



CENTRE NATIONAL  
DE LA RECHERCHE  
SCIENTIFIQUE



# *Audit d'une machine linux compromise*

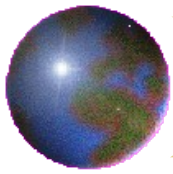
Denis Pugnère

Lyon - 15- 16- 17/ 11/ 2005



# *Origine de la formation*

- Initiative de RENATER / CINES
  - Titre : « analyse d'une machine Linux compromise »
  - Formation CIREN assurée par Kostya Kortchinsky
  - Annonce nationale
  - Objectifs :
    - Aspect légal
    - réflexes à avoir, recommandations
    - appropriation des outils
    - Incitation à acquérir l'expertise par les ASR



# *Contenu de la formation*

- **Guide des bonnes pratiques**
  - Sauvegarder tout ce qui est utile
  - Ne pas faire de modifications...
- **Présentation des outils**
  - dd, netcat, lsof, strings, grep...
  - Boîtes à outils : PLD- rescueCD, sleuthkit...
- **Présentation du challenge**
  - Rechercher les traces...
- **Analyse par les stagiaires**
  - Utilisation des outils, explications des commandes et de leurs options,
  - Que sauvegarder, comment ?
  - Idées de recherches (Où ? Quoi ? Comment ?)
  - Guidage au fil de la formation



## *Guide des bonnes pratiques*

- Ne pas faire de modifications sur le système en cours d'analyse
- Ne pas faire confiance aux outils installés sur le système en cours d'analyse
- Récupérer toutes les informations utiles :
- Garder une trace des actions réalisées
- Sauvegarder ces informations sur un support externe, d'une manière fiable,
- S'assurer que les informations sauvegardées sont intègres
- S'assurer qu'aucune modification a été faite ou ne peut se faire sur les informations sauvegardées.



## *Que faire ?*

- La débrancher du réseau ?
- Enlever la route par défaut ?
- L'isoler dans un VLAN ?
- 
- (se) préparer un plan d'action
  - Documentation
  - Boite à Outils
  - Infrastructure (réseau, espace de stockage)
  - Gérer les priorités (utilisateurs, services)
  - sauvegardes, outils de ré- installation..



## *Ne pas faire !*

- stopper la machine avant d'avoir sauvegardé certaines informations sur l'état de la machine



## *Considérations légales*

- principe de proportionnalité :
- pas d'image disque pour tout incident
- Importance des fichiers de logs et de la déclaration à la CNIL
- sont-ils complets ? - > centralisation des logs
- Synchronisation temporelle - > corrélation
- Reproductibilité de la procédure, documentation des actions
- intégrité des informations extraites



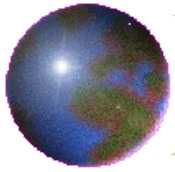
## *Les questions à se poser*

- depuis quand la machine est-elle piratée ?
- Quelle est la vulnérabilité utilisée ?
- Quel est le but du piratage ?



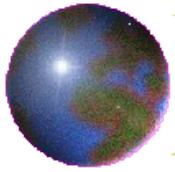
## *Différents types de traces*

- fichiers
  - cachés :
    - .fichier
    - masqués (kernel modules, attr)
  - Ouverts
- Les non fichiers : les blocs non utilisés du disque
- processus
  - inhabituels
  - Cachés
  - bibliothèques utilisées
- Traces mémoire (RAM, SWAP)
- connexions ouvertes



## *Les logs*

- logs systèmes
- logs applicatifs (apache, ssh, ftpd...)
- logs réseau (flots)
- logs IDS
  - HIDS : ensemble d'outils de détection d'intrusion vérifiant l'intégrité du système
  - NIDS : ensemble d'outils inspectant les flux réseau (inspection de paquets)



## *Les outils*

- dd: crée des images de disques bit à bit
- find et ls: examine les répertoires et fichiers
- ifconfig: configuration réseau (ipconfig pour Win)
- lsmod: liste les modules chargés par le noyau
- lsof: liste les fichiers ouverts (et les connexions réseau)
- md5sum & sha1sum :génère les checksums
- netcat & cryptcat: sauvegarde à travers le réseau
- netstat: collecte le statut des connexions réseau
- ps: collecte les données sur les processus (pslist pour Win)
- script: renregistre les sessions
- strace: system call tracer (truss for Sun)
- strings: liste les chaînes de texte dans les binaires



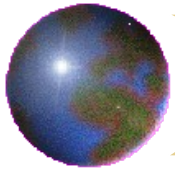
## *les boites à outils :*

- FIRE
- KNOPPIX- STD
- HELIX
- Outils spécialisés :
  - Sleuthkit & Autopsy
  - TCT ([www.porcupine.org/forensics/txt/html](http://www.porcupine.org/forensics/txt/html))
- Encase (commercial)



## *Les modes de compromission changent*

- Les outils de sauvegardes (dd, tar...) sont là depuis longtemps et tendent à être disponibles sur toutes les plate- formes (Un\*x, Win32, MacOSX...)
- Les outils de recherches (grep, netstat, ps, lsof, strings...) sont efficaces. On sait chercher (réponse à la question : comment ?) en maîtrisant ces outils
- L'expertise dans la recherche (réponse aux questions : Quoi ? Où ?) est difficile à acquérir, les idées de tout le monde sont les bienvenues : le travail en binôme est plus efficace.



## *Idées*

- Rechercher les exécutables en exécution qui ont été effacés
- Rechercher les fichiers effacés utilisés par un programme en cours d'exécution