



43-45 rue CHARLOT
75003 PARIS

FRANCE
✉ : benoit.hamet@hametbenoit.fr.st

Benoît HAMET

Microsoft Network Security Hotfix Checker et Microsoft Baseline Security Analyzer



*Ou comment vérifier le niveau de
sécurité de votre système informatique*



MS Network Security Hotfix Checker et Microsoft Baseline Security Analyzer

*Ou comment vérifier le niveau de
sécurité de votre système informatique*

Introduction.....	3
Utilisation de MS Network Hotfix Checker	4
Syntaxe d'utilisation de hfnetchk	6
Utilisation de Microsoft Baseline Security Analyzer.....	9
Utilisation de MBSA en ligne de commande.....	11
Utilisation de MBSA avec l'interface graphique	14

Introduction

Avec l'importance croissante de l'outil informatique, la nécessité de maintenir un niveau de sécurité et de disponibilité va croissante tant d'un point de vue personnel que professionnel. C'est pourquoi, afin de répondre à ce besoin, Microsoft propose deux outils, l'un vérifiant les correctifs et autres services pack installés ou manquants, l'autre validant le niveau de sécurité appliqué sur le réseau ou sur une simple station.

Ces outils sont utilisables soit localement soit à travers un réseau local.

Utilisation de MS Network Hotfix Checker

Pour obtenir une version de MS Network Hotfix Checker (hfnetchk), allez sur le site Web de Microsoft – www.microsoft.com/downloads/release.asp?releaseid=31154 – pour télécharger la dernière version (la version applicable au moment de l'écriture de cet article étant la 3.3).

Le MS Network Hotfix Checker va vérifier localement ou à travers un réseau la présence (ou l'absence) des différents correctifs pour les logiciels Windows NT, 2000 et XP, SQL Server 7 et 2000, Internet Information Server 4 et 5, Internet Explorer depuis la version 5 pour NT et 2000 ainsi que le moteur de base de donnée (MS Data Engine) version 1.0.

IMPORTANT : hfnetchk ne permet pas la vérification de poste sous Windows NT 4.0 en langues asiatiques (Japonais, Chinois, Coréen ou Chinois de Hong-Kong)

L'utilisation de cet outil (développé pour Microsoft par Shavlik Technologies) est possible sur les plates-formes Windows NT 4.0, Windows 2000 et Windows XP – donc sur les systèmes dits « professionnels » ; les versions Windows 9x et Millenium n'autorise pas son utilisation. De plus, afin de pouvoir interpréter les résultats, vous devrez avoir un parseur XML (intégré à Internet Explorer depuis sa version 5.01) – pour obtenir un parseur, allez sur le site Web de Microsoft (msdn.microsoft.com/downloads/default.asp?url=/downloads/sample.asp?url=/msdn-files/027/001/766/msdncompositedoc.xml). Ce parseur est nécessaire pour interpréter les informations contenues dans le fichier XML obtenu au premier lancement de hfnetchk.exe auprès du site Web de Microsoft.

Après avoir téléchargé la dernière version du Checker, lancer l'exécutable ainsi obtenu afin de lancer l'installation de l'outil ; cette opération va vous demander où placer les fichiers.

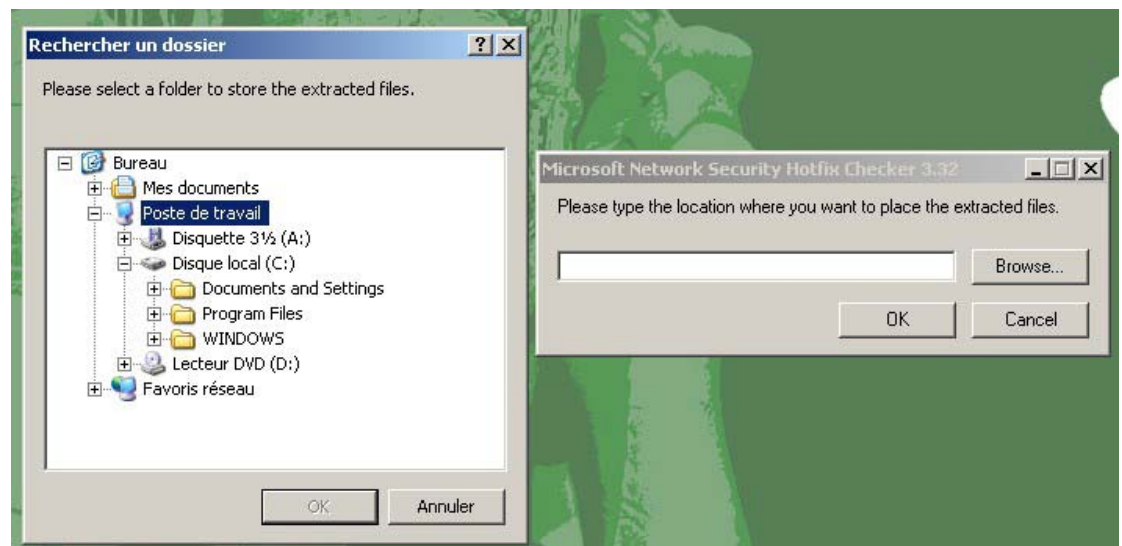
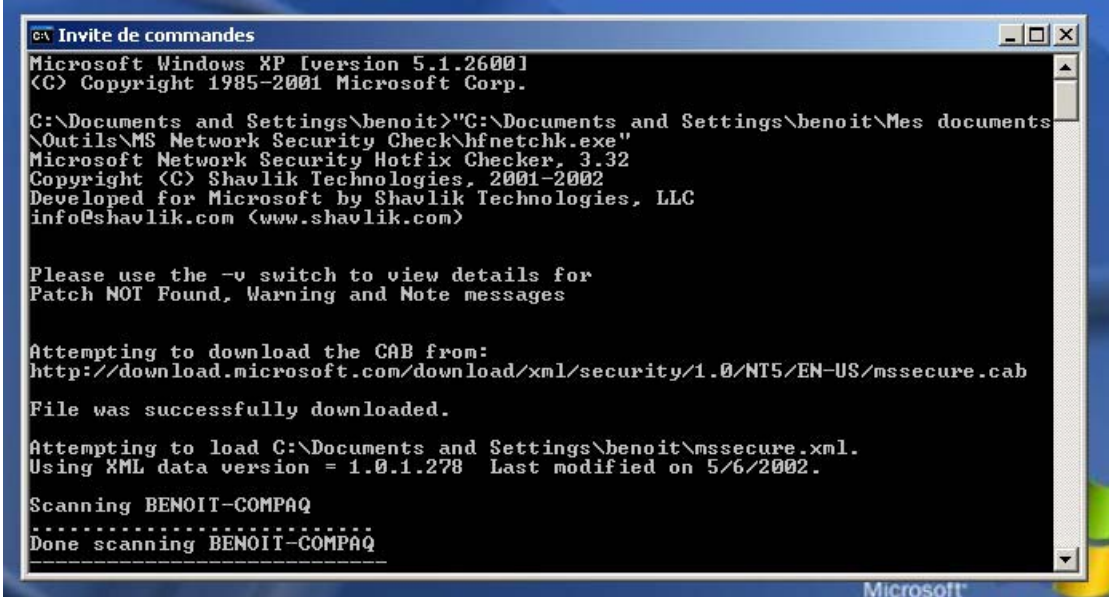


Figure 1 - Installation du Network Security Hotfix Checker

Une fois achevée, vous obtenez 4 fichiers (un exécutable et trois fichiers textes – pour la licence, un pour le mode d'emploi et un autre pour l'update par rapport aux versions précédentes).

Pour lancer l'outil, ouvrez une fenêtre de commande DOS, accédez au dossier dans lequel vous l'avez installé puis lancez l'exécutable (hfnetchk.exe) – ou plus simple, effectuez un « glisser-déposer » sur la fenêtre DOS de l'exécutable – avec les différentes options désirées. Le résultat de la vérification est affiché quelques minutes après.

Nota : à la première utilisation de hfnetchk, le logiciel va chercher à obtenir une copie de ce fichier XML « résultat » auprès du Centre de téléchargement de Microsoft ; vous devrez donc, au moins pour cette première exécution, avoir une connexion internet active.



```
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\benoit>\"C:\Documents and Settings\benoit\Mes documents
\Outils\MS Network Security Check\hfnetchk.exe\"
Microsoft Network Security Hotfix Checker, 3.32
Copyright (C) Shavlik Technologies, 2001-2002
Developed for Microsoft by Shavlik Technologies, LLC
info@shavlik.com (www.shavlik.com)

Please use the -v switch to view details for
Patch NOT Found, Warning and Note messages

Attempting to download the CAB from:
http://download.microsoft.com/download/xml/security/1.0/NT5/EN-US/mssecure.cab
File was successfully downloaded.

Attempting to load C:\Documents and Settings\benoit\mssecure.xml.
Using XML data version = 1.0.1.278 Last modified on 5/6/2002.

Scanning BENOIT-COMPAQ
Done scanning BENOIT-COMPAQ
```

Figure 2 - Première exécution de hfnetchk et obtention du fichier XML auprès de Microsoft

Syntaxe d'utilisation de hfnetchk

Vous pouvez obtenir la liste des options disponibles pour hfnetchk en tapant, dans la commande DOS, « hfnetchk.exe / ? ». Vous trouverez ci-après la liste des switches et leurs propriétés :

hfnetchk.exe [-h hostname] [-i ipaddress] [-d domainname] [-n] [-b] [-r range] [-history level] [-t threads] [-o output] [-x datasource] [-z] [-v] [-s suppression] [-nosum] [-u username] [-p password] [-f outfile] [-about] [-fh hostfile] [-fip ipfile]

- ✚ -h : permet de définir le nom NetBIOS d'un ordinateur à scanner ; par défaut, il s'agit de « localhost ». Vous pouvez lister une série d'ordinateur en séparant leur nom par une virgule. Ex. : hfnetchk -h *ordi1,ordi2,serveur1* va effectuer un scan de « ordi1 », « ordi2 » et « serveur1 »
- ✚ -fh : permet de définir un fichier texte contenant les noms NetBIOS des ordinateurs à scanner. Ce fichier ne peut contenir qu'un maximum de 256 lignes, correspondant chacune à un ordinateur à scanner. Ex. : hfnetchk -fh *ordi_a_scanner.txt* va scanner l'ensemble des hôtes contenus dans le fichier « ordi_a_scanner.txt »
- ✚ -i : permet de spécifier une ou plusieurs adresses IP correspondant aux différents postes à scanner. Ex. : hfnetchk -i *192.168.0.1,192.168.10.2* va scanner les postes ayant pour adresse IP 192.168.0.1 et 192.168.10.2
- ✚ -fip : autorise l'utilisation d'un fichier texte listant l'ensemble des adresses IP à scanner – avec les mêmes limitations que pour le fichier d'hôtes, à savoir un maximum de 256 lignes correspondant chacune à une adresse IP. Ex. : hfnetchk -fip *ipadress_to_scan.txt* va scanner l'ensemble des adresses IP contenues dans le fichier « ipadress_to_scan.txt »
- ✚ -r : définit une plage d'adresse, adresse de début et adresse de fin incluses. Ex. : hfnetchk -r *192.168.0.1-192.168.10.10* vérifie les postes ayant une adresse IP comprise entre 192.168.0.1 et 192.168.10.10 inclus

Astuces :

Vous pouvez combiner les paramètres précédents. Ex. : hfnetchk -h *poste1* -i *172.15.3.3* -r *192.169.0.2-192.169.0.35*

- ✚ -d : précise le domaine à vérifier. Tous les postes du domaine (ensemble des postes apparaissant dans le Voisinage réseau sous le nom de domaine choisi) seront scannés.

Attention : pour les réseau TCP/IP, UDP doit être supporté

Ex. : hfnetchk -d *mondomaine*

- ✚ -n : en utilisant ce paramètre, vous vérifiez l'ensemble des postes du réseau local – il est similaire à -d pour le domaine –, mais, ici, tous les postes apparaissant dans le Voisinage réseau seront vérifiés. Ex. : hfnetchk -n
- ✚ -history : retourne les *hotfixes* explicitement installés – c'est-à-dire installés de manière individuelle et non par le biais de service pack –, manquants ou

les deux. Ce paramètre n'est pas utile pour une utilisation courante, sauf cas spécifique.

- 1 : affiche les correctifs installés explicitement
- 2 : affiche les correctifs manquants
- 3 : affiche les correctifs installés et ceux manquants

N'utilisez ce paramètre que pour vérifier l'installation individuelle d'un correctif. Les correctifs inclus dans les services packs et autres packages correctifs n'apparaîtront pas comme étant explicitement installés malgré leur installation réelle.

Ex. : `hfnetchk -history 1`

✚ -b : ne vérifie l'installation de correctifs notés « critiques » par le Microsoft Security Response Center. Pour son utilisation, le dernier service pack disponible doit être installé sur le système vérifié.

✚ -t : permet de déterminer le nombre de threads – variant de 1 à 128 ; par défaut, 64 – utilisés durant le scan. Vous pouvez augmenter ou diminuer cette valeur afin d'influer sur la vitesse de l'opération de vérification.

✚ -o : spécifie le format du résultat de la vérification

- tab : utilise le format de délimitation par tabulation – à utiliser si vous vérifiez plus de 255 hôtes et est simple d'utilisation pour l'importation dans un tableur ou une base de données
- wrap : format par défaut

Ex. : `hfnetchk -o tab -f scan.txt` stocke le résultat de la vérification dans un fichier texte « scan.txt », délimité par des tabulations

✚ -x : spécifie le fichier XML contenant les informations des correctifs. La source pouvant être un fichier XML, un fichier XML compressé .cab ou une URL ; par défaut, il s'agit de mssecure.xml obtenu à partir du site Web de Microsoft. Ex. : `hfnetchk -x s:\securite\hotfixinfo.xml` va chercher le fichier hotfixinfo.xml sur le disque réseau s: dans le répertoire securite

Nota : s'il y a un espace dans le chemin d'accès au fichier, vous devrez utiliser les apostrophes.

✚ -s : annule l'affichage des messages « NOTE » et « WARNING » – par défaut, tous les messages sont affichés

- 1 : supprime seulement les messages « NOTE »
- 2 : supprime les messages « NOTE » et « WARNING »

✚ -nosum : n'effectue pas la vérification des checksum de validation des correctifs – les checksum étant réalisés sur des machines en langue anglaise, leur vérification sur des systèmes n'utilisant pas l'anglais peut produire des erreurs de checksum.

La version actuelle de hfnetchk détecte automatiquement la langue et n'effectue pas ce contrôle pour les systèmes « non anglais ».

✚ -z : n'effectue pas la vérification de la base de registre ; chaque correctif possédant une clé de registre spécifique, hfnetchk vérifie la présence de cette

clé pour déterminer l'installation d'un correctif – dans le cas où la clé est absente, le correctif n'est pas installé. Sachant qu'un correctif est considéré comme manquant dès lors qu'il y a au moins un échec sur les vérifications du registre, la version du fichier ou le checksum de validation, et que certains correctifs peuvent ne pas avoir de clé de registre spécifique bien qu'étant installés ; dans ces conditions, il est utile de ne pas effectuer cette vérification de registre

- ✚ -v : indique pourquoi un correctif est indiqué comme manquant ou lorsque vous recevez un message
- ✚ -f : spécifie le fichier où sera stocké le résultat des vérifications ; à utiliser combiné avec le paramètre -o pour spécifier le format du fichier
- ✚ -u : spécifie l'utilisateur à utiliser pour effectuer la vérification localement ou via un réseau local ; **à utiliser avec le paramètre -p** spécifiant le mot de passe associé à l'utilisateur. Ex. : `hfnetchk -d mondomaine -u mondomaine\admin -p password` va scanner tous les postes du domaine « mondomaine » en utilisant l'utilisateur « admin » de « mondomaine » et le mot de passe associé « password »

Vous pouvez, bien entendu, mixer les paramètres afin de répondre au plus près à vos besoins.

Exemples :

- ✚ `hfnetchk -v -z -x mssecure.xml` vérifie les correctifs manquants et nécessaires sur l'hôte local en ignorant les clés de registre et en affichant les raisons pour lesquelles un correctif est considéré comme manquant ; la vérification utilisera le fichier local `mssecure.xml`
- ✚ `hfnetchk -x « c:\path name\mssecure.xml »` ; `hfnetchk` utilisera le fichier « `mssecure.xml` » situé localement dans `c:\path name` lors de la vérification du poste local
- ✚ `hfnetchk -d domaine -history 1 -u domaine\administrateur -p password -o tab -x c:\hotfixes.xml` vérifie l'installation explicite des correctifs sur l'ensemble des postes de « domaine » en utilisant l'utilisateur « `domaine\administrateur` » et son mot de passe associé « `password` », le résultat étant renvoyé dans un fichier tabulé et utilisant le fichier « `hotfixes.xml` » situé dans `c:\`

Dans le cas où il serait détecté que des correctifs vous manquent, je vous propose de télécharger un outil de Microsoft permettant d'installer plusieurs correctifs à la suite sans avoir les redémarrages intermédiaires (www.microsoft.com/downloads/release.asp?ReleaseID=29821)

Utilisation de Microsoft Baseline Security Analyzer

Vous pouvez obtenir une version de MBSA (la version disponible à la rédaction de cet article est la version 1.0) sur le site Web de Microsoft – www.microsoft.com/FRANCE/TECHNET/Themes/SECUR/INFO/info.asp?mar=/FRANCE/TECHNET/Themes/SECUR/INFO/MBSA.html – **attention**, contrairement à hfnetchk, MBSA ne fonctionne que sous Windows 2000 et XP – par contre, il permet de scanner Windows NT, 2000, XP, IIS 4 et 5, SQL Server 7 et 2000, 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/msdncompositdoc.xml pour en obtenir un)

MBSA est un outils beaucoup plus complet que hfnetchk vu précédemment ; en effet, hfnetchk 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 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)

Une fois téléchargée la version disponible de MBSA, lancez le package d'installation. Outre l'éternelle demande d'agrément de la licence utilisateur, il vous sera demandé qui aura le droit d'utiliser MBSA, l'utilisateur courant ou tous les utilisateurs du poste sur lequel il sera installé.

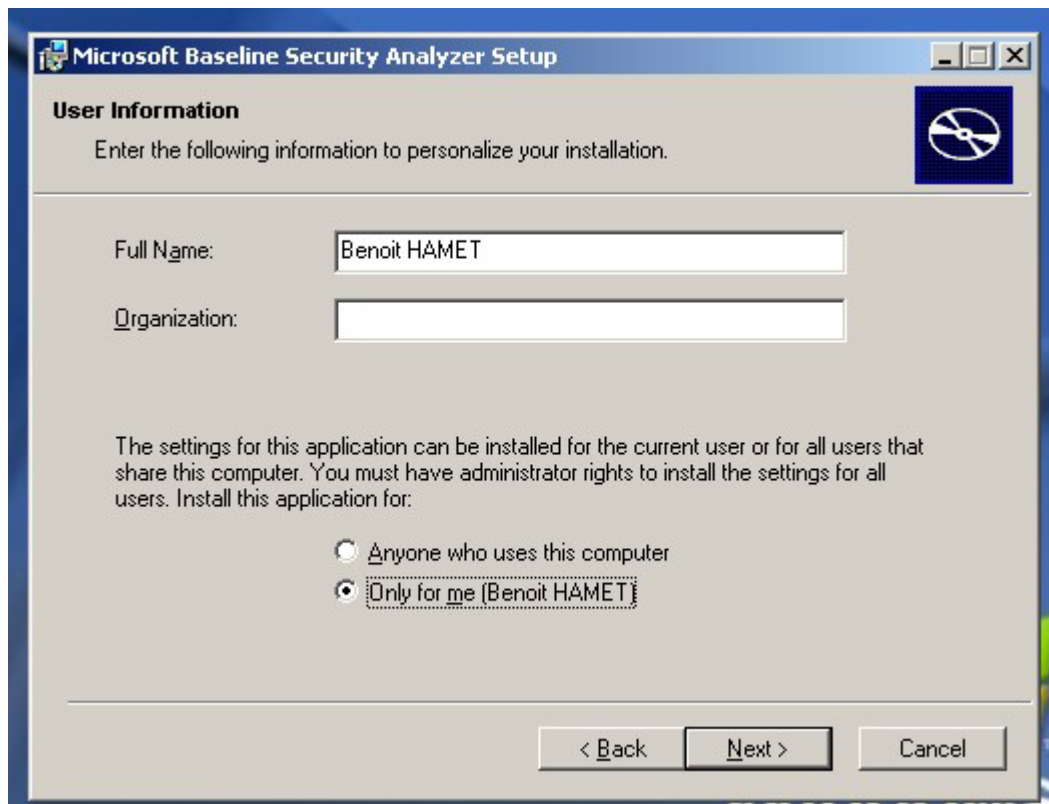
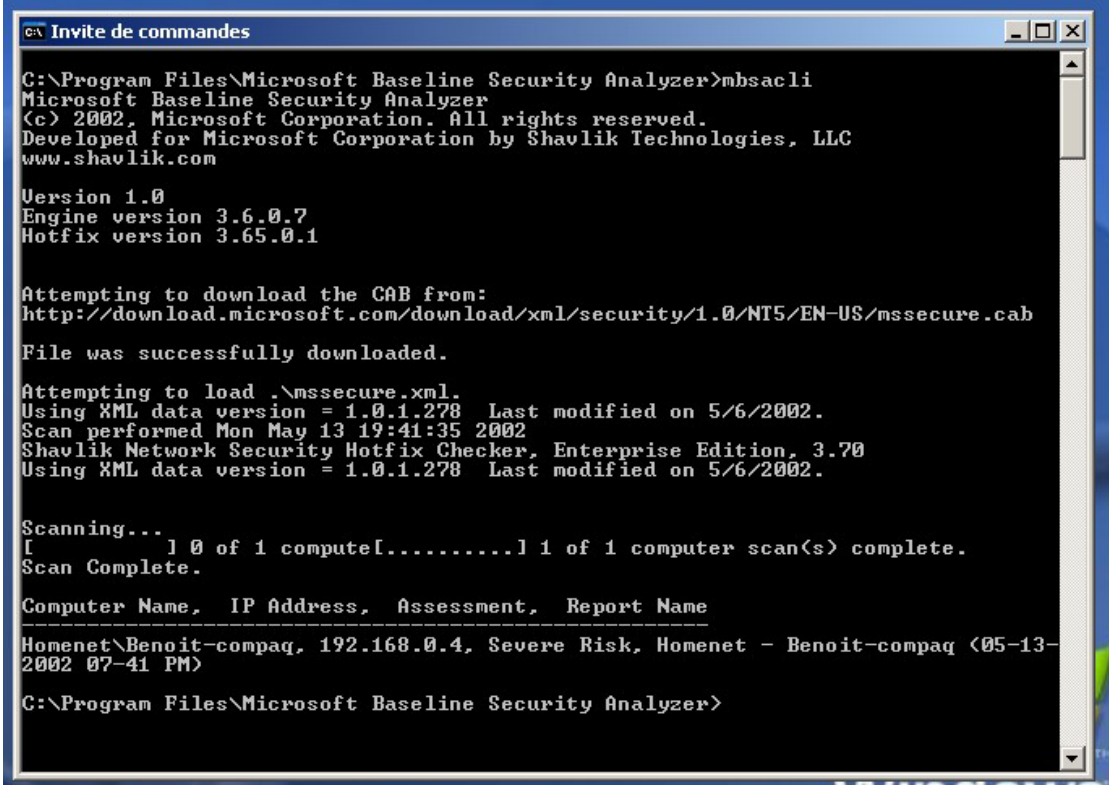


Figure 3 - Installation de MBSA

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

Ensuite l'installation se poursuit en vous demandant l'emplacement destination du programme ainsi que les différentes options à installer – ce qui est largement superflu puisqu'il n'y a pas d'options. Enfin, avant d'exécuter et finaliser l'installation, il vous est demandé ce qu'il faudra faire une fois l'installation achevée (création d'un raccourci sur le bureau, lire le fichier readme.txt et lancer l'application)

Utilisation de MBSA en ligne de commande



```
C:\Program Files\Microsoft Baseline Security Analyzer>mbsacli
Microsoft Baseline Security Analyzer
(c) 2002, Microsoft Corporation. All rights reserved.
Developed for Microsoft Corporation by Shavlik Technologies, LLC
www.shavlik.com

Version 1.0
Engine version 3.6.0.7
Hotfix version 3.65.0.1

Attempting to download the CAB from:
http://download.microsoft.com/download/xml/security/1.0/NT5/EN-US/mssecure.cab
File was successfully downloaded.

Attempting to load .\mssecure.xml.
Using XML data version = 1.0.1.278 Last modified on 5/6/2002.
Scan performed Mon May 13 19:41:35 2002
Shavlik Network Security Hotfix Checker, Enterprise Edition, 3.70
Using XML data version = 1.0.1.278 Last modified on 5/6/2002.

Scanning...
[ ] 0 of 1 computer[.....] 1 of 1 computer scan(s) complete.
Scan Complete.

Computer Name, IP Address, Assessment, Report Name
-----
Homenet\Benoit-compaq, 192.168.0.4, Severe Risk, Homenet - Benoit-compaq (05-13-2002 07-41 PM)

C:\Program Files\Microsoft Baseline Security Analyzer>
```

Figure 4 - Utilisation de MBSA en ligne de commande

Syntaxe d'utilisation

- ✚ Sélection des postes à scanner
 - pas d'option vérification du poste local
 - /c *domaine*\ordinateur vérification du poste *ordinateur* du domaine *domaine*
 - /i xxx.xxx.xxx.xxx scan de l'adresse IP
xxx.xxx.xxx.xxx
 - /r xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx vérifie la plage d'adresse
 - /d *domaine* vérification du domaine
domaine
- ✚ Sélection des options à NE PAS vérifier
 - /n IIS ne vérifie pas la sécurité de IIS (correctifs et paramètres de sécurité)
 - /n OS fait la même opération pour le système d'exploitation (correctifs, paramètres des comptes (mot de passe, expiration...)...)
 - /n password ne vérifie pas la force des mots de passe

- /n SQL idem pour SQL Server (rôle des utilisateurs, restriction d'accès, d'exécution...)
- /n Hotfix n'effectue pas la recherche des correctifs manquants

Affichage des résultats

- /e liste les erreurs de la précédente vérification
- /l liste tous les rapports de vérification disponibles
- /ls affiche l'ensemble des rapports du précédent scan
- /lr <nom de rapport> affiche le rapport *nom de rapport*
- /ld <nom de rapport> affiche le détail de la vérification enregistrée sous *nom de rapport*

Autres paramètres

- /? affichage de l'aide
- /qp n'affiche pas l'indicateur de progression
- /qe n'affiche pas les erreurs
- /qr n'affiche pas le rapport
- /q n'affiche ni les erreurs, ni le rapport
- /f redirige le résultat dans un fichier

Notes concernant la vérification

1. Les résultats des vérifications sont enregistrés dans **%userprofile%\SecurityScan** – situé dans **Documents & Settings** ; pour pouvoir éditer, renommer et supprimer les rapports, vous devrez utiliser l'Explorateur Windows.
2. La vérification des mots de passe peut prendre un certain temps, cela dépend du rôle du poste vérifié et du nombre de compte utilisateur présent sur celui-ci. **IMPORTANT** : cette vérification n'est pas effectuée sur les contrôleurs de domaine et réinitialise tout compte bloqué par les stratégies mais pas ceux bloqués manuellement durant l'opération.
3. Les vérifications concernant SQL Server ne s'effectuent que sur la première instance SQL trouvée sur le poste (default) – si **DEFAULT** n'est pas trouvé, la vérification s'effectue sur la première instance détectée. Le support de plusieurs instances SQL est prévu pour une version ultérieure.

4. La version actuelle de MBSA (version 1) peut ne pas être totalement supportée par les systèmes non anglais.
5. MBSA peut renvoyer des erreurs si :
 - a. L'utilisateur effectuant la vérification n'est pas un administrateur local de chaque poste scanné
 - b. L'ordinateur vérifié ne répond pas à un *ping* initial – ce qui peut être causé par une mauvaise adresse IP ou un mauvais nom d'hôte
 - c. Les postes vérifiés les services *Server* et *Remote registry* activés
 - d. IIS n'est pas installé et que MBSA vérifie IIS
 - e. Le poste exécutant MBSA ne possède pas d'accès à Internet – nécessaire pour le téléchargement du fichier XML contenant les informations pour la vérification du système

Utilisation de MBSA avec l'interface graphique

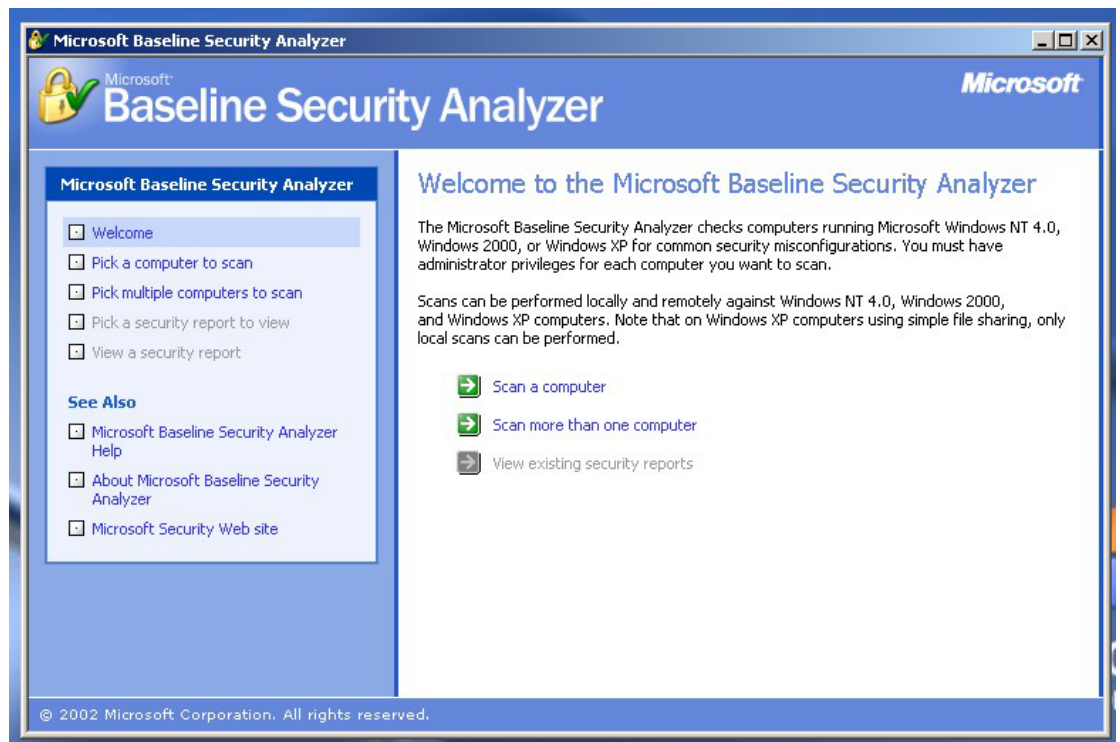


Figure 5 - Utilisation de MBSA avec l'interface graphique

L'utilisation de l'interface graphique de MBSA permet d'effectuer les mêmes vérifications que celles réalisées en ligne de commande avec les paramètres – cependant, il est quand même plus agréable de configurer la vérification d'un système avec les informations complètes plutôt qu'avec des paramètres dont on peut oublier la signification, quand on n'en oublie pas un.

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

Pour plus d'informations, n'hésitez pas à accéder aux newsgroups microsoft.public.security.baseline_analyser (accessible sur le serveur de news msnews.microsoft.com) ; au site sur la sécurité www.microsoft.com/security