour la machine sur laquelle est positionnée ce droit.

Ouvrir une session localement.

(SeInteractiveLogonRight)

Ce droit permet à un utilisateur d'ouvrir une session localement. Lorsque ce droit est donné sur un contrôleur de domaine à un utilisateur d'un domaine Windows NT, celui-ci lui est valide pour tous les autres contrôleurs du même domaine. Lorsque ce droit est accordé sur une machine Windows NT (Workstation ou Serveur) à un utilisateur local d'une machine, celui-ci n'est valide que pour la machine sur laquelle est positionnée ce droit.

Gérer le journal d'audit et de sécurité
(SeSecurityPrivilege)

Ce droit donne à un utilisateur la possibilité d'audit des accès à des fichiers et des répertoires (ainsi que sur tout autre objet sécurisable du système, comme des clefs de registre). Ce droit ne permet pas d'avoir accès à la stratégie d'audit du système. Lorsque ce droit est donné sur un contrôleur de domaine à un utilisateur d'un domaine Windows NT, celui-ci lui est valide pour tous les autres contrôleurs du même domaine. Lorsque ce droit est accordé sur une machine Windows NT (Workstation ou Serveur) à un utilisateur local d'une machine, celui-ci n'est valide que pour la machine sur laquelle est positionnée ce droit.

Restaurer des fichiers et des répertoires
(SeRestorePrivilege)

Ce droit permet à un utilisateur d'outrepasser les permissions NTFS d'un volume afin de réaliser une restauration des données (à l'inverse du doit de sauvegarder). Lorsque ce droit est donné sur un contrôleur de domaine à un utilisateur d'un domaine Windows NT, celui-ci lui est valide pour tous les autres contrôleurs du même domaine. Lorsque ce droit est accordé sur une machine Windows NT (Workstation ou Serveur) à un utilisateur local d'une machine, celui-ci n'est valide que pour la machine sur laquelle est positionnée ce droit.

Arrêter le système
(SeShutdown-Privilege)

Ce droit permet à un utilisateur de redémarrer le système. Lorsque ce droit est donné sur un contrôleur de domaine à un utilisateur d'un domaine Windows NT, celui-ci lui est valide pour tous les autres contrôleurs du même domaine. Lorsque ce droit est accordé sur une machine Windows NT (Workstation ou Serveur) à un utilisateur local d'une machine, celui-ci n'est valide que pour la machine sur laquelle est positionnée ce droit.

Prendre possession des fichiers ou d'autres objets
(SeTakeOwnershipPrivilege)

Ce droit permet à un utilisateur de prendre possession des objets sécurisables du système, comme des fichiers ou des répertoires. Ce droit est valide même si le propriétaire du fichier a révoqué ce droit à l'utilisateur souhaitant prendre possession de l'objet. Lorsque ce droit est donné sur un contrôleur de domaine à un utilisateur d'un domaine Windows NT, celui-ci lui est valide pour tous les autres contrôleurs du même domaine. Lorsque ce droit est accordé sur une machine Windows NT (Workstation ou Serveur) à un utilisateur local d'une machine, celui-ci n'est valide que pour la machine sur laquelle est positionnée ce droit

6.5.2. Droits avancés

Agir que tant que partie du système d'exploitation
(SeTcbPrivilege)

Ce droit donne à un utilisateur l'accès supplémentaire nécessaire pour utiliser des fonctions, comme si il faisait partie du système d'exploitation. Lorsqu'un utilisateur dispose de ce droit, il aura accès à des parties du système qui lui était jusqu'ici interdites, comme un accès direct à la SAM ou à la partie SECURITY de la base des registres.

Outrepasser le contrôle de parcours
(SeChangeNotifyPrivilege)

Ce droit permet à un utilisateur de traverser des répertoires d'une arborescence NTFS sur lesquels il n'a pas la permission de passage, en vue d'accéder à un fichier sur lequel il dispose de permissions suffisantes. Est utilisé par IIS pour autoriser l'accès sécurisé à une arborescence Web d'un serveur sans que le disque tout entier soit accessible à l'utilisateur. Ce privilège n'est pas auditable.

Créer un fichier d'échange
(SeCreatePagefilePrivilege)

Ce droit donne à un utilisateur la possibilité de créer des fichiers d'échanges (fichier de swap disque). Ce droit n'est pas utilisé dans Windows NT 4.0

Créer un objet-jeton
(SeCreateTokenPrivilege)

Ce droit permet de créer des jetons d'accès. Par défaut, seule la LSA dispose de ce droit. Ce privilège n'est pas auditable.

Créer des objets partagés permanents
(SeCreatePermanentPrivilege)

Ce droit donne à un utilisateur la possibilité de créer des objets partagés permanents, comme \\Device, pour une utilisation interne de Windows NT.

Déboguer des programmes
(SeDebugPrivilege)

Ce droit permet à un utilisateur de déboguer les applications et les services, ainsi que la possibilité de modifier le comportement des threads en temps réel. Le programme d'attaque SECHOLE.EXE exploite ce privilège pour modifier un processus en cours d'exécution. Ce privilège n'est pas auditable. Donner ce droit à un utilisateur revient à lui donner les privilèges d'administration puisqu'il lui est désormais possible de modifier le comportement de processus systèmes (comme le LSASS.EXE).

Générer des audits de sécurité
(SeAuditPrivilege)

Ce droit permet à un utilisateur d'accéder à la stratégie d'audit de sécurité d'un système.

Augmenter les quotas
(SeIncreaseQuotaPrivilege)

Ce droit permet à un utilisateur de positionner et de retailler des quotas de disques. Ce droit n'est pas utilisé dans Windows NT 4.0

Augmenter la priorité de planification
(SeIncreaseBasePriorityPrivilege)

Ce droit permet à un utilisateur d'augmenter la priorité d'exécution d'un processus. Il n'est pas recommandé de laisser ce droit à un utilisateur dans la mesure il est serra alors capable de donner une priorité de type "Temps réel" à un processus, ce qui occupera toutes les ressources CPU tant que le processus ne sera pas achevé.

Verrouiller des pages mémoire
(SeLockMemoryPrivilege)

Ce droit permet à un utilisateur de verrouiller des pages mémoire de sorte que celles-ci ne seront plus atteintes par le mécanisme de "Write Back" utilisé par le fichier de swap (ces pages resteront en mémoire vive).

Ouvrir une session en tant que tâche
(SeBatchLogonRight)

Ce droit permet à un utilisateur de se connecter à un système en utilisant un mécanisme de script. Ce droit n'est pas utilisé dans Windows NT 4.0.

Ouvrir une session en tant que service
(SeServiceLogonRight)

Ce droit permet à un utilisateur de se connecter à un système et de s'enregistrer comme un service Windows NT, ce qui lui donne accès à des sous-systèmes qui ne lui était pas jusqu'ici accessibles. En particulier, ce droit peut être utilisé par un Administrateur pour créer des comptes via des services systèmes comme le service Scheduler.

Modifier les valeurs d'env. de programmation
(SeSystemEnvironmentPrivilege)

Ce droit permet à un utilisateur de modifier les variables d'environnement système, stockées en RAM non-volatile pour les systèmes qui supportent ce type de configuration.

Optimiser un processus
(SeProfSingleProcess)

Ce droit, en conjonction avec le droit SeSystemProfilePrivilege (Régler les performances système), est utilisé pour gérer les performances de Windows NT. Il permet de tester les performances d'un processus.

Régler les performances système
(SeSystemProfilePrivilege)

Ce droit, en conjonction avec le droit SeProfSingleProcess (Optimiser un processus), est utilisé pour gérer les performances de Windows NT. Il permet de tester les performances de tout le système d'exploitation.

Remplacer un jeton niveau de processus
(SeAssignPrimaryTokenPrivilege)

Ce droit permet à un utilisateur de remplacer un jeton d'accès pour un processus, utilisé par le système pour vérifier les permissions sur les objets.

6.6. Sources d'information

6.6.1. Sources CELAR

Sécurité des Systèmes d'information / Réglementation :

Revue de presse SSI du CELAR : contacter M. Daniel ROLLAND au CELAR

Référentiel CASSIOPEE : contacter M. Eric DUPUIS au CELAR/CASSI

CD-Rom réglementation du ministère de la défense : contacter M. Hubert GARDIN au CELAR

Windows NT (Contacter M. Hervé LEGOFF, chef du département SSY du CELAR):

Rapport sur les vulnérabilités liées aux mots de passe

Guide de recommandations pour le paramétrage de Windows NT

Guide de recommandations pour le paramétrage de Lotus Notes

Guide de recommandations pour la sécurisation d'une chaîne Internet / Intranet (IIS / Apache)

Sécurité de Windows 2000 (présentation générale des nouvelles fonctionnalités de Windows 2000).

Guide de paramétrage sécurité Windows 2000

Guide de paramètrage Windows XP

Guide de paramétrage Internet Explorer

6.6.2. Livres

Halte aux Hackers seconde édition(*Hacking Exposed* dans sa version Anglo saxonne)
Auteurs : Stuart McClure - Joel Scambray - George Kurtz
Editeur : Osman Eyrolles Multimedia
ISBN : 2-7464-0292-0
Date de publication : 2001
Prix : 298 F

Au cœur de Windows NT - seconde édition
Auteurs : David A. Solomon
Editeur : Microsoft Press
ISBN : 2840822652
Date de publication : 09/98
Prix : 329 F

La sécurité des Ordinateurs : Guide clandestin
Auteurs : Alexander M.
Editeur : Vuibert
ISBN : 2841809625
Date de publication : 02/97
Prix : 200 F

Microsoft Windows NT : Securité, audit et Contrôle
Auteurs : Coopers, Lybrand
Editeur : Microsoft Press
ISBN : 2840823519

Date de publication : 02/99
Prix : 195 F

Guide pratique de la sécurité sous Windows NT
Auteurs : Tom Sheldon
Editeur : Vuibert
ISBN : 2711786234
Date de publication : 06/98
Prix : 320 F

Ressources d'experts sécurité optimale (avec CD-ROM)
Auteurs : Collectif
Editeur : CampusPress France
ISBN : 2744005010
Date de publication : 05/99
Prix : 369 F

NT Network Security
Auteurs : Strebe Matthew
Editeur : Sybex
ISBN : 0782120067
Date de publication : 05/99
Prix : 439 F

NT Network Security
Auteurs : Collectif
Editeur : Sybex
ISBN : 2736129458
Date de publication : 07/98
Prix : 399 F

Mastering Network Secuity
Auteurs : Brenton Chris
Editeur : Sybex
ISBN : 0782123430
Date de publication : 05/99
Prix : 299 F

Chevaliers d'internet et pirates informatiques
Auteurs : Collectif
Editeur : ???
ISBN : 2863919164
Date de publication : Récent
Prix : 100 F

Cybertraque : la chasse au pirate informatique la plus célèbre des Etats Unis
Auteurs : Shimomura Tsutomu
Editeur : PLON - Presses de la Cité
ISBN : 2259184022
Date de publication : ???
Prix : 139 F

Le nid du coucou (épuisé !)
Auteurs : Clifford Stoll
Editeur : ???
ISBN : ???
Date de publication : ???
Prix : ???

Les Cyberconflits : Internet, autoroutes de l'information et cyberespace : quelles menaces ?
Auteurs : Michel Wautelet
Editeur : Editions Complexes : les Livres du Grip 1998

ISBN : 2870277113
Date de publication : ???
Prix : 69 F

Sécurité et Protection
Auteurs : W. Gieseke
Editeur : Micro Application
ISBN : ???
Date de publication : ???
Prix : 100 F

6.6.3. Internet

La liste des pointeurs suivants n'est fournie ici qu'à titre indicatif, la plupart des sites « non officiels » ont la fâcheuse tendance à être très « volatils ». Il se peut donc que certains sites ne soient plus atteignables à la date de livraison de ce support.

Précisons également que, s'agissant de sources en général non maîtrisées, **il est préférable de ne pas télécharger des applications depuis ces sites pour un emploi opérationnel**. De même, les informations fournies sur ces sites ne sont pas certifiées : il conviendra donc de porter un jugement plus que critique sur celles-ci, et de tenter de vérifier ces informations en croisant les différentes sources.

Ressources Sécurité et Windows NT :

http://www.ntsecurity.net/ (Site entièrement dédié à la sécurité de NT, très à jour, très bien documenté)

http://packetstorm.securify.com/ (Gigantesque base de données sur les vulnérabilités des systèmes - descriptions et « exploits » - un MUST !)

http://www.sysinternals.com/ (quelques outils)

http://www.false.com/security/john/ (John the Ripper)

http://www.antionline.com/ (e-zine sur la sécurité)

http://www.anticode.com/ (e-zine sur la sécurité - orienté logiciels)

http://www.hackersclub.com/km/frontpage/ (site de hackers - pas très à jour)

http://www.rootshell.com/ (base de données sur les vulnérabilités des systèmes - à l'abandon)

http://www.infilsec.com/ (hacking)

http://www.dark-secrets.com/ (hacking)

http://www.zataz.com/ (e-zine sur la sécurité - en français - fonctionne également par mailing list)

http://www.insecure.org/ (hacking)

http://www.ntfaq.com/ (FAQ sur Windows NT très complète)

Sites Commerciaux :

http://www.microsoft.com/ (Site de Microsoft - Incontournable !)

http://www.coppernet.com/ (outils d'administration Windows NT)

http://www.iss.net/ (Site de la société ISS + X Force)

http://www.atstake.com/ (L0phtcrack)

http://www.securitydynamics.com/ (Kane Security Analyst)

6.7. Glossaire

ACL : Access Control List. Liste à contrôle d'accès, utilisée pour positionner des permissions sur des objets.

Adresse IP : Une adresse IP permet d'identifier les postes connectés sur le réseau. Elle se compose de quatre nombres séparés par un point. Chaque nombre peut aller de 0 à 255 (avec quelques contraintes). Généralement, les adresses sont données sous forme symbolique (par exemple www.microsoft.com) et un serveur de nom (nameserver) se charge de transformer l'adresse symbolique en une adresse numérique, comme 165.51.24.2.

Client : Un client est un logiciel demandant des services à un programme situé en local ou à distance qui gère l'information, le serveur. Par extension, la machine sur laquelle fonctionne le logiciel client.

CPU : Control Process Unit. Synonyme de Microprocesseur.

DCOM : Distributed Compatible Object Model. Modèle objet distribué développé par Microsoft, semblable dans ses principes au modèle objet de JAVA.

DNS : Domain Name Server. (Cf. serveur de noms, adresse IP)

Domaine : une entité administrative du point de vue des messages, de l'adressage IP ou des paramètres d'authentification, …

FTP : File Transfert Protocol. Permet de recevoir ou émettre des fichiers sur un site connecté au réseau. Souvent, les sites FTP contiennent des archives du domaine public et sont accessibles de façon anonyme, sans devoir posséder un accès sur le poste distant (anonymous ftp).

Hash : Motif binaire, résultat d'un calcul (généralement cryptographique), appelé Fonction de Hachage, sur un flux d'octets. Permet d'obtenir une empreinte, ou signature, d'un flux d'octets.

HKCC : Acronyme de HKEY_CURRENT_CONFIG

HKCR : Acronyme de HKEY_CLASSES_ROOT.

HKCU : Acronyme de HKEY_CURRENT_USER.

HKLM : Acronyme de HKEY_LOCAL_MACHINE.

HKU : Acronyme de HKEY_USERS.

HTTP : HyperText Transport Protocol. Protocole utilisé pour le transfert des pages web.

Lan Manager : Système de gestion de données partagées sur un réseau, développé à l'origine pour OS/2.

LM Hash : Mot de passe Windows NT sous sa forme chiffrée, calculé avec l'algorithme Lan Manager.

LSA : Local Security Authority, Serveur d'autorité de la sécurité locale. Processus responsable de la stratégie locale de sécurité du système, de l'authentification des utilisateurs et de l'envoi de messages d'audit de sécurité au journal des événements.

Mail / E-mail : Messages électroniques (expéditeur vers destinataire).

MD4 : Fonction de hachage, utilisée pour calculer des empreintes sur un flux d'octets.

NETLOGON : Pour NETwork LOGON. Processus de connexion dans un domaine Windows NT. Egalement le nom d'un volume partagé sur un Serveur Windows NT.

netmask : ou masque de sous réseau, permet de définir un sous-réseau IP (i.e. : @IP 135.51.90.8 + masque 255.255.255.0 => sous-réseau 135.51.90.XXX)

News : Messages publics (expédiés dans un forum pour des lecteurs, qui peuvent commenter ensuite le message et les réponses).

NNTP : Network News Transport Protocol : Protocole de transfert de news utilisant TCP sur le réseau.

NT Hash : Mot de passe Windows NT sous sa forme chiffré, calculé par un algorithme MD4.

PDC/BDC : Principal/Backup Domain Controler, Contrôleur de domaine NT principal/secondaire: Poste sous Windows NT Server (par opposition à NT Workstation pour les postes clients). Il assure au sein de son domaine tous les aspects d'authentification.

Récursif : Voir « Récursif ».

Routeur : Dispositif permettant le passage de paquets entre deux réseaux (ou sous-réseaux).

SAM : Security Account Manager, base de données contenant les noms des utilisateurs, leurs mots de passe chiffrés, les groupes définis…

SAS : Security Attention Sequence. Combinaison de touches (généralement CTRL-ALT-SUPPR), permettant, entre autre, d'ouvrir la boite d'ouverture de session.

Serveur : Logiciel traitant les requêtes des clients et par extension le poste sur lequel tourne le logiciel.

Serveur de noms : Un serveur de correspondance entre adresse IP et nom de machine. On parle aussi de DNS.

SID : Security IDentificator. Identificateur de sécurité.

SRM : Security Reference Database, ou Moniteur de Référence de Sécurité

TCP : Transmission Control Protocol. Protocole offrant une liaison fiable entre deux postes.

TCP/IP : Transmission Control Protocol / Internet Protocol. Ensemble de 2 protocoles qui définit les notions d'adresse de machine, de numéro de port (utilisable pour différencier les protocoles de haut niveau comme ftp, http, etc.), de datagramme (paquet de données). Utilisé sur l'Internet pour établir et maintenir des connexions de bout en bout.

UNICODE : format de codage de caractères étendus, permettant de coder les jeux de caractères internationaux. Dans ce format, les caractères sont codés sur 2 octets.

Volume : disque dur ou répertoire partagé par un serveur.

WWW : World Wide Web. Système d'information distribué et multimédia basé sur le protocole HTTP.

6.8. L'éditeur de stratégie système (Poledit.exe)

6.8.1. Principe de fonctionnement

L'éditeur de stratégie système est un outil fourni en standard dans les versions Serveur de Windows NT. L'objectif initial de cet outil peut être résumé en une seule phrase :

"positionner, lors d'une ouverture de session, un jeu de paramètres prédéfinis dans la base de registres."

Le cœur de l'outil est constitué d'un exécutable, **poledit.exe**, situé sous `%systemroot%\system32`. Le principe de fonctionnement est le suivant :

- Des fichiers particuliers, au format texte et ayant pour extension ADM, sont lus par Poledit. Ces fichiers précisent, à l'aide d'un langage spécifique, les différents paramétrages qu'il est possible de mettre en œuvre.
- Lorsque Poledit est lancé, une interface graphique permet de sélectionner les paramètres qui seront à appliquer lors de l'ouverture de session.
- A partir de ce point, il est alors possible d'écrire directement dans le registre les modifications ou de compiler le tout dans un fichier de stratégie (fichiers POL)
- Dans le second cas de figure, le fichier (généralement NTConfig.pol) doit être placé dans l'arborescence NETLOGON du serveur et cette stratégie sera alors appliquée lors de l'ouverture de session d'un utilisateur

6.8.2. Les fichiers ADM

L'éditeur de stratégie système utilise des fichiers ADM afin de déterminer les valeurs de clefs qui peuvent être modifiées et comment elles doivent être modifiées. Un fichier ADM est un modèle hiérarchique, contenant des catégories et des sous-catégories, indiquant ce qui est modifiable au travers de l'IHM de Poledit.

Les fichiers ADM servant à Poledit définissent donc les jeux de paramètres qu'il est possible de modifier à l'aide de l'outil. Il en existe trois par défaut :

- **Winnt.adm** : fichier de description spécifique à Windows NT
- **Windows.adm** : fichier de description spécifique à Windows 9x
- **Common.adm** : fichier de description des paramètres communs à Windows NT et Windows 9x.

Les chapitres qui suivent expliquent les différentes étapes de la création d'un fichier ADM propre.

6.8.2.1. Sections des fichiers ADM

Les fichiers ADM disposent de 3 sections distinctes :

- Une section définissant les paramètres relatifs à la ruche HKEY_LOCAL_MACHINE (CLASS MACHINE)
- Une section définissant les paramètres relatifs à la ruche HKEY_CURRENT_USER (CLASS USER)
- Une section décrivant les chaînes de caractères utilisées dans l'IHM de poledit ([strings])

(Ce qui suit un point-virgule - ; - dans ces fichiers est considéré comme un commentaire).

Squelette général d'un fichier ADM :

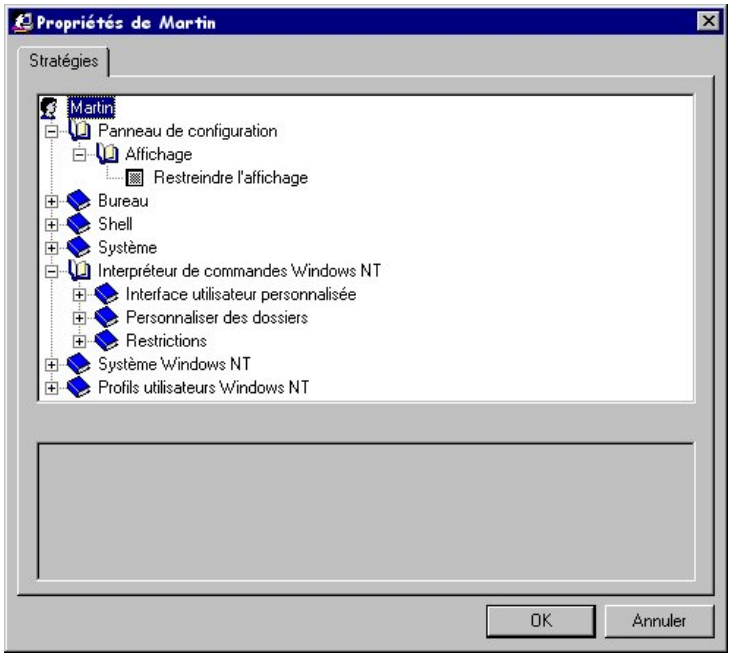
```
; Section pour la ruche HKEY_LOCAL_MACHINE
CLASS MACHINE
…
; Section pour la ruche HKEY_CURRENT_USER
CLASS USER
…
; Section des chaînes de caractères
[strings]
…
```

6.8.2.2. Catégories

Au sein d'une des deux premières sections, on crée une "catégorie" par le mot clef "*CATEGORY*", suivi d'un espace et d'un paramètre sous la forme *!!variable* (où variable représente une chaîne de caractères définie à la section [strings]).

Le mot clef "*END CATEGORY*" indique la fin d'une catégorie.

Dans l'IHM de Poledit, une catégorie apparaît comme un petit livre bleu représentant un nœud d'une arborescence :



A l'intérieur d'une catégorie, il est possible de définir d'autres catégories, afin de créer des sous-catégories (pour gérer une arborescence comme le montre la capture d'écran ci-dessus).

Exemple :

```
CATEGORY !!Categorie1
    CATEGORY !!Categorie2
      CATEGORY !!Categorie3
      ...
      ...
      END CATEGORY ; Catégorie 3
    END CATEGORY   ; Catégorie 2
END CATEGORY      ; Catégorie 1
```

Ne pas oublier ensuite de spécifier les valeurs des variables *!!CategorieX* dans la section [strings] de la manière suivante :

```
Categorie1="Ma première catégorie"
Categorie2="Ma seconde catégorie"
Categorie3="Ma troisième catégorie"
```

6.8.2.3. Keynames

Pour chaque catégorie, il est alors nécessaire de définir quelle clef de registre sera modifiée. Cette opération est réalisé en saisissant le mot clef "*KEYNAME*", suivi d'un espace et du chemin de la clef (relative à la section en cours). Ainsi, pour la section HKLM, on pourra avoir :

```
CATEGORY !!Categorie1
    KEYNAME System\CurrentControlSet\Services\LanManServer\Parameters
    …
END CATEGORY      ; Catégorie 1
```

6.8.2.4. Policies

Au sein d'une catégorie, on définit ensuite une ou plusieurs "policies", qui seront le cœur des paramètres de base de registre à modifier. Cette opération est réalisée en saisissant le mot clef "*POLICY*" suivi d'un espace et de *!!variable*. On termine une policy par le mot clef "*END POLICY*".

```
CATEGORY !!Categorie1
    KEYNAME System\CurrentControlSet\Services\LanManServer\Parameters
    POLICY !!mapolicy1
    …
    END POLICY
    POLICY !!mapolicy2
    …
    END POLICY
END CATEGORY      ; Catégorie 1
```

6.8.2.5. Options de Policy

Dans chaque Policy, on définit alors la ou les valeurs à modifier pour la policy considérée. On utilise pour cela le mot clef "*VALUENAME*", suivi d'un espace et du nom de la valeur encadré par des doubles-quotes :

```
CATEGORY !!Categorie1
    KEYNAME System\CurrentControlSet\Services\LanManServer\Parameters
    POLICY !!mapolicy1
    VALUENAME "mavaleur1"
    …
    END POLICY
    POLICY !!mapolicy2
    VALUENAME "mavaleur2"
    …
    END POLICY
END CATEGORY      ; Catégorie 1
```

Si rien d'autre n'est spécifié, la valeur définie par *VALUENAME* sera de type REG_DWORD et sera positionnée à 1 si la boîte est cochée, et à 0 si elle est décochée.

Si l'on souhaite pouvoir définir d'autres types de données ou de valeurs, ou si l'on souhaite pouvoir saisir soi-même la modification à apporter, ou encore si l'on désire faire des contrôles sur les valeurs à saisir, il est nécessaire de positionner la ligne *VALUENAME* dans une section "*PART !!variable flag"*, terminée par "*END PART*", et de spécifier les options à l'aide du langage :

```
CATEGORY !!Categorie1
```

```
    KEYNAME System\CurrentControlSet\Services\LanManServer\Parameters
    POLICY !!mapolicy1
       ; valeur de type Texte (REG_SZ), champ obligatoire
       PART !!Mapartie EDITTEXT REQUIRED
          MAXLEN 255        ; taille maximale = 255
          DEFAULT "bonjour" ; valeur par défaut="bonjour"
          VALUENAME Mavaleur
       END PART
    …
    END POLICY
END CATEGORY      ; Catégorie 1
```

6.8.2.6. Autres mots-clefs

Le mot clef PART est employé pour spécifier des options, des listes, des textes, etc. dans la partie basse de l'éditeur de stratégie système. La syntaxe de PART est :

```
PART !!Mavariable FLAG

  ...

END PART
```

Dans laquelle FLAG est un (ou plus) des mots clef suivants :

- TEXT - Affiche un texte, par exemple :

```
PART !!MyPolicy TEXT
END PART
```

- NUMERIC - Précise que la valeur est de type numérique (REG_DWORD). Par exemple :

```
PART !!MyPolicy NUMERIC
VALUENAME ValueToBeChanged
END PART
```

- DROPDOWNLIST - Affiche une liste d'options dans une "selection box" :

```
PART !!MyPolicy DROPDOWNLIST
VALUENAME ValueToBeChanged
  ITEMLIST
   NAME “First” VALUE NUMERIC 1
   NAME “Second” VALUE NUMERIC 2
   NAME “Third” VALUE NUMERIC 3
   NAME “Fourth” VALUE NUMERIC 4
  END ITEMLIST
END PART
```

- EDITTEXT - Précise que la valeur est de type texte (REG_SZ) :

```
PART !!MyPolicy EDITTEXT
VALUENAME ValueToBeChanged
END PART
```

- REQUIRED - Génère une erreur si l'utilisateur ne rentre aucune valeur :

```
PART !!MyPolicy EDITTEXT REQUIRED
VALUENAME ValueToBeChanged
END PART
```

- EXPANDABLETEXT - Précise que la valeur est de type REG_EXPAND_SZ :

```
PART !!MyPolicy EDITTEXT EXPANDABLETEXT
VALUENAME ValueToBeChanged
END PART
```

- MAXLEN - Précise la taille maximum d'un texte :

```
PART !!MyPolicy EDITTEXT
VALUENAME ValueToBeChanged
MAXLEN 4
END PART
```

- DEFAULT - Précise la valeur par défaut :

```
PART !!MyPolicy EDITTEXT
DEFAULT !!MySampleText
VALUENAME ValueToBeChanged
END PART
```

ou

```
PART !!MyPolicy NUMERIC
DEFAULT 5
VALUENAME ValueToBeChanged
END PART
```

- MIN et MAX - Précisent les valeurs minimales et maximales d'une valeur :

```
PART !!MyPolicy NUMERIC
MIN 100 MAX 999 DEFAULT 55
VALUENAME ValueToBeChanged
END PART
```

- Utiliser les mots clefs VALUEOFF et VALUEON pour écrire des valeurs spécifiques selon l'état coché ou décoché de l'option :

```
POLICY !!MyPolicy
KEYNAME ....
VALUENAME ValueToBeChanged
VALUEON “Turned On” VALUEOFF “Turned Off”
END POLICY
```

ou

```
POLICY !!MyPolicy
KEYNAME ....
VALUENAME ValueToBeChanged
VALUEON 5 VALUEOFF 10
END POLICY
```

6.8.3. Création et application d'une stratégie système

Après avoir créé ses fichiers ADM, ou après avoir copié les fichiers par défaut sous `%systemroot%\inf`, lancer l'éditeur de stratégie système.

Sous Windows NT, les fichiers Winnt.adm et Common.adm seront systématiquement pris en compte lors du lancement de poledit.

Si l'on souhaite ajouter son propre fichier ADM (ou n'utiliser QUE son propre fichier ADM), on peut aller dans le menu "Options/Exemple de stratégie" et y sélectionner le ou les fichiers ADM que l'on souhaite utiliser.

Ensuite, pour créer une nouvelle stratégie, sélectionner "Fichier/Nouvelle Stratégie".

Par défaut, Poledit génère deux stratégies qui sont applicables à la machine locale et à l'ensemble des utilisateurs. On peut créer une nouvelle stratégie, grâce au menu "Modifier" et qui sera spécifique :

- A un utilisateur,
- A un groupe d'utilisateurs,
- Ou à une machine.

Lorsque l'on double clique sur l'un des éléments de la fenêtre de travail Poledit, l'IHM propose alors une arborescence dont les feuilles sont les différents paramètres à modifier.

Concernant les boîtes à cocher de l'IHM, celles-ci peuvent se retrouver dans trois états distincts :

- Cochée : le paramètre est modifié
- Grisée : le paramètre n'est pas modifié
- Décochée : si la valeur existe, celle-ci est **supprimée**, sinon rien n'est modifié.

Lorsque l'on a paramétré les stratégies systèmes, on sauvegarde alors le résultat dans un fichier portant l'extension POL. Par défaut, et en mode automatique, le fichier doit porter le nom NTCONFIG.POL et être positionné dans le répertoire partagé NETLOGON des serveurs. Lors de l'ouverture de session d'un utilisateur, la machine locale va télécharger le fichier NTCONFIG.POL depuis le serveur et appliquer les jeux de paramètres en fonction du nom de l'utilisateur, de ses groupes d'appartenance et de la machine depuis laquelle il se connecte.

Les paramètres sont d'abord modifiés au niveau de la machine, puis des groupes, puis de l'utilisateur (dans cet ordre). Ainsi, si la même valeur est modifiée au niveau de la machine ET au niveau de l'utilisateur, c'est la valeur modifiée au niveau de l'utilisateur qui sera effective.

Il est également possible d'utiliser un mode de chargement manuel : dans ce mode, le nom du fichier POL à télécharger, ainsi que son chemin d'accès est récupéré dans la base de registre locale d'un poste. Ceci est particulièrement utile pour appliquer une stratégie à une Workstation hors domaine. Pour ce faire :

- Sur la machine locale, en tant qu'administrateur, et avec un éditeur de la base de registre (regedit par exemple), aller sous la clef `HKLM\System\CurrentControlSet\Control\Update`,
- Positionner la valeur "`UpdateMode`" à 2
- Changer (ou créer la valeur si elle n'existe pas) le contenu de la valeur "`NetworkPath`" (de type REG_SZ) en saisissant le chemin complet du fichier POL (exemple : `C:\maconfig.pol` ou `\\serveur\partage\maconfig.pol`).
- Rebooter la machine

Lors de la prochaine ouverture de session, c'est le fichier `maconfig.pol` situé sous `C:\` qui sera alors appliqué.