



# Journées FedeRez 2011

19 mars 2011

# Sécurité informatique

## « Sécurité en profondeur »

**Raphaël Marichez**
Raphael.Marichez@(hsc.fr|polytechnique.org)
Falco@(Falco.in|gentoo.org|m4x.org)

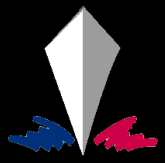
# Présentation

- Le sujet
  - Sécurité informatique
    - FedeRez 2005
      - « l'avenir de la sécurité informatique » et « sécurité et mobilité »
      - Discussions autour du warez, de la responsabilité des associations en tant qu'hébergeur...
    - Entre 2005 et aujourd'hui :
      - Nombreuses jurisprudences LCEN, arrivées de DADVSI (2006), d'HADOPI (2009), de la LOPPSI (2011)...
      - Incidents de sécurité informatique médiatisés : Conficker (2008), Stuxnet (2010), Bercy (2011)...
  - La question : comment se protéger, simplement, pas cher
  - La réponse : sécurité et/ou défense « en profondeur »


# Présentation

- L'auteur


  - Consultant SSI chez Hervé Schauer Consultants (HSC)
    - Pentests, audits, forensics, gestion du risque, formations...



  - Officier de réserve opérationnelle, Marine Nationale
    - Soutien à la coordination SSI à l'Etat-Major Marine

  - Auditeur « jeune » de l'IHEDN, comité d'études « cyberdéfense »

  - Ancien responsable de la veille SSI pour Gentoo Linux

  - Ancien de FedeRez (BR)
    - Présent aux premières journées (2005 chez VIA)
    - Organisation des secondes journées (2006 à l'X)


# La sécurité en profondeur

- Comment se protéger ?
  - Acheter des pare-feux
  - Acheter des IPS, des WAF
  - Acheter des IDS
  - Acheter des systèmes de gestion d'événements (SIEM)
  - Acheter des certificats HTTPS à $200 (minimum)
  - Utiliser SHA256 plutôt que MD5, et forcer SSLv3
  - Définir des politiques de sécurité
  - Mettre en place un système de management de la sécurité
  - Et....

# La sécurité en profondeur

- Et...
  - Mots de passe par défaut (tomcat/tomcat, admin/admin)
  - Mises à jour non faites
  - Systèmes oubliés dans un coin
    - Sniffing, relais d'attaques...
  - Injections SQL triviales
  - Mots de passe partagés
    - Voire pas d'authentification du tout

# La sécurité en profondeur

Est-ce un échec ?

# La sécurité en profondeur

Alors réfléchissons...

- Qu'est-ce que nous craignons ?
- Quoi/qui est susceptible de nous attaquer ?
- Quels sont les scénarios d'attaque ?

# La sécurité en profondeur

- Ce qu'on craint
  - Arrêt d'activité (temporaire ou permanent)
  - Conséquences juridiques, civiles ou pénales
  - Mauvaise notoriété (presse)
  - Sanction d'une tutelle (université, école, Renater...)
  - Divulgation de secrets (peu redouté dans nos associations...)
  - Dommages matériels, humains voire vitaux (pas dans nos assoces)

# La sécurité en profondeur

- Quoi/Qui nous menace
  - Un peu de systémique...
  - Humains
    - Gentils
      - Utilisateur de nos systèmes, ou partenaire, mais maladroit
    - Méchants
      - Utilisateur de nos systèmes, ou partenaire, malveillant
      - Pirate, extérieur à notre organisation
  - Non-humains
    - Virus
    - Environnement physique
    - Fournisseurs ou prestataires de services

# La sécurité en profondeur

- On fait de la combinatoire...
- On regarde l'histoire

  Affaire ENST/Brel (1996), ESPCI (2000)

  Nombreux « defacements » de sites... et coupures d'accès réseau

  Perturbations des services (Conficker...)

  et d'autres événements méconnus ?

- On discute, on arbitre...

# La sécurité en profondeur

- Finalement, ce qu'on redoute le plus :
  - Attaque externe non ciblée (virus, script-kiddie)

    transformant notre SI en relais d'attaques, ou hébergement de contenus litigieux
  - Utilisateur malveillant engageant notre responsabilité :

    en lançant des attaques sur des tiers

    en hébergeant du contenu litigieux

    en fragilisant notre SI devenu vulnérable à des attaques externes

    → Problème plutôt humain que technique
  - Attaque ciblée d'un pirate ayant pour motivation(s) :

    chantage

    dé-crédibiliser la tutelle (l'école, l'université)

    fuites de données à caractère personnel (?)


# La sécurité en profondeur

- Quels scénarios mènent aux événements redoutés ?
  - Attaque non ciblée :
    - Infection virale / malware
      Laptops nomades, clés USB, mails, navigation dangereuse...
    - Force-brute
      Mots de passe faibles (SSH, FTP, CMS Web)
    - Compromission distante
      Mises à jour de serveurs non faites, injections SQL ou shell...
  - Attaque ciblée :
    - Vulnérabilités dans les développements maisons
      Injections SQL, XSS, CSRF...
    - Mots de passe faibles


# La sécurité en profondeur

- Vous venez de faire une analyse du risque ! (enfin presque)
- Les principaux risques :
  - La compromission distante non ciblée menant à une utilisation frauduleuse de nos systèmes, avec un risque juridique
  - L'attaque ciblée externe, par compromission d'un serveur, pour nuire à l'image de l'organisme
- Pour s'en protéger on construit plusieurs barrières...

# La sécurité en profondeur

- Un parallèle avec la sûreté nucléaire (retex 1999)
  - Scénario : arrêt des pompes des circuits de refroidissement
  - → Prévenir la menace :

    Construire le site au-dessus de la cote de sécurité (CMS)

    Assurer un secours électrique indépendant par tranche
  - → Bloquer la menace :

    Construire des digues autour du site

    Assurer un secours diesel
  - → Confiner / Limiter les impacts :

    Obturer les voies d'entrées de l'eau dans les locaux menacés

    Multiplier les équipements (redondance 2N)
  - Que manque-t-il d'essentiel ?

# La sécurité en profondeur

- Prévenir, bloquer, renforcer...
  - et **détecter** : sondes, capteurs, système d'alerte, état des protections

    à toutes les étapes
  - et **réagir** : gestion de crise

# La sécurité en profondeur

- 28/12/1999, Blayais : « près de la catastrophe »
  - Multiples défaillances
    - Travaux de ré-haussement de la digue repoussés
    - Niveau du site sous la cote majorée de sécurité
    - Perte d'alimentation électrique (mais compensée par les générateurs)
    - Tempête de 1999 + forte marée
    - Non-respect d'une procédure (déclenchement d'alerte)
  - La moitié des locaux de pompage étaient hors service
    - Situation délicate mais viable
    - Arrivée de pompage externe (pompiers, eau de mer) en réaction
  - Multiples niveaux de défense
  - Multiples scénarios à franchir

  → Pas de catastrophe

# La sécurité en profondeur

- Sécurité informatique : un mauvais exemple
  - Faille DVI (CVE-2010-2640) (Jon Larimer, IBM)
  - Ubuntu 32 bits / GNOME, durci :

    ASLR

    AppArmor

    NX, PIE


# La sécurité en profondeur

- Scénario : tuer l'écran de veille en attaque locale (physique)
  - Clé USB (nécessite l'accès physique – c'est dans les hypothèses)
  - Automount (c'est standard)
  - Autoexec ??

    Viewer automatique evince pour les fichiers DVI (standard)

    Faille CVE-2010-2640 → exécution de commande (difficile)

    Contourner ASLR → attaque probabiliste (~3000 essais)

    Contourner AppArmor → utiliser un symlink + mmap W+X

    « killall gnome-screensaver »...

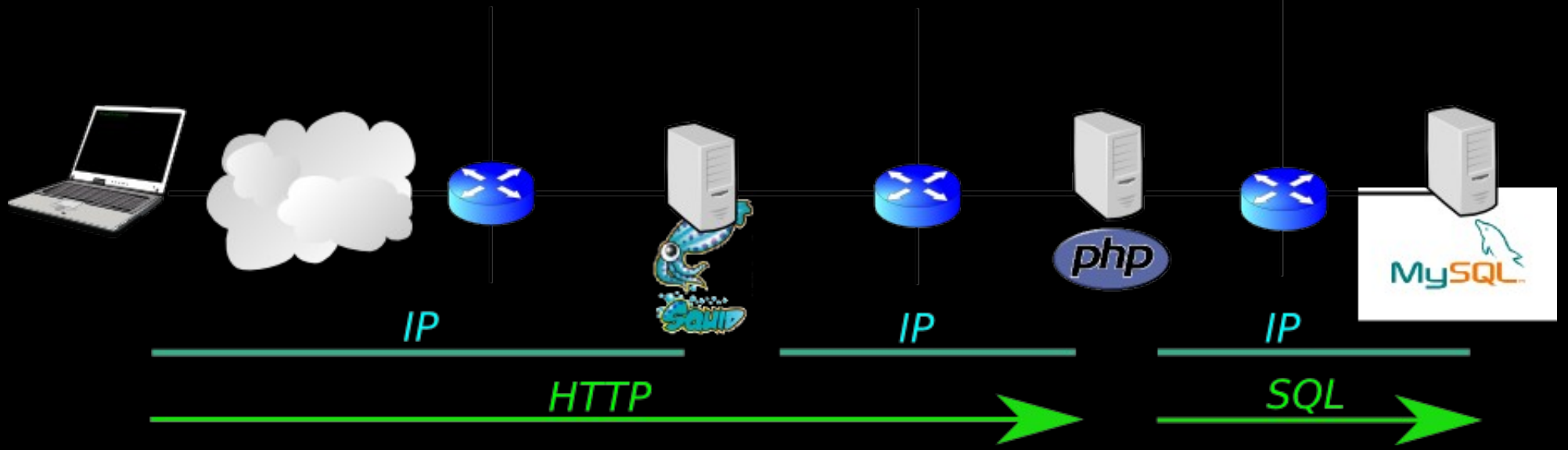
# La sécurité en profondeur

- Autre (mauvais) exemple

  Architecture 3 tiers, correctement cloisonnée

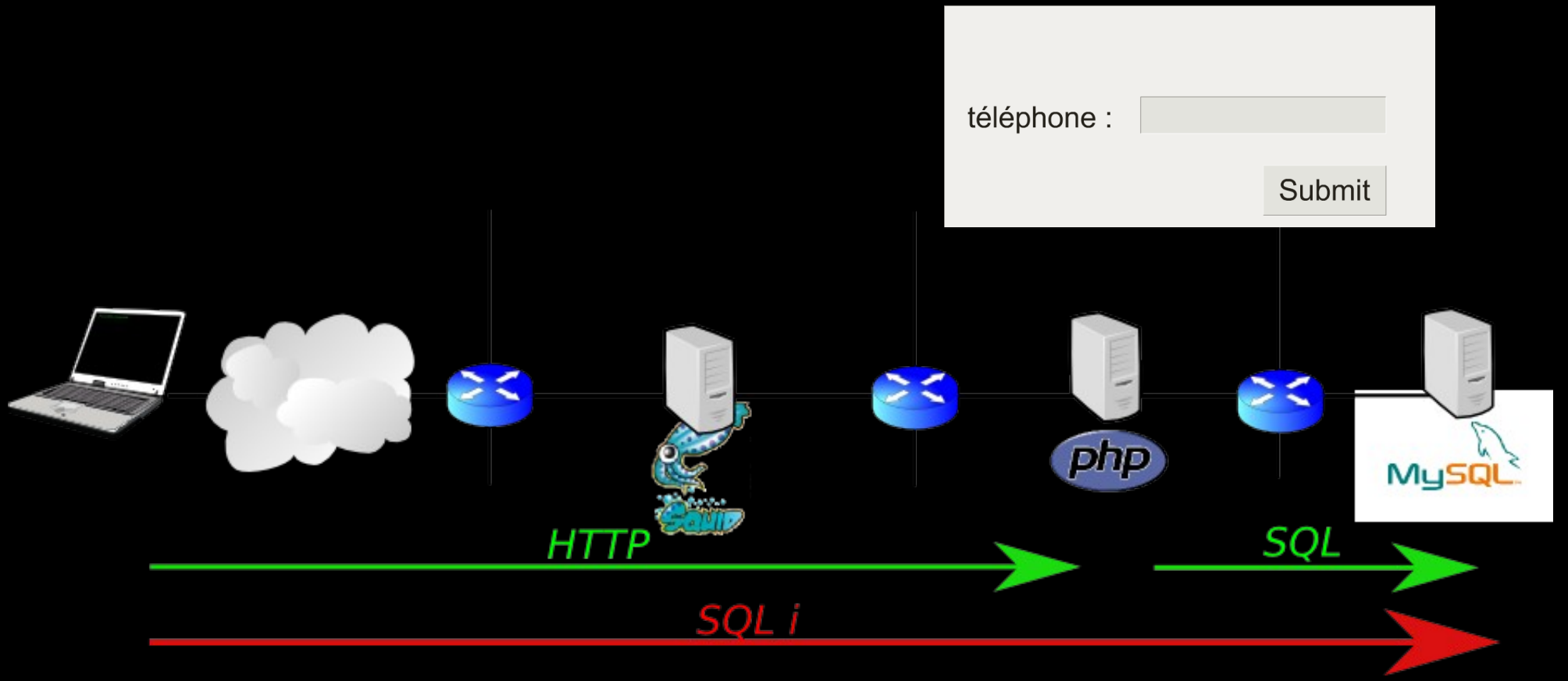
  Mots de passe robustes, pas d'autre accès que HTTP

  Sorties HTML correctement filtrées, pas de fuite d'information



# La sécurité en profondeur

- MAIS injection SQL « aveugle », bit par bit, MD5 + rainbow-tables




→ accès administrateur !

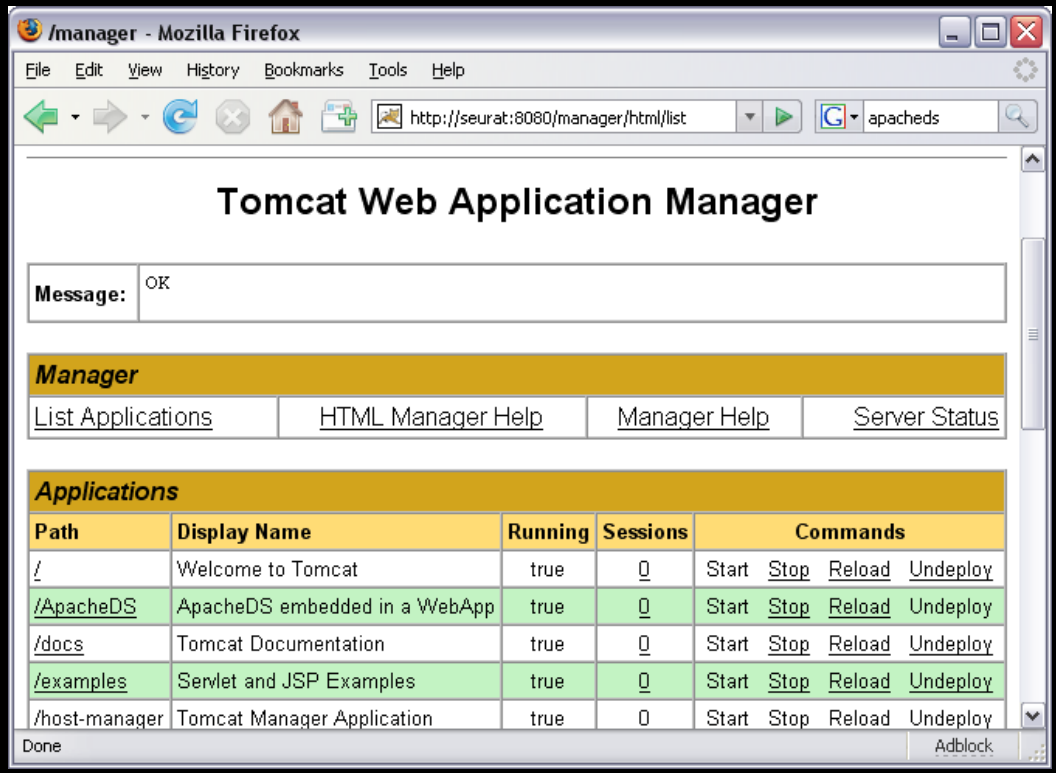
# La sécurité en profondeur

- Un autre
  - Tomcat dont le « Manager » n'est pas publié sur internet...

# La sécurité en profondeur

- Un autre
  - Tomcat dont le « Manager » n'est pas publié sur internet...

Jusqu'à CVE-2007-1860 (« /../ » directory traversal)




# La sécurité en profondeur

- Un autre autre
  - Désactivation et effacement des empreintes LM
  - Désactivation des caches des authentifications Windows (mscash)

# La sécurité en profondeur

- Un autre autre
  - Désactivation et effacement des empreintes LM
  - Désactivation des caches des authentifications Windows (mscash)
  - sauf.... sur 1 serveur

    celui sur lequel l'administrateur est en ce moment-même connecté

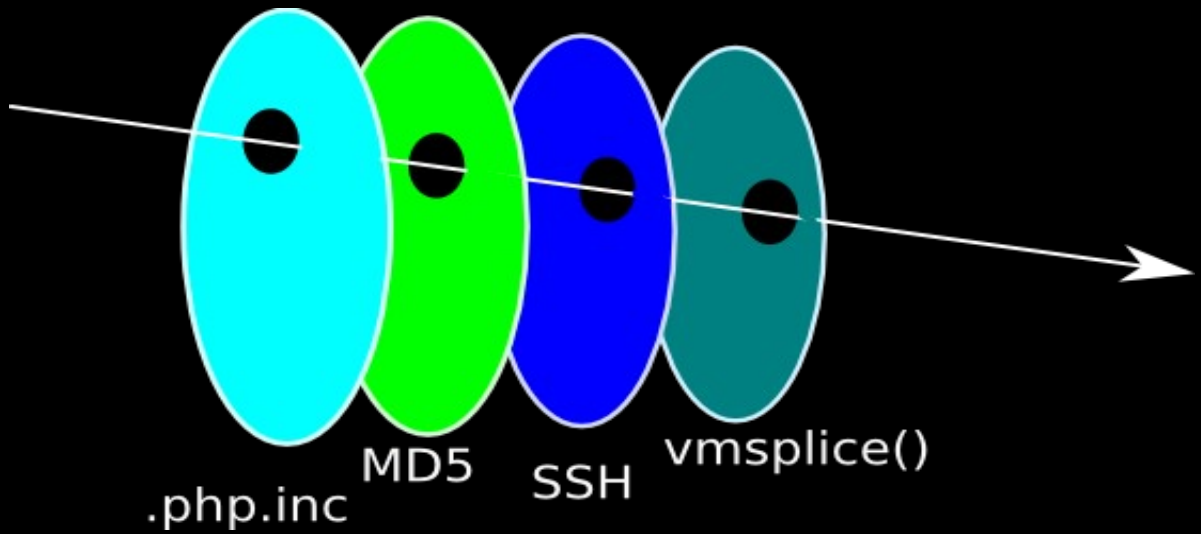

# La sécurité en profondeur

- Un dernier
  - un certain week-end de février 2008

    vmsplice()

# La sécurité en profondeur

- Conclusion : l'incident a lieu lors d'un alignement de failles...




- Parfois... il suffit d'attendre le bon alignement

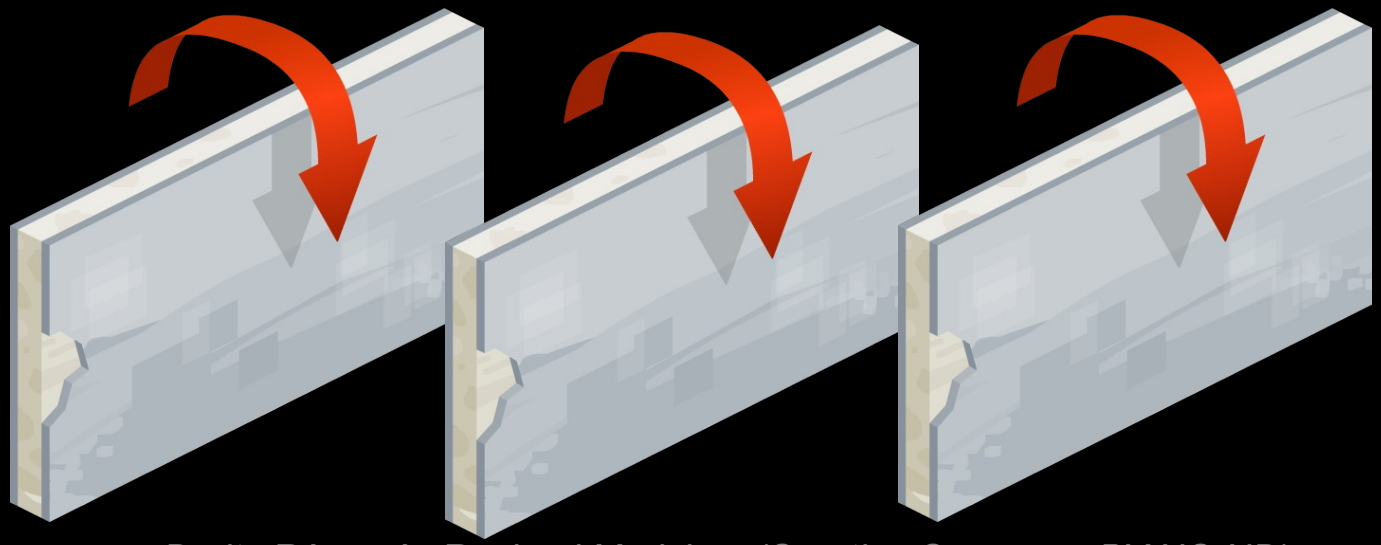

# La sécurité en profondeur

- L'alignement dépend...
  - des capacités de l'attaquant
  - du bon moment
    - failles publiées, failles non publiées, correctifs publiés, appliqués (?)
- Les trous ne présagent pas de la gravité des conséquences
  - Impossible de dire quel « trou » est plus grave qu'un autre

# La sécurité en profondeur

- Sécurité ?
  - Non : **défense en profondeur**

    Prévenir / Bloquer / Confiner / Détecter / Réparer
  - Il y **aura** des trous
  - Compliquez la tâche de l'attaquant avec plusieurs barrières



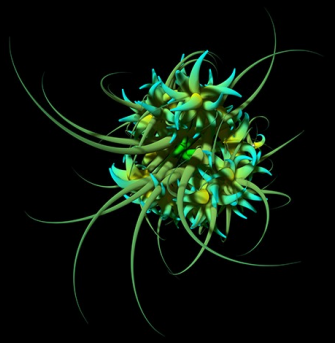
# La sécurité en profondeur

- Scénario 1 : se défendre contre les virus...
  - Cas 1 : virus bloqué par l'anti-virus
  - Cas 2 : virus nouveau (ou modifié)
    - propagation par USB (autoexec)

      Blocage 1 : fermer les ports USB

      Blocage 2 : désactiver l'autoexec

    - Infection d'un exécutable
      - Bloquer :
        signatures cryptographiques
      - Limiter :
        Compte non privilégié (non-administrateur / restrictions applicatives)
        Confinement réseau (SMB, RPC)



# La sécurité en profondeur

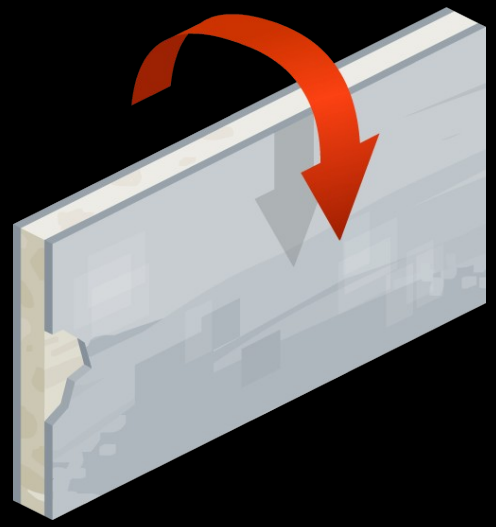
- AUCUNE barrière n'est parfaite

  Signatures cryptographiques → Stuxnet

  Confinement réseau → USB

  Autoexec et ports USB → quelques oublis...

- TOUTES sont nécessaires



# La sécurité en profondeur

- Scénario 2 : PDF

  Compromission par un PDF malveillant et récupération de documents

  - Prévenir :

    Avoir un lecteur PDF maintenu
    et à jour de ses correctifs

  - Bloquer :

    Désactiver les fonctionnalités du lecteur PDF : JavaScript, Flash, 3D...
    Activer DEP sous Windows
    (?) Convertir les fichiers dans un format statique type PS

  - Limiter :

    Circonscrire la fuite d'information ? difficile

# La sécurité en profondeur

- Scénario 3 : usurpation de comptes du domaine

  Dans un AD, via le compte administrateur local (empreintes...)

| | | | | | |
|---|---|---|---|---|---|
| md5 | e53cc072934b25e45dc273c6c342556d | | processing3 | 0:58:7 | 2006-11-11 09:48:10 |
| md5 | d38ad0e58c9525343f492161b87400a1 | htmldb | cracked | 0:58:23 | 2006-11-11 09:44:01 |
| md5 | d926dbaeb7fac97612ec219f7f172610 | | processing3 | 1:4:30 | 2006-11-11 09:41:47 |
| md5 | fcf2483ced1768308584987713 4fd50c | | processing3 | 1:6:32 | 2006-11-11 09:39:45 |
| md5 | 377a8f80271a6f920df0e4aa84d1029a | bombi | cracked | 0:43:12 | 2006-11-11 09:38:26 |
| md5 | 85d95e2ad51bfcd5d6d352486fbe2769 | pupsi | cracked | 1:8:2 | 2006-11-11 09:28:25 |
| md5 | 96bc2c727049b5dce27bd8b9e8b264bf | | processing3 | 1:19:6 | 2006-11-11 09:27:11 |
| md5 | 8aa12bbde69504ba86b942726b4d7623 | | notfound | 1:18:15 | 2006-11-11 09:02:54 |
| md5 | 5ce1d8097499634487676 22e0ca8169f | 28264451 | cracked | 0:48:15 | 2006-11-11 09:02:35 |

  - Prévenir :

    Appliquer les correctifs
    Restreindre les droits des utilisateurs
    Empêcher le boot sur disque externe
    Minimiser les logiciels installés

  - Bloquer :

    Désactiver + effacer les empreintes LM (Win2K compatibles)
    Limiter les empreintes en cache

  - Limiter :

    Mots de passe différents pour chaque système
    Empêcher la connexion depuis les comptes locaux

# La sécurité en profondeur

- Détecter ?
  - Journaliser et centraliser (syslog) (même sous Windows)
  - Scripter sur les événements (tenshi, logwatch...)
  - (?) Corrélation d'événements ?
  - Tester régulièrement les protections

    Nagios (authentification, bannières...)

    crontabs (scripts)

    audits (scripts), scanneurs de vulnérabilités


# La sécurité en profondeur

- Conclusions
  - Plusieurs barrières, toutes sont utiles :

    D'abord pour se défendre contre les attaques de masses

    Ensuite pour se défendre contre les attaques plus expertes

  - À penser dès la conception

# La sécurité en profondeur

- Conclusions
  - Ne pas oublier :

    Agir sur l'environnement

    → Prévenir / empêcher

    Agir sur le système (bloquer/durcir/confiner)

    → Bloquer

    → Limiter les impacts / Confiner

    → DÉTECTER les incidents
    sur les systèmes
    sur toutes les autres barrières

    → PRÉVOIR de réagir

# La sécurité en profondeur

- Dans la vraie vie
  - Discours des experts en sécurité informatique depuis 15-20 ans
  - Personne n'arrive à l'appliquer à une grande échelle

  ...

  Applications monolithiques

  Centralisation de l'AAA (authentification/autorisation/traçabilité)

  Modèles « 3 tiers » offrant un semblant de défense en profondeur

  Présentation (Frontal) / Traitement (Serveur d'applications) / SGBD

  Sous-traitance de la sécurité

  Perte de la compétence interne


# La sécurité en profondeur

- Pour aller plus loin...
  - Conférences et retours d'expérience
    - Panoramas du CLUSIF sur la cybercriminalité (www.clusif.fr)
    - SSTIC (Rennes), CCC, BlackHat (USA, Europe), Defcon, JSSI...
      - « Application de la cyberdéfense » (J. Sterckeman, C&ESAR 2010)
      - « Pourquoi la sécurité est un échec » (N. Ruff, SSTIC 2009)
  - Portail SSI du gouvernement
    - www.ssi.gouv.fr
  - Discussions, mailing-lists et ressources sur la sécurité technique
    - seclists.org
    - oss-security.openwall.org
    - www.hsc.fr/ressources
    - www.ossir.org
    - www.gentoo.org/doc/en/security
  - PAS Wikipedia


# La sécurité en profondeur

- Petit test

```
-r-sr—rwx   1  root   root   1001  Jan 16 19:05  give_me_a_shell
```

  - écrire dans ce fichier un fork vers un shell pour passer root :

    exploitable sous linux ?

# La sécurité en profondeur

- Petit test

```
-r-sr-rwx   1  root   root   1001  Jan 16 19:05  give_me_a_shell
```

  - écrire dans ce fichier un fork vers un shell pour passer root :

    exploitable sous linux ?

  - `open(..., O_RDWR)` → perte du bit SUID

```
-r-xr-rwx   1  root   root   1001  Jan 16 19:05  give_me_a_shell
```

  - alors, exploitable ?

# La sécurité en profondeur

- Petit test

```
-r-sr-rwx   1  root   root   1001  Jan 16 19:05  give_me_a_shell
```

  - écrire dans ce fichier un fork vers un shell pour passer root :

    exploitable sous linux ?

  - `open(..., O_RDWR)` → perte du bit SUID

```
-r-xr-rwx   1  root   root   1001  Jan 16 19:05  give_me_a_shell
```

  - alors, exploitable ?

  - écrire via mmap() → pas de perte du SUID
    (cf newsletter HSC février 2011)


# La sécurité en profondeur

- Petite question

  Pourquoi changer ses mots de passe tous les XX jours ?
  (XX = 42 ou 90)


# La sécurité en profondeur

- Merci de votre attention

Mail :
Raphael.Marichez@(hsc.fr|polytechnique.org)
Falco@(Falco.in|gentoo.org|m4x.org)
Slides :
vrac.arctik.net/federez-20110319.pdf