Révision 2.0

Benoît HAMET

Microsoft Network Security Hotfix Checker et Microsoft Baseline Security Analyzer

Date de publication : 27 juin 2003

Cet article est une mise à jour d'une précédente rédaction (publiée sur le site de Microsoft [www.microsoft.com/france/WINDOWS/xp/securite/info/info.asp?mar=/france/WINDOWS/xp/securite/info/20020614-checkniveausecurite.html] et sur le site de l'auteur [www.hametbenoit.fr.st/fr/fr_winxpert.htm] ; cette mise à jour prend en compte les nouveautés de la version 1.1 de Microsoft Baseline Security Analyser.

Cette nouvelle mouture de l'outil d'analyse de la sécurité (configuration, présence/absence de correctifs) des produits Microsoft a la possibilité d'analyser la présence des correctifs pour Exchange et Media Player ou la détection de multiples instances SQL Server.

Vous pouvez obtenir une version de MBSA (la version disponible à la rédaction de cet article est la version 1.1) sur le site Web de Microsoft – www.microsoft.com/FRANCE/TECHNET/Themes/SECUR/INFO/info.asp?mar=/FRANCE/TECHNET/Themes/SECUR/INFO/MBSA.html

MBSA ne peut être utilisé pour des vérifications locales que sur les plate-formes Windows 2000 ou XP (utilisant le partage de fichier simple) et enfin sur Windows 2003 Server; par contre, il permet de scanner Windows NT, 2000, XP, 2003, IIS 4 – 5 et 6 SQL Server 7 et 2000, Exchange 5.5 et 2000, Windows Media Player 6.4 et ultérieur, IE 5.01 et ultérieur et Office 2000 et XP.

De plus, vous aurez également besoin d'un parseur XML (pour les utilisateurs de IE antérieur à la version 5.01 – msdn.microsoft.com/downloads/default.asp?url=/downloads/sample.asp?url=/msdn-files/027/001/766/msdncompositedoc.xml pour en obtenir un)

MBSA est un outils beaucoup plus complet que mbsacli /hf vu précédemment ; en effet, mbsacli /hf ne vérifie que l'installation des correctifs tandis que MBSA vérifie également les niveaux de sécurité du système – c'est-à-dire les vulnérabilité de Windows, IIS, Exchange et SQL ainsi que les mots de passe. De plus, MBSA est utilisable à l'aide d'une interface graphique intuitive – une version exécutable en ligne de commande est également disponible (mbsacli.exe)

Nota : pour effectuer l'installation de MBSA, vous devrez avoir les droits administrateurs pour l'installer avec un accès pour tous les utilisateurs

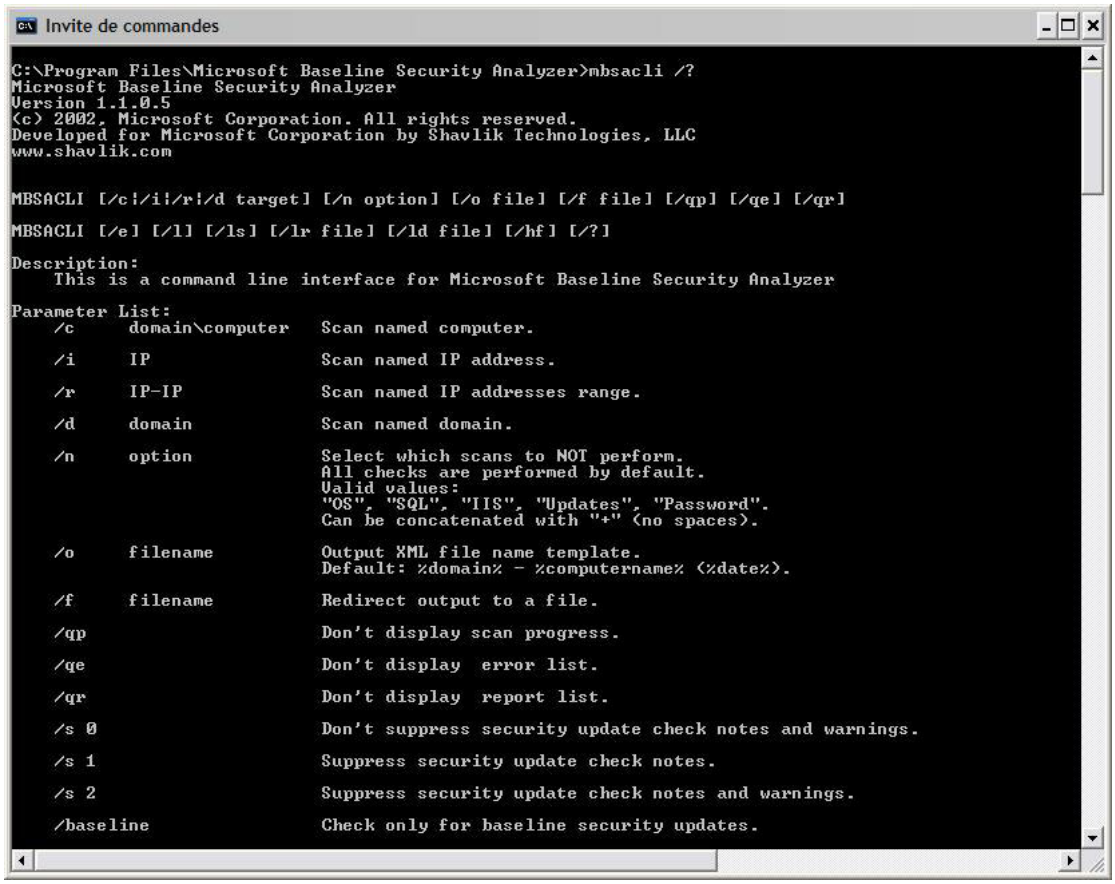

Figure 1 - Utilisation de MBSA en ligne de commande

Nota : à la première utilisation de mbsacli /hf, le logiciel va chercher à obtenir une copie d'un fichier XML « résultat » auprès du Centre de téléchargement de Microsoft ; vous devrez donc, au moins pour cette première exécution, avoir une connexion internet active. Il sera stocké dans le répertoire de lancement de la vérification, vous pourrez ainsi le récupérer pour une utilisation « hors réseau » (sans connexion à internet) ; il contient les informations concernant les patchs de sécurité (nom, plate-forme, numéro d'article de la base de connaissance…)

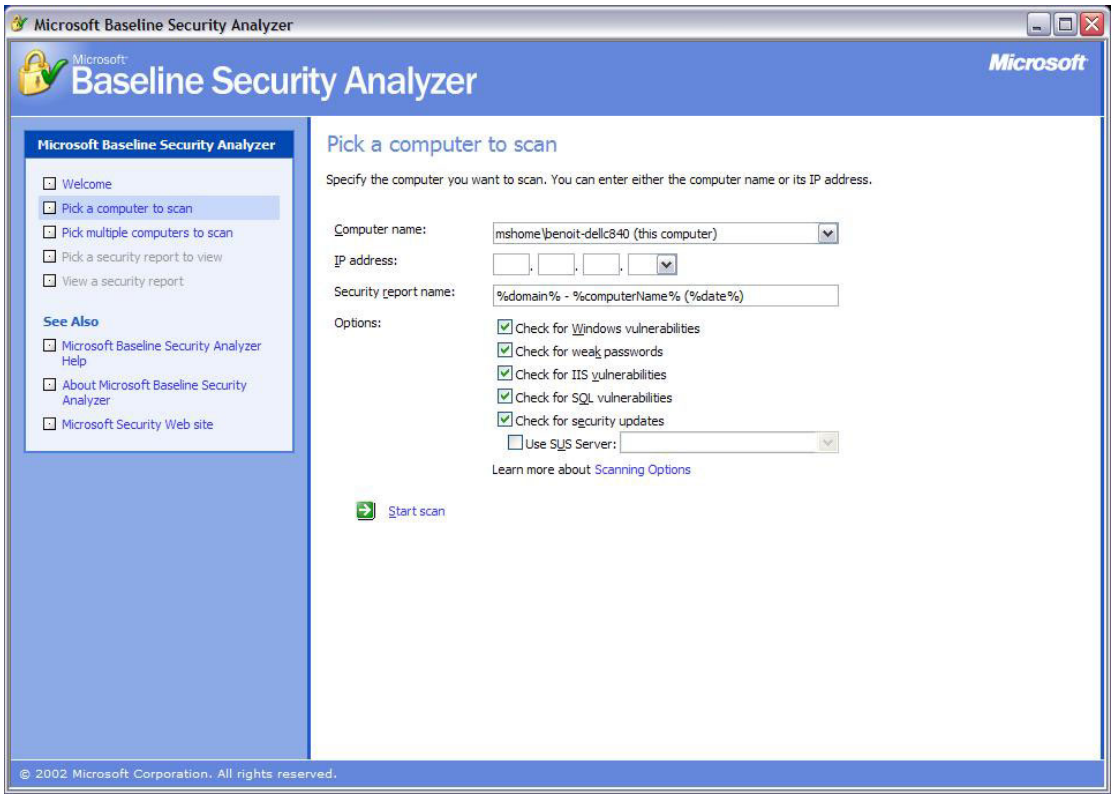

Figure 2 - Utilisation de MBSA avec l'interface graphique

L'utilisation de l'interface graphique de MBSA permet d'effectuer les mêmes vérifications que celles réalisées en ligne de commande.

De plus, vous avez plus facilement accès aux différents rapports ainsi générés.

Pour plus d'informations, n'hésitez pas à accéder aux newsgroups ayant pour sujet la sécurité (sur msnews.microsoft.com choisir microsoft.public.security, microsoft.public.security.baseline_analyser, microsoft.public.security.hfnetcjk, microsoft.public.security.toolkit, microsoft.public.security.virus) et au site sur la sécurité www.microsoft.com/security