

Votre nouveau mag technique et culturel de hacking et sécurité informatique

HACKADEMY MAGAZINE

L 12757 - 4 - F: 6,00 € - RD



N° 4 / MAI - JUIN 2006 / DOM : 6,85 euros - Bel : 6,95 euros - CH : 11,50 FS - Can : 9,50 \$CAN - Mar : 45 Dh - May : 8,20 euros

LiveBox • FreeBox • C-Box



Des millions d'utilisateurs piratables par négligence

Sommaire 04

Windows Server 2003 et la sécurité	p.4
Des millions d'usagers piratables par négligence	p.10
Cracké ou pas cracké ?	p.15
Cracker une calculatrice CASIO	p.16
Le chiffre de la France Libre ?	p.20
Surf Session spécial initiation	p.24
Surf Session (suite)	p.26
Réalité augmentée	p.29
Packers et unpackers en C	p.32
Injection PHP par les headers	p.38
Faites parler MySQL	p.42
Coder un espace sécurisé en PHP	p.44
Crypter sans l'avouer	p.48
GCC 3 et les « off-by-one »	p.50
Dossier : Comment régler le Net ?	p.54
À la sortie de l'Assemblée Nationale	p.55
Le périple parlementaire de DADVSI	p.56
Un marché schizophrénique	p. 57
Surveiller les réseaux de P2P	p.60
DEUX PIONNIERS DU CINÉMA ÉLECTRONIQUE	p.62
Voix de la communauté	p.64

Join us !

Forum, chat, blogs...

<http://www.thehackademy.net>

Windows Server 2003

Comment Microsoft se rachète une conduite...



By Artyc

La principale force de Server 2003 est sans aucun doute sa facilité de déploiement. Il paraît donc tout naturel de s'intéresser aux différentes méthodes permettant de rendre cohérente une politique de sécurité dans un tel environnement. Cet article ne sera bien évidemment pas exhaustif car les possibilités offertes par ce système sont extrêmement nombreuses, bien que rarement innovantes.

Général

Les rôles :

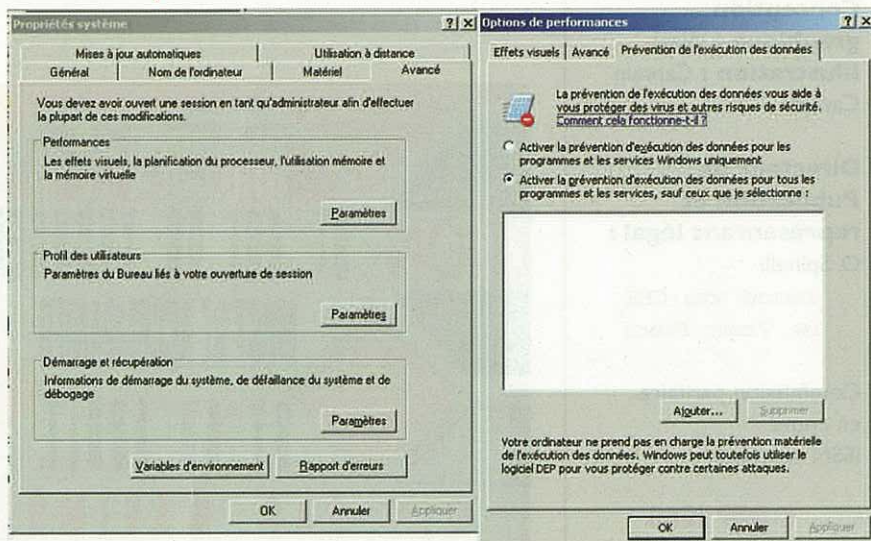
La première règle en matière de sécurité sur un environnement, quel qu'il soit, est bien sûr de ne lui faire faire que ce qui est nécessaire. Plus un système a de services activés, plus il y a de chance que l'un d'entre eux soit vulnérable. Cette règle relevant du bon sens n'est pas pour autant systématiquement appliquée. Il faut dans la mesure du possible répartir les rôles sur plusieurs serveurs. Ainsi la compromission d'un des serveurs, bien que dramatique, le sera d'autant moins que tous les oeufs n'auront pas été mis dans le même panier. Par défaut, tous les rôles (regroupement de services) sont désactivés. Leurs activations/désactivations s'effectuent simplement via le panneau : *Outils d'Administration, Assistant Configurer votre serveur*. Vous pourrez alors ajouter ou supprimer des rôles.

Exploitation de failles de type overflow :

Windows serveur 2003 offre une sécurité contre les exploitations de type « buffer overflow ». La méthode utilisée est similaire à celle de stackguard [1] qui a déjà quelques années mais qui rend l'exploitation d'un buffer overflow [2] beaucoup plus contraignante voir souvent impossible. La technique consiste à placer un canary devant le registre contenant l'adresse de retour qui doit

Les débats font et feront toujours rage à propos de Linux et de Windows. Même si la philosophie de Linux est sans équivoque face à la firme de Redmond, de réelles avancées ont été faites, chez Microsoft notamment sur Windows Server 2003.

Une protection bien connue



Mise en place de la protection DEP

être écrasée pour modifier le comportement du programme. Ainsi l'attaquant écrasera aussi le canary. Avant de « sauter » sur l'adresse de retour, le canary sera vérifié et si sa valeur diffère, le processus sera arrêté. Cette sécurité provient du flag GS activé par défaut lors de la compilation sous Visual Studio .NET. Néanmoins ce mécanisme a été contourné par David Litchfield de NGSSoftware [3].

Une autre protection, très intéressante, permet de rendre extrêmement difficile l'exploitation de Heap Overflow. Pour ceux désirant aller plus loin, se référer à l'article de Carib dans le manuel I2 [4]. Depuis le Service Pack 1, un système DEP (Data Execution Prevention) a été inclus dans Windows. Il prend en charge le mode « No Execute » des derniers processeurs comme par exemple l'Athlon 64, l'Opteron ou l'Itanium 2. Il rend ainsi certaines zones mémoires non exécutables et empêche ainsi d'y loger des shellcodes pendant l'exploitation d'une faille.

Pour vérifier l'activation de cette option, il faut aller dans les propriétés du poste de travail, *Avancé, Performances, Prévention de l'exécution des données*. Dans cet onglet, il est possible d'ajouter des applications pour lesquelles cette protection n'aura pas lieu. Ceci peut être utile car certains programmes peuvent mal supporter ce mode.

Globalement on peut dire que de réels efforts ont été faits en matière de prévention des failles applicatives.

Authentification

N.TLM vs KERBEROS :

Sous tous les systèmes d'exploitation actuels, l'authentification est incontournable (Windows 9x n'est pas actuel...). Sur les machines de technologie NT la pression des touches [Ctrl]+[Alt]+[Suppr] permet généralement de s'authentifier. La combinaison des touches est une sécurité empêchant un programme malicieux de récupérer les utilisateurs et mots de passe.

03 et la sécurité



“Kerberos V5 est désormais utilisé sur windows”

Syskey

Sous windows les informations sur les mots de passe des comptes utilisateurs sont stockés dans la base SAM (Security Accounts Manager). Cette base peut être facilement attaquée et décryptée. L'utilitaire SysKey crypte cette base sécurisant un peu plus le système. Par défaut Syskey utilise un mot de passe généré par le système, enregistre la clé de démarrage localement. Mais il est possible de renforcer la sécurité en utilisant soit un mot de passe demandé à chaque démarrage, soit en utilisant une disquette contenant la clé. Pour faire ces modifications : *Executer, syskey, Mettre à jour.*

Lors d'une authentification, le système consulte une base de données de comptes et valide ou non le couple utilisateur/mot de passe et établit ainsi les droits dont disposera cet utilisateur durant toute sa session. Ceci est valable lors d'une authentification sur une machine locale ou sur un domaine. Si une machine Windows appartient à un domaine, elle pourra choisir son fournisseur de sécurité (l'endroit où elle s'authentifiera) en le sélectionnant dans le menu déroulant *se connecter à*.

Windows Server 2003 supporte (entre autres [5]) deux méthodes d'authentification

qui sont NTLM pour Nt Lan Manager et Kerberos. Ces deux méthodes permettent de faire une authentification en SSO (Signle Sign On) c'est-à-dire qu'une fois enregistré, l'utilisateur n'aura plus à se réenregistrer pour accéder à un autre service réseau. La première est propriétaire et est moins rapide et sécurisée que Kerberos. Cependant ce mode d'authentification est possible quelque soit la version de Windows. Il existe 3 versions de NTLM : LM que l'on retrouve sur les postes sous 95, 98 et NT4 .NTLMV1 qui fut par défaut sur NT4 jusque au service pack 3. Et maintenant NTLM V2 que l'on retrouve sur XP,2000,2003. NTLM utilise un mécanisme de challenge réponse. Il est vraiment préférable d'utiliser Kerberos, mais pour ceux qui désirent tout de même utiliser NTLM vous pouvez le configurer en allant dans *les stratégies ordinateur locales, Stratégies locales, Options de sécurité, Niveau d'authentification LAN Manager.*

Il est conseillé de refuser LM et NTLM v1 et d'autoriser seulement NTLM v2. Si vous disposez encore de machines sous 9x ou NT je vous invite à lire ce document pour les sécuriser et utiliser NTLM v2 [6].

Kerberos V5 est désormais utilisé sur Windows et tend à supplanter NTLM. Hormis le fait qu'il est plus performant que NTLM, celui-ci n'est pas propriétaire et repose sur la RFC1510 [7]. Kerberos utilise un système de ticket à durée limitée, qui empêchera un pirate de conserver l'accès. Le tout repose sur un système de clés privées en chiffrement symétrique. Un autre avantage de Kerberos est qu'il est très simple d'installation sous linux. Il est ainsi possible d'avoir un parc hétérogène basé sur un Active Directory avec une authentification Kerberos. Les utilisateurs pourront alors avoir accès à leur partage, le site intranet ... Quelque soit leur système d'exploitation et ce toujours en SSO.

“Un parc hétérogène basé sur un AD”