Acquisition d'Informations sur une Machine Piratée

Frédéric Bongat (CNRS-IPSL),
Nicole Dausque (CNRS-UREC),
Christophe Dubois (CERT-A),
Matthieu Herrb (CNRS-LAAS),
Marie-Claude Quidoz (CNRS-UREC),
Denis Pugnère (INPL/IN2P3)

31 mars 2009, Toulouse

Plan

Plan

Programme de la formation

9h00	Introduction	MH
9h30	Principes de base et bonnes pratiques	MH
10h15	Acquisition des données - principes généraux	BV
11h00	Pause	
11h15	Spécificités des systèmes Linux	CH
12h00	Spécificités des systèmes Windows	BV
12h45	Pause repas	
14h00	Présentation de la boite à outils Linux/Windows	CH
14h30	TP Acquistion données à chaud	
15h45	Pause	
16h00	TP Acquisition données à froid	
17h30	Fin	

Objectifs de la formation

Acquérir/actualiser/approfondir vos connaissances

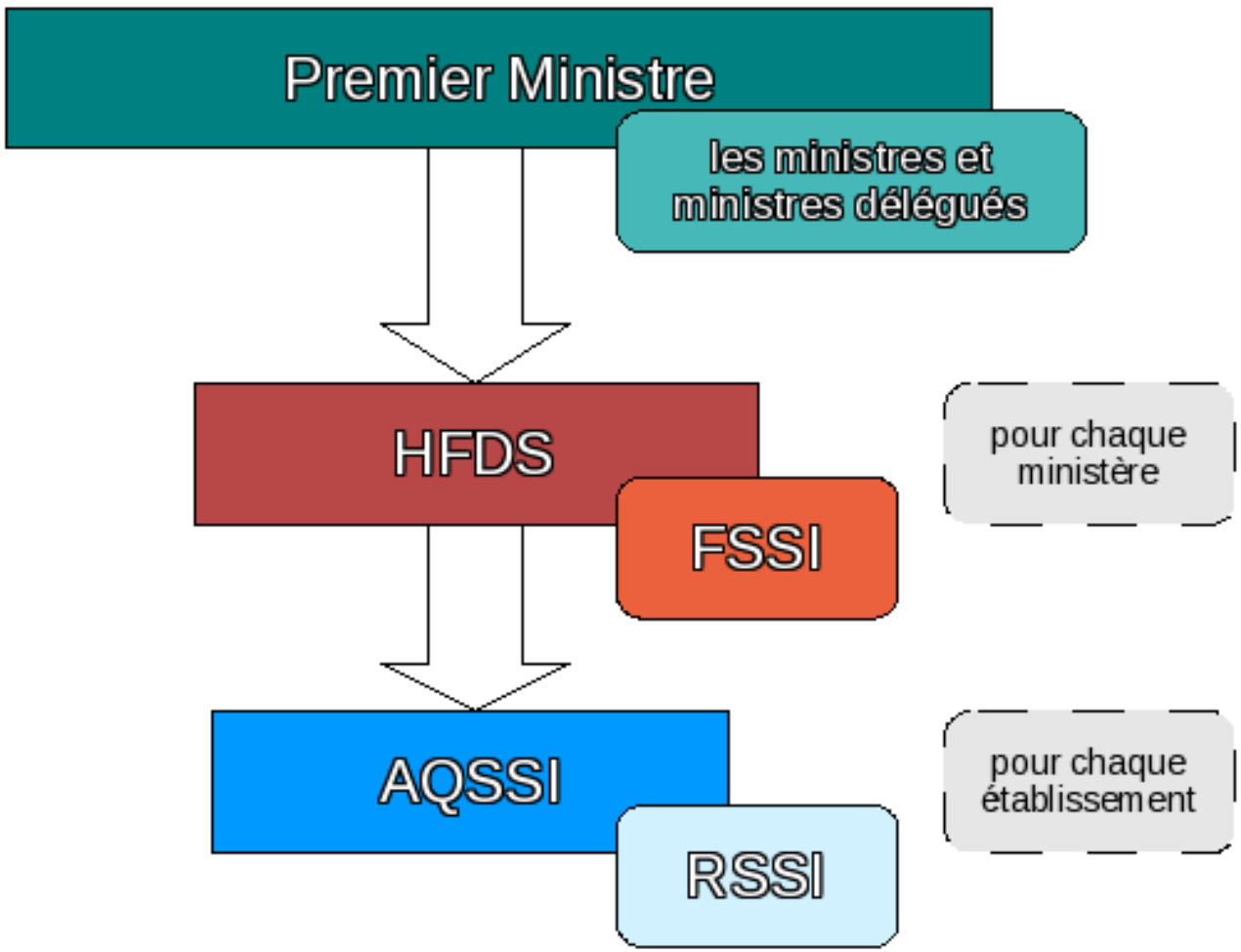
- acquérir les bons réflexes
- en situation d'urgence
- pour sauvegarder les données indispensables
- tout en leur gardant une recevabilité juridique
- sur différents systèmes d'exploitation (Unix/Linux, Windows, Mac OS X)

Remarque

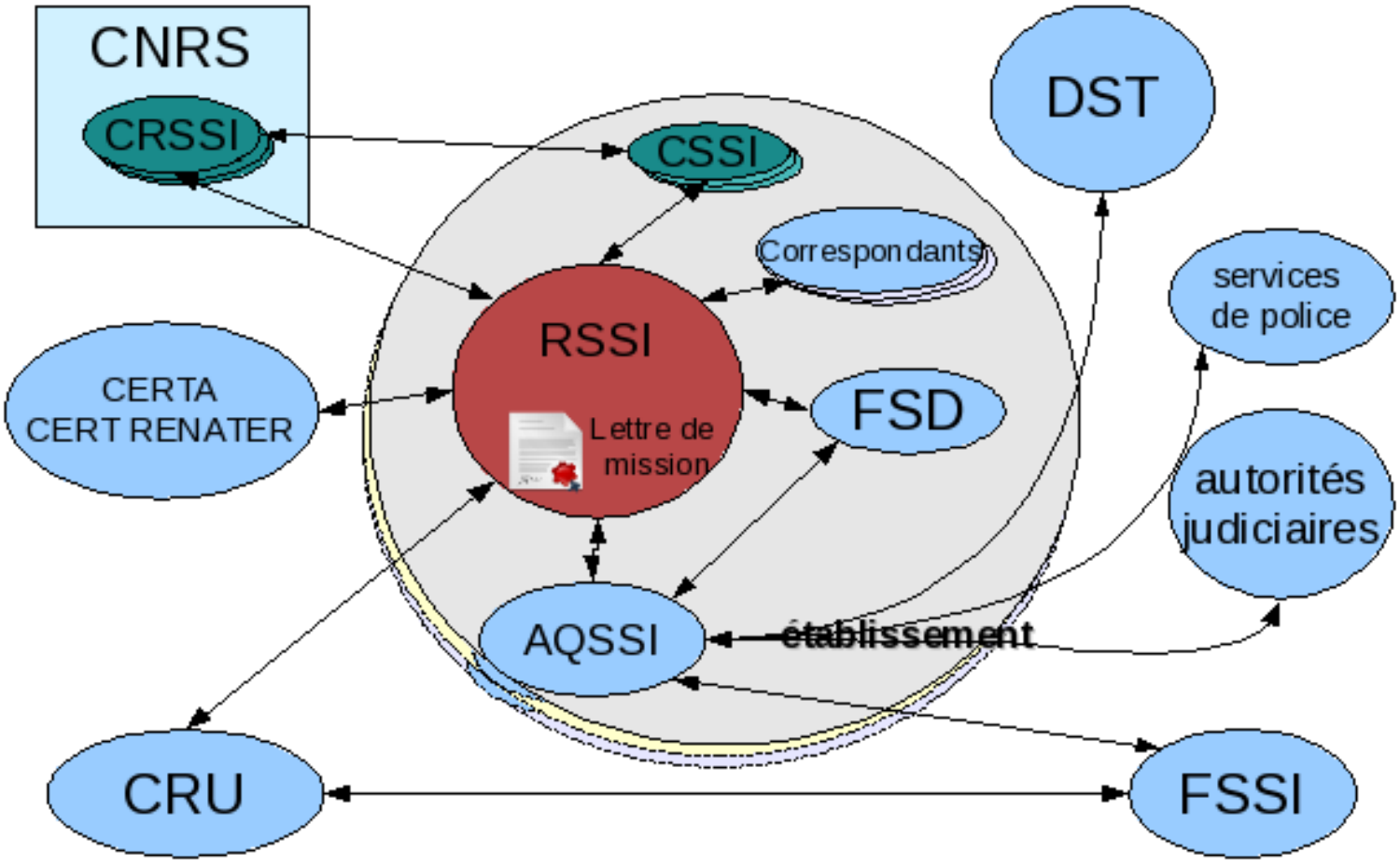
Il s'agit *d'acquérir* des données sur une machine piratée et non *d'analyser* une compromission.

Plan

Organisation de la sécurité des systèmes d'information



Niveau local



Correspondant sécurité

En concertation avec le directeur d'unité :

- Appliquer les recommandations/instructions venant des instances nationales (FSD)
- Lire les avis des CERT et mettre en place les protections nécessaires
- Sensibiliser les utilisateurs à la sécurité
- Si incident :
  - suivre les procédures d'alerte et prendre les mesures qui s'imposent
  - faire un bilan de fin d'intrusion avec les RSSI/CRSSI

CRSSI CNRS

- 1 à 5 par région CNRS. À la DR14 :

Roland Dartiguepeyron	Laurent Bardi
Frédéric Rodriquez	Matthieu Herrb
Cédric Hillembrandt	

- Courroie de transmission (FSD, UREC) $\Leftrightarrow$ unités (correspondants, directeurs)
- Interlocuteurs du délégué régional
- (relative) expertise technique
- Aide aux correspondants :
  - sensibilisation des directeurs
  - en cas d'incidents
- Animation
  - liste de diffusion
  - Réunions/formations

RSSI Universités

UT 1	Fabrice Prigent et Xavier Marty (mail : `réseau@univ-tlse1.fr`)
UT 2	Jean-François Parrache
UT 3	Anne Berckmans Martinez et Viviane Corrégé (mail : `rssi@ups-tlse.fr`)
INP	Vincent Chong-Wing et Brigitte Sor
INSA	Boris Valera et Stéphane Larroque

Les CERT

- CERT : Computer Emergency Response Team (CMU)
- Réseau mondial
- En France :
  - CERT Renater : éduc/recherche, 1995
  - CERTA : administrations, 1999
  - CERT-IST : industrie, 1999
- Notre CERT de tutelle : CERT Renater
- Nous concerne de très près : CERTA

CERT Renater

- 5 personnes
- Basé à Montpellier
- Diffusion d'informations : VULN, STAT, INFO, ALER
- Action plutôt en amont des incidents

CERTA

- 20 personnes
- Basé à Paris, Hôtel des Invalides
- Diffusion d'informations : avis, alertes, infos, recommandations, bulletins hebdomadaires
- Intéressé par l'analyse des données de machines compromises

Plan

Exemples d'incidents

- Agression
  - scans intempestifs de ports
  - déni de service
- Prise de contrôle pour site *warez*
  - fichiers musique, vidéos, logiciels piratés,
  - plus grave: réseaux pédophiles, néo-nazi, terroristes...
- Incrimination/dénigrement
  - défacage de site web
- Ver/virus
- Vol de mots de passe
  - *phishing* (ameçonnage / attrape-nigaud)
  - force brute (SSH, FTP)

Script kiddies ou pirates professionnels ?

Le « marché » de la sécurité informatique se professionalise.
Un « chercheur » en sécurité qui trouve une faille peut :

- contacter l'éditeur du logiciel et aider à la corriger
- la vendre à un des clients informés en exclusivité.
- la mettre aux enchères sur le marché noir des pirates.

Ainsi il est possible d'acheter pour un prix variable des vulnérabilités et les outils pour les exploiter...

- pas encore publiques (pas de patches)
- comme vecteur pour un vers/virus
  (pour construire un botnet)
- pour une attaque ciblée contre un site particulier, représentant une valeur spécifique pour le pirate

Machine piratée : symptômes

- Machine lente, figée, inaccessible
- Trafic réseau anormalement élevé, saturé
- Activité de certains services anormalement élevée, saturation
- Reboot(s) inexplicable(s)
- Modification du comportement attendu d'une machine
  - Erreurs Bizarres, incompréhensibles
  - Incidents en série
  - Processus inconnus, étranges

Machine piratée : symptômes (2)

- Fichiers
  - incongrus
  - disparition
  - saturation du système de fichiers
- Logs inattendus
- Modifications système
  - création d'utilisateurs
  - crontab
  - fichiers de configuration
- Comportement modifié de certaines commandes (ls, ps, netstat...)
- Signalement par l'extérieur (CERT-Renater, administrateur d'une machine attaquée, etc.)

Symptômes : conclusion

- Ne pas se voiler la face
- Quand l'attaque est visible, le mal est déjà fait
- Est-ce vraiment un incident ?
  - Conjonction de symptômes évidents
  - Symptômes décrits dans des avis de sécurité récents
  - Incidents similaires dans le voisinage
- Déclarer l'incident (chaîne fonctionnelle, CERT Renater)
- Tenter d'acquérir un maximum d'informations
- Éventuellement : porter plainte

Plan

Contexte juridique

Contexte juridique

- **Articles 323-1 à 327-7 du code pénal:** Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende...

Contexte juridique

- **Articles 323-1 à 327-7 du code pénal:** Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende...
- **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 (2)

- **Art. 434-4 du Code pénal:**
  Est puni de trois ans d'emprisonnement et de 45000 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 des indices soit par l'apport, le déplacement ou la suppression d'objets quelquonques;
  2. De détruire ou de 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 75000 euros d'amende.

Porter plainte : quand ?

- Vol de matériel ou de support de données
- Incident sérieux
- Dans une unité sensible :
  - ERR : Établissement à Régime Restrictif
  - ES : Établisement Sensible
  - ERO : Établissement à Régime Ordinaire

Porter plainte : intérêt ?

- Pour tenter de trouver un coupable
- Pour se protéger de :
  - la justice (warez, pédophilie, musique illégale, etc.)
  - les autres victimes (phishing, rebonds d'attaques, etc.)
- Contextes particuliers :
  - unité sensible
  - contrats avec un industriel
  - accueil de mineurs

Porter plainte : inconvénients

- Procédure longue et énergivore
- Si incident grave et sensible : immobilisation de la machine (serveur...)
- Conclusion
  - Ne pas porter plainte à la légère
  - Consulter systématiquement les tutelles concernées.

Porter plainte : comment ?

Dépend de la tutelle principale pour la SSI :

- CNRS : `http://www.dsi.cnrs.fr/bo/2008/11-08/49-bo1108-cir080001dAj.htm`
  $\longrightarrow$ Délégation régionale ou fonctionnaire de défense.
- Universités et écoles : AQSSI

Services de police compétents

DCRI: Direction Centrale du Renseignement Intérieur

BEFTI: Brigade d'enquète sur les Fraudes aux Technologies de l'Information (Paris uniquement)

OCLCTIC: Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication

SRPJ: Service Régional de Police Judiciaire

ESCI: Enquêteur Spécialisé Criminalité Informatique

Plan

Synchronisation des horloges

Les horloges internes des machines ne sont pas fiables
$\longrightarrow$ dérive dans le temps.
Il existe des références précises :

- radio (DCF77)
- GPS
- accessibles via le réseau : protocole NTP (RFC 1305)
  - précision 1 milliseconde ou mieux
  - liste : `http://www.cru.fr/NTP/serveurs_francais.html` (`ntp.laas.fr`)
  - pool : `pool.ntp.org`
  - accessibles librement ou soumis à déclaration ou autorisation d'utilisation

Quoi et comment synchroniser ?

Tout, par ordre de priorité :

- serveurs
- matériels réseau
- postes clients

Utiliser le protocole NTP en strates, avec redondance.
Exemple :

- 2 ou 3 serveurs, clients de serveurs français différents
- autres machines et matériels réseau interne synchronisés sur ces serveurs

Futur : sécuriser NTP...

Synchronisation d'un routeur

Important ! Permet de corréler les traces des routeurs avec celles des machines.

- Certains routeurs peuvent être à la fois client et serveur NTP

Exemple : Cisco

```
! Client de ntp.laas.fr
ntp server 195.83.132.135
! Definition VLAN avec serveur NTP
interface Vlan1
    description vlan interne labo
    ip address 192.168.1.1 255.255.255.0
    ntp broadcast destination 192.168.1.255
```

Synchronisation Unix

Service NTP inclus de base dans tous les systèmes récents.

Configuration dans `/etc/ntp.conf`

Exemple

```
driftfile /var/run/ntp.drift
authenticate no

server ntp1.laas.fr
server ntp2.laas.fr
```

Vérifier que le service est démarré.

Interroger le serveur: `ntpq -p`

Synchronisation Windows

Nativement sous Windows NT/2000/XP
Vérifier que le service **Horloge Windows** est démarré.

- Configuration : `net time /setsntp:pool.ntp.org`
- Vérification : `net time /queysntp`

Pour versions plus anciennes:
`http://nettime.sourceforge.net/`

Heure locale ?

- UTC : Coordinated Universal Time (ex. GMT) référence pour NTP et pour les Unix traditionnels.
- Heure locale, avec heure d'été : référence pour Windows, Mac OS X et certains Linux.
- Routeurs : ça dépend, souvent pas de passage automatique à l'heure d'été.

Pas toujours facile de choisir une référence commune.
Pour chaque type de d'appareil savoir quelle horloge est utilisée.

Les traces (logs)

- Capturer et enregistrer les évènements significatifs
- Souvent répartis :
  - par système
  - par application/service (Apache, authentification, firewall,...)
- Hétérogènes :
  - Format (Cisco IOS, iptables, pf, syslog, apache...)
  - Type : évènements mélangés : alertes, info, debug
- Sur serveurs, postes clients

Centralisation des traces

Technique qui consiste à ce que chaque élément actif du 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

  Grâce aux post-traitements rendus possibles

Possibilités supplémentaires :

- écriture sur support WORM (écriture unique)
- signature numérique/chiffrement

Valeur ajoutée

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

Exemple de traces : Cisco

Routeurs et commutateurs implémentent un client syslog capable d'envoyer des logs sur plusieurs évènements :

- état des interfaces
- connexion au routeur (configuration)
- violation de la politique de filtrage

Exemple

```
logging trap debugging
logging facility local5
! envoie les logs sur le serveur interne
logging 192.168.1.1
! log dans les ACL
access-list 101 permit tcp any host 192.168.1.22 eq 22 log
access-list 101 permit tcp any host 192.168.1.80 eq 80
access-list 101 deny ip any any log
```

Syslog serveur

- **syslogd**
  - lancer le démon avec l'option `-r` (`-u` sur BSD).
  - laisser passer les connexions sur 514/UDP
- **syslog-ng**
  - optimisé pour traiter un grand nombre de clients
  - Possibilités de tri sur le contenu des messages
  - Utilisation de TCP en plus de UDP
  - Possibilité d'exécution en cage

Plan de reprise sur incident

Pour une reprise rapide et sereine après un incident :

- Sauvegardes des données
- Procédures de re-démarrage des serveurs permettant d'accéder aux volumes de stockage:
  - CDs de boot avec tous les drivers (systèmes RAID, cartes réseau)
  - Procédure de boot réseau sur un serveur de réserve
  - ...
- Tester régulièrement et mettre à jour ces procédures (suite aux mises à jour matérielles ou logicielles des serveurs)

La boite à outils A2IMP n'est adaptée qu'aux postes clients ou aux petits serveurs (architecture Intel).