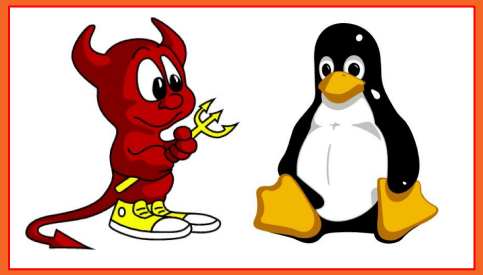

Unix/Linux
ISEN - AP4

E - TP SSH / Keys / Sécurité

2019 - J. Hochart

Objectif

- SSHd est un composant clef de la sécurité d’un unix en ligne
- Ici, on traite OpenSSH
- Fichier de conf: /etc/ssh/sshd_config

Préparation

- Backup du fichier de conf
- Un fichier de conf sshd se teste avec “sshd -t”
- Le service se reload avec
  - systemctl reload sshd
  - /etc/init.d ssh reload
  - service ssh reload
  - …
- On peut aussi restart, mais plus lourd en général et peut killer des daemons

Directives de conf

- PermitRootLogin no
  - Variantes: yes, without-password, forced-commands-only
- ClientAliveInterval 600
- ClientAliveCountMax 2
- AllowUsers [whitelist]

Note

- Certains admins changent le port de SSHD
  - Sécurité par l’obscurité: :(
  - La sécurité d’un système doit reposer sur
    - Le secret et la qualité des clefs
    - Une configuration adaptée

Key based authentication

- Sur la machine client (la clef privée ne doit jamais quitter son lieu de naissance)
  - Typique: ssh-keygen -t rsa -b 2048
- Copier-coller la clef publique dans le /home/$user/authorized_keys de la machine serveur
- Test avec ssh -i privkey user@host

Hostkey / fingerprint

- Editer /etc/hosts pour ajouter un alias “linuxbox” sur 127.0.0.1
- SSH user@linuxbox
- Constater le message de warning, et noter les 4 1ers digits de la fingerprint
- Se connecter / exit
- Se connecter / exit (encore): constat?

Hostkey / fingerprint

- Afficher le contenu (coté compte client) de .ssh/known_hosts
- Constat?

Hostkey / fingerprint

- Rechercher linuxbox dans known_hosts (ssh-keygen -H -F linuxbox)

Man in the middle (simulation)

- Objectif: simuler une machine qui se met en coupure entre client et server
  - Comme l’attaquant ne peut pas connaitre la hostkey privée, elle présentera une hostkey publique nouvelle (la sienne)
  - Simulation: on regénère la hostkey ssh du serveur

Man in the middle (simulation)

- Rm -rf /etc/ssh/ssh_host_*
- dpkg-reconfigure openssh-server (debian)

- SSH user@linuxbox
- Lire le message, comprendre et agir en conséquence.