03/12/2025

Dossier Complet de Sécurisation et Durcissement — Serveur Debian 13 (Trixie)

Aziz benyamina

Table des matières

1. INTRODUCTION

Ce document détaille les opérations techniques effectuées pour durcir le serveur Debian. L'objectif est de passer d'une installation par défaut à un niveau de sécurité "Production", résistant aux attaques courantes (Brute force, Spoofing, Rootkits).

---

2. PHASE I : GESTION DES ACCÈS ET IDENTITÉS

2.1. Création de l'utilisateur Administrateur

L'usage du compte root a été supprimé au profit d'un utilisateur nommé.

- **Commandes exécutées :**

Bash

```
# Création de l'utilisateur
sudo useradd -m -s /bin/bash deploy


# Définition du mot de passe
sudo passwd deploy


# Attribution des droits sudo
sudo usermod -aG sudo deploy
```

2.2. Configuration du Serveur SSH

Le service SSH a été obscurci et verrouillé cryptographiquement.

- **Fichier modifié :** /etc/ssh/sshd_config
- **Configuration appliquée :**

Plaintext

```
Port 5956
PermitRootLogin no
PasswordAuthentication no
PubkeyAuthentication yes
```

MaxAuthTries 3

MaxSessions 2

AllowTcpForwarding no

X11Forwarding no

AllowAgentForwarding no

- **Correction spécifique (Socket Systemd) :** Désactivation du socket pour forcer l'usage du service SSH standard sur le port 5956.

Bash

sudo systemctl stop ssh.socket

sudo systemctl disable ssh.socket

sudo systemctl mask ssh.socket

sudo systemctl restart ssh

2.3. Mise en place des Clés SSH

Authentification unique par clé (Ed25519) et sécurisation des permissions.

- **Commandes exécutées (Serveur) :**

Bash

Création du dossier et fichier

mkdir -p /home/deploy/.ssh

Verrouillage strict des permissions (Critique)

chmod 700 /home/deploy/.ssh

chmod 600 /home/deploy/.ssh/authorized_keys

chown -R deploy:deploy /home/deploy/.ssh

---

3. PHASE II : SÉCURITÉ RÉSEAU ET PARE-FEU

3.1. Pare-feu UFW (Uncomplicated Firewall)

Application d'une politique de "Refus par défaut".

- **Commandes exécutées :**

Bash

Installation

sudo apt install ufw

```
# Configuration des règles
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow 5956/tcp
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp

# Désactivation IPv6 (dans /etc/default/ufw -> IPV6=no)

# Activation
sudo ufw enable
```

3.2. Défense Active (Fail2Ban)

Bannissement automatique des IP attaquantes.

- **Fichier créé :** /etc/fail2ban/jail.local
- **Configuration appliquée :**

Ini, TOML

```
[sshd]
enabled = true
port = 5956
maxretry = 3
mode = aggressive
bantime = 1h
```

- **Commande de redémarrage :**

Bash

```
sudo systemctl restart fail2ban
```

3.3. Correction DNS (Infrastructure)

Suppression des serveurs DNS IPv6 défectueux injectés par l'hébergeur.

- **Action 1 (Resolvconf) :** Modification de /etc/resolvconf/resolv.conf.d/head.
    - *Ajout :* nameserver 1.1.1.1 et nameserver 8.8.8.8.
- **Action 2 (DHCP) :** Modification de /etc/dhcp/dhclient.conf.

- *Suppression :* Références à dhcp6 dans la ligne request.

- **Application :**

Bash

sudo resolvconf -u

sudo systemctl restart networking

---

4. PHASE III : DURCISSEMENT DU NOYAU ET DU SYSTÈME

4.1. Paramètres Sysctl (Noyau)

Protection mémoire et réseau.

- **Fichier créé :** /etc/sysctl.d/99-hardening.conf
- **Contenu :**

Ini, TOML

net.ipv4.conf.all.rp_filter = 1

net.ipv4.conf.default.rp_filter = 1

kernel.kptr_restrict = 2

net.ipv4.conf.all.log_martians = 1

- **Commande d'application :**

Bash

sudo sysctl -p /etc/sysctl.d/99-hardening.conf

4.2. Blacklisting des Modules

Réduction de la surface d'attaque matérielle et protocolaire.

- **Fichiers créés dans /etc/modprobe.d/ :**
  - blacklist-uncommon-net.conf : Bloque dccp, sctp, rds, tipc.
  - blacklist-peripherals.conf : Bloque usb-storage, firewire-core.
- **Commande d'application :**

Bash

sudo update-initramfs -u

4.3. Permissions Fichiers et UMASK

- **Fichier modifié :** /etc/login.defs (Ajout de UMASK 027).
- **Commandes de verrouillage :**

Bash

sudo chmod 700 /home/deploy

sudo chmod 700 /root

---

5. PHASE IV : AUDIT, SURVEILLANCE ET INTÉGRITÉ

5.1. Auditd (Temps Réel)

- **Commandes exécutées :**

Bash

sudo apt install auditd

Création des règles dans /etc/audit/rules.d/10-custom.rules

sudo /sbin/augenrules --load

- **Configuration Logs :** Rotation interne configurée dans /etc/audit/auditd.conf.

5.2. AIDE (Intégrité des Fichiers)

- **Commandes exécutées :**

Bash

sudo apt install aide aide-common

sudo aide --init --config /etc/aide/aide.conf

sudo cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db

5.3. Rkhunter & Debsums

- **Rkhunter :** Scan effectué, correction du faux positif /etc/.updated (whitelisté).
- **Debsums :** Installation et vérification des binaires.

Bash

sudo apt install debsums

sudo debsums sudo

sudo debsums openssh-server

---

6. PHASE V : MAINTENANCE ET GESTION DES PAQUETS

6.1. Réparation des Dépôts APT

Le fichier source était vide, bloquant les mises à jour de sécurité.

- **Action :** Reconstruction de /etc/apt/sources.list.
- **Ajout critique :**

Plaintext

deb http://security.debian.org/debian-security trixie-security main contrib non-free-firmware

- **Nettoyage :**

Bash

sudo rm /etc/apt/sources.list.d/debian.sources

sudo apt update

6.2. Automatisation

Installation des outils de maintenance automatique.

- **Commande :**

Bash

sudo apt install unattended-upgrades apt-listbugs needrestart

---

7. SÉCURITÉ AVANCÉE (AppArmor)

Mise en place du Contrôle d'Accès Obligatoire (MAC).

- **Installation :**

Bash

sudo apt install apparmor apparmor-utils

sudo systemctl start apparmor

- **Confinement SSHD :** Nous avons identifié le binaire et appliqué le mode strict.

Bash

Localisation

sudo find / -name "sshd"

Application du mode Enforce

sudo aa-enforce /usr/sbin/sshd

---

8 : Analyse et durcissement du système avec Lynis

8.1 Présentation de Lynis

Lynis est un outil open-source d'audit de sécurité conçu pour analyser en profondeur les systèmes Unix/Linux. Il est principalement utilisé pour :

- évaluer le niveau de sécurité d'un serveur,
- détecter les mauvaises configurations,
- proposer des recommandations,

- générer un **Hardening Index** (score de durcissement).

Lynis est souvent utilisé dans les environnements professionnels, les audits de conformité, et les systèmes nécessitant un haut niveau de sécurité (santé, finance, infrastructures critiques).

8.2 Installation de Lynis

Sous Debian/Ubuntu, l'installation est simple :

sudo apt update

sudo apt install lynis -y

Pour vérifier la version installée :

lynis show version

8.3 Fonctionnement général

Lynis procède à une analyse complète du système selon différents modules :

- **Boot & Services**
- **Authentification**
- **Réseau**
- **Système de fichiers**
- **Permissions & Ownership**
- **Logs et monitoring**
- **Firewall**
- **Malwares, sécurité avancée, auditd, AppArmor**

Chaque module réalise plusieurs tests, qui génèrent :

- **OK** → conforme
- **WARNINGS** → points critiques
- **SUGGESTIONS** → améliorations possibles

8.4 Lancer un audit complet

Commande d'audit standard :

sudo lynis audit system

9. CONCLUSION

Le serveur a été redémarré avec succès via sudo reboot.

État final : Le serveur est opérationnel, accessible uniquement via clé cryptographique, protégé par un pare-feu strict, et dispose d'une surveillance complète de l'intégrité du système et des actions utilisateurs. Toutes les vulnérabilités détectées par l'audit initial ont été corrigées.