

---

# Sécurité et Linux

---

**Philippe Biondi** <biondi@cartel-securite.fr>

**Cédric Blancher** <blancher@cartel-securite.fr>

—

**14 mai 2002**

- Aperçu d'un SI Linux
  - ▶ Aperçu
  - ▶ Points forts
  - ▶ Points faibles
- Sécurité et Linux
  - ▶ Tour d'horizon
  - ▶ Durcissement
- Exemple
  - ▶ Architecture d'un réseau d'entreprise
  - ▶ Zoom : le firewall
  - ▶ Zoom : le frontal HTTP

## ■ Aperçu d'un SI Linux

- ▶ Aperçu
- ▶ Points forts
- ▶ Points faibles

## ■ Sécurité et Linux

- ▶ Tour d'horizon
- ▶ Durcissement

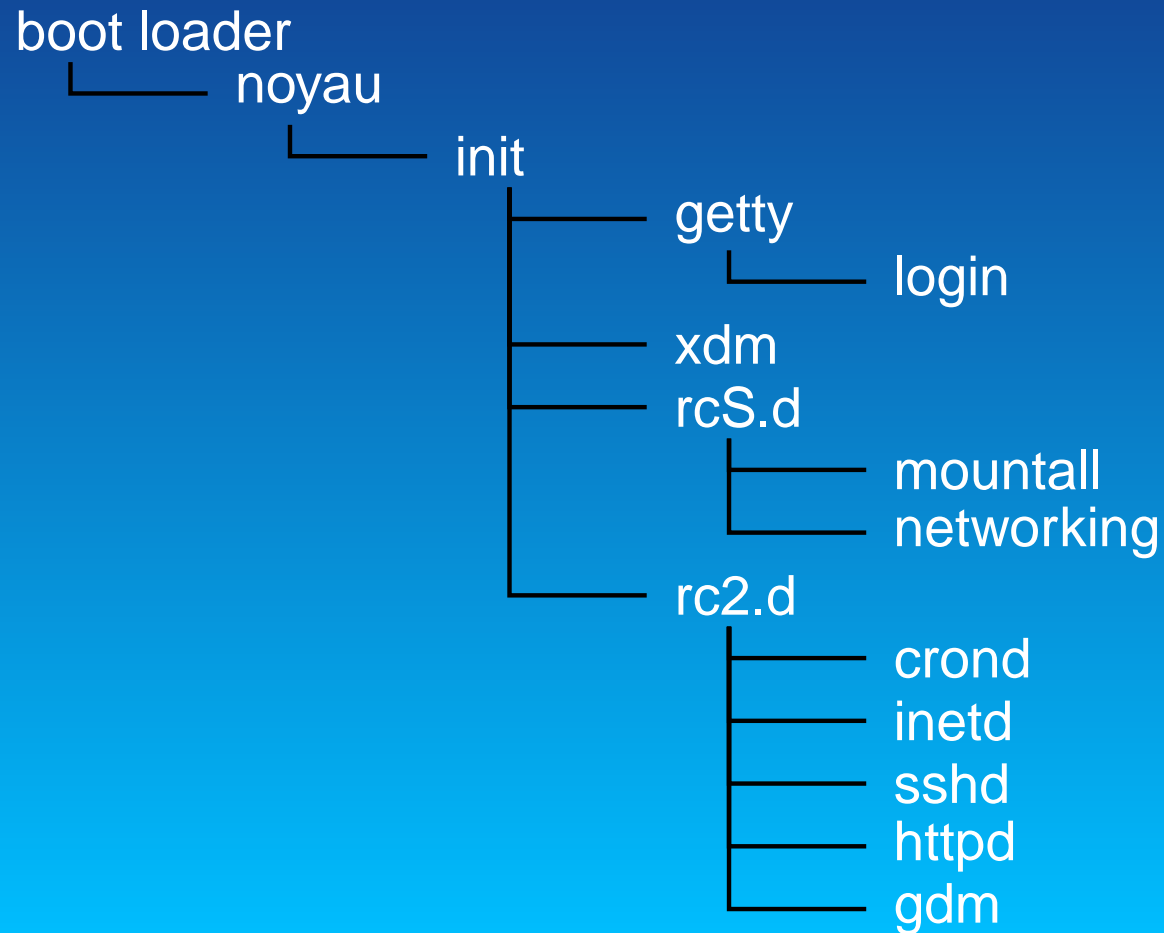
## ■ Exemple

- ▶ Architecture d'un réseau d'entreprise
- ▶ Zoom : le firewall
- ▶ Zoom : le frontal HTTP

## Vocabulaire

- Linux = noyau
- OS = noyau plus utilitaires de base (ex: GNU/Linux, GNU/Hurd)
- SI = OS+applications

Déroulement du boot:



## ■ OS

- ▶ Modularité
- ▶ Extensibilité
- ▶ Transparence
- ▶ Profusion de logiciels

## ■ Noyau

- ▶ tourne sur une quinzaine d'architectures
  - ▶ supporte une trentaine de systèmes de fichiers ainsi que la plupart des formats de disques (Sun, SGI, Ultrix, etc.)
- ➔ possibilité d'une couche logicielle cohérente sur une couche matérielle hétéroclite

## ■ Logiciel libre

- ▶ pérennité (ex: les noyaux 2.0 sont toujours maintenus, possibilité de maintenir soi-même un vieux logiciel, etc.)
- ▶ sûreté de fonctionnement (audits internes, pas de spyware, etc.)
- ▶ réaction rapide face aux failles (full disclosure, possibilité de corriger soi-même, etc.)

## ■ Points faibles

- ▶ nécessite une bonne connaissance pour l'utiliser sûrement
- ▶ parfois trop de choix

- Aperçu d'un SI Linux

- ▶ Aperçu
- ▶ Points forts
- ▶ Points faibles

- Sécurité et Linux

- ▶ Tour d'horizon
- ▶ Durcissement

- Exemple

- ▶ Architecture d'un réseau d'entreprise
- ▶ Zoom : le firewall
- ▶ Zoom : le frontal HTTP

## ■ Applications

- ▶ Authentification (PAM, LDAP, etc.)
- ▶ Proxys (HTTP, FTP, SMTP, DNS, Socks, etc.)
- ▶ Wrappers
- ▶ NIDS (*Prelude, Snort, Firestorm, Tamandua, FWLogWatch, FireParse, etc.*)
- ▶ HIDS (*Tripwire, AIDE, md5mon, bsign, Abacus (LogCheck, PortSentry, HostSentry), Swatch, etc.*)
- ▶ etc.

## ■ Noyau

- ▶ Firewalling (*iptables/netfilter*)
- ▶ Emprisonnement (*chroot()*)
- ▶ Capabilities
- ▶ IPSec (*FreeS/WAN*)
- ▶ Systèmes de fichiers chiffrés
- ▶ patchs divers (ACL, etc.)
- ▶ Durcissement (*OpenWall, GrSecurity, LIDS, LoMaC, SELinux, LSM, etc.*)
- ▶ etc.

## ■ Outils, audit

- ▶ Scanners automatiques (*hping2, nmap, nessus, etc.*)
- ▶ Analyseurs réseau (*tcpdump, ethereal, etc.*)
- ▶ Pots de miels virtuels (*User-Mode Linux, Plex86, Bochs*)
- ▶ etc.

## ■ Sureté de fonctionnement

- ▶ Systèmes de fichier journalisés (ext3, ReiserFS, XFS, etc.)
- ▶ LVS (Linux Virtual Server) (failover, répartition de charge)
- ▶ LVM (Logical Volume Manager) (hotplug sans RAID matériel)
- ▶ etc.

## ■ Premières mesures

- ▶ Désactiver les services inutiles
- ▶ Désinstaller les packages inutiles ( $\text{\LaTeX}$ , compilateurs, X11, packages contenant des programmes SUID/SGID)
- ▶ Utiliser des applications robustes, simples, minimales. Éviter les SUID/SGID
- ▶ Possibilité d'utiliser des wrappers
- ▶ Firewalling (la machine filtre ses propres flux réseaux )
- ▶ Filtrer les logs, remonter les alertes
- ▶ Vérification d'intégrité

- Pour aller plus loin...
  - ▶ capabilities, UID non privilégié, chroot
  - ▶ Retirer `CAP_SYS_MODULE` et `CAP_SYS_RAW_IO` du système
  - ▶ Recompilation du noyau minimal, sans module, et retirer le `CAP_SYS_RAW_IO`
  - ▶ Utilisation de bibliothèques du type *libsafe*
  - ▶ Utilisation d'extensions de compilateurs (*StackGuard*, *StackShield*, etc.)
  - ▶ Utilisation de distributions sécurisées (*Immunix*, *Engarde*, etc.) ou des scripts de durcissements
  - ▶ Utilisation de patchs de sécurité (durcissement, contrôle d'accès)

- Aperçu d'un SI Linux

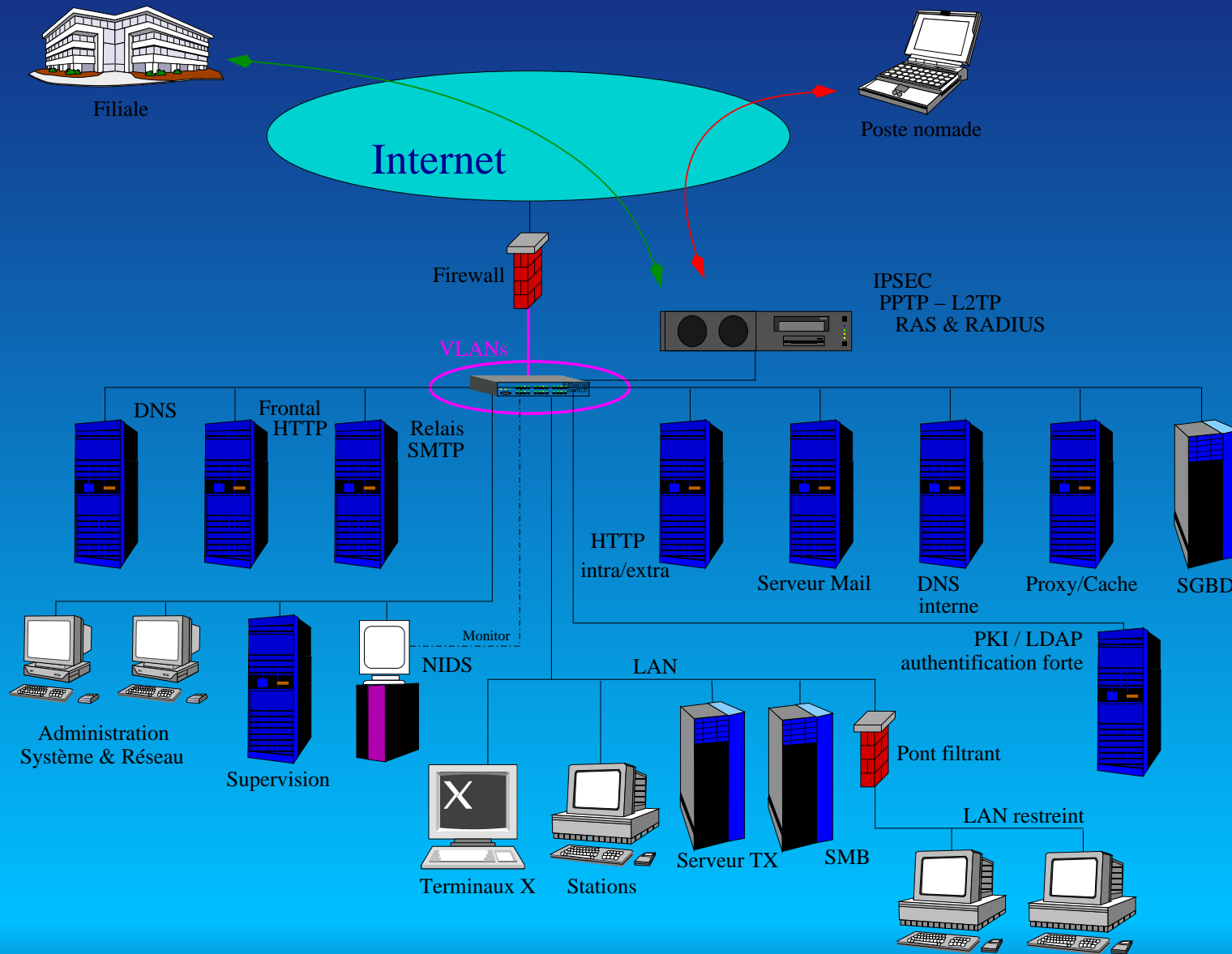
- ▶ Aperçu
- ▶ Points forts
- ▶ Points faibles

- Sécurité et Linux

- ▶ Tour d'horizon
- ▶ Durcissement

- Exemple

- ▶ Architecture d'un réseau d'entreprise
- ▶ Zoom : le firewall
- ▶ Zoom : le frontal HTTP



## ■ Le firewall

- ▶ Environnement applicatif minimal
  - ▶ Serveur SSHv2 sur l'interface d'admin seulement
  - ▶ Noyau minimum avec restriction d'accès (LIDS)
  - ▶ Pas de service sur les interfaces réseau
- ➔ Un firewall peut fonctionner en runlevel 0 (halt) !

## ■ Le frontal HTTP

- ▶ Apache avec support PHP, SSL, rewrite et proxy
- ▶ Serveur HTTP en environnement restreint
- ▶ PHP restreint, `safe_mode` activé
- ▶ Authentification forte par certificats
- ▶ Firewalling
- ▶ Accès SSHv2 seulement depuis le réseau d'administration
- ▶ restrictions d'accès au niveau noyau (LIDS).

## ■ Linux

- ▶ <http://www.linux.org/>
- ▶ <http://www.linuxdoc.org/>

## ■ Noyau

- ▶ <http://www.kernel.org/>
- ▶ <http://www.lids.org/>
- ▶ <http://www.grsecurity.net/>

## ■ Réseau

- ▶ <http://www.netfilter.org/>
- ▶ <http://www.freeswan.org/>

## ■ Applications

- ▶ <http://www.prelude-ids.org/>
- ▶ <http://www.openssh.org/>
- ▶ <http://www.insecure.org/namp/>
- ▶ <http://www.nessus.org/>
- ▶ <http://www.LinuxVirtualServer.org/>

## ■ Distributions

- ▶ <http://www.debian.org/>
- ▶ <http://immunix.org/>