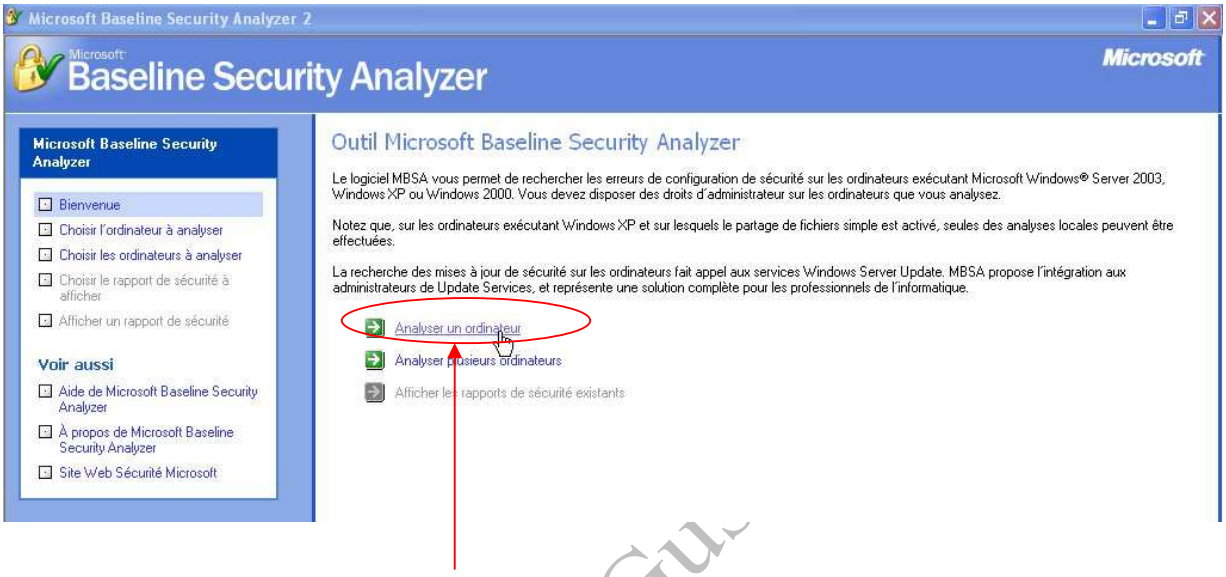
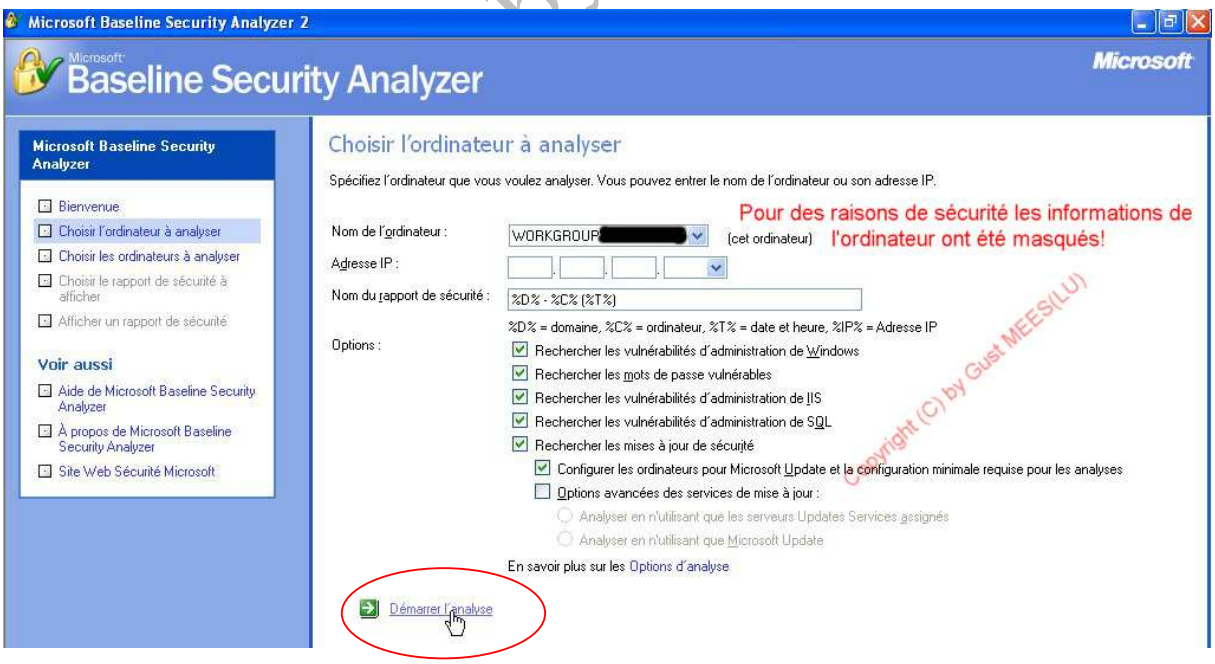
MICROSOFT BASELINE SECURITY ANALYZER 2

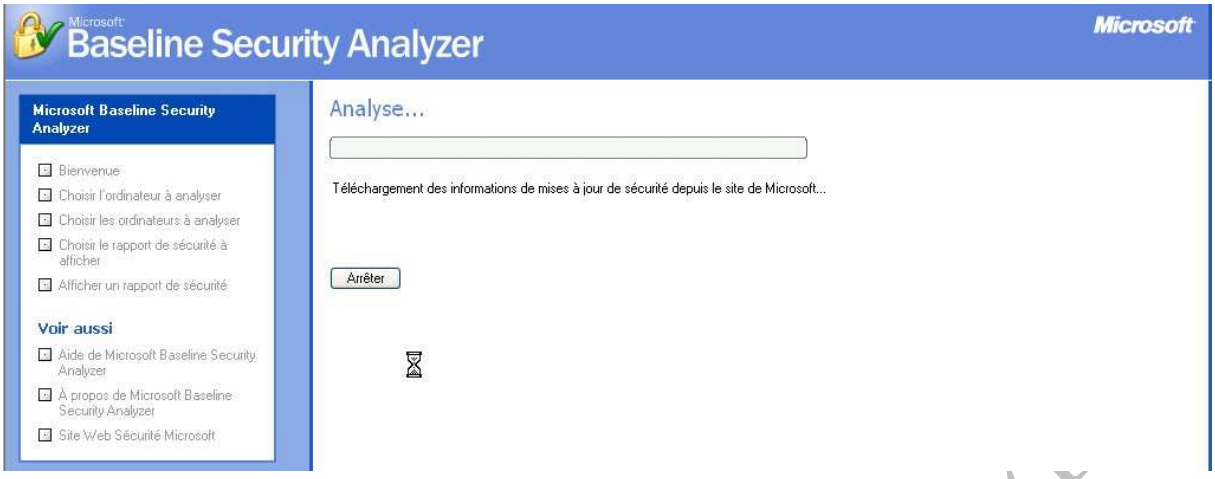
Le „**MBSA**“ de chez **MICROSOFT®** est un outil d'analyse de sécurité de votre ordinateur. Le logiciel **MBSA** vous permet de rechercher les erreurs de configuration de sécurité sur les ordinateurs exécutant **MICROSOFT WINDOWS® SERVER 2003**, **WINDOWS XP** ou **WINDOWS 2000**. **Vous devez disposer des droits d'administrateur sur les ordinateurs que vous analysez !**



Pour utiliser le „**MBSA**“ vous devez être connecté à Internet. Après lancement du logiciel, veuillez suivre le lien „**Analyser un ordinateur“**, comme montré sur la figure ci-dessus.

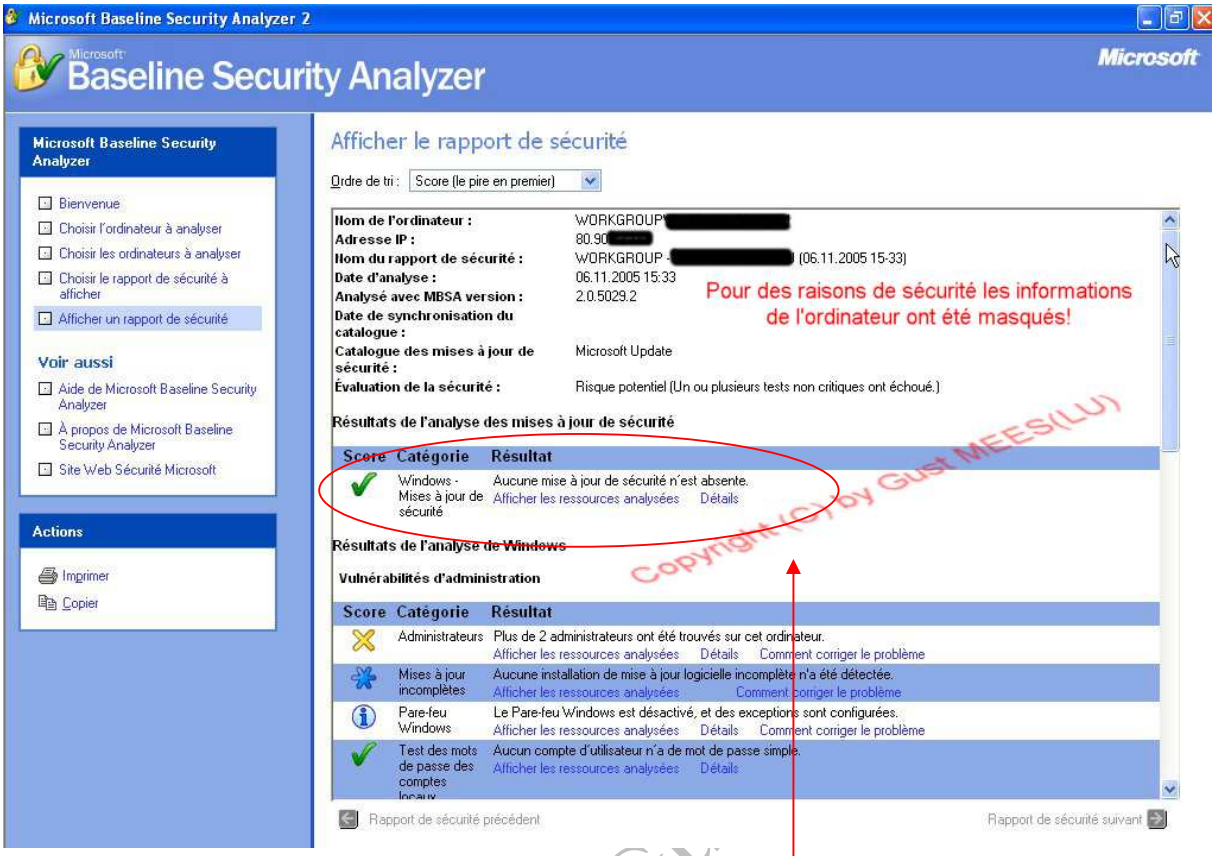


Une nouvelle fenêtre s'ouvre (voir figure ci-dessus) et nous devons cliquer le lien „**Démarrer l'analyse**“.



Ensuite la fenêtre suivante ci-dessus apparaîtra et restera telle que pendants quelques minutes. Après un laps de temps (dépendant du nombre de logiciels installés) l'état de la figure changera comme montré ci-dessous.

Votre ordinateur est maintenant scanné en ligne par les services de **MICROSOFT®** et le résultat vous sera communiqué par l'intermédiaire de l'interface **MBSA**.

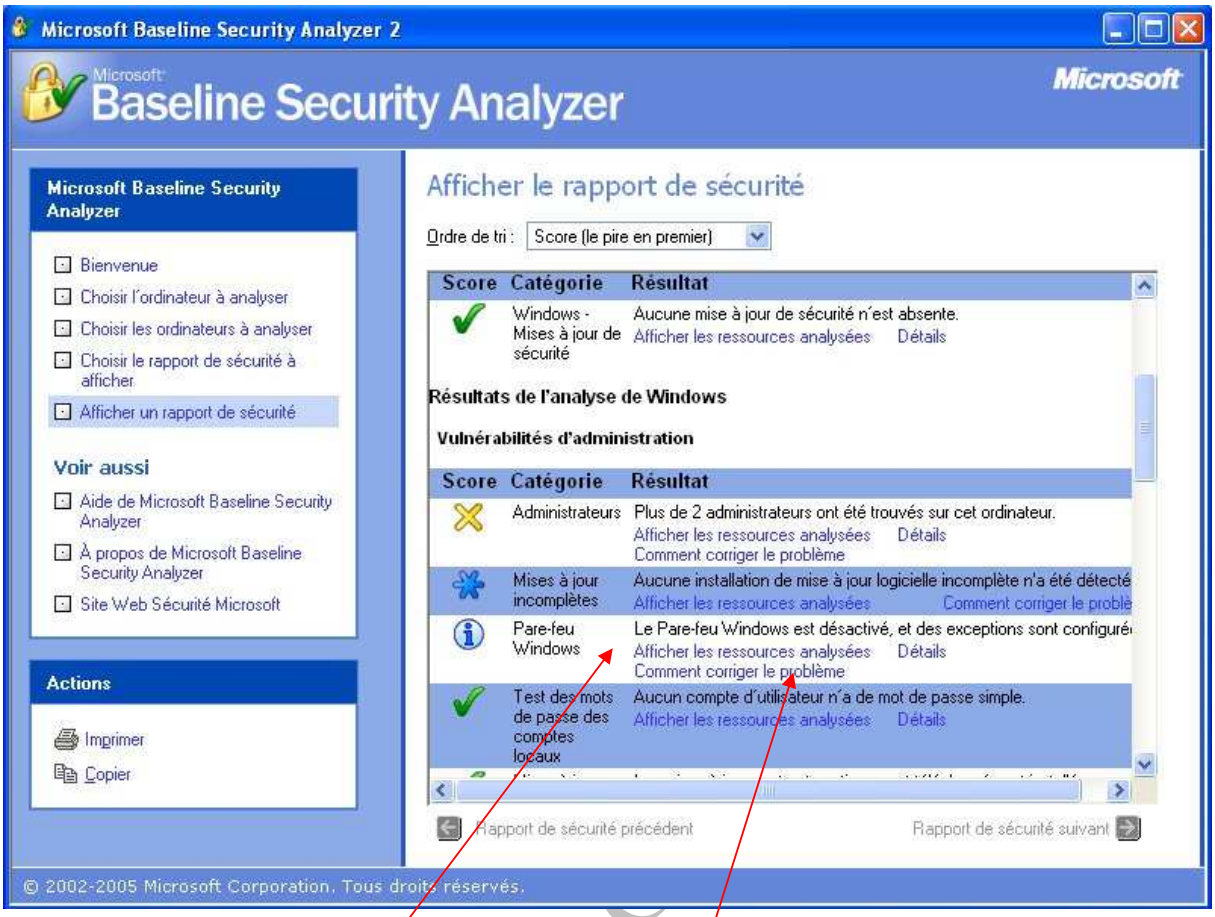


L'interface du **MBSA** nous montre maintenant les résultats obtenus :

1. Nom de l'ordinateur (dans la figure l'adresse a été masquée pour des raisons de sécurité)
2. Adresse IP (dans la figure l'adresse a été masquée pour des raisons de sécurité)
3. Nom du rapport de sécurité
4. Date d'analyse
5. Analysé avec **MBSA** version 2.0.5029.2
6. Évaluation de la sécurité
7. **Résultats de l'analyse des mises à jour de sécurité : Dans notre exemple l'ordinateur testé est muni de toutes les mises à jour.**

Dans la catégorie „**Vulnérabilités d'administration**" le rapport nous indique qu'il y a plus de deux comptes d'administrateur. Dans notre cas c'est normal, car le propriétaire utilise un ordinateur multilingue et qu'il a configuré trois comptes d'administrateur (DE, FR, EN) et un **compte limité** pour surfer sur Internet.

Le „compte limité" ne dispose pas de droits d'administrateur et présente donc moins de risques de sécurité pour surfer sur Internet ! Il est d'ailleurs conseillé de configurer son ordinateur de cette manière !



L'analyse nous montre aussi que le pare-feu (firewall) de **WINDOWS®** est désactivé. Dans notre cas c'est normal, car sur l'ordinateur analysé le firewall de **ZONEALARM®** est installé et activé.

Il ne faut jamais installer plus qu'un seul firewall et un seul antivirus !

Si le message „**Le pare-feu WINDOWS est désactivé**" s'affiche sur votre ordinateur, sans que vous ayez installé un autre pare-feu, il faudra activer le pare-feu de **WINDOWS®.**

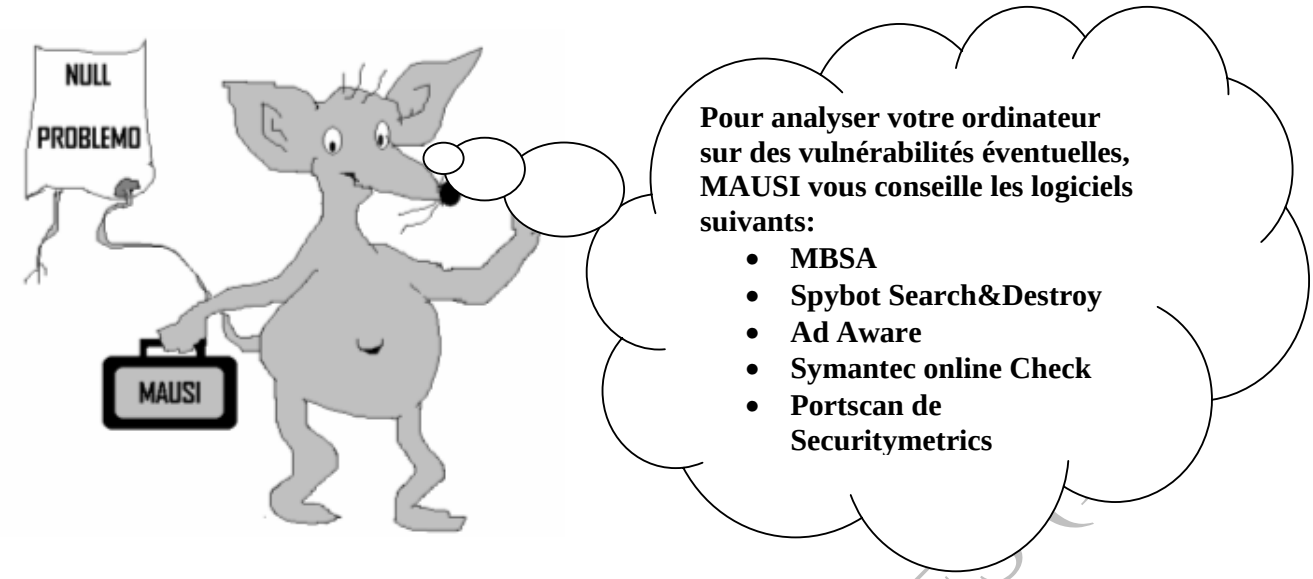
Si vous ne savez pas comment procéder, veuillez cliquer le lien „**Comment corriger le problème**" et/ou suivre le didacticiel de **CASES** http://www.cases.lu/ !

Pour le reste du protocole d'analyse procédez de la même façon. S'il y a une croix orange et/ou rouge, veuillez toujours suivre les liens de texte „**Comment corriger le problème**" et ensuite corriger les failles trouvées, puis refaites le test autant de fois qu'il s'avère nécessaire jusqu'à ce que le „**MBSA**" vous fournit un rapport positif.

Comme vous pouvez le constater, l'ordinateur qui a servi pour créer ce didacticiel est bien configuré !

Récapitulatif :

- **Un antivirus est obligatoire.**
- **Un firewall (pare-feu) est obligatoire.**
- **Les updates (mises à jour/patches) de chez WINDOWS® sont obligatoires.**
- **Les mots de passe doivent être choisis de telle façon à ce qu'ils ne soient aisément devinables et déchiffrables ! Un mot de passe sécurisé doit comporter au minimum huit caractères, dont minuscules, majuscules, chiffres et caractères spéciaux mélangés !**
- **Un compte limité pour surfer est à conseiller. La plupart des malware ne peuvent s'installer que sous droits d'administrateur !**



Vous trouverez les liens concernant les logiciels proposés sur le site Internet suivant :

http://www.internetmonitor.lu