Sécuriser Mac OS X

OSSIR/SUR - 14/12/2004

G. Arcas - guillaume.arcas@free.fr

Sommaire

- Présentation Mac OS X v. 10.2 (Jaguar)
- Contexte et philosophie
- Etat des lieux après installation «□□OB□
- Sécurité physique
- Sécurité logique
  - Outils et préférences du système
  - Intégration des logiciels libres
- Quelques exemples

Présentation Mac OS X

- Mac OS X (10 et non «□□)
  - 2001 : Steve Jobs, Next
  - Darwin
    - Noyau MACH 3
      - Pilotes & gestion des entrées/sorties
    - FreeBSD 5
      - Systèmes de fichiers
      - Gestion réseau
      - Gestion des processus
  - Aqua
    - Interface graphique (partie immergée de l'iceberg)
  - Carbon & Cocoa (développement)

Contexte & Philosophie

- Culture «graphique»
  - Pas de «shell» avant Mac OS X
- Esprit «tout le monde il est beau tout le monde il est gentil»
- Communauté
  - Attitude ouverte dans un monde fermé
- Environnement fortement mono-utilisateur

Sécuriser le démarrage

- Open Firmware : équivalent du BIOS
- Par défaut : pas de mot passe, niveau de sécurité none.
- Actions :
  - Activer le mot de passe
  - Choisir un niveau de sécurité apdaté
    - None : aucun
    - Command : mot de passe OF pour modifier les options OF ou booter depuis un périphérique externe mais pas de mot de passe pour booter sur le disque principal
    - Full : mot de passe pour chaque action.

Etat des lieux

- Mac OS X par défaut :
  - Installation pléthorique…
  - quelques bons choix de sécurité
    - Services réseau désactivés par défaut
    - OpenSSH pour les connexions distantes
    - OpenSSL pour les services de chiffrement
  - Quelques actions :
    - Environnement Classic (Mac OS 9)
    - Programmes SETUID
    - Remplacer inted par xinetd
    - Désactiver BlueTooth

Administration Utilisateurs

- Compte «□root□» désactivé par défaut
  - Activation par NetInfo
  - Sinon, utilisation de sudo pour les utilisateurs disposant dus privilèges Administrateur -> /etc/sudoers
- Authentification pour chaque action d'administration
- NetInfo pour gérer les comptes
  - Ajout de comptes par édition du fichier /etc/passwd ne suffit pas.

Maintenance du système

- Gestion des mises à jour
  - Software Update
- Gestion des paquetages
  - Images Apple
  - Fink
  - Source
    - Kit Développement Apple -> gcc 3.1
  - Gnu OSXPM

Le pare-feu Mac OS X

- Héritage FreeBSD 2.0
- Manipuler via Préférences Systèmes
  - Mode «□licodrome□
- Gestion en ligne de commandes
  - Ipfw
- Interfaces graphiques
  - FirewalkX, BrickHouse
  - SunShield

Le trousseau de clefs

- Gestion des mots de passe des applications Apple
- Mémorisation des mots de passe
- Verrouillage automatique d'applications sur inactivité

Supervision & Journalisation

- /var/log
  - System.log, netinfo.log, secure.log
- Utilitaires Unix : ps, top, lsof
- Utilitaires système
  - Visualiseur d'opérations, moniteur CPU
- GeekTool
- Sauvegarde : client Bacula

Remplacer / ajouter

- MS IE 5 -> FireFox
- Client Mail Apple -> ThunderBird
- Fink Commander
- Xdarwin
- ClamAV
  - Même si les virus Apple ne courrent pas les rues et que le virus pour OS X(Opener/Repeno) n'en est - officiellement - qu'au stade de «□roof of concept□»

En guise de conclusion

- Jaguar : à mi-chemin entre l'ancienne culture Mac OS 9 et la nouvelle génération Mac OS X Panther. Version de transition douce ?
- Certains «□manques□ de Jaguar sont apparemment comblés dans Panther, notamment le chiffrement disque (FileVault).

Quelques liens

- Apple - http://www.apple.fr
- Mac Security - http://www.macsecurity.org
- Ultimate Guide - http://homepage.mac.com/macbuddy/SecurityGuide.html
- NSA SNAC Security Configuration Guide Panther - http://www.nsa.gov/snac/os/applemac/osx_client_final_v.1.pdf