AYI NEDJIMI Consultants

Durcissement Linux 2026 : Guide Hard

10 mai 2026 • Mis à jour le 17 mai 2026 • 20 min de lecture • 4172 mots •

Guide durcissement Linux 2026 : CIS Benchmark, SELinux, AppArmor, ker
production.

À RETENIR

À retenir — Durcissement Linux 2026

Le durcissement Linux repose sur cinq couches complémentaires : noyau, audit.

Le CIS Benchmark reste la référence opérationnelle (250+ contrôles par di
ANSSI et NIST 800-53.

SELinux (RHEL/Fedora) et AppArmor (Debian/Ubuntu) sont deux mécanisr
jamais désactiver en production.

Les paramètres sysctl et la configuration kernel module blacklisting ferme
DoS réseau.

> L'**audit** via *auditd* et l'envoi vers SIEM sont indispensables pour répondre à

Le durcissement Linux est un exercice à la fois ancien et toujours actuel. Ancien, p
inutiles, séparation des privilèges, journalisation) sont stables depuis vingt ans. Ac
(rootkits eBPF, kernel exploits modernes, attaques sur la chaîne d'approvisionnem
réglementaires se durcissent (NIS2, ISO 27001:2022, certification HDS, qualificatio
une méthodologie opérationnelle de hardening pour serveurs Linux Debian, Ubunt
Benchmark v3 et le guide d'hygiène ANSSI. Vous y trouverez les commandes prêt
commentés, les pièges classiques et un script d'audit complet à intégrer dans votr

---

1. Pourquoi durcir Linux en 2026 ?

Linux est partout : selon le rapport StackOverflow Developer Survey 2025, plus de
sous Linux, et la part de marché des containers Linux sur l'edge dépasse 90%. Ce
les attaquants. Le rapport CrowdStrike 2026 indique que les compromissions de s
2025, portées par trois familles de menaces : les rootkits eBPF capables de masqu
ransomwares Linux ciblant les hyperviseurs ESXi et Proxmox, et les attaques de su
dans l'incident XZ Utils CVE-2024-3094).

1.1 Conformité réglementaire

Plusieurs cadres réglementaires imposent désormais un niveau de durcissement v

NIS2 — Article 21 : mesures techniques et organisationnelles, dont le durcissem

ISO 27001:2022 — Contrôle A.8.9 : *Configuration* e une base

HDS (Hébergeur de Données de Santé) — Référe apitre 7.10 :

Réponse sous 24h

Devis gratuit →