e-securIT

[Sécurisation d'un système Windows NT 4.0]

[pour l'installation d'un service critique]

http://securit.free.fr

[securIT@free.fr]

TABLE DES MATIÈRES

1. PRÉAMBULE

1.1. OBJET DU DOCUMENT

Ce document présente l'ensemble des étapes nécessaires à la sécurisation d'un système Windows NT 4.0 devant recevoir une application critique. Dans le cas présent, nous considérerons que le système doit accueillir un logiciel firewall.

Quelque soit le type d'application installée sur un système Windows NT, un certain nombre d'actions de sécurisation d'ordre général doit être mis en œuvre afin d'assurer un niveau de confiance suffisant pour un serveur dont la sensibilité est critique.

1.2. AVERTISSEMENTS

Quelques informations essentielles à propos du présent document :

- Ce document présente l'ensemble des étapes à suivre pour sécuriser un serveur devant recevoir une application critique. L'installation et le paramétrage de cette application ne sont pas évoqués dans le présent document.
- Les actions de sécurisations conseillées dans ce document sont valables à la date de rédaction. Elles doivent donc être mises à jour en fonction des vulnérabilités découvertes par la suite.
- Les informations contenues dans ce document proviennent de différentes sources officielles ainsi que des expériences concrètes de mise en œuvre.
- Pour toutes remarques, contacter securit@free.fr.

2. PRÉPARATION POUR L'INSTALLATION

Ce chapitre présente les différentes étapes à exécuter avant toute installation du système d'exploitation sur un serveur sensible.

2.1. ISOLATION DU SYSTÈME AU COURS DE L'INSTALLATION

Au cours de la phase d'installation du système d'exploitation, il est nécessaire de déconnecter la machine du réseau de production et de l'Internet[1].

Cependant, afin de permettre l'installation des composants réseau du système, il est conseillé de connecter la machine en cours de préparation à un réseau de test physiquement isolé.

En outre, aucune personne autre que les responsables de la phase d'installation ne doit pouvoir accéder physiquement ou logiquement (via le réseau par exemple) à la machine ainsi qu'au réseau de test lors de la préparation et de l'installation du système.

2.2. SUPPRESSION DES PÉRIPHÉRIQUES INUTILES

Tout périphérique non nécessaire au fonctionnement de la machine doit être supprimé.

En effet, certains éléments inutiles peuvent compliquer l'installation ou ajouter des vulnérabilités au système, voire parfois atténuer les performances. Ce sont notamment :

- Les contrôleurs et *adapters* : IDE[2], SCSI[3], parallèles…
- Les dispositifs de stockage et les périphériques amovibles (disques durs, CD-ROM, lecteurs de disquettes, dispositifs de sauvegardes…).
- Les interfaces réseau inutilisées.
  Dans le cas d'un firewall, le nombre et la nature des interfaces (Ethernet, Token-Ring, ATM…) doivent être réduits au strict essentiel, d'autant que le système d'exploitation Windows NT n'est pas conseillé pour un nombre d'interfaces réseau excédant quatre (problèmes de performances).

Remarque : dans le cas où l'on supprime les dispositifs physiques de stockage, il est nécessaire de s'assurer de la présence d'un autre moyen permettant la sauvegarde des configurations et des données.

[1] Cette action devrait d'ailleurs être toujours effectuée au cours des opérations importantes d'exploitation (migration de version de logiciel, installation de nouvelles interfaces ou de périphériques, modifications de configuration, opérations de restauration…).

[2] IDE : Integrated Device Electronics.

[3] SCSI : Small Computer Systems Interface.

2.3. INSTALLATION DES COMPOSANTS MATÉRIELS

Après suppression de tous les éléments inutiles, il convient de vérifier la présence des périphériques indispensables à l'installation et au fonctionnement de la machine :

- Dimensionnement de la RAM nécessaire pour supporter le système d'exploitation et les différents logiciels qui seront installés par la suite.
- Disques durs en taille et nombre suffisants pour des configurations éventuelles en reprise sur erreur (2 disques pour RAID[4] 1 et 3 disques pour RAID 5).
- Les cartes réseau nécessaires.
- Un écran compatible VGA et une carte vidéo adaptée.
- Un lecteur de disquette.
- Un lecteur de CD-ROM.
- Un clavier.
- Une souris.

2.4. PRIORITÉS À L'AMORÇAGE DU SYSTÈME

La machine étant hors tension, il est nécessaire de configurer physiquement les cavaliers des différents disques afin de définir les priorités lors de l'amorçage du système.

Il est indispensable de toujours configurer la machine afin que l'amorçage soit réalisé en premier lieu sur le disque supportant le système d'exploitation (disque de *boot*) :

- Pour les interfaces de type IDE :
  - S'assurer que les cavaliers sont disposés sur le disque de *boot* de telle sorte qu'il soit configurer en *master*.
  - S'assurer que le disque de *boot* est relié à la première interface IDE.
- Pour les interfaces de type SCSI :
  - Au cours de la séquence d'amorçage du BIOS, s'assurer que l'identité (SCSI ID) du disque de *boot* est bien définie en première position.
  - Configurer l'interface SCSI pour qu'elle soit prioritaire à l'amorçage. Pour les systèmes supportant à la fois des interfaces SCSI et IDE, s'assurer que les possibilités d'amorçage sur les interfaces IDE sont annulées.

[4] RAID : Redundant Array of Independent Disks.

2.5. CONFIGURATION DU BIOS[5]

Quelques paramètres d'accès à la machine (dépendants du type de BIOS) sont configurables depuis le démarrage du BIOS et permettent un meilleur niveau de protection :

- **Boot Device Order.** Le démarrage doit toujours s'effectuer depuis le disque de *boot* interne. Toujours s'assurer qu'aucun CD-ROM ni aucune disquette ne permet d'amorcer un autre système d'exploitation sur la machine.
- **Remote Boot Capabilities.** Cette option doit toujours être annulée de telle sorte qu'un amorçage depuis un dispositif distant soit impossible.
- **Supervisor Password.** N'importe quel utilisateur peut, par défaut, accéder au BIOS et modifier sa configuration. Un mot de passe pour la supervision du BIOS doit être mis en place et distribué aux seules personnes habilitées.

[5] BIOS : Basic Input Output System.

3. INSTALLATION DE WINDOWS NT 4.0

3.1. RECOMMANDATIONS INITIALES

Quelques éléments importants avant de débuter l'installation du système :

- N'installer que des **versions US** du système d'exploitation (y compris *Service Pack* et *Hot-fixes*) et des différents logiciels.
- Toujours installer le système d'exploitation sur un disque vierge de toute autre installation. **Ne jamais procéder par réparation d'une ancienne version.**
  Dans le même ordre d'idée, si la machine est livrée avec le système pré-installé, il est obligatoire de formater le disque et de réinstaller complètement le système afin de connaître exactement quels dispositifs et services sont mis en œuvre.
- **Ne jamais installer Windows NT depuis un autre système d'exploitation** (Dos ou Windows 95 par exemple).
- La machine étant disposée sur un réseau isolé, il est important, avant de débuter la phase d'installation et de configuration, de s'assurer que tous les éléments nécessaires sont disponibles :
  - Disquette d'amorçage.
  - CD d'installation des différents logiciels et du système d'exploitation.
  - Pilotes des différents périphériques.
  - *Service Pack* et *Hot-fixes*.

  Remarque : veiller à ne disposer que de logiciels en provenance de sources officielles (CD-Rom, disquettes…).
- **Choix du système d'exploitation.** Dans le cas présent, l'installation d'un firewall sur un système Windows NT requiert la version *Server* du système d'exploitation et non *Workstation*.
  Plusieurs raisons imposent ce choix :
  - En standard, la version *Server* permet la gestion des disques en miroir (RAID 1).
  - La version *Workstation* ne supporte que 5 connexions concurrentes par défaut alors que la version *Server* en permet beaucoup plus.
- **Ne jamais installer plusieurs instances du même système d'exploitation.** Certains administrateurs installent une copie de réparation d'urgence de Windows NT sur la même machine. Ceci n'est pas à envisager dans le cadre d'un serveur sensible.

3.2. INSTALLATION

La phase d'installation débute par une interface de commande en ligne :

- Installer le système d'exploitation sur une partition **NTFS** formatée préalablement.

L'interface graphique permet ensuite de définir les différentes options d'installation et de configuration du système :

- Toujours installer un firewall sur une machine Windows NT configurée en mode *Stand-alone*.

- Parmi les composants installés par défaut, **éliminer** *Communications*, *Multimedia* et *Accessibility*.
  Parmi les différents éléments composant l'option *Accesories*, ne conserver que ceux qui seront utiles par la suite.
- Un firewall ne devant faire que du filtrage ou du relayage, **ne jamais installer** d'autre composants serveur tels que *IIS Web Server*.
- **Configuration réseau.**
  Par défaut, le système installe IPX et TCP/IP. **Ne conserver que TCP/IP.**
  Attention : la plupart des firewalls sur Windows NT ne filtrent pas les flux IPX. Dans ce cas, si le système route les paquets IPX, ceux-ci ne seront pas contrôlés par le firewall.
  Retirer la liaison entre TCP/IP et l'interface Netbios. Pour cela, sélectionner l'onglet Liaisons dans la fenêtre réseau et choisir de désactiver la liaison.
- **Services.**
  Par défaut, le système installe *RPC*, *NetBIOS*, *Workstation* et *Server*.
  Ces services ne peuvent pas être désélectionnés ici mais ils le seront par la suite lors de la configuration du système d'exploitation.
  Le seul service pouvant être éventuellement ajouté à cette étape est **SNMP** dans le cadre de l'administration distante du firewall.
- **Configuration de la pile TCP/IP :**
  - Indiquer les différentes adresses IP et serveur de noms DNS pour chaque interface réseau le nécessitant.
    Seule l'interface connectée à l'Internet doit disposer d'une route par défaut.
  - **Ne jamais configurer de serveur WINS ou relais DHCP.**
  - Toujours autoriser l'option *Enable IP forwarding* pour permettre au firewall de router le trafic.
  - La dernière étape précise dans quel domaine ou groupe de travail la machine sera installée. **Dans le cas d'un firewall, toujours choisir un *Workgroup* inexistant dans lequel seule cette machine sera présente.**
- Terminer la phase d'installation puis relancer la machine.

4. CONFIGURATIONS POST-INSTALLATION

4.1. DÉMARRAGE ET ARRÊT DU SYSTÈME

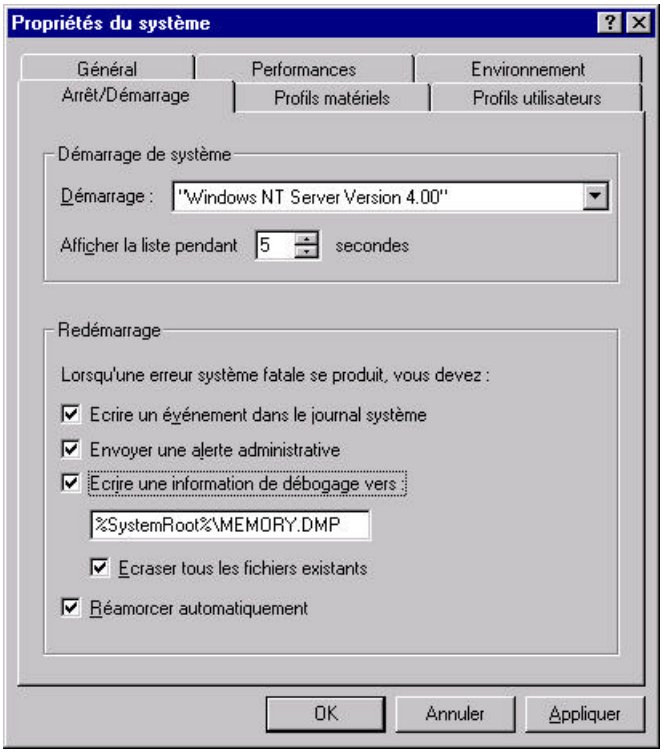

Figure 1 : Propriétés Arrêt/Démarrage du système

Par défaut, le démarrage du système après une durée de 5 secondes de présentation de la liste des boots possibles. Désactiver cette fonction en indiquant la valeur 0 seconde, ou en renseignant la section [boot loader] du fichier c:\boot.ini comme suit :

```
[boot loader]
timeout=0
```

4.2. SÉCURISATION DE L'ENVIRONNEMENT RÉSEAU

4.2.1. Désactivation du filtrage et de la sécurité

Dans la configuration IP approfondie, aucun filtre PPTP ne doit avoir lieu. En outre, la sécurité (filtrage de services TCP/IP) ne doit pas être activé.

Tous ces éléments seront à la charge du logiciel firewall qui sera installé puis paramétré dans ce but.

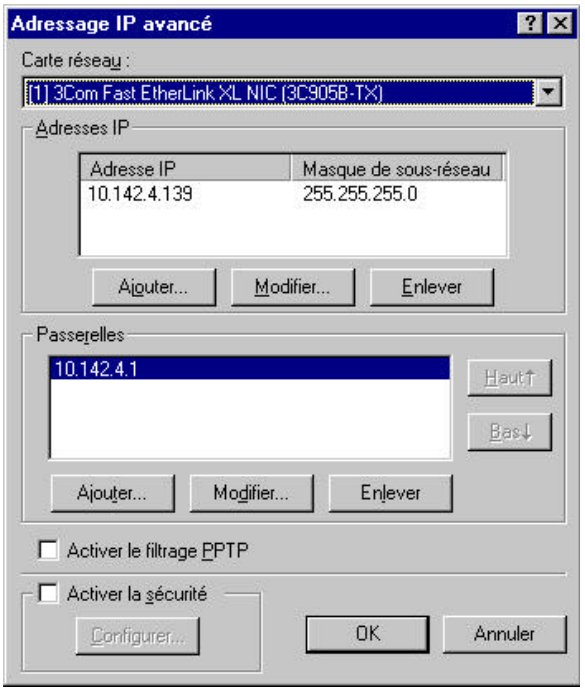

Figure 2 : Configuration IP avancée

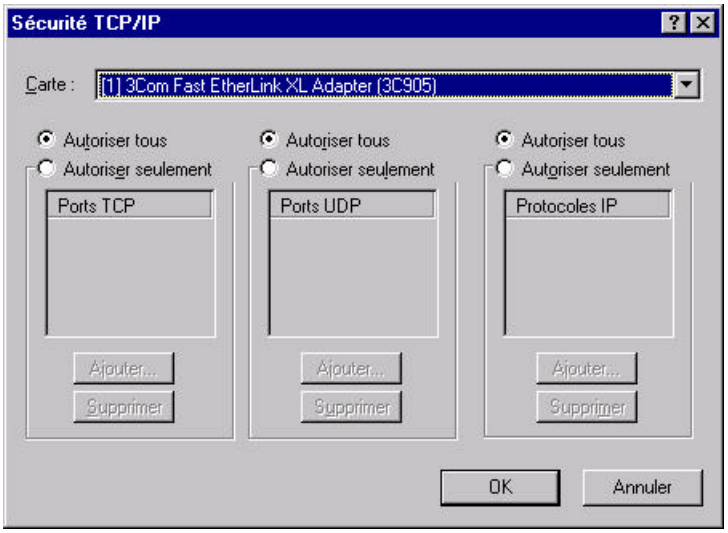

Figure 3 : Configuration des ports et protocoles IP filtrés

4.3. CONFIGURATION DES SERVICES

4.4. SERVICE PACK ET HOT-FIXES

Une fois la phase d'installation du système effectuée, il est nécessaire d'installer les différents éléments complémentaires au système.

Remarques: toujours installer des **versions US** des différents éléments. Ne jamais télécharger les différents éléments (service pack, hot-fixes) depuis le firewall mais depuis des postes de travail sécurisés. D'ailleurs, ledit firewall ne doit pas disposer de navigateur ou tout autre élément logiciel destiné à se connecter sur Internet. En outre, un utilisateur ne doit jamais établir de connexions avec Internet depuis ce firewall, notamment avec un compte disposant de droits administrateur.

4.4.1. Service Pack

Le dernier *Service Pack* en cours pour Windows NT est la version 6a. **Il est donc nécessaire d'installer ce service pack.**

4.4.2. Hot-fixes

Un certain nombre de correctifs post *Service Pack* 6a permettent de régler des failles et vulnérabilités de sécurité.

> Ces correctifs peuvent être téléchargés depuis l'URL suivante :
>
> ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postsp6a

Parmi les différents correctifs, il est nécessaire d'installer notamment :

- *C2-fix (Q241041, Q243404, Q243405, Q244599).*
- *Patch NTLMSSP Privilege Elevation Vulnarability (Q280119).* *http://download.microsoft.com/download/winntsp/patch/q280119/nt4/en-us/q280119i.exe*.

La nécessité d'installer d'autres hot-fixes doit être étudiée au cas pas cas.

Remarque : il est possible de contrôler les fixes déjà installés sur une machine Windows NT grâce à des outils spécifiques gratuits comme SPCheck (téléchargeable à l'adresse http://www.altusnet.com/download.htm). L'outil doit être mis à jour régulièrement afin de prendre en compte les derniers fixes publiés par Microsoft.

4.5. SUPPRESSION DES SERVICES INUTILES

Après l'installation du *Service Pack* et des différents *Hot-fixes*, il est nécessaire d'épurer la configuration du système.

4.5.1. Services réseau inutiles

Comme évoqué précédemment, un certain nombre de services inutilisés sont installés par défaut.

Aucun de ces services n'est nécessaire à une machine faisant office de firewall et ne peut qu'apporter des vulnérabilités supplémentaires. Il convient donc de supprimer les services suivants :

- *RPC Configuration*.
- *NetBIOS Interface*.
- *Workstation*.
- *Server*.
- *Computer Browser*.

Remarque : comme évoqué précédemment, le service *SNMP* peut être activé si l'on désire surveiller l'état du firewall. La fenêtre des services réseau ne contient alors que *SNMP*.

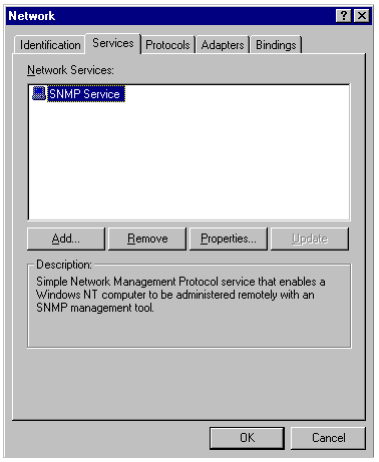

Figure 4 : Fenêtre des services réseau

4.5.2. Autres services à supprimer

4.5.2.1. WINS

Sur chaque interface réseau (*Network Interface Cards*), il faut éliminer les services *WINS* (Network Properties -> Bindings -> All Protocols -> WINS Client (TCP/IP)).

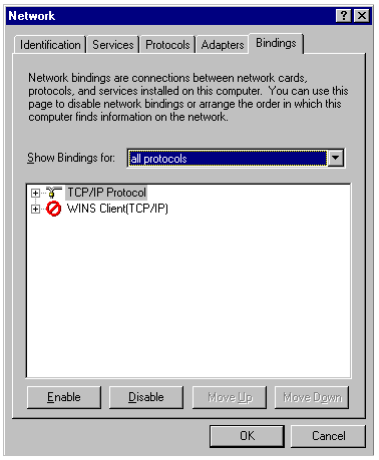

Figure 5 : Suppression du service WINS

4.5.2.2. Menu Services

Enfin, il est nécessaire de vérifier l'ensemble des services démarrés automatiquement à l'amorçage du système, ou manuellement (Settings -> Control Panel -> Services).

A titre d'exemple, certains services à inactiver sont :

- *Plug and Play*.
- *Protected storage*.
- *TCP/IP NetBIOS Helper*.

A chaque autorisation de service, il est nécessaire de se demander pourquoi un tel service est mis en œuvre et si son utilité est essentielle.

Aucun service supplémentaire (*Telnet, FTP, PCAnywhere…*) ne doit être installé sur un firewall.

4.6. COMMANDES CRITIQUES

Déplacer les outils administratifs les plus utilisés dans un répertoire différent de %systemroot% et disposer un contrôle d'accès (*Access List*) n'autorisant le plein accès qu'aux administrateurs. Par exemple, créer un répertoire CommonTools et y placer :

xcopy.exe	wscript.exe	cscript.exe	net.exe	ftp.exe	telnet.exe
arp.exe	edlin.exe	ping.exe	route.exe	at.exe	finger.exe
posix.exe	rsh.exe	atsvc.exe	qbasic.exe	runonce.exe	syskey.exe
cacls.exe	ipconfig.exe	rcp.exe	secfixup.exe	nbtstat.exe	rdisk.exe
debug.exe	regedt32.exe	regedit.exe	edit.com	netstat.exe	tracert.exe
Nslookup.exe	rexec.exe	cmd.exe			

Attention : cette opération doit être envisagée avec prudence car certains firewalls utilisent ces commandes dont le chemin est codé en dur dans leur programme (ex. : Firewall-1 utilise rexec).

Remarque : la variable path peut être modifiée en conséquence afin de prendre en compte cette nouvelle localisation pour les administrateurs. Mais il est préférable que les administrateurs précisent le chemin direct à chaque ligne de commande.

5. GESTION DES UTILISATEURS

5.1. COMPTES

Des modifications doivent être effectuées sur les comptes et les permissions des utilisateurs :

- Désactivation du compte invité (*guest*), choix d'un mot de passe robuste et interdire la possibilité de changement de mot de passe.
- Modification du nom du compte *Administrator*.
- Création d'un compte *Administrator* sans aucun droit et audit de ce compte (group invité).
  Ceci permet de vérifier si quelqu'un essai de se connecter sur la machine en utilisant ce compte par défaut.
- Il est conseillé de ne disposer que d'un seul groupe d'utilisateurs (groupe des administrateurs de la machine).

Rappel important : ne jamais utiliser un système de sécurité pour un usage courant (notamment lorsque l'on utilise un profil avec des droits d'administrateur). En outre, ne jamais utiliser de navigateur depuis une machine dédiée au rôle de firewall pour consulter un site Internet ou télécharger des fichiers (cela revient à contourner les règles de sécurité établies). D'ailleurs, aucun navigateur ne doit être installé.

5.2. RÈGLES ET AUDIT SÉCURITÉ

La gestion des droits utilisateurs se fait à partir de la console *User Manager*, option *Policies*.

5.2.1. Gestion des mots de passe

5.2.1.1. Stratégie de constitution des mots de passe

La politique de gestion des mots de passe des comptes du système doit être robuste. Ainsi, il est nécessaire de forcer la stratégie des mots de passe en installant passfilt. Les mots de passe doivent alors contenir au moins 3 caractères de chacun des types suivants :

- Caractères majuscules (A, B, …).
- Caractères minuscules (a, b… sans les caractères accentués).
- Chiffres arabes (0,1,…,9).
- Caractères spéciaux (ponctuation).

Pour activer passfilt :

- Vérifier que passfilt.dll est présent dans le répertoire \winnt\system32.
- Éditer la base de registre et créer dans HKEY_LOCAL_MACHINE la clé : SYSTEM\CurrentControlSet\Control\LSA\Notification Packages

  Dont la valeur est positionnée à « passfilt ».

5.2.1.2. Sécurisation du stockage des mots de passe

Il est nécessaire de renforcer la sécurité sur le stockage des mots de passe dans le registre en utilisant l'utilitaire syskey.exe (disponible depuis le *Service Pack 3*). Cet utilitaire chiffre les données concernant les mots de passe via une clé à 128 bits. Il est donc nécessaire d'effectuer une déclaration auprès du DCSSI (ex-SCSSI).

5.2.2. Gestion des comptes utilisateurs

Les comptes utilisateurs de la machine doivent suivre une politique rigoureuse :

- Durée de vie :
  - Maximale (*Maximum Password Age*) : 180 jours.
  - Minimale (*Minimum Password Age*) : 1 jours.
- Longueur minimale des mots de passe (*Minimum Password Length*) : 8 caractères.
- Maintien d'un historique (*Password Uniqueness*) de 5 mots de passe.
- Verrouillage des comptes (*Account Lockout*) après 3 tentatives infructueuses.
- Déverrouillage automatique (*Lockout Duration*) au bout de 24 heures.
- Changement des mots de passe utilisateurs à la première ouverture de session (*User must log on in order to change password*).

Remarque : la gestion des comptes utilisateurs s'effectue à l'aide du gestionnaire des utilisateurs (*Users Manager*), menu *Policies*, onglet *Account Policy*.

En outre, il est important de configurer l'ensemble des comptes autorisés à se loguer directement sur le serveur un écran de veille verrouillé après un temps d'inactivité de 10 minutes. L'écran de veille sera choisi *Blank Screen* afin de ne pas consommer de ressources excessives.

5.2.3. Protection du compte administrateur

Il est nécessaire de permettre à l'administrateur de se connecter en interactif tout en étant verrouillé d'un point de vue réseau. Ceci permet de verrouiller le compte administrateur en cas d'attaque en force brut sans provoquer de déni de service sur le compte.

Pour cela, exécuter la commande adminlockout de l'outil Passprop, disponible dans le Ressource Kit de Windows NT.

5.2.4. Règles d'audit (audit policy)

La stratégie d'audit doit permettre de suivre les évènements suivants :

- Succès et échec d'ouverture et de fermeture de session (*Logon and Logoff-Success/Failure*).
- Succès et échec des modifications des stratégies de sécurité (*Security Policy Changes-Success/Failure).*
- Succès et échec des redémarrage et arrêts du système (*Restart, Shutdown, and System-Success/Failure*).

Remarque : la stratégie d'audit est définie dans le gestionnaire des utilisateurs (*Users manager*), menu Stratégie (*Policies*), onglet *Audit*.

5.3. DROITS DES UTILISATEURS

Les différents droits des utilisateurs sur le serveur doivent être adaptés. Pour cela, il convient de modifier les droit avancés des utilisateurs (*Users manager, Policies, User rights*) comme présenté ci-dessous :

POLITIQUE		DROITS
1.	Accéder à cet ordinateur depuis le réseau	Administrators
2.	Agir en tant que partie du système d'exploitation	
3.	Ajouter des stations de travail au domaine	
4.	Sauvegarder des fichiers et des répertoires	Administrators Backup Operators
5.	Outrepasser le contrôle de parcours	
6.	Modifier l'heure du système	Administrators
7	Créer un fichier d'échange	Administrators
8.	Créer un objet-jeton	
9.	Créer des objets partagés permanents	
10.	Déboguer des programmes	Administrators
11.	Forcer l'arrêt à partir d'un système distant	Administrators
12.	Générer des audits de sécurité	
13.	Augmenter les quotas	Administrators
14.	Augmenter la priorité de planification	Administrators
15.	Charger et décharge des pilotes de périphériques	Administrators
16.	Verrouiller des pages mémoire	
17.	Ouvrir une session en tant que tâche	
18.	Ouvrir une session en tant que service	
19.	Ouvrir une session localement	Administrators Backup Operators
20.	Gérer le journal d'audit et de sécurité	Administrators
21.	Modifier les valeurs d'env. de microprogrammation	Administrators
22.	Optimiser un processus	Administrators
23.	Régler les performances système	Administrators
24.	Remplacer un jeton niveau de processus	
25.	Restaurer des fichiers et des répertoires	Administrators Backup Operators Server Operators
26.	Arrêter le système	Administrators Backup Operators
27.	Prendre possession des fichiers ou d'autres objets	Administrators

Il convient de vérifier chaque élément disposant d'un droit d'accès. **En particulier, le groupe « Tout le monde » (*Everyone)* ne doit disposer d'aucun accès.**

5.4. AVERTISSEMENTS DES UTILISATEURS

Il convient d'afficher un message d'avertissement lorsqu'un utilisateur ouvre une session sur le serveur.

Pour cela, éditer le registre et positionner dans HKEY_LOCAL_MACHINE la clé SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\LegalNoticeCaption à « Avertissement » (type REG_SZ).

Dans HKEY_LOCAL_MACHINE, la clé SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\LegalNoticeText doit recevoir pour valeur le message d'avertissement destiné aux utilisateurs.

6. SÉCURISATION DU SYSTEME DE FICHIERS

Remarque : le format de fichier doit nécessairement être NTFS.

6.1. RESSOURCES PARTAGÉES

6.1.1. Préconisations

Aucun élément ne doit être mis en partage sur le serveur, que ce soit le lecteur de disquettes, le lecteur de CD-ROM, et surtout aucun fichier.

Dans le cas ou le service *Server* (nécessaire au partage de ressources) est démarré, tous les éléments partagés (documents ou répertoires) doivent être supprimés :

- Pour vérifier quels sont les éléments partagés en cours, lancer la commande `net share` depuis une fenêtre de commande en ligne.
- Éliminer tous les éléments partagés à l'aide de la commande `net share /d`.
- Il convient également d'éviter tous les partages à but administratif (C$, D$, ADMIN$). Pour ce faire, il est nécessaire de modifier la base de registre :

RUCHE	HKEY_LOCAL_MACHINE\SYSTEM
CLÉ	CurrentControlSet\Services\LanManServer\Parameters
NOM	AutoShareServer
TYPE	REG_DWORD
VALEUR	0

6.1.2. Droits sur les partages éventuels

Dans le cas où un partage de fichiers est imposé par des besoins spécifiques, il convient de restreindre les permissions sur ces partages :

LOCAL GROUP	PERMISSIONS
Authenticated Users	Read
Administrators	Full Control

6.2. PERMISSIONS SUR LES RÉPERTOIRES

Les permissions doivent être appliquées de manière récursive sur l'ensemble des sous-répertoires de chacun des répertoires évoqués dans ce paragraphe.

6.2.1. Partitions

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
Creator / Owner	Read
Authenticated Users	Read
System	Full Control

6.2.2. Répertoires temporaires (\Temp)

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
Creator / Owner	Full Control
Authenticated Users	Full Control
System	Full Control

6.2.3. Répertoire \Program Files

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
Account Operators	Special (All)(None)
Backup Operators	Special (All)(None)
Server Operators	Special (All)(None)
Creator / Owner	Read
Authenticated Users	Read
System	Full Control

6.2.4. Répertoire \Program Files\NTReskit

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
System	Full Control

6.2.5. Répertoire %systemroot% (\winnt)

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
Creator / Owner	Full Control
Authenticated Users	Read
System	Full Control

6.2.6. Répertoire %systemroot%\Repair\

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
System	Full Control

6.2.7. Sous- répertoires %systemroot%\

SOUS-RÉPERTOIRES	LOCAL GROUP	PERMISSIONS
\Cookies	Administrators	Full Control
\Forms	Creator / Owner	Full Control
\History	Authenticated Users	Add / Read
\Occache	System	Full Control
\Profiles		
\Sendto		
\Temporary Internet Files		

6.2.8. Répertoire %systemroot%\system

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
Creator / Owner	Full Control
Authenticated Users	Read
System	Full Control

6.2.9. Répertoire %systemroot%\system32

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
Creator / Owner	Full Control
Authenticated Users	Read
System	Full Control

6.2.10. Répertoire %systemroot%\system32\drivers

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
Creator / Owner	Full Control
Authenticated Users	Read
System	Full Control

6.2.11. Répertoire %systemroot%\system32\config

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
Creator / Owner	Full Control
Authenticated Users	List
System	Full Control

6.2.12. Fichier %systemroot%\system32\config\SecEvent.Evt

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
System	Full Control

6.2.13. Répertoire %systemroot%\system32\spool

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
Creator / Owner	Full Control
Authenticated Users	Read
System Operators	Change
System	Full Control

6.3. PERMISSIONS SUR LES FICHIERS

6.3.1. Fichiers *.bat, *.exe, *.com et *.dll

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
Authenticated Users	Read
System	Full Control

6.3.2. Fichiers exécutables spécifiques

Ceci concerne les fichiers suivants (avec leur localisation par défaut) :

- Policy Editor (\winnt\poledit.exe)
- Registry Editor (regedit) (\winnt\regedit.exe)
- ACL Control (\winnt\system32\cacls.exe)
- File conversion (\winnt\system32\convert.exe)
- DHCP Admin (\winnt\system32\dhcpadmin.exe)
- Event Viewer (\winnt\system32\eventvwr.exe)
- IIS Installation (\winnt\system32\inetins.exe)
- User Manager (local) (\winnt\system32\musrmgr.exe)
- NT Backup (\winnt\system32\ntbackup.exe)
- RAS Administrator (\winnt\system32\rasadmin.exe)
- Emergency Disk (\winnt\system32\rdisk.exe)
- Registry Editor (regedt32) (\winnt\system32\regedt32.exe)
- Remote Boot Manager (\winnt\system32\rplmgr.exe)
- Server Manager (\winnt\system32\srvmgr.exe)
- System Keu (\winnt\system32\syskey.exe)
- System Editor (\winnt\system32\sysedit.exe)
- Trivial FTP (\winnt\system32\tftp.exe)
- User Manager (domain) (\winnt\system32\usrmgr.exe)
- Disk Administrator (\winnt\system32\windisk.exe)
- WinMSD (\winnt\system32\winmsd.exe)
- WINS Administrator (\winnt\system32\winsadmin.exe)

Avec les permissions précisées ci-dessous :

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
System	Full Control

Remarque : le fichier exécutable rollback.exe doit être supprimé.

6.3.3. Fichiers \Boot.ini, \Ntdetect.com, \Ntldr

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
System	Full Control

6.3.4. Fichiers \Autoexec.bat et \Config.sys

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
Authenticated Users	Read
System	Full Control

6.3.5. Fichiers *.ini (sauf boot.ini)

LOCAL GROUP	PERMISSIONS
Administrators	Full Control
Authenticated Users	Read
System	Full Control

7. BASE DES REGISTRES

Remarque importante : avant toute modification, créer une disquette de réparation avec la commande rdisk /s. Toutes les modifications de la base de registre s'effectuent à l'aide de l'utilitaire regedt32.exe et non pas regedit.exe.

7.1. MODIFICATION DES PERMISSIONS

7.1.1. Permissions

Pour chacune des clés listées ci-dessous, les changements suivants doivent être effectués :

- Remplacer le groupe *Everyone* par le groupe *Authenticated Users* et lui donner les permissions suivantes sur les clés :
  - QueryValue.
  - Enumerate Subkeys.
  - Notify.
  - Read Control.
- Hormis lorsque cela est explicitement précisé, ne pas appliquer les permissions sur les sous-clés.

7.1.2. Liste des clés

- Dans la ruche HKEY_LOCAL_MACHINE :
  - \Software (do not replace permissions on existing subkeys).
  - \Software\Microsoft\RPC (et ses sous-clés)
  - \Software\Microsoft\Windows NT\CurrentVersion
  - \Software\Microsoft\Windows NT\CurrentVersion\Profile List
  - \Software\Microsoft\Windows NT\CurrentVersion\AeDebug
  - \Software\Microsoft\Windows NT\CurrentVersion\Compatibility
  - \Software\Microsoft\Windows NT\CurrentVersion\Drivers
  - \Software\Microsoft\Windows NT\CurrentVersion\Embedding
  - \Software\Microsoft\Windows NT\CurrentVersion\Fonts
  - \Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
  - \Software\Microsoft\Windows NT\CurrentVersion\Font Drivers
  - \Software\Microsoft\Windows NT\CurrentVersion\Font Mapper
  - \Software\Microsoft\Windows NT\CurrentVersion\Font Cache
  - \Software\Microsoft\Windows NT\CurrentVersion\GRE_initialize
  - \Software\Microsoft\Windows NT\CurrentVersion\MCI
  - \Software\Microsoft\Windows NT\CurrentVersion\MCI Extensions
  - \Software\Microsoft\Windows NT\CurrentVersion\PerfLib (enlever le groupe *Authenticated Users* et mettre la permission Read access au group INTERACTIV)

- \Software\Microsoft\Windows NT\CurrentVersion\Port (et ses sous-clés)
- \Software\Microsoft\Windows NT\CurrentVersion\Type1<>Installer
- \Software\Microsoft\Windows NT\CurrentVersion\WOW (et ses sous-clés)
- \Software\Microsoft\Windows NT\CurrentVersion\Windows3.1MigrationStatus (et ses sous-clés)
- \System\CurrentControlSet\Services\LanmanServer\Shares
- \System\CurrentControlSet\Services\UPS

➢ Dans la ruche HKEY_CLASSES_ROOT :

- \HKEY_CLASSES_ROOT (et toutes ses sous-clés)

➢ Dans la ruche HKEY_USERS :

- .\DEFAULT

7.2. PROTECTION DE LA BASE DE REGISTRES

Il est nécessaire d'empêcher les accès distants à la base de registre. Seul les administrateurs ont ce droit d'accès distants.

BASE	CLÉ	LOCAL GROUP	PERMISSIONS
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServer			
	Winreg	Administrators	Full Control

En outre, il est également nécessaire de vérifier que la clé Winreg\AllowedPath ne contient ne contient que les valeurs suivantes :

➢ System\CurrentControlSet\Control\ProductOptions

➢ System\CurrentControlSet\Control\Print\Printers

➢ System\CurrentControlSet\Services\Eventlog

➢ Software\Microsoft\Windows NT\CurrentVersion

➢ System\CurrentControlSet\Services\Replicator

7.3. VALEURS DE LA BASE DES REGISTRES

➢ Restriction d'installation d'une imprimante :
Modifier la clé :

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Providers\LanMan Print Services\Servers AddPrintDrivers

de type REG_DWORD et de valeur 1.

➢ Contrôle d'accès à l'observateur d'événements par le réseau (accès réservé aux administrateurs) :
Modifier les clés :

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security

de type REG_SZ et de valeur 1.

- Contrôle de l'accès à distance aux journaux d'évènements :
  Modifier les clés :
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\RestrictGuestAccess
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System\RestrictGuestAccess
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security\RestrictGuestAccess

  de type REG_DWORD et de valeur 1.
- Contrôle de la commande AT (autorisation pour les opérateurs système uniquement) :
  Modifier la clé :
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl

  de type REG_DWORD et de valeur 1.
- Empêcher l'arrêt du serveur lorsque les fichiers de logs sont pleins :
  Modifier la clé :
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\CrashOnAuditFail

  de type REG_DWORD et de valeur 0.
- Interdiction des sessions nulles :
  Modifier la clé :
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RestrictAnonymous

  de type REG_DWORD et de valeur 1.
- Désactivation du support de LanManager :
  Modifier la clé :
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\LMCompatibility

  de type REG_DWORD et de valeur 2.
- Désactivation de la mise en cache des jetons :
  Modifier la clé :
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\CachedLogonsCount

  de type REG_DWORD et de valeur 0.
- Effacement de la mémoire virtuelle (*swap*) à l'arrêt du serveur :
  Modifier la clé :
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager \Memory Management\ClearPageFileAtShutdown

  de type REG_DWORD et de valeur 1.
- Désactivation de la fonction d'AutoRun du CDROM :
  Modifier la clé :
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom\Autorun

  de type REG_DWORD et de valeur 0.
- Désactivation des sous-systèmes PSOIX et OS/2 :
  Supprimer toutes les clé sous :
  - HKEY_LOCAL_MACHINES\SOFTWARE\Microsoft\OS/2 Subsystem for NT

  Supprimer la clé
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\Os2LibPath

Supprimer toutes les valeurs sous la clé :

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Subsystems\Optional

Supprimer toutes les valeurs relatives à OS/2 et POSIX sous la clé :

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Subsystems

Supprimer ensuite le répertoire %systemroot%\system32\os2 et tous ses répertoires, ainsi que les exécutables os2ss.exe et psxss.exe (répertoire %systemroot%\system32).

- Désactivation de l'affichage du dernier utilisateur logué dans la bannière d'ouverture de session :
  Modifier la clé :
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\DontDisplayLastUserName

  de type REG_SZ et de valeur 1.
- N'autoriser que les utilisateurs ayant ouvert une session à redémarrer ou arrêter le serveur :
  Modifier la clé :
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ShutdownWithoutLogon

  de type REG_SZ et de valeur 0.
- Annulation de l'association de l'éditeur de registre avec les fichiers d'extension .reg :
  Éditer la clé :
  - HKEY_LOCAL_MACHINE\Software\Classes\regfile\shell\open\command

  et remplacer regedit par notepad.
- Désactivation de DCOM :
  Modifier la clé :
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Ole\EnableDCOM

  et remplacer la valeur Y par N.
- Désactivation de la génération automatique de noms 8.3 par NTFS (aucune application 16 bits ne doit être installée) :
  Modifier la clé :
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation

  de type REG_DWORD et de valeur 1.
- Audit de l'utilisation du service *Planning* :
  Modifier la clé :
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\Submit Control

  de type REG_DWORD et de valeur 1.

8. MAINTIEN DU NIVEAU DE SÉCURITÉ

Régulièrement, un administrateur doit effectuer un audit et une vérification du niveau de sécurité du firewall :

- Analyse des journaux et des fichiers de log.
- Un certain nombre d'outils dédiés aux opérations d'audit peuvent être utilisés (cf. la boite à outils de e-securIT).
- Des commandes système permettent de vérifier l'état des connexions courantes. A titre d'exemple `netstat –an` renvoie la liste des ports en écoute.
- Abonnement à des listes de distributions relatant les différentes vulnérabilités de sécurité du système (NTBugTraq[6], NTSecurity[7], CERT[8] notamment).
- Suivi des différents *Service Pack* et *Hot-fixes* du système NT[9].
- Exécution régulière de `chkdsk /f` deux fois consécutivement afin d'éliminer les streams NTFS cachés.

6 www.ntbugtraq.com

7 www.ntsecurity.ntadvice.com

8 www.cert.org

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