N°181

INFO-AIVM37

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer

Présentation du logiciel (MBSA)

Deux versions

Il existe une version 32 bits (x86) et une version 64 bits (x64).
Vous pouvez les télécharger depuis cette page ;
http://www.microsoft.com/downloads/fr-fr/details.aspx?FamilyID=02be8aee-a3b6-4d94-b1c9-4b1989e0900c&displaylang=fr
Attention de bien prendre la version française (car il existe une version en allemand et une en anglais sur la même page. Les versions précédentes fonctionnez parfaitement.

Commentaires Microsoft (trouvés sur le site de Microsoft)

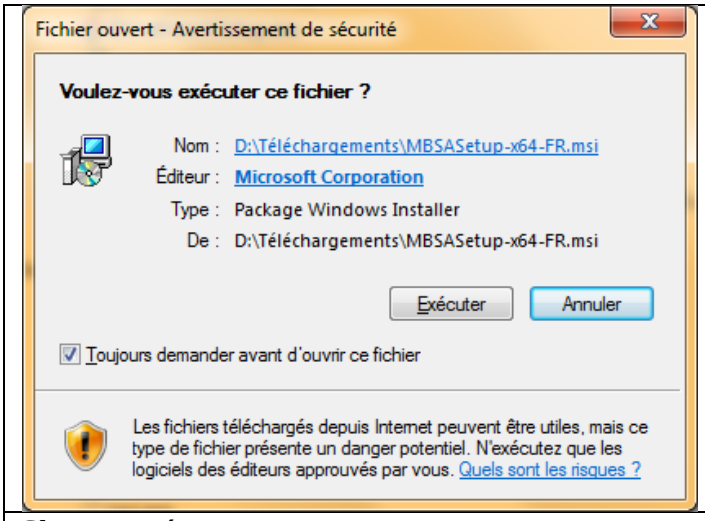
Nouvelles fonctionnalités et améliorations dans MBSA 2.2

- Ajout de la possibilité de choisir le mode hors ligne depuis les interfaces graphique et de ligne de commande
- Ajout de la prise en charge de catalogues de sécurité supplémentaires (pour utilisation ultérieure)
- Ajout/cabpath de l'option de ligne de commande afin d'obtenir des catalogues depuis un répertoire sélectionné par l'utilisateur ou depuis un emplacement réseau
- Correction du retour de secours automatique au mode hors ligne si les serveurs Microsoft Update ou WSUS ne sont pas disponibles
- Suppression du lien de téléchargement dans les rapports d'analyse terminés puisqu'il n'est plus possible d'identifier de manière précise le bon package lors d'un téléchargement en présentant plusieurs
- Suppression de la version du produit dans le chemin de répertoire cache lors de l'utilisation du fichier (CAB) du catalogue hors ligne
- Mise à jour et révision des fichiers d'aide afin de décrire les fonctionnalités nouvelles et corrigées
- Prise en charge de Windows 7et Windows Server 2008 R2
- Mise à jour de l'interface graphique utilisateur
- Prise en charge complète des plateformes 64 bits et des contrôles d'évaluation de vulnérabilité sur les composants et plateformes 64 bits.
- Amélioration de la prise en charge de la plateforme Windows XP Embedded
- Amélioration de la prise en charge des contrôles d'évaluation de vulnérabilité de SQL Server 2005
- Inscription et mise à jour d'agent Microsoft Update automatiques (si sélectionné) à l'aide de l'interface graphique ou à partir d'un outil en ligne de commande à l'aide de la fonctionnalité /ia.
- Nouvelle fonctionnalité permettant de générer des rapports d'analyse complets dans un répertoire sélectionné par l'utilisateur ou sur un partage réseau (fonctionnalité /rd sur la ligne de commande)
- Compatibilité avec les Services WSUS (Windows Server Update Services) 2.0 et 3.0

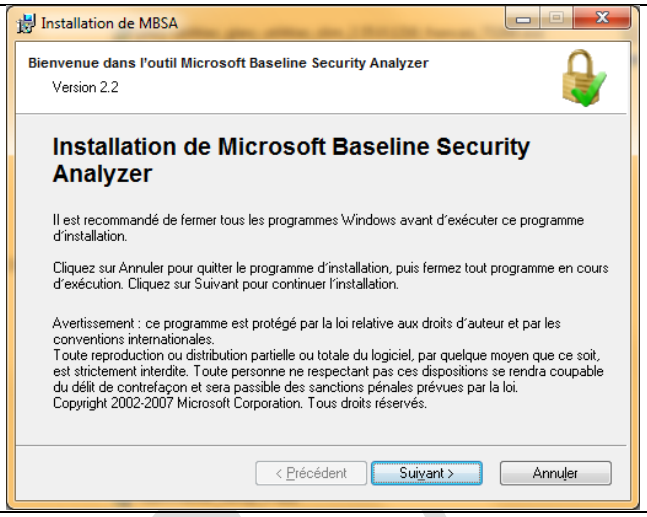
A l'heure présente, sur mon portable, déconnecté d'Internet.

- Cette nouvelle version 64 bits peut rse plante, même en désactivant la recherche avancée de sécurité qui fait appel à Internet. (J'étais hors connexion).
- Impossible de poursuivre l'analyse, la barre de progression se fige au ¾. Impossible de réinitialiser et d'interrompre le processus avec [Alt] [CTRL] [Suppr].
- Impossible de lancer une autre application en parallèle.
- Je suis obligé d'éteindre mon PC « en force ». Voir en page 4, les bons réglages.

Installation sur Windows 7 64 bits

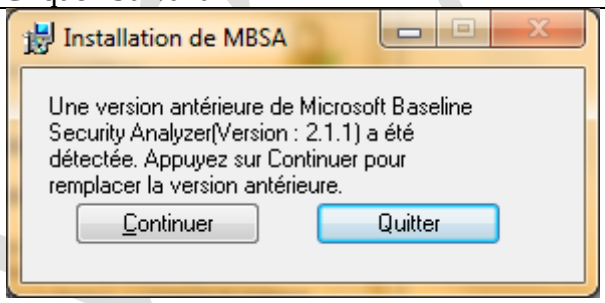


Cliquez Exécuter

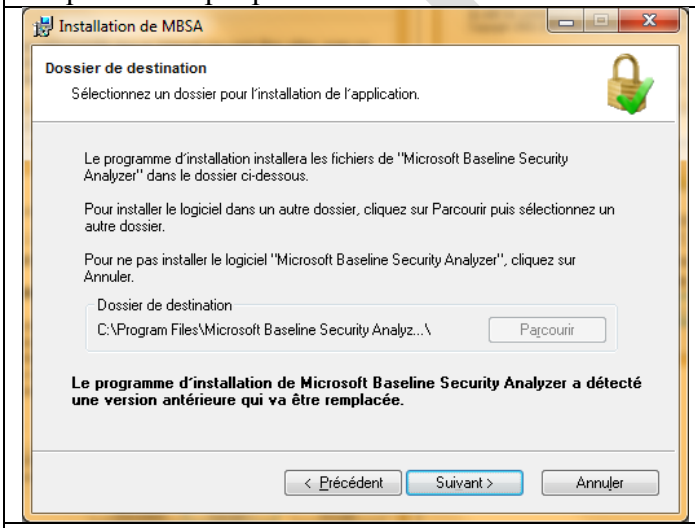


Cliquez Suivant

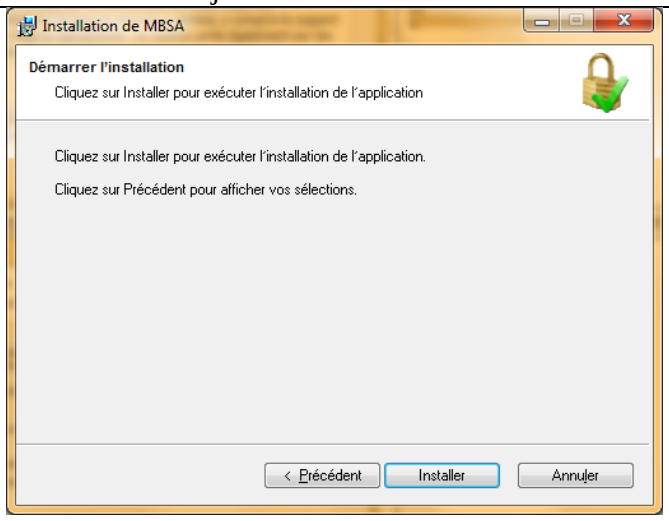
Cliquez J'accepte puis Suivant



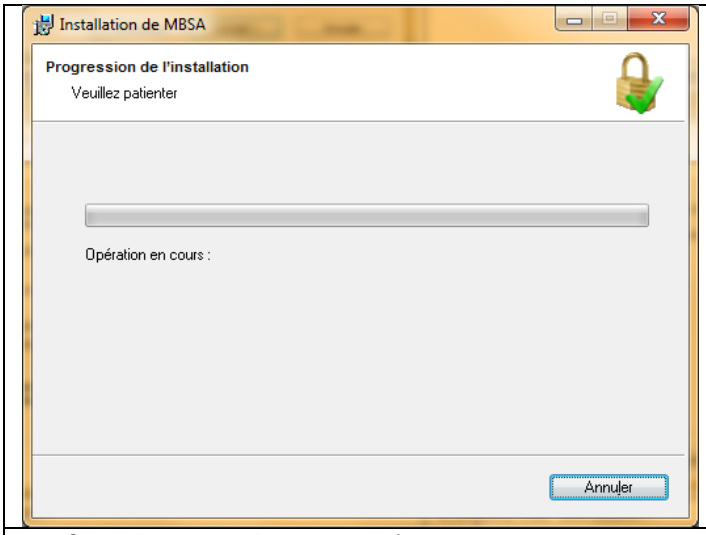
Si vous aviez déjà une version antérieure



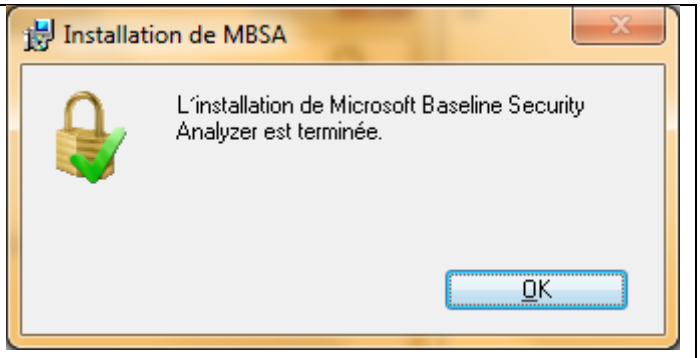
Cliquez Suivant



Cliquez sur Installer



Fenêtre classique de progression…



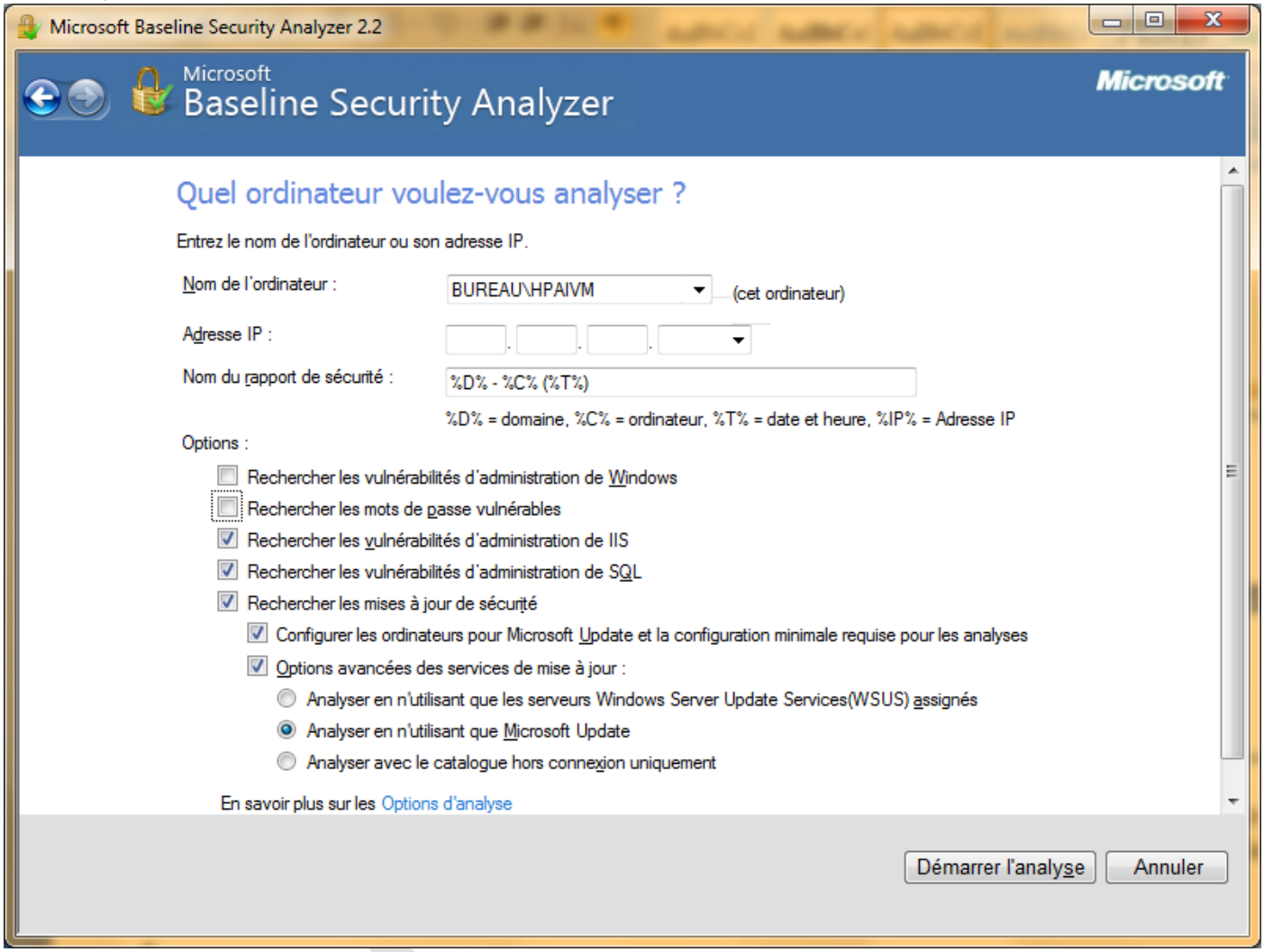
Cliquez OK

Pour créer un raccourci, voici le chemin d'accès
"C:\Program Files\Microsoft Baseline Security Analyzer 2\mbsa.exe"
Je place personnellement se raccourci dans mon répertoire de maintenance. Il se peut que program files soit noté Programmes avec Windows 7 64 bits.

Utilisation

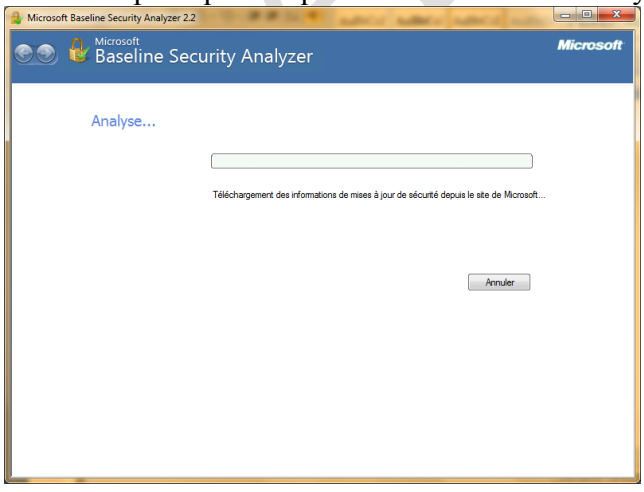
Cliquez sur le raccourci.

Comme vous pouvez le constater, ce logiciel est particulièrement puissant, car il peut depuis un poste analyser tout un réseau. Génial, non ? Je choisis personnellement « Un ordinateur » et j'obtiens la fenêtre suivante ;



Voici les réglages que j'ai personnellement choisis, mais c'est à voir selon les cas et les configurations, car avec cette configuration le logiciel s'est planté (voir la suite). Personnellement, je sais que certains de mes mots de passe associés à des choses sans importances sont faibles, mais cela ne me pose pas de problème. Je risque simplement que le pirate paye mes factures à ma place, alors…

Il ne reste plus qu'à cliquer sur « Démarrer l'analyse ».



Il suffit d'attendre. Des MAJ de base de données peuvent se faire car j'ai coché ci-dessus Windows update.

Dans la figure ci-dessus, j'ai modifié les réglages, en décochant IIS, SQL et les rechercher des MAJ dans la mesure où je n'étais pas connecté.

Rapport obtenu

Afficher les rapports d'analyse de sécurité existants