# Analyse de machines UNIX compromises

**Cert-IST - www.cert-ist.com**

**Philippe.Bourgeois@cert-ist.com**



## Objectifs de l'investigation

- **Comprendre les événements survenus**
  - Nature de l'attaque
  - Activité illicite sur le système
- **Identifier les altérations du système**
  - Backdoors, Troyans
  - Données altérées, ajoutées, détruites
- **Identifier l'attaquant et les motivations**

**=> qui, quand, comment, pourquoi, etc...**

## Principes d'investigation (1/2)

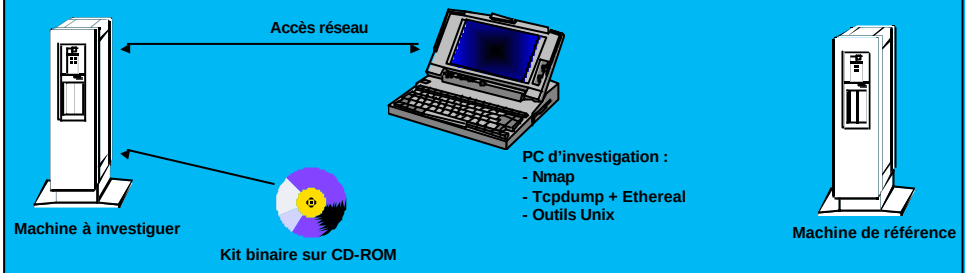
- **Démarche générale**
  - Identifier la date de la compromission (T0)
  - Reconstituer l'activité du système depuis T0
- **Moyens disponibles**
  - Anomalies trouvées sur le système
  - Log, accounting, données d'audit
  - Contrôle d'intégrité
  - Techniques d'autopsie (fichiers effacés, analyse de binaires, etc…)



## Principes d'investigation (2/2)

- **Les préoccupations majeures**
  - La machine peut-être « piégée »
  - Ne pas altérer les données du système
- **Les principes retenus**
  - Capturer l'état du système (préserver l'existant)
  - Analyser les données sur une machine tierce (poste d'investigation)

# Le matériel d'investigation

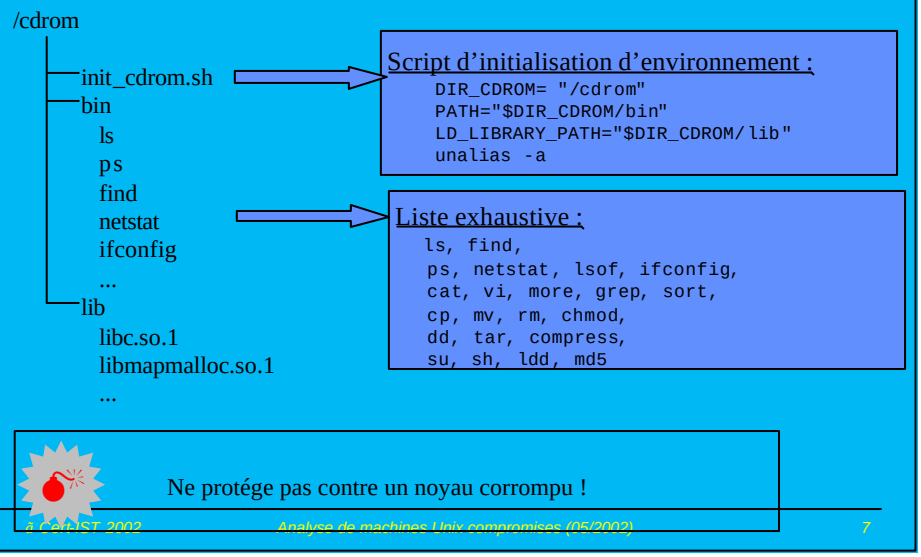





# RootKits, LKM, etc

- **Types de piéges :**
  - Binaires ou librairies dynamiques corrompus
  - Noyaux corrompus (LKM)
  - Mécanismes d'effacements pré-programmés
- **Prévoir des moyens d'éviter les piéges classiques**
  - Kits binaires d'intervention (par ex. sur CD-ROM)
  - Garder à l'esprit que les données collectées peuvent être incomplètes

# Kit binaire d'intervention






# Capture de l'état du système (1/2)

- **Eléments à capturer, par ordre de volatilité**
  - Dates associées aux fichiers
    - « graverobber –m » ou programme spécifique
  - Processus, connexions réseau, fichiers ouverts
    - « ps », « netstat », « ifconfig », « lsof »
    - En profiter pour capturer aussi le résultat des commandes natives (détection de root-kits)
  - Copie physique (dd) des disques
    - Si possible (problème de volume), toutes les partitions
    - Copier aussi l'espace de swap
    - Ne pas oublier de noter la géométrie et le partitionnement

## Capture de l'état du système (2/2)

- **Copie de disque au travers du réseau**
  - « rsh poste_compromis "dd if=/dev/c0t0d0s* bs=1024 "
    | dd bs=1024 of=./img_c0t0d0s* »
  - « nc –l –p 60000 >./img_c0t0d0s* »
    « dd if=/dev/c0t0d0s* bs=1024 | ./nc 192.168.0.1 60000 –w 3 »
- **Accès à un fichier « image disque »**
  - mount –t ufs –o loop,ro,noexec,nodev ./img_c0t0d0s0 /DISK
- **Attention à la limite 2Go de Linux 2.2.x**



## Survol de la phase d'Analyse

- **Trouver des éléments anormaux et les dater (approcher le « T0 »)**
  - Recherche de rootkits
  - Recherche d'anomalies classiques
  - Recherche de toutes les modifications du système (ex. : Tripwire)
- **Reconstituer l'activité du système depuis T0**
  - Avec les Logs
  - Avec MACTIME
- **Analyse de détail**
  - Récupération de fichiers effacés
  - Analyse de binaires, analyse de swap, etc..

## Recherche de rootkits


- **Cas d'un rootkit conventionnel**
  - « ls.sain » vs « ls.natif » suffit pour identifier les fichiers cachés

[Démonstration]

- **Cas d'un rootkit LKM**
  - « ancheck » (outil Cert-IST ☺)



## Recherche d'anomalies classiques (les trucs et astuces qui marchent)


- **Contrôle du contenu de certains fichiers**
  « /etc/passwd », « /etc/inetd.conf », « shell history »

- **Recherche de répertoires/fichiers**
  - Fichiers réguliers sous « /dev » (ex. « /dev/ptyr »)
    - find /dev -type f -print | cat -tve
  - Répertoires « … », « .. »
    - find / -name « .* » -type d -print -xdev | cat –tve

[Démonstration]

- **Recherche de certaines traces « syslog »**

[Exemple]

## Recherche de toutes les modifications du système

- **Tripwire**
- **Comparaison avec une machine « saine »**
  « find / -xdev -type f -exec md5 {} \; |sort »
- **Rpm –v**



## Reconstituer l'activité : Par les Logs

- **Les LOGS sont la source d'information principale prévue pour conserver une trace de l'activité du système**
- **Ils peuvent cependant avoir été :**
  - Effacés
  - Ou brouillés (ex. : sauts de dates)
- **Un examen minutieux des logs est incontournable.**

## Reconstituer l'activité : Dates MAC sur les fichiers


- **Dates associées aux fichiers et répertoires**
  - M: modification du contenu « ls -l »
  - A: accès « ls -lu »
  - C: modification d'un attribut « ls -lc »
- **Exploitation au moyen de « mactime » du TCT**

[Démonstration]



## Récupération de fichiers effacés


- **Facile dans le cas de Linux**
  - Utiliser « icat » du TCT

[Démonstration]

- **Facile aussi de chercher un fichier ASCII précis**
  - Savoir ce que l'on cherche
  - Déterminer le pattern correspondant
  - Strings /dev/hda1 |more …

[Démonstration]

- **Lazarus ? (du TCT)**

## Analyse de binaires


- **Analyse « externe »**
  - File, strings
- **Observation de l'exécution**
  - Truss, strace
- **Décompilation ?**
  - Nécessite beaucoup de temps … et d'expertise



## Analyse de swap


- **Un simple « strings » peut révéler des informations intéressantes.**

[Exemple]

- **Impossible (?) cependant de dater les événements observés.**

## Quelques liens intéressants


- **TCT : The Coroner's Toolkit**
  http://www.fish.com/forensics/ http://www.porcupine.org/tct/
- **Basic steps in forensic analysis of Unix systems**
  http://staff.washington.edu/dittrich/misc/forensic
- **Incident handling step by step**
  http://www.sans.org/y2k/DDOS.htm
- **The forensic challenge**
  http://project.honeynet.org/challenge/