

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

Marie-Claude QUIDOZ & Nicole DAUSQUE
CNRS/UREC

V2 – 11/12/2002

Ce document a été élaboré à partir des conseils donnés par le CERT-Renater lors des réponses aux déclarations d'incident.

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.

Analyser la machine :

- Vérifier le fichier de mots de passe afin de découvrir si un compte a été ajouté puis changer tous les mots de passe et en prévenir vos utilisateurs.
- Vérifier le fichier des groupes pour détecter la présence de groupes intrus.
- Vérifier les processus démarrés à l'aide d'une commande *ps* propre (provenant de supports *a priori* intègres comme le CD-ROM ou la disquette d'installation par exemple) pour détecter la présence de processus intrus (souvent avec des noms proches de nom de processus courant).
- Vérifier les fichiers/scripts de démarrage de la machine. Le but est essentiellement de vérifier que le pirate n'a pas laissé derrière lui, des processus destructifs, permettant de faire disparaître toute trace de sa présence, éventuellement détruire le système, s'il venait à être découvert.
 - Analyse du fichier *rc.sysinit* et des programmes lancés au démarrage par les scripts d'initialisation *rc**. Il se peut que des routines pirates aient été ajoutées : « backdoors », routines destructrices, ... lancés en cas de reboot système.
 - Analyse de la *crontab* : des tâches périodiques pirates ont peut-être été insérées parmi les tâches définies par l'administrateur du système.
- Vérifier la présence d'un rootkit (exemples : « X-Org SunOS Rootkit v2.5DXE », « rk », « KNARK », « lrk5 », ...) à l'aide de commandes propres (provenant de supports *a priori* intègres comme le CD-ROM ou la disquette d'installation par exemple).
 - Vérifier si les ports *1524/tcp* et *14500/tcp* sont ouverts.
 - Regarder le contenu des fichiers *inetd.conf* et */etc/rc.** afin de vérifier les services qui tournent sur la machine.
 - Rechercher la présence de répertoires *bob*, *joe*, ..., et *espace*.
 - Vérifier la taille de binaires comme *login*, *find*, *netstat*, *ls*, *ps*, *du* (très souvent remplacés par des versions complaisantes pour le pirate pour masquer sa présence).

- Essayer les commandes ' netstat -/ ', ' ps -/ ', ' ls-/ ' (avec les commandes présentes sur la machine qui sont peut-être compromises '-/' n'étant pas une option normale de ces commandes, ces essais ne devraient retourner que des erreurs ; dans le cas contraire, la machine est certainement compromise et un rootkit a été installé).
- => Dans le cas d'installation de rootkit, parmi les commandes utiles qui ne sont pas modifiées, utiliser les commandes "locate", "socklist" et "ifconfig", "strings > ~/fichier|more" pour analyser la machine.
- Consulter les fichiers d'historique (logs) de la machine (pour savoir comment sont enregistrées les informations, se référer au fichier "syslog.conf") ; regarder, par exemple, les messages affichés par le système dans "/var/log/messages", pour chercher la trace d'un éventuel redémarrage de la machine ; regarder le résultat de la commande "last".
- Si l'accounting tourne sur la machine, regarder les fichiers correspondants aux commandes qui ont été exécutées, cela donne parfois de bonnes pistes.
- Rechercher les sniffers qui peuvent avoir été installés (exemples : « lpsys », « esniff », « dsniff », « linsniffer », « sn00py2 », « sniffit », ...).
- Rechercher la présence d'interfaces en mode promiscuous (et déterminer s'il est légitime ou non que cette interface soit dans ce mode) à l'aide de la commande "ifconfig".
- Rechercher la présence éventuelle de robots irc (exemples : « eggdrop », « darkbot »,...) ; les pirates en installent souvent sur les machines qu'ils compromettent afin de pouvoir contrôler la confidentialité de leurs discussions. Le port par défaut assigné à cette application est le port 6667.
- Vérifier la présence d'agents d'outils de déni de service distribué (DDOS). Pour cela, vous pouvez utiliser les outils suivants :
 - **find_ddos** (<http://www.nipc.gov/warnings/alerts/1999/trinoo.htm>) permet de retrouver un agent de DDOS. Après compilation, lancer sous root : ./find_ddos [-g grabdir] [-l logfile] [-p] [-v] [-V] [-x exclude1] [scandir]
 - **sickenscan** (<http://staff.washington.edu/dittrich/misc/ddos/> « defensive tools : gag »)
 - **ddos_scan** (<http://staff.washington.edu/dittrich/misc/ddos/> « defensive tools : dds »)
 - ou ceux décrits dans la note d'information du CERTA (CERTA-2000-INF-003) : « [Évolution des outils de déni de service distribué](#) ».
- Faire le bilan sur les services présents (exemples : telnet, sunrpc, WU-ftp, bind,...) avec leurs versions (exemple : 2.4.2). Pour cela, vous pouvez utiliser les outils suivants :
 - **nmap** (<http://www.nmap.org/nmap/>) : découverte des ports ouverts (services disponibles)
 - **nessus** (<http://www.nessus.org/>) : découverte des ports ouverts + analyse des vulnérabilités
- Vérifier le résultat de la commande netstat -an
- Vérifier le résultat de la commande lsof -i et lsof (<ftp://ftp.cert.dfn.de/pub/tools/admin/lsof/>)

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](#) ».

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

- * Machine compromise (nom+ip) : ??
- * Date : ??
- * OS : ??
- * Ports ouverts : ??
- * Rootkit installé : ??
- * Log : ??
- * Impact : (exemples : vol de mot de passe, attaque par rebond, DDOS,...)
- * Mode d'action : ??
- * backdoors : ??
- * binaires modifiés : ??