

Recherche d'une intrusion : quelques conseils pour analyser votre machine WINDOWS

Marie-Claude QUIDOZ & Nicole DAUSQUE
CNRS/UREC

V4 – 16/07/2003

Ce document a été élaboré en partie à partir des recommandations donnés par le CERT-Renater.

Quelques recommandations générales (en cas de doute) :

- 1 - Isoler au moins temporairement la machine du réseau.
- 2 - Si possible faire une sauvegarde complète de la machine avant analyse et effectuer les recherches sur la copie ; cela peut vous permettre, dans le cas où la décision de porter l'affaire en justice serait prise, de préserver l'intégrité des données présentes sur la machine.
- 3 - Analyser la machine.
- 4 - Contactez le CERT-Renater à l'adresse : certsvp@renater.fr

Le but de cette analyse est de pouvoir répondre aux questions suivantes :

- * Machine compromise (nom+ip) : ?
- * Type d'utilisation normale (DNS, WEB, Firewall...) : ?
- * OS (date) : ?
- * Ports ouverts : ?
- * backdoor(s) installées : ?
- * Log : (date et type de l'attaque) ?
- * Outil(s) illicite(s) installé(s) : (exemples : serv-u ftp...)
- * Liste et taille des binaires ajoutés ou modifiés : ?
- * Impact : (exemple : sniffer = vol de mot de passe = changement des mots de passes) ?

Conseil : n'ouvrir les fichiers suspects qu'avec une application n'interprétant pas les macros (exemple d'éditeur de texte: WordPad, UltraEdit...).

Analyser la machine :

1^{ère} étape : Faire le bilan sur les services présents et leurs ports associés.

Pour les services, indiquez le nom (exemple : IIS, telnet, microsoft-ds...) ainsi que la version (exemple : 2.4.2).

Pour cela, vous pouvez utiliser les outils suivants :

- **superscan** (<http://www.foundstone.com/resources/proddesc/superscan.htm>): découverte des ports ouverts (services disponibles)
- **Nmapwin** (http://download.insecure.org/nmap/dist/nmapwin_1.3.0.exe) : découverte des ports ouverts (services disponibles)
- **nmap** (produit unix) (<http://www.nmap.org/nmap/>) : découverte des ports ouverts (services disponibles)
- **nessus** (produit windows+unix) (<http://www.nessus.org/>) : découverte des ports ouverts + analyse des vulnérabilités

Vérifier l'association entre les ports ouverts et les applications lancées à l'aide du produit « fport » (<http://www.foundstone.com/knowledge/proddesc/fport.html>). Ce produit fournit plus d'informations que la commande « netstat -an ». Prendre la version 1.33 dans le cas d'un windows NT. Vérifier l'existence d'un service associé à un port suspect en lançant une socket telnet.

2^{ème} étape : Vérifier les services démarrés.

Ces services sont accessibles par le « gestionnaire des tâches (ControlAltSupp) » ou par le programme « service » du « panneau de configuration ». Cette vérification permet de détecter la présence de services intrus (souvent avec des noms proches de nom de services courant).

Vérifier aussi les tâches programmées sur la machine afin de détecter si de nouvelles tâches périodiques ont été insérées parmi les tâches définies par l'administrateur du système (commande « at » ou « tâches planifiées »). Vérifier la présence de services en démarrage invisible.

3^{ème} étape : Consulter les journaux de « l'observateur d'événements » de la machine locale et du contrôleur de domaine.

Vérifier les dernières connexions faites (réussie, échouée, ...) sur votre machine, que ce soit en interactif ou par le réseau, dans le journal « sécurité » de l'observateur d'événements. Cela est possible si l'audit des succès et des échecs des ouvertures et fermetures de sessions avaient été mis en place ! Vous pouvez aussi utiliser le produit « ntlst » (<http://www.foundstone.com/resources/proddesc/ntlast.htm>).

Vérifier les événements relatifs à l'utilisation des ressources (création, ouverture ou suppression de fichiers, tentative d'accès interdit à une ressource, baisse importante de l'espace disque disponible par exemple). À condition bien sûr que vous ayez configuré les types d'événements à enregistrer !

4^{ème} étape : Vérifier, pour les ressources partagées, si :

- Le partage n'a pas été activé alors qu'il ne doit pas l'être.
- Des modifications ont été faites (au niveau des droits). Utiliser la commande « net share » (ou le produit « dumpsec » (<http://www.somarsoft.com/>) qui donne des informations plus complètes sur le système).
- Le taux d'occupation (utile si vous êtes à la recherche d'un site warez)

Vous pouvez utiliser la boîte à outils « The Forensic Toolkit™ » qui permet d'obtenir des informations sur les fichiers d'une partition NTFS (activités non autorisées, derniers accès aux fichiers, fichiers cachés, dump d'un fichier, ...)

(<http://www.foundstone.com/resources/proddesc/forensic-toolkit.htm>).

5^{ème} étape : Vérifier dans le « gestionnaire des utilisateurs » (sur le domaine et en local) si un utilisateur ou un groupe a été ajouté (c:\winnt\profile). Vérifier aussi s'il existe des comptes sans mot de passe, ou des comptes « administrateur » avec des mots de passe faibles. Cela peut ensuite vous permettre de faire des recherches dans les fichiers journaux avec comme critère ce type de nom de comptes.

6^{ème} étape : Faire une recherche sur toutes les arborescences

- Des fichiers avec l'extension « zip » (ils peuvent cacher des chevaux de troie).
- En cas de suspicions de serveur ftp warez, nous vous recommandons d'orienter vos recherches vers la présence d'outils comme : serv-u ftp (serv-u.ini), Servudaemon (servudaemon.ini), Sfv Checker (javsvf.ini) et autres outils ftp. Attention, en même temps que l'installation d'un site warez, un robot IRC est souvent installé pour annoncer le contenu du serveur FTP (par exemple dans un des cas connus, le robot IRC de type Iroffer avait été installé dans un répertoire identd sous le nom svchost.exe).

- Des fichiers au format divx (15000000 Octets) (utile pour rechercher les films installé sur la machine).
- Faire une recherche systématique dans les répertoires : « c:\ » , « c:\recycled » , « c:\recycler\temp » , « c:\WINNT\system32 » , « c:\WINNT\system32\win32host » , « c:\WINNT\system32\spool\drivers\color\temp » , « c:\winnt\temp\backup » et « c:\winnt\system\win\fl » souvent utilisés pour cacher des outils warez.

7^{ème} étape : Faire une recherche à l'aide de votre logiciel d'antivirus ou avec un outil spécialisé dans la détection des chevaux de troie (exemple : The Cleaner) pour débusquer la présence de chevaux de troie (Netspy, webEx, TrojanCow, Bla1.1, socket23, ..). Attention, d'autres outils plus familier comme VNC ou Damware (outil d'administration en remote contrôle) peuvent tous aussi bien jouer le rôle de backdoor.

8^{ème} étape : Vérifier la base de registre afin de détecter si des modifications suspectes ont eu lieu (cf. produit « dumpreg » <http://www.somarsoft.com/>).

- Vérifier les dll utilisées à l'aide du produit « listdlls » (<http://www.incident-response.org/windowstools/listdlls.exe>).
- Vérifier les .ini installés

Autres outils :

Filemon v4.33 : cet ensemble d'outils montre l'activité, en temps réel, de tout le système de fichiers pour Windows NT, Windows 2000, Windows 9x/Me ; les sources sont inclus (<http://www.sysinternals.com/ntw2k/source/filemon.shtml>)

Process Explorer v5.0 : cet utilitaire donne quels sont les fichiers, clefs de registres et processus ouverts ainsi que les DLLs qui sont chargées (<http://www.sysinternals.com/ntw2k/freeware/procexp.shtml>)

PsTools v1.82 : ensemble d'utilitaires en ligne de commande pour lister les processus, les fichiers ouverts, etc. (<http://www.sysinternals.com/ntw2k/freeware/pstools.shtml>)

Win32 Analyser Toolset v1.1 : script permettant de collecter tout un ensemble d'informations vitales sur un système (http://readyresponse.dynu.com/isso/projects/Win32_Analyzer/)

D'autres outils sont disponibles sur le site (<http://www.sysinternals.com/>)

À titre préventif si vous avez un doute :

- Poser des filtres au niveau du routeur, en vous appuyant sur les statistiques envoyées hebdomadairement par le CERT-Renater, si vous avez une politique du type :« Tout autorisé sauf » ; sinon revoyez votre politique de filtrage afin de bien cerner les systèmes et les services ouverts au public (en général web, ftp, dns).
- Surveiller et enregistrer si possible, au moins temporairement, tout le trafic à destination des machines compromises pour les jours à venir, en particulier le trafic icmp, les connexions telnet, ftp, et ssh.

- Transmettre au CERT-Renater vos fichiers de logs afin qu'il puisse contacter les administrateurs des machines d'où est lancée l'attaque. Ces fichiers de logs doivent impérativement contenir la date et l'heure des connexions suspectes (si vous le pouvez, essayez de trier par adresses IP sources).

Pour en savoir plus, vous pouvez aussi vous référer aux liens suivants :

Pour les cas d'intrusion il y a sur le site de l'UREC un descriptif en français, bien fait, des mesures à prendre : <http://www.urec.cnrs.fr/securite/CNRS/quefaire.html>

Vous pouvez aussi consulter:

http://www.cert.org/tech_tips/intruder_detection_checklist.html

<http://www.pasteur.fr/infosci/FAQ/computer-security/compromise-faq>

<http://www.cert.org/nav/recovering.html>

<ftp://ftp.jpCERT.or.jp/pub/ciac/ciacdocs/ciac2305.pdf>

<http://www.cert.org/security-improvement/modules/m01.html>

<http://ciac.llnl.gov/ciac/ToolsUnixNetMon.html>

Et d'une façon générale lire ou relire la note d'information du CERTA du 17 juin 2002 (CERTA-2002-INF-002) : « [Les bons réflexes en cas d'intrusion sur un système d'information](#) ».