CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Cinquièmes Journées Informatique IN2P3 / CEA-DAPNIA

Gérer une intrusion

Valpré – 18 au 21/09/2006

Denis PUGNÈRE – IPNL / IN2P3 - <d.pugnere@ipnl.in2p3.fr>

Plan

- Introduction : contexte et objectifs
- Incidents et attaques, symptomes
- Éléments techniques
- Les traces
- Contexte juridique
- Le dépôt de plainte
- L'acquisition des traces
- Démarche
- Les boites à outils
- Plan de reprise après incident

Contexte de cette présentation

- Action concertée de l'UREC : A2IMP (Aide à l'Acquisition d'Informations sur une Machine Piratée)
- Élaboration : F. Bongat (CNRS/IPSL), N. Dausque (CNRS/UREC), C. Dubois (CERTA), M. Herrb (CNRS/LAAS), D. Pugnère (IN2P3/IPNL), M-C. Quidoz (CNRS/UREC)
- Formation nationale de même type que SIARS :
  - Des coordinateurs sécurité régionaux (42 coordinateurs, 8 correspondants, 1 CERT-RENATER, 1 CERTA, 4 autres)
  - Redonner ce cours aux correspondants sécurité (CSSI) des laboratoires

Objectif

- Permettre d'acquérir, d'actualiser ou d'approfondir les connaissances
  - Pour acquérir les bons réflexes
  - En situation d'urgence
  - Pour sauvegarder les données indispensables
  - Tout en leur gardant une recevabilité juridique
  - Et cela sur différents types de systèmes d'exploitation (linux, windows, macosX)

Plan

- Introduction
- Incidents et attaques, symptomes
- Éléments techniques
- Les traces
- Contexte juridique
- Le dépôt de plainte
- L'acquisition des traces
- Démarche
- Les boites à outils
- Plan de reprise après incident

Incidents et attaques actuels

- Dysfonctionnement dû à modifications frauduleuses de sites par défiguration (cf. par exemple CERT-Renater : 2006/STAT034)
- Altération des caractéristiques via phishing (cf. par exemple CERT-Renater : 2006/STAT031)
- Ver/Virus toujours !
  - Cf. CERTA-2006-COM-015 [Ver MocBot ou WargBot] du 30/08/06 18:27
  - Ver exploitant la vulnérabilité MS06-040 (vulnérabilité du service serveur ports TCP 139 et 445) et appelé MocBot ou WargBot et se propageant via le logiciel AOL Instant Messenger
- Vol de mot de passe toujours !
  - Cf. CERT-Renater : 2006/STAT032
  - …plusieurs couples login/mot de passe étaient trop simples
  - …intrusion ssh par vol de mot de passe sur une machine

Symptomes

- Machine figée, ne répond plus et écran normal
- Système inaccessible
- Temps de réponse lent
- Réseau saturé
- Reboot bizarre de la machine
- Message affiché à l'écran (d'erreur demandant une action, ironique et provocateur, Fenêtre popup bizarre...)
- Incidents en série
- Espace disque plein

Symptomes (2)

- Informations inattendues dans fichiers traces (des équipements, des applications, …)
- Fichiers incompatibles avec système (exemple sur macOS X : .exe)
- Disparition de fichiers
- Processus inconnus
- Modification de la crontab
- Création de comptes utilisateurs
- Commande ne renvoyant pas les informations escomptées
- Application dont la configuration apparaît comme étant modifiée

Symptomes : épilogue

- Un symptôme observé ==> ne pas « se voiler la face » !
- « Quand l'attaque est visible le mal est déjà fait… » (Stanislas de Maupeou – CERTA)
- Peut-on décider qu'il y a un incident ?
  - D'autres symptômes évidents ?
  - De mémoire, plusieurs avis CERTs faisaient état de ce/ces types de symptômes
  - Sur le campus, le réseau régional …, plusieurs sites ont été compromis

=> Je lance une procédure de déclaration d'incident, mais surtout je tente d'acquérir le maximum d'informations

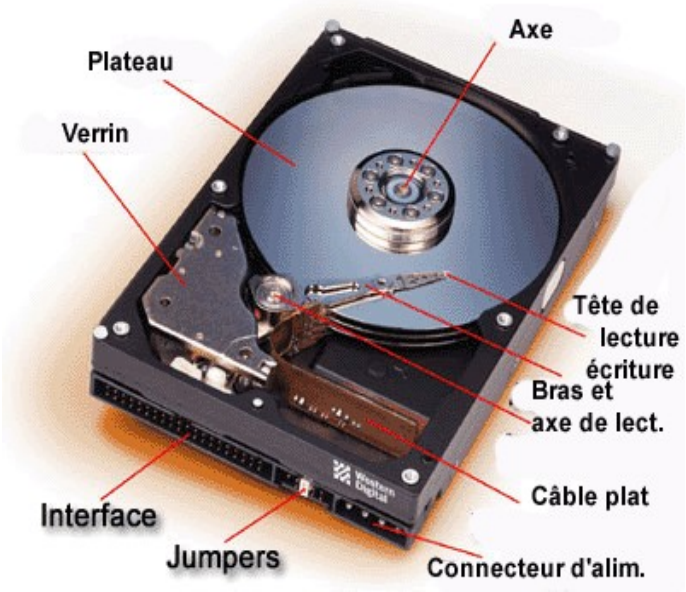
Plan

- Introduction
- Incidents et attaques, symptomes
- Éléments techniques
  - Disques, interfaces,
  - partitions,
  - structure des systèmes de fichiers,
  - les systèmes de fichiers locaux
- Les traces
- Contexte juridique
- Le dépôt de plainte
- L'acquisition des traces

...

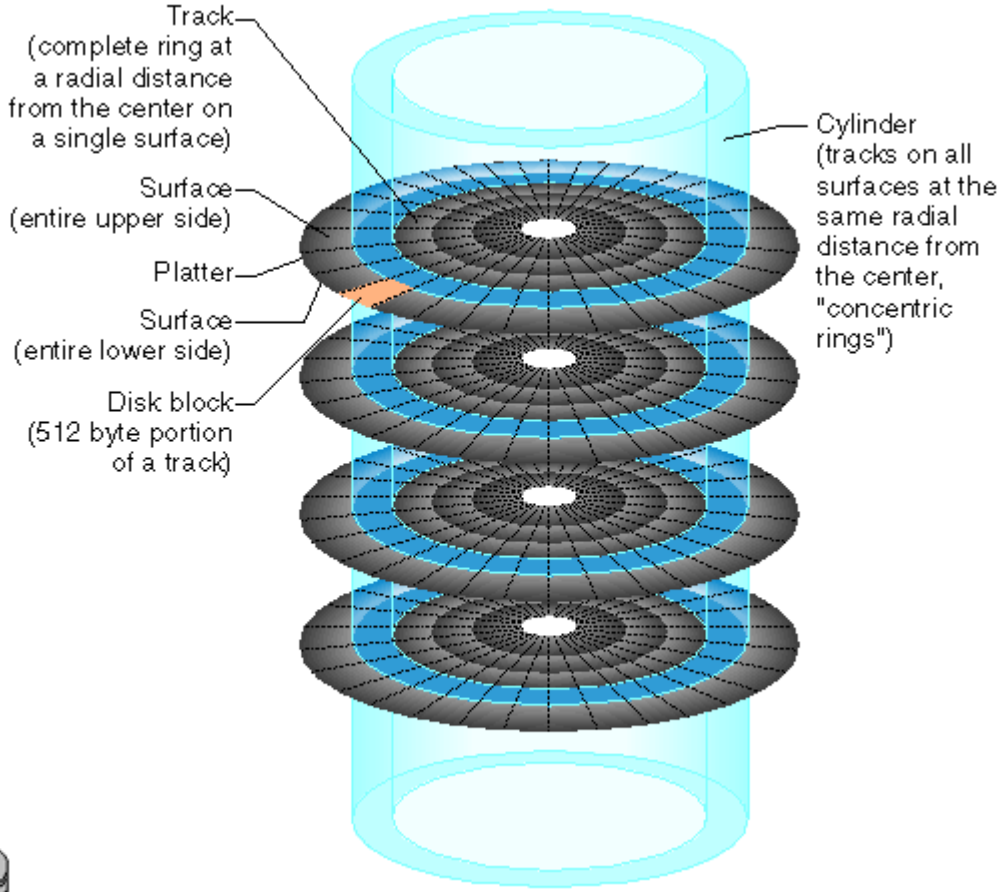
Structure d'un disque

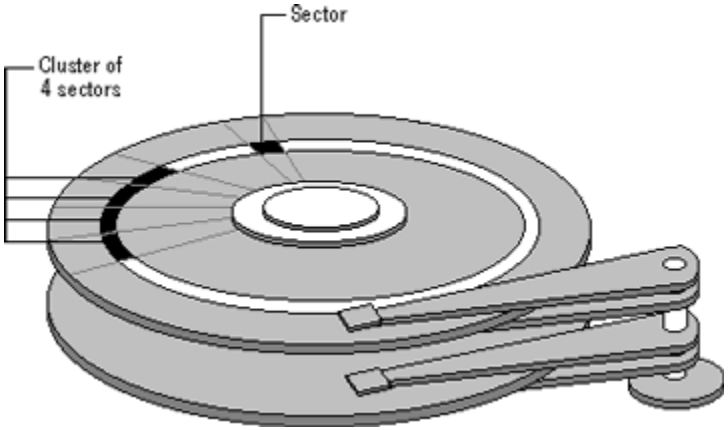
- Caractéristiques physiques
  - Nombre de plateaux
  - Nombre de têtes : NB plateaux x 2
  - Nombre de pistes par plateau
  - Nombre de secteurs par piste
- Type d'interface
- Protocole de transfert
- Vitesse de rotation : 5 400, 6 400, 7200, 10000 et même 15 000 tr/min



CHS : Cylinders, Heads, Sectors

- CHS : cylindres (Cylinder), les têtes (Heads) et les secteurs (Sectors)
- Pistes : cercles concentriques
- Cylindres : ensemble des mêmes pistes de toutes les faces des plateaux
- Secteur : bloc de 512 octets
- Clusters : regroupement de secteurs contigus





IDE (Integrated Device Electronics)

- généralement 2 bus par contrôleur (primaire, secondaire),
- sur chaque bus : 2 périphériques maximum : 1 maître + 1 esclave
- soit 4 périphériques au maximum,
- Longueur bus 46 cm maximum
- Limitations :
  - CHS : (1024 * 16 * 63) * 512 octets = 528 Mo,
  - CHS étendu : 8 Go,
  - LBA (adressage linéaire des secteurs sur 28 bits) : 2^{28} * 512 = 128 Go
  - LBA à partir ATA/133 (adressage linéaire des secteurs sur 48 bits, norme ATA/ATAPI-6) : 2^{48} * 512 = 128 Po

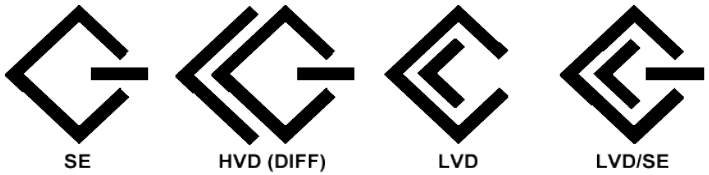
	Mode					
	PIO-3	**PIO-4**	**DMA-33**	**DMA-66**	**DMA-100**	**DMA-133**
Fréquence bus	8,33 Mhz	8,33 Mhz	33 Mhz	66 Mhz	100 Mhz	133 Mhz
Taux transfert	11,1 Mo/s	16,67 Mo/s	33,4 Mo/s	66,8 Mo/s	101,2 Mo/s	133,6 Mo/s

SATA (Serial AT Attachment)

- Bus série interne destiné à remplacer l'ATA/133
- Pas de maître / esclave, chaque périphérique est connecté à un port physique du contrôleur
- Hotplug
- Longueur câble 1 mètre
- SATA1 : 150 Mo/s
- SATA2 : 300 Mo/s

SCSI (Small Computer System Interface)

- Bus externe parallele permettant de gérer plusieurs périphériques
- Bus = 1 HBA + périphériques + terminaisons
- Narrow (8 bits, 50 broches) <=> 7 périphériques
- Wide (16bits, 68 broches) <=> 14 périphériques
- Différentes tensions :



Nom	Narrow	Wide	Longueur		
			Single Ended	High Voltage Diff	Low Voltage Diff
SCSI-1	5Mo/s		6	25	N/A
SCSI-2 (fast)	10Mo/s	20Mo/s	3	25	N/A
SCSI-3 (ultra)	20Mo/s	40Mo/s	1,5	25	N/A
Ultra 2 SCSI	40Mo/s	80Mo/s	N/A	25	12
Ultra 3 SCSI	80Mo/s	160Mo/s	N/A	25	12
Ultra 320 SCSI		320 Mo/s	N/A	N/A	12
Ultra 640 SCSI		640 Mo/s	N/A	N/A	12

SCSI (2)

- SAS : Serial Attached SCSI
  - Chaque disque est attaché au contrôleur
  - Chaque disque dispose de 3Gbits/s
- FC : Fiber Channel
  - SCSI sur média optique
  - mutualisation du stockage pour un ensemble de serveurs
  - 1 HBA (+ switch optionnel) + périphérique
- iSCSI : utilisation d'un réseau IP (LAN, WAN) avec des paquets qui encapsulent les commandes du protocole SCSI

Firewire

- Firewire :
  - bus interne / externe
  - Hotplug
  - Adressage des périphériques sur 16 bits (65535 périphériques)
- IEEE 1394a (Apple : Firewire, Sony : i.Link)
  - IEEE 1394a-S100 : 100 MBits/s
  - IEEE 1394a-S200 : 200 Mbits/s
  - IEEE 1394a-S400 : 400 Mbits/s
- IEEE 1394b (Apple : Firewire 2)
  - IEEE 1394b-S800 : 800 Mbits/s
  - IEEE 1394b-S1200 : 1200 Mbits/s
  - IEEE 1394b-S1600 : 1600 Mbits/s
  - IEEE 1394b-S3200 : 3200 MBits/s

USB : Universal Serial Bus

- Caractéristiques
  - Bus externe série
  - Hotplug
  - Adressage des périphériques sur 7 bits (127 périphériques)
- Versions
  - USB 1.0 et 1.1 : 1,5M Bits/s / 12 M Bits/s
  - USB 2.0 : 480M Bits/s

RAID

- Redondant Array of Independant Disks : aggregation de la capacité d'un ensemble de disques, sécurisation par la redondance :
  - 0 : striping,
  - 1 : mirroir,
  - 10 : striping + mirroir,
  - 3, 5, 6 : disque supplémentaire, stockage de la parité calculée
- Matérielle : processeur spécialisé (intégré ou sur une carte aditionnelle) dédié à cette tâche
- Logicielle : le processeur du système réalise cette tâche, c'est le système d'exploitation qui offre (ou non) cette fonctionnalité

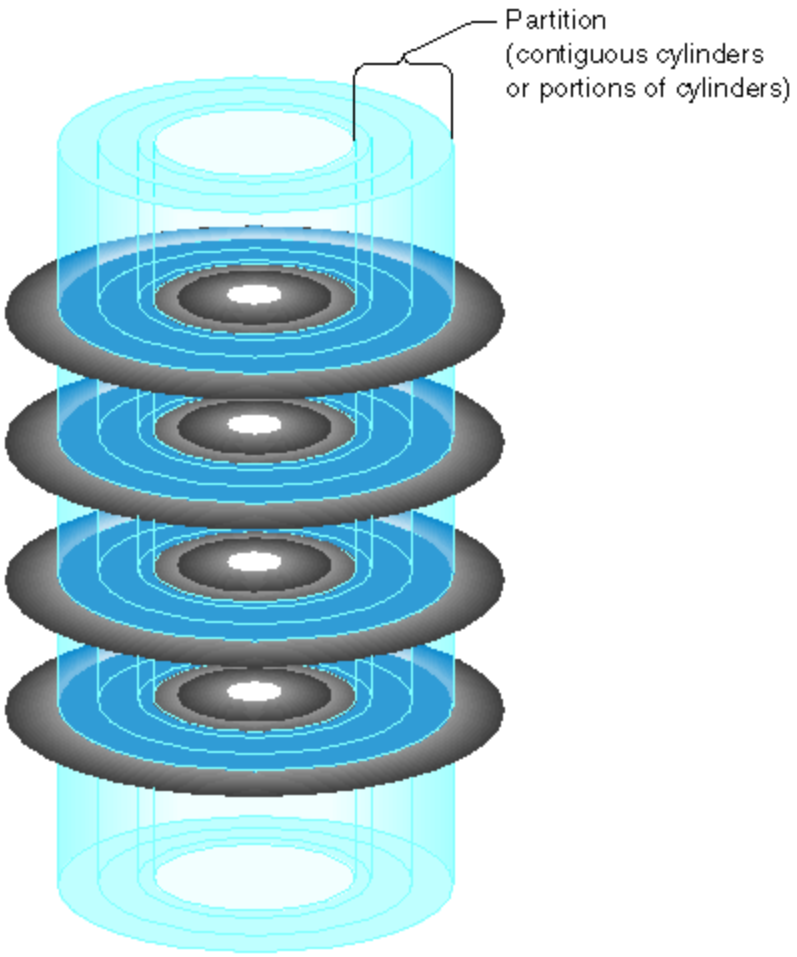
Plan

- Introduction
- Incidents et attaques, symptomes
- Éléments techniques
  - Disques, interfaces,
  - partitions,
  - structure des systèmes de fichiers,
  - les systèmes de fichiers locaux
- Les traces
- Contexte juridique
- Le dépôt de plainte
- L'acquisition des traces

...

Partitionnement de disques

- Types de tables de partitions (labels) : Dos, BSD, SUN, SGI...
- Structure différente pour chaque type de tables de partitions
  - SGI : 16 partitions
  - DOS : 4 primaires max, 1 étendue contenant des partitions logiques
  - ...



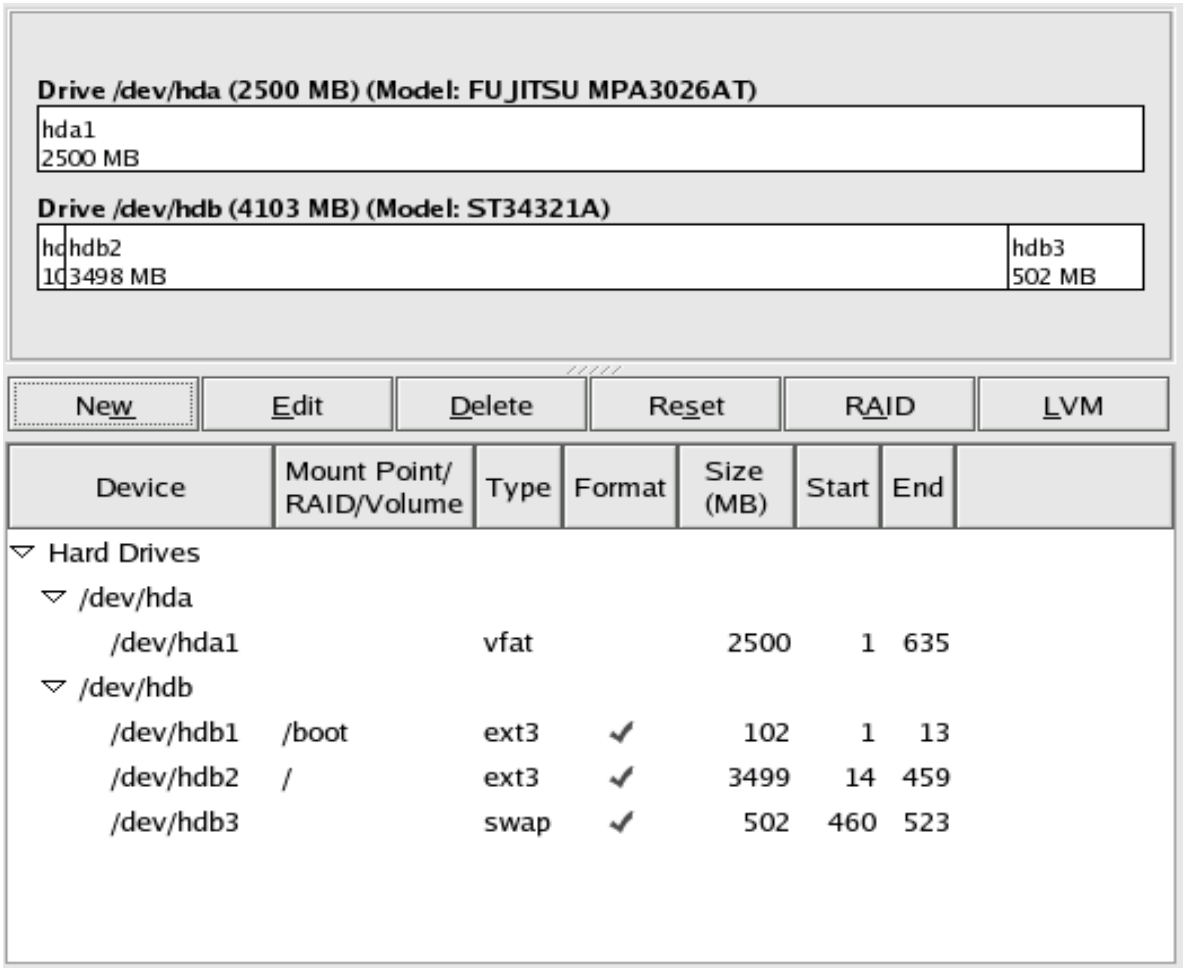
Partitions

- Caractéristiques d'une partition :
  - Bootable (drapeau : o/n)
  - Début
  - Fin
  - Type :

0	Empty	1e	Hidden W95 FAT1	75	PC/IX	be	Solaris boot
1	FAT12	24	NEC DOS	80	Old Minix	bf	Solaris
2	XENIX root	39	Plan 9	81	Minix / old Lin	c1	DRDOS/sec (FAT-
3	XENIX usr	3c	PartitionMagic	82	Linux swap	c4	DRDOS/sec (FAT-
4	FAT16 <32M	40	Venix 80286	83	Linux	c6	DRDOS/sec (FAT-
5	Extended	41	PPC PReP Boot	84	OS/2 hidden C:	c7	Syrinx
6	FAT16	42	SFS	85	Linux extended	da	Non-FS data
7	HPFS/NTFS	4d	QNX4.x	86	NTFS volume set	db	CP/M / CTOS / .
8	AIX	4e	QNX4.x 2nd part	87	NTFS volume set	de	Dell Utility
9	AIX bootable	4f	QNX4.x 3rd part	**8e**	**Linux LVM**	df	BootIt
a	OS/2 Boot Manag	50	OnTrack DM	93	Amoeba	e1	DOS access
b	W95 FAT32	51	OnTrack DM6 Aux	94	Amoeba BBT	e3	DOS R/O
c	W95 FAT32 (LBA)	52	CP/M	9f	BSD/OS	e4	SpeedStor
e	W95 FAT16 (LBA)	53	OnTrack DM6 Aux	a0	IBM Thinkpad hi	eb	BeOS fs
f	W95 Ext'd (LBA)	54	OnTrackDM6	a5	FreeBSD	ee	EFI GPT
10	OPUS	55	EZ-Drive	a6	OpenBSD	ef	EFI (FAT-12/16/
11	Hidden FAT12	56	Golden Bow	a7	NeXTSTEP	f0	Linux/PA-RISC b
12	Compaq diagnost	5c	Priam Edisk	a8	Darwin UFS	f1	SpeedStor
14	Hidden FAT16 <3	61	SpeedStor	a9	NetBSD	f4	SpeedStor
16	Hidden FAT16	63	GNU HURD or Sys	ab	Darwin boot	f2	DOS secondary
17	Hidden HPFS/NTF	64	Novell Netware	b7	BSDI fs	**fd**	**Linux raid auto**
18	AST SmartSleep	65	Novell Netware	b8	BSDI swap	fe	LANstep
1b	Hidden W95 FAT3	70	DiskSecure Mult	bb	Boot Wizard hid	ff	BBT
1c	Hidden W95 FAT3						

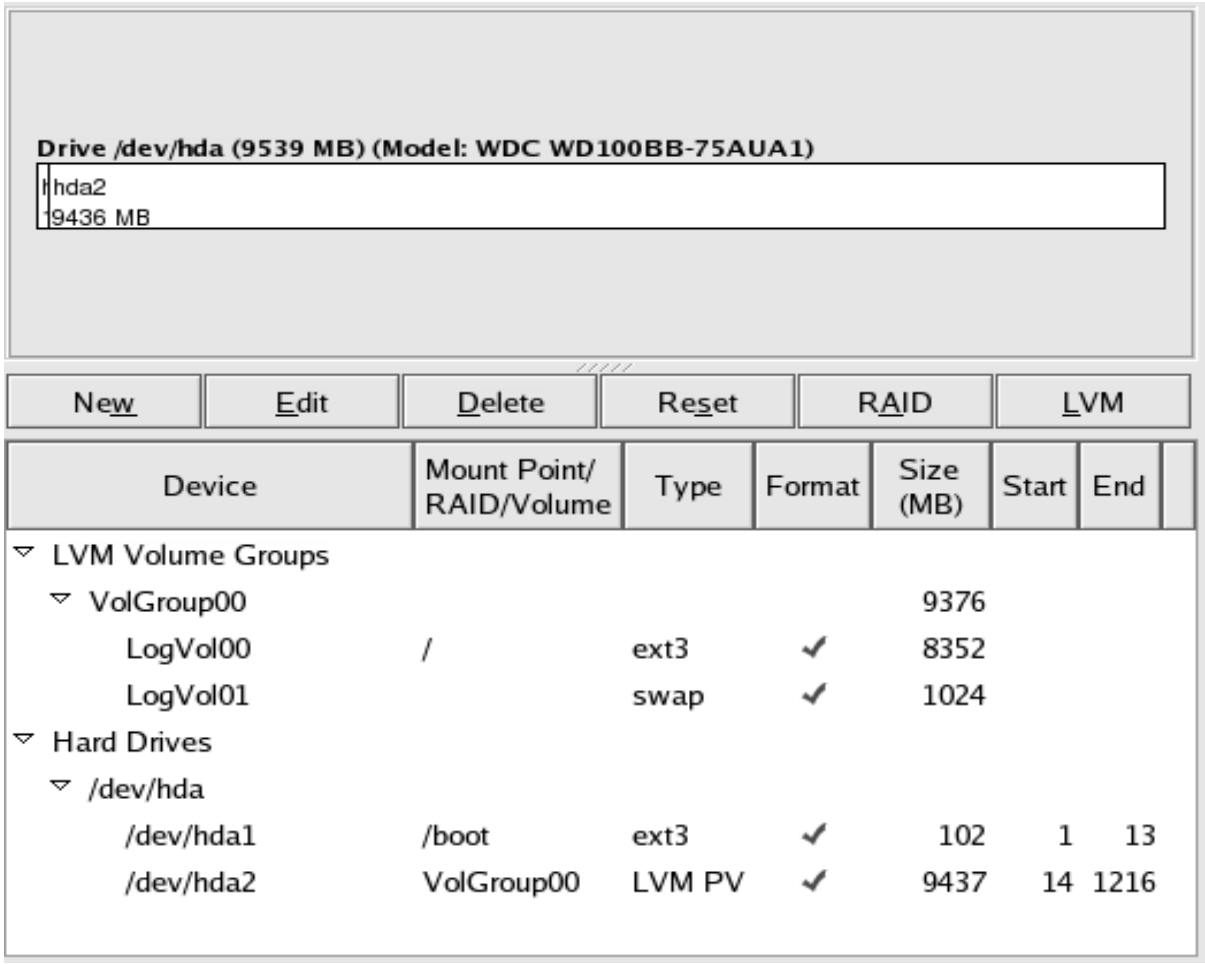
Exemples de partitionnements (1)

- Partitions natives



Exemples de partitionnements (2)

- Partitions à l'intérieur d'un gestionnaire de volumes (LVM, EVMS)



Plan

- Introduction
- Incidents et attaques, symptomes
- Éléments techniques
  - Disques, interfaces,
  - partitions,
  - structure des systèmes de fichiers,
  - les systèmes de fichiers locaux
- Les traces
- Contexte juridique
- Le dépôt de plainte
- L'acquisition des traces

...

Structure des systèmes de fichiers

- 3 entités :
  - Le superbloc : décrit l'état d'occupation des secteurs alloués au système de fichiers, contient :
    - La taille (en blocs) de la liste des inodes,
    - la taille (en blocs) du système de fichiers,
    - le nom du système de fichiers,
    - la liste des blocs et des inodes libres,
    - le nombre de blocs et d'inodes libres
  - Les inodes : élément fondamental
    - Référence au propriétaire
    - les droits d'accès du fichier,
    - la taille du fichier
    - les dates (MAC : modification, access, change + deletion time)
    - le type de fichier (répertoire, fichier, device, pipe...)
  - Les fichiers de données

Plan

- Introduction
- Incidents et attaques, symptomes
- Éléments techniques
  - Disques, interfaces,
  - partitions,
  - structure des systèmes de fichiers,
  - les systèmes de fichiers locaux
- Les traces
- Contexte juridique
- Le dépôt de plainte
- L'acquisition des traces

...

Systèmes de fichiers locaux

- Différents types suivant les systèmes :
  - FAT, FAT32, (DOS, Windows 98/Me)
  - NTFS (Windows NT/2000/XP/2003) : data + ADS (streams)
  - Ext2 / ext3 (Linux)
  - UFS : Unix File System (Sun, *BSD)
  - HFS et HFS+ (Apple MacOS) : data + ressource
  - XFS (SGI Irix, Linux),
  - JFS (IBM Aix, Linux)

=> Différencier taille d'un bloc physique du disque et unité d'allocation (cluster) du système de fichier

Plan

- Introduction
- Incidents et attaques, symptomes
- Éléments techniques
- Les traces
  - Les traces sur le matériel
  - Les traces systèmes
  - La synchronisation
  - La centralisation des logs
- Contexte juridique
- Le dépôt de plainte

...

Traces

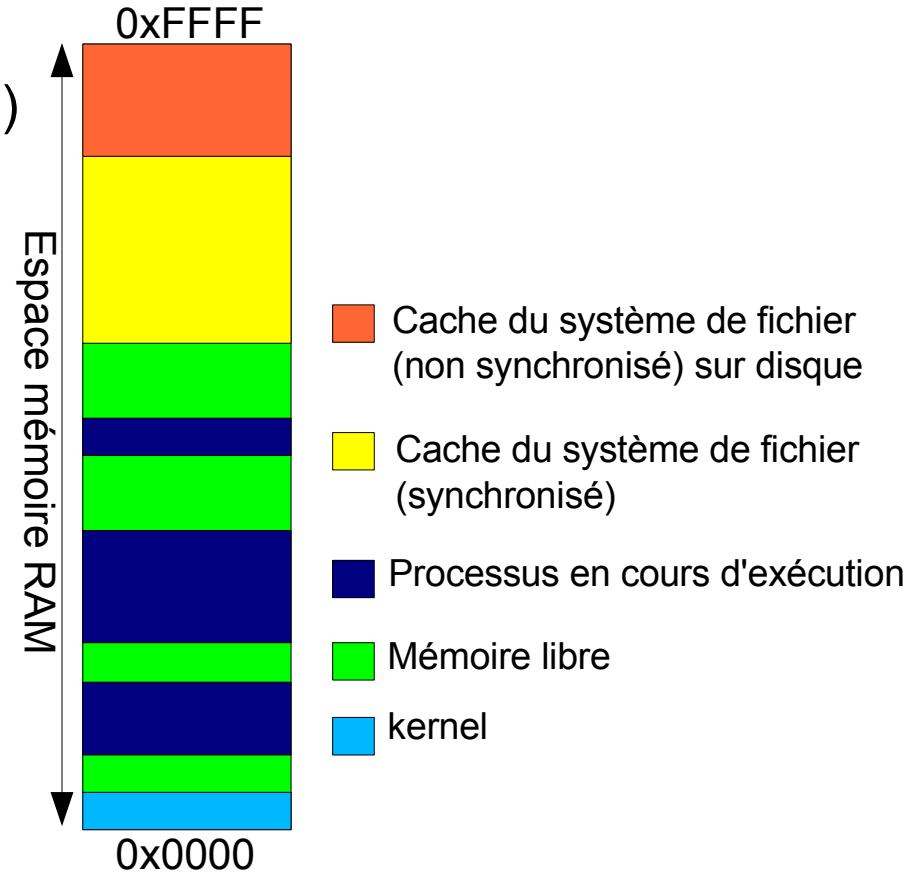
- Définition : influence d'un événement sur son environnement
- Qu'est ce qui diffère un événement d'un incident ?
  - La connaissance de ce qu'est un événement
  - La connaissance de ce qu'est un incident
  - Exemple :
    - 1 Connexion ssh depuis 198.81.129.x
    - 10 connexions ssh depuis 193.49.159.x

```
IP range     : 193.49.159.0 - 193.49.159.255
Network name : FR-RENATER
Infos        : RENATER
Infos        : 151, Boulevard de l'hopital,
Infos        : 75013 Paris, FRANCE
Country      : France (FR)
Abuse E-mail : certsvp@renater.fr
Source       : RIPE
```

```
IP range     : 198.81.128.0 - 198.81.191.255
Network name : OIT-BLK1
Infos        : Central Intelligence Agency
Infos        : Washington
Country      : United States of America (US)
Abuse E-mail : abuse-mail@mci.com
Source       : ARIN
```

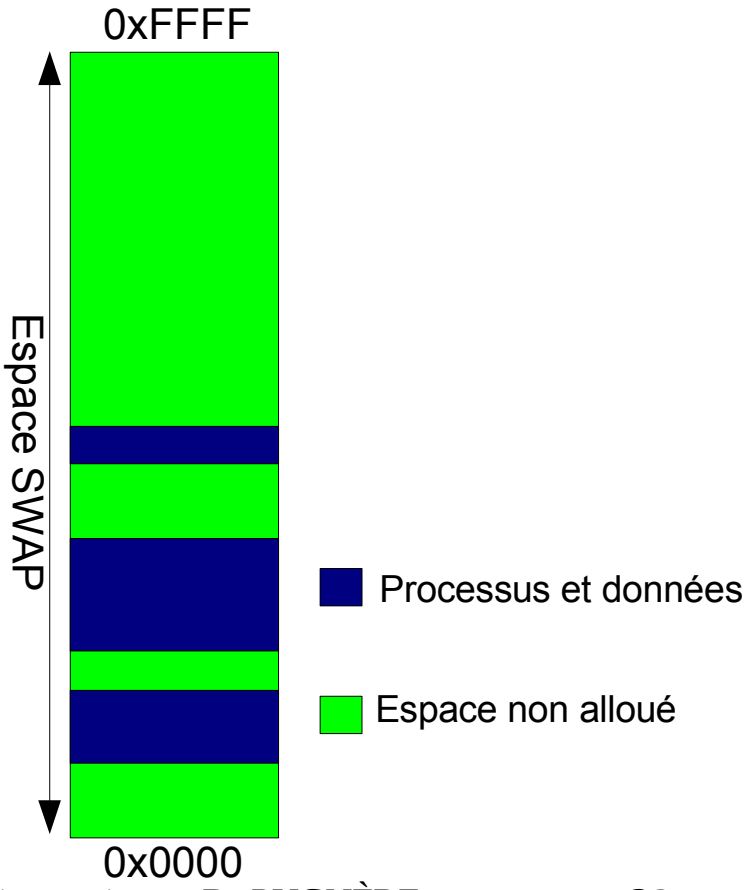
Traces en RAM

- Informations volatiles
  - Processus en cours d'execution
  - Connexions ouvertes
  - Cache des systèmes de fichiers
  - La mémoire libre (non réallouée) contient potentiellement des traces de processus précédemment lancés



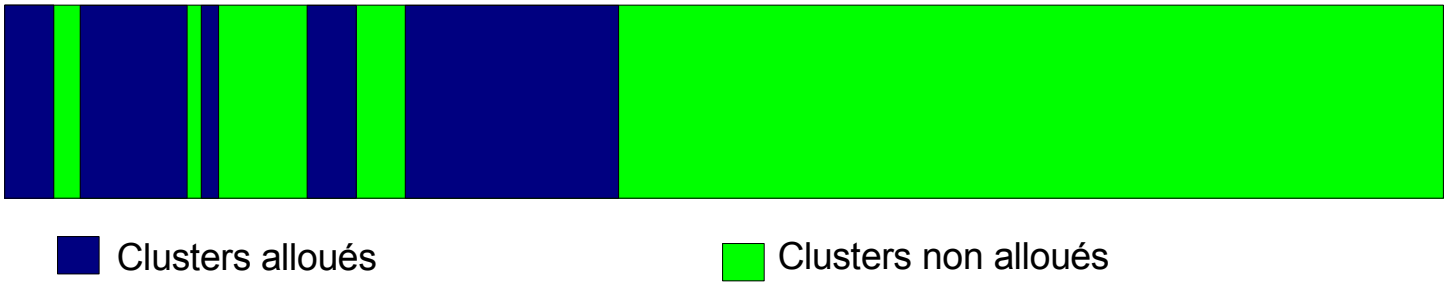
Traces en SWAP

- Zone temporaire sur disque utilisée en cas de manque d'espace RAM pour l'allocation mémoire aux processus en cours d'exécution
  - SWAPPER : Le kernel déplace l'espace allouée au processus de la RAM vers le SWAP, ou dans l'autre sens
  - Le SWAP contient potentiellement des traces d'exécution de processus précédemment lancés

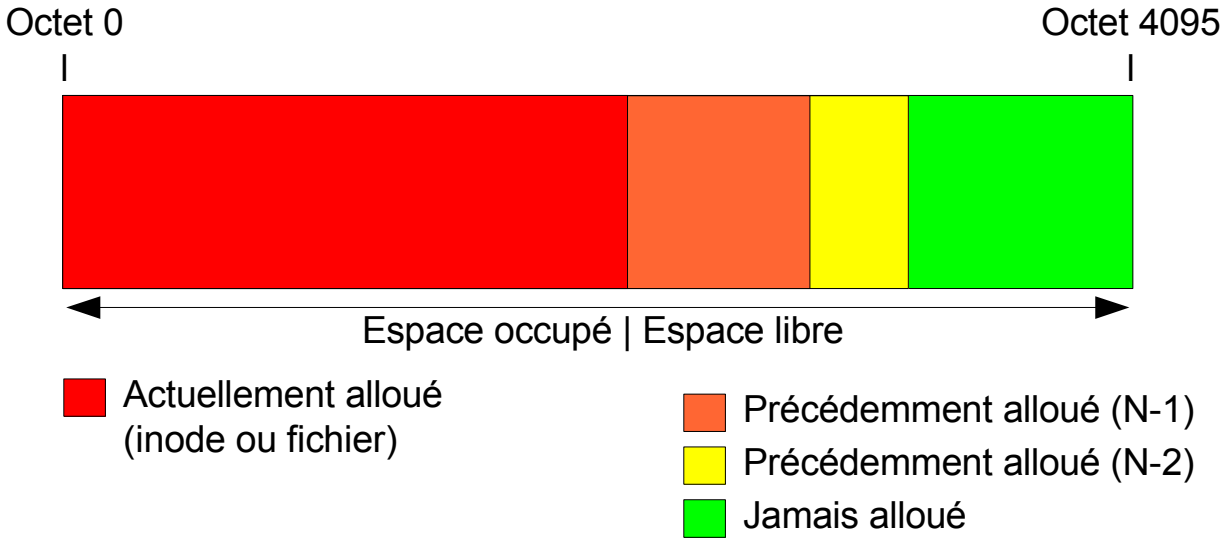


Traces sur disque

- Espace d'une partition



- Cluster partiellement alloué : slackspaces ?



Plan

- Introduction
- Incidents et attaques, symptomes
- Éléments techniques
- Les traces
  - Les traces sur le matériel
  - Les traces systèmes
  - La synchronisation
  - La centralisation des logs
- Contexte juridique
- Le dépôt de plainte

...

Traces Système

- Logs systèmes et applicatifs
- Logs des services réseaux (web, proxy, SMTP, POP, IMAP SSH,DNS, SSH, FTP, LDAP...)
- Pour chaque fichier du système :
  - MAC Time (Modification, Access, Change)
  - taille,
  - empreinte (MD5, SHA)
- Fichiers ouverts,
- librairies dynamiques chargées
- Connexions ouvertes par les processus
- Modules du noyau (pour les noyaux modulaires)

Traces Réseau

- Connexions ouvertes depuis ou vers un système particulier
- Flux réseaux
  - Métrologie :
    - Flux =
      - ip source, ip destination, protocole,
      - TCP, UDP : port source + port destination
      - ICMP : type + code
      - Date début + date fin
      - Nombre d'octets, nombre de paquets
- Logs des matériels réseau : gardes barrière, commutateurs, routeurs, bornes d'accès WIFI

Exemples :

Accès à un service réseau à distance : cas d'un client ssh

```
# lsof -p 24170
COMMAND   PID     USER   FD   TYPE  DEVICE    SIZE    NODE NAME
ssh     24258 testuser  rtd    DIR     8,1    4096       2 /
ssh     24258 testuser  txt    REG     8,1  266008 1087545 /usr/bin/ssh
ssh     24258 testuser  mem    REG     8,1 1572460  178516 /lib/tls/libc-2.3.2.so
ssh     24258 testuser  mem    REG     8,1   76712  146095 /usr/kerberos/lib/libgssapi_krb5.so.2.2
ssh     24258 testuser  mem    REG     8,1   52096  470589 /lib/libnss_files-2.3.2.so
ssh     24258 testuser  mem    REG     8,1   14812  471349 /lib/libdl-2.3.2.so
ssh     24258 testuser  mem    DEL     8,1          470498 /lib/libcrypto.so.0.9.7a;45061585
ssh     24258 testuser  mem    REG     8,1   76488  470601 /lib/libresolv-2.3.2.so
ssh     24258 testuser  mem    REG     8,1   12488  470607 /lib/libutil-2.3.2.so
ssh     24258 testuser  mem    REG     8,1   23332  470567 /lib/libcrypt-2.3.2.so
ssh     24258 testuser  mem    REG     8,1   72552  146099 /usr/kerberos/lib/libk5crypto.so.3.0
ssh     24258 testuser  mem    REG     8,1  106888  470556 /lib/ld-2.3.2.so
ssh     24258 testuser  mem    REG     8,1   52584 1168199 /usr/lib/libz.so.1.1.4
ssh     24258 testuser  mem    REG     8,1   89668  470573 /lib/libnsl-2.3.2.so
ssh     24258 testuser  mem    REG     8,1   18576  470586 /lib/libnss_dns-2.3.2.so
ssh     24258 testuser  mem    REG     8,1  385252  146758 /usr/kerberos/lib/libkrb5.so.3.1
ssh     24258 testuser  mem    REG     8,1   11844  146140 /usr/kerberos/lib/libdes425.so.3.0
ssh     24258 testuser  mem    REG     8,1    5540  146138 /usr/kerberos/lib/libcom_err.so.3.0
ssh     24258 testuser    0u   CHR  136,39             41 /dev/pts/39
ssh     24258 testuser    1u   CHR  136,39             41 /dev/pts/39
ssh     24258 testuser    2u   CHR  136,39             41 /dev/pts/39
ssh     24258 testuser    3u  IPv4 2852817            TCP testclientssh.fr:57130->
                                                          testserveurssh.fr:ssh (ESTABLISHED)
```

Plan

- Introduction
- Incidents et attaques, symptomes
- Éléments techniques
- Les traces
  - Les traces sur le matériel
  - Les traces systèmes
  - La synchronisation
  - La centralisation des logs
- Contexte juridique
- Le dépôt de plainte

...

Synchronisation

- Les horloges internes des machines (serveurs, PC...) ne sont pas fiables => dérive dans le temps
- Il existe des références précises :
  - Radio : émetteurs de France Inter à Allouis, norme DCF77 à Mainflingen),
  - GPS
  - Accessibles via le réseau : Protocole ntp (RFC 1305)
    - 1 milliseconde < Précision < quelques 10èmes de millisecondes
    - Liste : http://www.cru.fr/NTP/serveurs_francais.html
    - Accessibles librement ou soumis à déclaration ou autorisation d'utilisation

Quoi et comment synchroniser ?

- Tout, par ordre de priorité :
  - Serveurs et matériels réseau
  - Postes clients
- Exemple : utiliser le protocole NTP diffusé sur le réseau :
  - Serveurs références, hiérarchisés (strates)
  - Paquets de type UDP, port distant n° 123
  - Peut être re-diffusé sur le réseau local par un serveur NTP local

Plan

- Introduction
  - Incidents et attaques, symptomes
  - Éléments techniques
  - Les traces
    - Les traces sur le matériel
    - Les traces systèmes
    - La synchronisation
    - La centralisation des logs
  - Contexte juridique

...

Les logs

- Capturer et enregistrer les évènements significatifs
- Souvent répartis :
  - par système : windows (format propriétaire interne), unix
  - Application/service : serveur web (apache, IIS, Active Directory, contrôle d'accès
- Hétérogènes :
  - En format (cisco IOS, cisco PIX, iptables, ipchains, pf, ipfilter...)
  - Type : évènements mélangés : type ALERT, INFO
- Sur serveurs, postes clients

Centralisation des logs

- Technique qui consiste à ce que chaque élément actif d'un système d'information envoie ses journaux à un système dédié qui les réceptionne et les enregistre.
- Avantages recherchés :
  - Pérénité : en rapport avec la législation en vigueur
  - Intégrité : localisation différente de la source
  - Corrélation : facilité apportée par la centralisation

Valeur ajoutée de la centralisation

- Post-traitements rendus possibles :
  - Traitement de logs de pare-feux (detescan, anapirate, fwlogwatch...)
  - Alertes, visualisation
  - Archivage
- IDS (Systèmes de détection d'intrusion) :
  - Réseau : Snort...
  - Hybride (réseau et système) : prelude-ids...
  - Systèmes :
    - Surveillance des fichiers journaux : logcheck, logwatch, swatch, OSSEC...
    - Contrôles d'intégrité des fichiers : tripwire, samhain, AIDE
    - Détection de comportements douteux : portsentry, scanlogd, lids, systrace...

Plan

- Introduction
- Incidents et attaques, symptomes
- Éléments techniques
- Les traces
- Contexte juridique
- Le dépôt de plainte
- L'acquisition des traces
- Démarche
- Les boites à outils
- Plan de reprise après incident

Contexte juridique : Art 40 CPP

Article 40 du code de procédure pénale :

« Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs. »

Contexte juridique : Art 434-4 CP

Art. 434-4 du Code pénal

Est puni de trois ans d'emprisonnement et de 45.000 euros d'amende **le fait, en vue de faire obstacle à la manifestation de la vérité :**

1°) De modifier l'état des lieux **d'un crime ou d'un délit** soit par altération, la falsification ou l'effacement des traces ou indices soit par l'apport, le déplacement ou la suppression d'objets quelconques ;

2°) De détruire soustraire, receler ou altérer un document public ou privé ou un objet de nature à faciliter la découverte d'un crime ou d'un délit, la recherche des preuves ou la condamnation des coupables ;

Lorsque les faits prévus au présent article ont été commis par une personne qui, par ses fonctions est appelée à concourir à la manifestation de la vérité, la peine est portée à cinq ans d'emprisonnement et à 75.000 euros d'amende.

Plan

- Introduction
- Incidents et attaques, symptomes
- Éléments techniques
- Les traces
- Contexte juridique
- Le dépôt de plainte
- L'acquisition des traces
- Démarche
- Les boites à outils
- Plan de reprise après incident

Dépôt de plainte : intérêts

Attention : l'objet de cette section n'est pas de présenter « comment faire un dépôt de plainte et qui le fait » mais de présenter les intérêts et les éléments nécessaires

- Trouver un coupable
- Protéger l'unité, son directeur voire l'organisme
  - Vis-à-vis de la justice après attaque de type « site warez à caractère pédophile », « site dépôt de musiques, films, séries télévisées, … »
  - En cas d'attaque en justice par un tiers sur incident de type « phishing »

Contexte du laboratoire, de l'organisme

- Type de laboratoire
  - Si unité est classée sensible
  - Si contrat(s) avec industriel(s)
- Éléments nécessaires :
  - État daté de la machine
  - Sauvegarde/duplication de la machine dans son état au moment de l'incident/de l'attaque

Plan

- Introduction
- Incidents et attaques, symptomes
- Éléments techniques
- Les traces
- Contexte juridique : statut des traces
- Le dépôt de plainte
- L'acquisition des traces
  - Objectifs
  - Principes
- Démarche
- Les boites à outils
- Plan de reprise après incident

Objectif

- Conservation des traces de la meilleure qualité possible en vue de l'analyse
- Traces : tout ce qui est visible et invisible
- Analyse : répondre aux questions
  - Qui ?
  - Quand ?
  - Comment ?
  - Pourquoi ?

Qui ?

- La réponse à cette question intéresse typiquement les services de police
- Cas particulier : malveillance interne
- En général, la réponse se trouve dans les journaux

Quand ?

- La réponse à cette question intéresse également les services de police
- qui + quand => identification possible
- Parfois utile pour comprendre quelle vulnérabilité a été utilisée
- En général, la réponse se trouve dans les journaux et sur les dates des fichiers

Comment ?

- La réponse à cette question intéresse les CSIRT (CERT-RENATER et CERTA) et la victime
- A des conséquences sur l'administration des machines
- En général, la réponse se trouve dans les journaux

Pourquoi ?

- La réponse à cette question intéresse les CSIRT et la victime
- Permet parfois de découvrir des faiblesses sur le réseau
- Permet aussi de comprendre comment a eu lieu l'intrusion dans certains cas
- Pour répondre à cette question, il est nécessaire d'analyser tout le disque

Temps d'analyse

- Répondre aux questions qui, quand et comment ne prend que quelques heures (voire quelques minutes)
- Répondre à la question pourquoi prend plusieurs jours voire plusieurs semaines
- L'analyse d'un incident permet parfois de mettre en évidence d'autres attaques éventuellement réussies

Plan

- Introduction
- Incidents et attaques, symptomes
- Éléments techniques
- Les traces
- Contexte juridique : statut des traces
- Le dépôt de plainte
- L'acquisition des traces
  - Objectifs
  - Principes
- Démarche
- Les boites à outils
- Plan de reprise après incident

Principes

- 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,
- Garder une trace horodatée des actions réalisées,
- Penser également à recencer et récupérer les traces laissées sur le système d'information en bordure de cette machine (logs et filtres des routeurs, métrologie, contrôles d'accès...)
- Sauvegarder les informations sur un support externe, d'une manière fiable,
- S'assurer que les informations sauvegardées sont intègres,
- S'assurer qu'aucune modification n’a été faite ou ne peut se faire sur les informations sauvegardées.

Quelques principes généraux

Ce que l'expert attend :

- Tout élément qui permettrait de répondre aux questions qu'il se pose
- Dans l'ordre d'importance (point de vue de C.Dubois) :
  - Copie du disque dur (signée pour éviter la contestation)
  - Journaux du réseau
  - Main courante
  - Copie du swap
  - Informations volatiles

Plan

- Introduction
- Incidents et attaques, symptomes
- Éléments techniques
- Les traces
- Contexte juridique : statut des traces
- Le dépôt de plainte
- L'acquisition des traces
- Démarche
- Les boites à outils
- Plan de reprise après incident

Démarche : avant de commencer

- Gérer les priorités :
  - identifier les services impactés
  - informer sa hiérarchie,
  - informer les utilisateurs,
- Se munir de documentation,
- Avoir la boite à outils A2IMP-linux gravée sur CD
- Disposer d'un switch rapide (100Mb/s minimum)
- Posséder des cordons RJ45 droits et/ou croisés,
- Avoir à disposition un espace de stockage suffisant : Autre PC connecté via RJ45 ou disque externe ou boitier dédié...

Démarche

- Créer une main courante
- Analyse des processus et du système
- Si le doute existe :
  - Récupération des informations volatiles (RAM, processus, connexions, environnement)
  - Isoler la machine du réseau et la stopper proprement
  - Démarrer sur un support externe (LiveCD...) sans toucher au disque dur (pas d'utilisation du SWAP, ni de montage des systèmes de fichiers)
  - Sauvegarder le SWAP et les partitions
  - Signer toutes les informations sauvegardées

Prélever le temps

- Préciser le décalage entre l'heure du système et l'horloge parlante
- Dans l'idéal, tous les systèmes sont synchronisés NTP avant l'incident

Main courante (1)

- Noter toutes les opérations effectuées et les communications échangées
  - Particulièrement utile en cas de dépôt de plainte => la police demande la meilleure précision possible lors de l'audition
  - Les incidents engendrent souvent des situations de stress => tendance à l'oubli de ce que l'on fait
  - Permet, dans certains cas lors de l'analyse, de distinguer l'action du pirate de l'action de l'administrateur (journaux des connexions, commandes système, etc.)

Main courante (2)

- Horodater chacune des opérations effectuées, en se synchronisant avec l'horloge parlante (un petit décalage n'est pas très important)
- En croisant avec les dates de la main courante avec celles du système, on arrive parfois à horodater les actions de l'intrus (encadrement des actions du pirate dans un intervalle de temps)

Main courante (3)

- Inclure des éléments de contexte dans la main courante, comme les messages électroniques relatifs à l'incident (ex : message du CERT-RENATER) et retranscrire les éléments les plus pertinents des conversations téléphoniques

Mémoire volatile

- Instantané de la mémoire
- Pas forcément représentatif de l'activité récente de la machine
- Pas le plus important, mais peu coûteux à récupérer

À chaud ou à froid ?

- Problèmes avec les copies à chaud :
  - Le système évolue pendant la copie, des fichiers peuvent ne pas être copiés
  - Il y a des écritures dans les journaux (éventuellement nombreuses si des erreurs disque surviennent) => des blocks de données peuvent être écrasés
- La copie peut nécessiter un fsck avant remontage
- Pourquoi faire une copie à chaud ?
  - Souvent par besoin de disponibilité

=> Préférer des copies à froid dans la mesure du possible !

Éteindre la machine

Deux écoles :

- Arracher le câble d'alimentation
  - Risque de mettre le système dans un état instable
  - Risque d'endommager le disque physiquement
- Arrêter proprement la machine avec les commandes du système
  - Risque que ces commandes aient été sabotées, mais il s'agit d'un risque improbable
- Au CERTA, préférence pour l'arrêt propre du système

Physique ou logique ?

- Problèmes avec les copies logiques :
  - Ne copie pas le « slackspace » (fin des fichiers)
  - Ne copie pas les blocs de données non utilisés (fichiers effacés)
  - Souvent réalisées sur le disque compromis => écrase des traces
- Nécessité absolue de faire des copies physiques !

Avertissement : Toute manipulation de disques durs (démontage physique, déplacement, etc.) risque d'endommager définitivement le disque !

Outils pour la copie

- De nombreux outils permettent de faire des copies, mais certains font des copies propriétaire (Encase par exemple), et nécessitent ces mêmes outils pour pouvoir remonter l'image => risque de ne pas pouvoir exploiter l'image
- Un bon outil gratuit et natif sur linux : dd

Le swap

- Le swap est un fichier sur le disque (pagefile.sys) ou une partition.
- Contient énormément d'informations, mais celles-ci sont non datées et non classées
- Pour le moment, pas d'outils permettant d'analyser efficacement le swap => utilisation de strings et de grep en général
- Fréquent de retrouver l'adresse IP d'un intrus (lors d'une compilation par exemple)

  => intéressant mais pas facilement exploitable

Faire une signature numérique

- De nombreux outils natifs pour le faire : md5sum...
- Signature de l'original stockée dans un fichier puis on vérifie la copie, exemple :
  - md5sum /dev/hda1 > /mnt/disk/hda1.md5sum
  - md5sum /mnt/disk/hda1.dd
- Si le résultat est différent, la copie est ratée
- Quand on n'arrive pas à obtenir une copie identique, ou que l'on utilise conv=noerror, il est important de le préciser dans la main courante
- Inutile d'essayer de signer une copie faite à chaud => impossible de savoir si la copie a réussi…
- La signature numérique permet de vérifier l'état de la copie et d'éviter certaines contestations

Plan

- Introduction
- Incidents et attaques, symptomes
- Éléments techniques
- Les traces
- Contexte juridique : statut des traces
- Le dépôt de plainte
- L'acquisition des traces
- Démarche
- Les boites à outils
- Plan de reprise après incident

Boites à outils : Leur construction

- Approche différente suivant la situation
  - Système (encore) fonctionnel : online
    - Utilisation d'utilitaires statiques depuis le support amovible
  - Système stoppé : offline
    - Démarrage sur un système qui permet d'accéder au stockage
  - Disque (physique), image disque ou images des partitions disponibles

Boites à outils : Fonctionnalités

- Copie d'images disques et RAM et swap
- Énumération des processus
- Énumération des connexions ouvertes
- Énumération de l'environnement (configuration)
- Recouvrement de données effacées
- Suivi activité système
- Capture réseau
- Transfert de données à distance
- Contrôle d'intégrité (calcul du hash)
- Détection de types et propriétés des fichiers
- Boite à outils statique (indépendante de la machine hôte)

Boites à outils : Knoppix std

- URL : http://s-t-d.org
- Fonctionnalités
  - Basée sur la knoppix : Générique, bonne détection matérielle
  - Un grand nombre d'outils classés par fonction : authentification, encryption, forensics (dont dcfldd), firewall, honeypots, ids, network utilities, password tools, packet sniffers
    - Beaucoup d'outils de recherche de données et de tests de vulnérabilités
  - Version actuelle (au 12/09/2006) : 0.1
- Mais :
  - Outils pas très à jour
  - Kernel 2.4.21
  - Attention à la modification du swap au boot

Boites à outils : Fire

- URL : http://fire.dmzs.com/
- Fonctionnalités :
  - Contient des outils pour créer des images disques (rda, dd, dcfldd

  Exemple : dcfdd (Department of Defense Computer Forensics Lab) :
    - Affiche progression
    - Calcule le hash à la volée
    - Peut découper l'image en parties

```
# dcfldd if=/dev/sda of=/media/usb/images-disques/sda.dd \
        conv=noerror,sync hashwindow=0 hashlog=sda.dd.md5
```

Boites à outils : Helix

- URL : http://www.e-fense.com/helix/
- Fonctionnalités
  - Basée sur la knoppix : Générique, bonne détection matérielle
  - Annonce : « *Helix has been modified very carefully to NOT touch the host computer in any way and it is forensically sound* »
  - Un grand nombre d'outils orientés sur l'acquisition (dd, sdd, dcfldd, 2hash, ...), l'analyse de structure d'images disques (sleuthkit, autopsy), la recherche de fichiers sur le contenu (foremost, Scalpel...)
  - Également : boite à outils pour Windows
  - Version actuelle (au 12/09/2006) : 1.7 (Kernel 2.6.14)
  - Très bonne documentation : « Helix for Beginners »
  - Contient des binaires pour Windows, Linux et Solaris

Boites à outils : a2imp

- Certains outils statiques ne sont pas utilisables sur certains systèmes...
- Choix :
  - Nous avions déjà des outils compilés en statique => utilisation sur système Linux *online*
  - Création d'un CD bootable Linux de type LiveCD => utilisation sur système (Linux, Windows) *offline* également
- Intégration des utilitaires dédiés à l'acquisition de données :
  - Utilitaires binaires statiques a2imp-linux
  - Utilitaires binaires a2imp-windows
- Modification des scripts de démarrage
  - Non altération de l'espace de stockage

Principaux outils d'analyse système

- Tct (The Coroner's Toolkit) : http://www.porcupine.org/forensics/tct.html

  Collection d'outils d'analyse de systèmes de fichiers
- Sleuthkit : http://www.sleuthkit.org/sleuthkit/desc.php
  - reconnaît différents types detables de partitions (DOS, BSD, MAC, SUN)
  - Ensemble d'outils permettant d'analyser différents types de systèmes de fichiers (NTFS, FAT, UFS 1, UFS 2, EXT2FS, EXT3FS, ISO 9660),
  - Plate-formes : Linux, Mac OS X, Open & FreeBSD, Solaris, CYGWIN
- Autopsy : http://www.sleuthkit.org/autopsy/desc.php
  - Interface graphique (html) à la boite à outils Sleuthkit
  - Scalpel, foremost : dérection / récupération de fichiers sur images disques

Plan

- Introduction
- Incidents et attaques, symptomes
- Éléments techniques
- Les traces
- Contexte juridique : statut des traces
- Le dépôt de plainte
- L'acquisition des traces
- Démarche
- Les boites à outils
- Plan de reprise après incident

Plan de reprise sur incident

- Il se peut que les CD utilisés pour l'installation système ne permettent pas toujours de redémarrer les serveurs ou d'accéder au volume de stockage (ajout de contrôleurs additionnels, suites à mises à jour systèmes, firmware...)
- Importance d'avoir à disposition une boite à outil testée
- Cela fait partie de la gestion de sinistre (crash disque, panne serveur, piratage...)
- Cela constitue un « plan de reprise après sinistre » dont le but recherché :

Reprise après incident (la plus courte et la plus sereine possible)

Questions ?