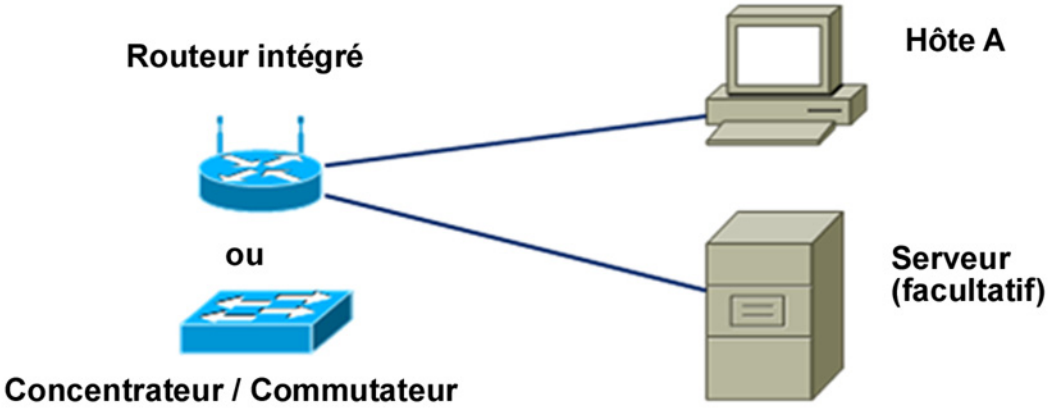
Travaux pratiques 8.4.3 Analyse de la vulnérabilité

ATTENTION : ces travaux pratiques peuvent violer les mesures de sécurité juridiques et organisationnelles. L'analyseur de sécurité téléchargé dans ces travaux pratiques doit être uniquement utilisé dans le cadre d'une formation dans un environnement de travaux pratiques. Avant d'utiliser un analyseur de sécurité sur un réseau actif, vérifiez avec votre formateur et le personnel d'administration du réseau les mesures internes concernant l'utilisation de ces outils.



Objectifs

- Télécharger et installer un logiciel d'analyse de la sécurité
- Tester un hôte visant à déterminer les vulnérabilités de sécurité potentielles

Contexte / Préparation

Les analyseurs de sécurité sont des outils précieux que les administrateurs réseau et les auditeurs utilisent pour identifier les vulnérabilités du réseau et de l'hôte. Il existe plusieurs outils d'analyse de la vulnérabilité, également connus sous le nom de scanners de sécurité, disponibles pour tester la sécurité des réseaux et des hôtes. Dans ces travaux pratiques, vous allez télécharger et installer Microsoft Baseline Security Analyzer (MBSA). MBSA est conçu pour identifier des problèmes de sécurité potentiels précisément liés aux systèmes d'exploitation, aux mises à jour et aux applications Microsoft. Il identifie également des services inutiles qui sont peut-être exécutés comme des ports ouverts.

MBSA fonctionne sur les systèmes Windows Server et Windows XP et analyse les mauvaises configurations de sécurité courantes et les mises à jour de sécurité manquantes pour le système d'exploitation ainsi que sur la plupart des versions du serveur d'informations Internet (IIS), SQL Server, Internet Explorer (IE) et les produits Office. MBSA offre des recommandations spécifiques pour corriger les problèmes potentiels.

Ces travaux pratiques peuvent être réalisés seul ou par groupe de deux.

Ressources requises :

- Un ordinateur fonctionnant sous Windows XP Professionnel servant de station test
- Une connexion Internet haut débit pour le téléchargement de MBSA (à moins qu'il ne soit préinstallé)
- L'ordinateur doit être relié au commutateur du routeur intégré ou à un concentrateur ou commutateur autonome
- Facultatif : un serveur pouvant exécuter une combinaison de DHCP, HTTP, FTP et Telnet (préconfiguré)

Étape 1 : téléchargement et installation de MBSA

a. Ouvrez un navigateur Web et rendez-vous sur la page Web de MBSA. http://www.microsoft.com/technet/security/tools/mbsa2/default.mspx

b. Quelle est la dernière version de MBSA disponible ? _____

c. Quelles sont certaines caractéristiques que MBSA fournit ? _____

_____

d. Faites défiler la page et sélectionnez la langue désirée pour commencer le processus de téléchargement.

e. Cliquez sur **Continuer** pour valider l'exemplaire de Microsoft Windows que vous exploitez.

f. Cliquez sur **Télécharger les fichiers ci-dessous** et sélectionnez le fichier que vous voulez télécharger. (Le fichier de configuration en anglais est MBSASetup-EN.msi). Cliquez sur le bouton **Télécharger** à droite du fichier. Combien de mégaoctets le fichier à télécharger fait-il ?

_____

g. Lorsque la boîte de dialogue **Télécharger fichier – Avertissement de sécurité** s'affiche, cliquez sur **Enregistrer** et téléchargez le fichier vers un dossier précis ou sur le bureau. Vous pouvez également l'exécuter à partir du site Web de téléchargement.

h. Une fois le téléchargement terminé, assurez-vous que toutes les autres applications sont fermées. Double-cliquez sur le fichier téléchargé. Cliquez sur **Exécuter** pour démarrer le programme de Configuration puis cliquez sur **Exécuter** si un message Avertissement de sécurité apparaît. Cliquez sur **Suivant** sur l'écran de configuration MBSA.

i. Sélectionnez la case d'option pour accepter le contrat de licence puis cliquez sur **Suivant**. Acceptez les valeurs par défaut à mesure que l'installation avance, puis cliquez sur **Terminer**. Cliquez sur **OK** dans le dernier écran de Configuration MBSA et fermez le dossier pour retourner sur le bureau de Windows.

Étape 2 : création du réseau et configuration des hôtes

a. Connectez les ordinateurs hôtes au routeur intégré, à un concentrateur ou à un commutateur comme l'indique le schéma topologique. L'hôte Host-A est la station test où MBSA va être installé. Le serveur est facultatif.

b. Configurez les paramètres IP du ou des hôtes à l'aide des connexions réseau de Windows XP et des propriétés TCP/IP. Si l'hôte est connecté au routeur intégré, configurez-le en tant que client DHCP ; sinon, passez à l'étape 2c.

c. Si l'hôte est connecté à un concentrateur ou à un commutateur et qu'un serveur DHCP n'est pas disponible, configurez-le manuellement en lui attribuant une adresse IP statique.

Quelle est l'adresse IP et quel est le masque de sous-réseau de l'hôte A et du serveur (en option) ?

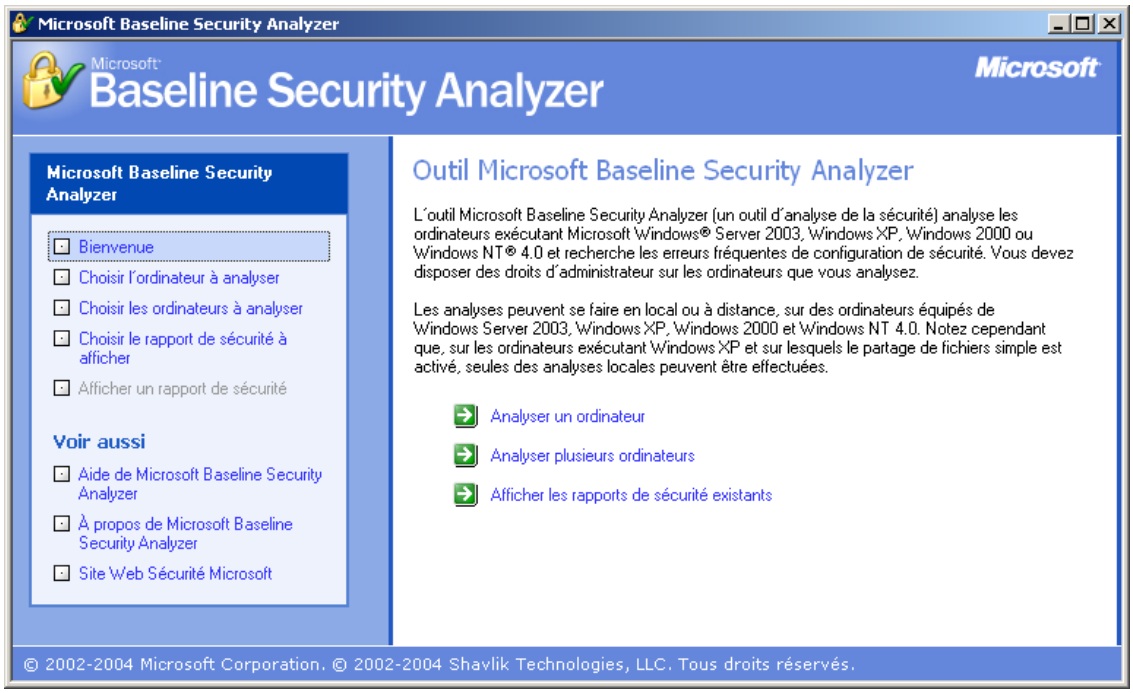
_____

Étape 3 : exécution de MBSA sur un hôte

a. Double-cliquez sur l'icône du bureau de MBSA ou lancez-le depuis **Démarrer > Tous les programmes**.

À l'affichage de l'écran principal, quelles options sont disponibles ? _____

_____



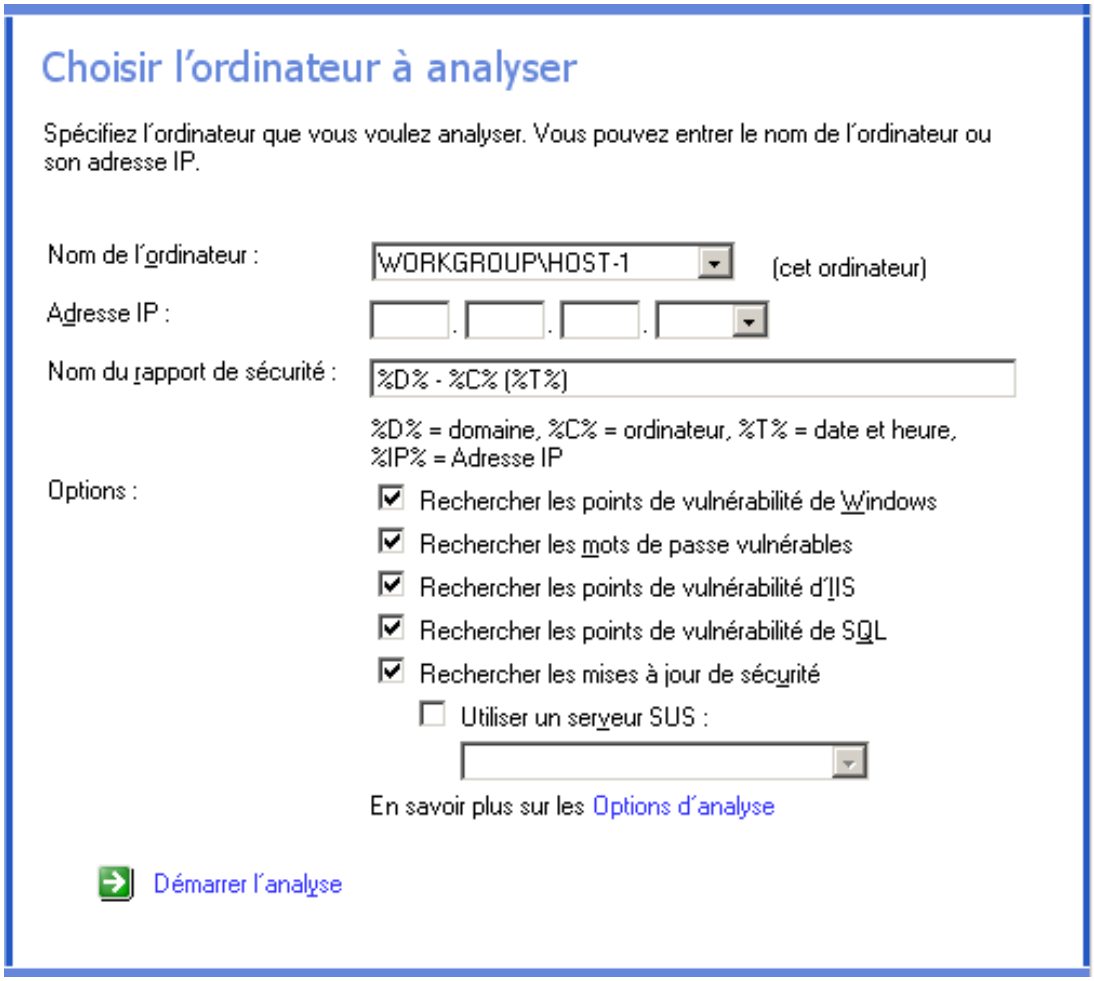
Étape 4 : sélection d'un ordinateur à analyser

a. À gauche de l'écran, cliquez sur **Choisir l'ordinateur à analyser**. L'ordinateur affiché est par défaut l'ordinateur sur lequel MBSA est installé.

b. Quelles sont les deux façons d'indiquer un ordinateur à analyser ? _____

_____

c. Acceptez l'ordinateur à analyser par défaut. Désactivez Vérifier les vulnérabilités administratives IIS et SQL puisque ces services ne sont pas susceptibles d'être installés sur l'ordinateur en cours d'analyse. Cliquez sur **Démarrer l'analyse**.



Étape 5 : affichage des résultats d'analyse de sécurité mis à jour

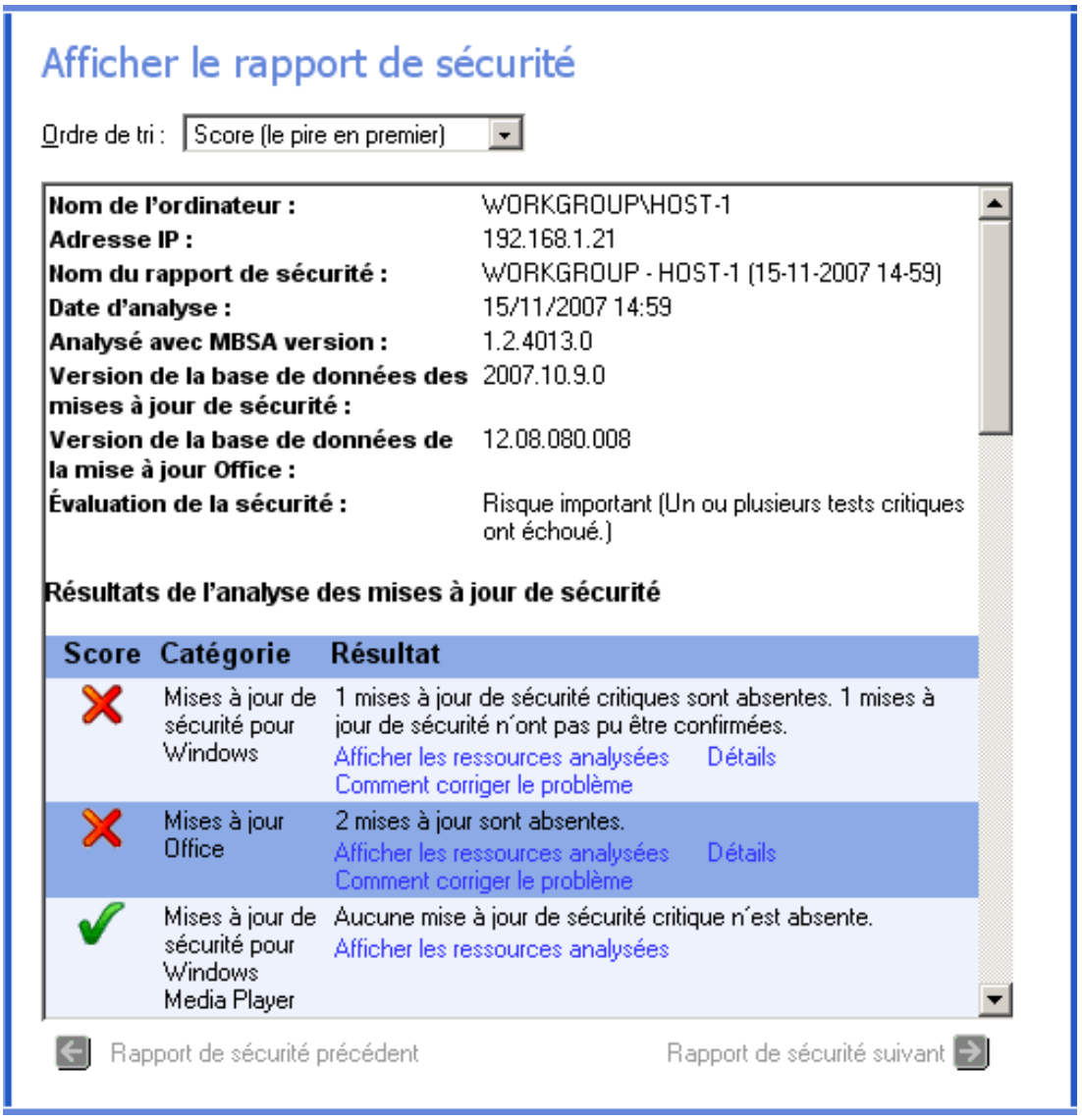
a. Affichez le rapport de sécurité. Quels sont les résultats de l'analyse de mise à jour de sécurité ?

_____

_____

b. S'il y a des X rouge ou jaune, cliquez sur **Comment corriger le problème**. Quelle est la solution recommandée ?

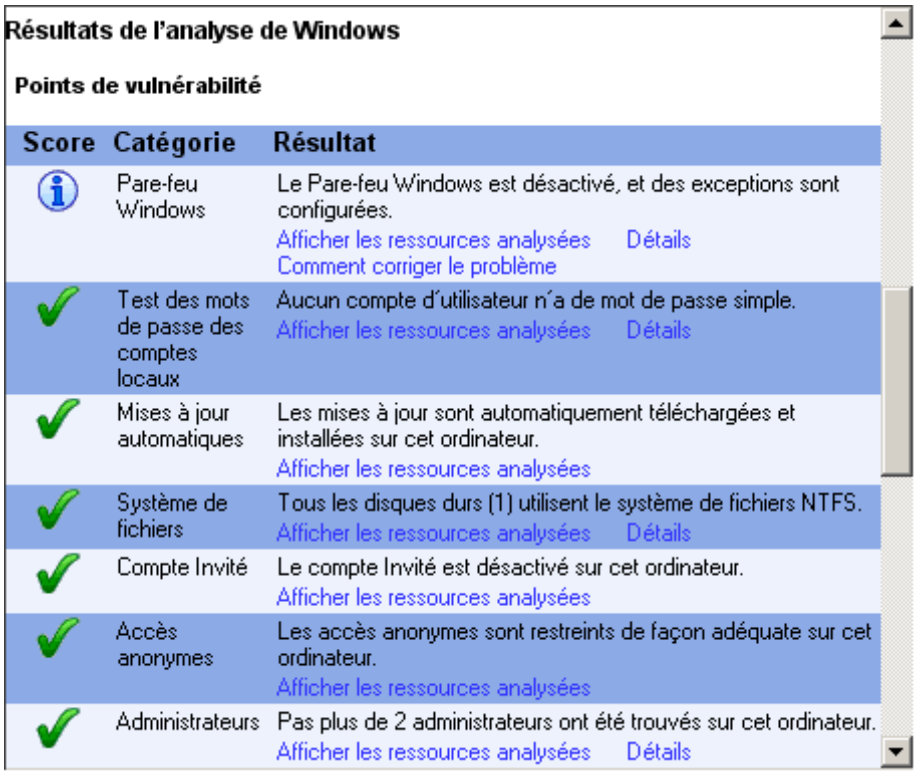
_____



Étape 6 : affichage des résultats d'analyse de Windows dans le rapport de sécurité

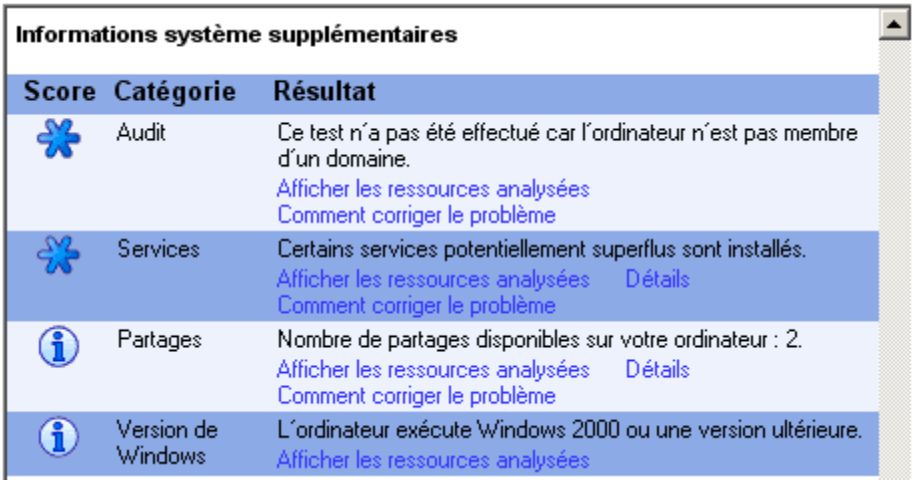
a. Faites défiler l'écran pour afficher la deuxième partie du rapport affichant les **Résultats de l'analyse de Windows**. Des vulnérabilités administratives ont-elles été identifiées ?

_____



b. Dans la section de l'écran **Informations système supplémentaires** (ci-dessous), dans la colonne **Problème** de la ligne **Services**, cliquez sur **Afficher les ressources analysées** et cliquez sur **Détails** sous la colonne **Résultat** pour obtenir la description du contrôle effectué. Qu'avez-vous trouvé ? Lorsque vous avez terminé, fermez les deux fenêtres contextuelles pour revenir au rapport de sécurité.

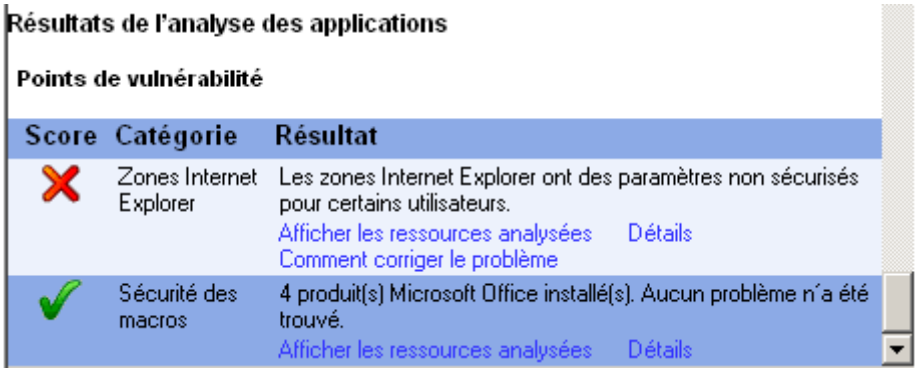
_____



Étape 7 : affichage des résultats d'analyse des applications du bureau dans le rapport de sécurité

a. Faites défiler l'écran pour afficher la dernière partie du rapport affichant les **Résultats de l'analyse des applications**. Des vulnérabilités administratives ont-elles été identifiées ?

_____



b. Combien de produits Microsoft Office sont installés ? _____

c. Y a-t-il eu des problèmes de sécurité avec **Sécurité des macros** pour l'un d'entre eux ?

_____

Étape 8 : analyse d'un serveur, si disponible

a. Si un serveur avec plusieurs services est disponible, cliquez sur Choisir un ordinateur à analyser à partir de l'écran principal de MBSA et entrez l'adresse IP du serveur, puis cliquez sur Démarrer l'analyse. Quelles vulnérabilités de sécurité ont été identifiées ?

_____

_____

_____

b. Y a-t-il eu des services éventuellement inutiles qui ont été installés ? Quels sont les numéros de port qui s'y trouvaient ?

_____

_____

Étape 9 : désinstallation de MBSA à l'aide du Panneau de configuration Ajout/Suppression de programmes

a. Cette étape est facultative, cela dépend de l'existence d'un processus réseau chargé de rétablir la configuration des hôtes automatiquement.

b. Pour désinstaller MBSA, cliquez sur **Démarrer > Panneau de configuration > Ajout/Suppression de programmes**. Recherchez l'application MBSA et désinstallez-la. Elle doit figurer dans la liste sous le nom de Microsoft Baseline Security Analyzer 2.0.1. Cliquez sur **Supprimer** puis sur **Oui** pour confirmer la suppression de l'application MBSA. Lorsque vous avez terminé, fermez toutes les fenêtres pour retourner sur le bureau.

Étape 10 : remarques générales

a. L'outil MBSA est conçu pour identifier les vulnérabilités sur les ordinateurs fonctionnant sous Windows. Recherchez sur Internet si d'autres outils existent. Dressez la liste des outils que vous avez découverts.

_____

b. Quels outils existent pour les ordinateurs qui n'exploitent pas Windows ? Recherchez sur Internet d'autres outils et dressez-en la liste ici.

_____

c. Quelles autres étapes pourriez-vous suivre pour sécuriser un ordinateur contre les attaques provenant d'Internet ?

_____