# Checklist Sécurité UBUNTU LINUX 24.04 LTS — SERVEUR

**Ayi NEDJIMI Consultants**
ayinedjimi-consultants.fr
v1.0 — 2026-04-04 | **Classification :** CONFIDENTIEL | **Auteur :** AYI NEDJIMI CONSULTANTS · 177 controles

# Sommaire

## 1.0 — CONFIGURATION INITIALE ET SYSTÈME DE FICHIERS

### 1.1.1 *Désactiver le montage du système de fichiers cramfs*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1005 (Data from Local System)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R1 — Minimiser les services et modules noyau

**DESCRIPTION :**
Le système de fichiers cramfs (Compressed ROM File System) est un système de fichiers en lecture seule conçu pour les systèmes embarqués. Il n'est généralement pas nécessaire sur un serveur Ubuntu et peut être utilisé comme vecteur d'attaque pour monter des images malveillantes. La désactivation de cramfs réduit la surface d'attaque du noyau en empêchant le chargement automatique du module.

```
# Vérifier que le module est désactivé
modprobe -n -v cramfs 2>/dev/null | grep -E '(install|/bin/(true|false))'
# Vérifier que le module n'est pas chargé
lsmod | grep cramfs
```

**AUDIT :**

- **Fichier :** `/etc/modprobe.d/cramfs.conf`
- **Valeur attendue :** `install /bin/true ou install /bin/false`
- **Résultat attendu :** Le module ne doit pas être chargé et la commande modprobe doit retourner `install /bin/false`

```
# Désactiver cramfs
echo 'install cramfs /bin/false' | sudo tee /etc/modprobe.d/cramfs.conf
echo 'blacklist cramfs' | sudo tee -a /etc/modprobe.d/cramfs.conf
# Décharger le module si chargé
sudo modprobe -r cramfs 2>/dev/null
```

**VALEUR PAR DÉFAUT :**
Le module cramfs est disponible mais pas chargé par défaut sur Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.1.2 *Désactiver le montage du système de fichiers squashfs*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1005 (Data from Local System)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R1 — Minimiser les services et modules noyau

**DESCRIPTION :**
Le système de fichiers squashfs est un système de fichiers compressé en lecture seule utilisé principalement pour les images snap et les live CD. Sur un serveur de production, sauf si des paquets snap sont nécessaires, squashfs doit être désactivé. Attention : la désactivation de squashfs empêchera l'utilisation des paquets snap.

```
# Vérifier que le module est désactivé
modprobe -n -v squashfs 2>/dev/null | grep -E '(install|/bin/(true|false))'
# Vérifier que le module n'est pas chargé
lsmod | grep squashfs
```

**AUDIT :**

- **Fichier :** `/etc/modprobe.d/squashfs.conf`
- **Valeur attendue :** `install /bin/true ou install /bin/false`
- **Résultat attendu :** Le module ne doit pas être chargé et la commande modprobe doit retourner `install /bin/false`

```
# Désactiver squashfs
echo 'install squashfs /bin/false' | sudo tee /etc/modprobe.d/squashfs.conf
echo 'blacklist squashfs' | sudo tee -a /etc/modprobe.d/squashfs.conf
# Décharger le module si chargé
sudo modprobe -r squashfs 2>/dev/null
# NOTE : Cela empêchera l'utilisation de snap
```

**VALEUR PAR DÉFAUT :**
Le module squashfs est chargé par défaut (utilisé par snap)
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.1.3 *Désactiver le montage du système de fichiers udf*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1091 (Replication Through Removable Media)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R1 — Minimiser les services et modules noyau

**DESCRIPTION :**
Le système de fichiers UDF (Universal Disk Format) est utilisé pour les supports optiques (DVD, Blu-ray). Sur un serveur, ce format n'a aucune utilité et peut servir de vecteur pour monter des médias amovibles contenant du code malveillant. La désactivation du module udf fait partie du durcissement de la surface d'attaque.

```
# Vérifier que le module est désactivé
modprobe -n -v udf 2>/dev/null | grep -E '(install|/bin/(true|false))'
# Vérifier que le module n'est pas chargé
lsmod | grep udf
```

**AUDIT :**

- **Fichier :** `/etc/modprobe.d/udf.conf`
- **Valeur attendue :** `install /bin/true ou install /bin/false`
- **Résultat attendu :** Le module ne doit pas être chargé et la commande modprobe doit retourner `install /bin/false`

```
# Désactiver udf
echo 'install udf /bin/false' | sudo tee /etc/modprobe.d/udf.conf
echo 'blacklist udf' | sudo tee -a /etc/modprobe.d/udf.conf
sudo modprobe -r udf 2>/dev/null
```

**VALEUR PAR DÉFAUT :**
Le module udf est disponible mais pas chargé par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.1.4 *Désactiver le montage du système de fichiers freevxfs*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1005 (Data from Local System)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R1 — Minimiser les services et modules noyau

**DESCRIPTION :**
Le système de fichiers freevxfs (Free Veritas VxFS) est une implémentation libre du système de fichiers Veritas. Ce système de fichiers est rarement utilisé sur les serveurs Linux modernes et représente une surface d'attaque inutile. Sa désactivation empêche le montage de volumes VxFS potentiellement malveillants.

```
# Vérifier que le module est désactivé
modprobe -n -v freevxfs 2>/dev/null | grep -E '(install|/bin/(true|false))'
# Vérifier que le module n'est pas chargé
lsmod | grep freevxfs
```

**AUDIT :**

- **Fichier :** `/etc/modprobe.d/freevxfs.conf`
- **Valeur attendue :** `install /bin/true ou install /bin/false`
- **Résultat attendu :** Le module ne doit pas être chargé et la commande modprobe doit retourner `install /bin/false`

```
echo 'install freevxfs /bin/false' | sudo tee /etc/modprobe.d/freevxfs.conf
echo 'blacklist freevxfs' | sudo tee -a /etc/modprobe.d/freevxfs.conf
sudo modprobe -r freevxfs 2>/dev/null
```

**VALEUR PAR DÉFAUT :**
Le module freevxfs est disponible mais pas chargé par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.1.5 *Désactiver le montage du système de fichiers jffs2*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1005 (Data from Local System)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R1 — Minimiser les services et modules noyau

**DESCRIPTION :**
JFFS2 (Journalling Flash File System 2) est un système de fichiers conçu pour les mémoires flash. Il est principalement utilisé dans les systèmes embarqués et n'a aucune utilité sur un serveur Ubuntu standard. La désactivation de ce module réduit la surface d'attaque du noyau.

```
# Vérifier que le module est désactivé
modprobe -n -v jffs2 2>/dev/null | grep -E '(install|/bin/(true|false))'
# Vérifier que le module n'est pas chargé
lsmod | grep jffs2
```

**AUDIT :**

- **Fichier :** `/etc/modprobe.d/jffs2.conf`
- **Valeur attendue :** `install /bin/true ou install /bin/false`
- **Résultat attendu :** Le module ne doit pas être chargé et la commande modprobe doit retourner `install /bin/false`

```
echo 'install jffs2 /bin/false' | sudo tee /etc/modprobe.d/jffs2.conf
echo 'blacklist jffs2' | sudo tee -a /etc/modprobe.d/jffs2.conf
sudo modprobe -r jffs2 2>/dev/null
```

**VALEUR PAR DÉFAUT :**
Le module jffs2 est disponible mais pas chargé par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 1.1.6 *Désactiver le montage du système de fichiers hfs*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1091 (Replication Through Removable Media)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R1 — Minimiser les services et modules noyau

**DESCRIPTION :**
HFS (Hierarchical File System) est le système de fichiers historique d'Apple Macintosh. Il n'a aucune utilité sur un serveur Ubuntu et peut être exploité via des médias amovibles formatés en HFS contenant du code malveillant. La désactivation empêche le montage automatique de tels volumes.

```
# Vérifier que le module est désactivé
modprobe -n -v hfs 2>/dev/null | grep -E '(install|/bin/(true|false))'
# Vérifier que le module n'est pas chargé
lsmod | grep hfs
```

**AUDIT :**

- **Fichier :** `/etc/modprobe.d/hfs.conf`
- **Valeur attendue :** `install /bin/true ou install /bin/false`
- **Résultat attendu :** Le module ne doit pas être chargé et la commande modprobe doit retourner `install /bin/false`

```
echo 'install hfs /bin/false' | sudo tee /etc/modprobe.d/hfs.conf
echo 'blacklist hfs' | sudo tee -a /etc/modprobe.d/hfs.conf
sudo modprobe -r hfs 2>/dev/null
```

**VALEUR PAR DÉFAUT :**
Le module hfs est disponible mais pas chargé par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 1.1.7 *Désactiver le montage du système de fichiers hfsplus*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1091 (Replication Through Removable Media)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R1 — Minimiser les services et modules noyau

**DESCRIPTION :**
HFS+ (HFS Plus) est le successeur de HFS, utilisé par macOS. Comme HFS, il n'est pas nécessaire sur un serveur Linux et constitue une surface d'attaque potentielle via les médias amovibles. La désactivation du module hfsplus complète la stratégie de durcissement des systèmes de fichiers.

```
# Vérifier que le module est désactivé
modprobe -n -v hfsplus 2>/dev/null | grep -E '(install|/bin/(true|false))'
# Vérifier que le module n'est pas chargé
lsmod | grep hfsplus
```

**AUDIT :**

- **Fichier :** `/etc/modprobe.d/hfsplus.conf`
- **Valeur attendue :** `install /bin/true ou install /bin/false`
- **Résultat attendu :** Le module ne doit pas être chargé et la commande modprobe doit retourner `install /bin/false`

```
echo 'install hfsplus /bin/false' | sudo tee /etc/modprobe.d/hfsplus.conf
echo 'blacklist hfsplus' | sudo tee -a /etc/modprobe.d/hfsplus.conf
sudo modprobe -r hfsplus 2>/dev/null
```

**VALEUR PAR DÉFAUT :**
Le module hfsplus est disponible mais pas chargé par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 1.1.8 *Désactiver le montage du système de fichiers usb-storage*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1091 (Replication Through Removable Media)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R1 — Minimiser les services et modules noyau

**DESCRIPTION :**
Le module usb-storage permet le montage des périphériques de stockage USB (clés USB, disques externes). Sur un serveur, les périphériques USB de stockage représentent un risque majeur d'exfiltration de données et d'introduction de logiciels malveillants. La désactivation de ce module est fortement recommandée en environnement serveur.

```
# Vérifier que le module est désactivé
modprobe -n -v usb-storage 2>/dev/null | grep -E '(install|/bin/(true|false))'
# Vérifier que le module n'est pas chargé
lsmod | grep usb_storage
```

**AUDIT :**

- **Fichier :** `/etc/modprobe.d/usb-storage.conf`
- **Valeur attendue :** `install /bin/true ou install /bin/false`
- **Résultat attendu :** Le module ne doit pas être chargé et la commande modprobe doit retourner `install /bin/false`

```
echo 'install usb-storage /bin/false' | sudo tee /etc/modprobe.d/usb-storage.conf
echo 'blacklist usb-storage' | sudo tee -a /etc/modprobe.d/usb-storage.conf
sudo modprobe -r usb_storage 2>/dev/null
```

**VALEUR PAR DÉFAUT :**
Le module usb-storage est chargé par défaut si des ports USB sont détectés

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 1.2.1 *Vérifier l'existence d'une partition séparée pour /tmp*

**Profil :** Niveau 2 (L2) — Serveur
**MITRE ATT&CK :** T1499.001 (Endpoint Denial of Service)
**NIST SP 800-53 :** CM-6 (Configuration Settings), SC-39 (Process Isolation)
**ANSSI :** R28 — Partitionnement du système de fichiers

**DESCRIPTION :**
La partition /tmp doit être sur une partition séparée pour empêcher un utilisateur malveillant de remplir le système de fichiers racine. Une partition /tmp séparée permet également d'appliquer des options de montage restrictives (nodev, nosuid, noexec) qui limitent l'exploitation de fichiers temporaires.

```
# Vérifier le montage
findmnt --kernel /tmp
```

**AUDIT :**

- **Fichier :** `/tmp`
- **Valeur attendue :** Une ligne montrant /tmp comme point de montage séparé

```
# Option 1 : Créer une partition /tmp dans /etc/fstab
sudo systemctl unmask tmp.mount
sudo systemctl enable tmp.mount

# Option 2 : Ajouter dans /etc/fstab
# tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime,size=2G 0 0
sudo mount -o remount /tmp
```

**VALEUR PAR DÉFAUT :**
Non configuré par défaut — nécessite un partitionnement manuel lors de l'installation
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.2.2 *Vérifier les options nodev, nosuid, noexec sur /tmp*

**Profil :** Niveau 2 (L2) — Serveur
**MITRE ATT&CK :** T1036.005 (Masquerading: Match Legitimate Name)
**NIST SP 800-53 :** CM-6 (Configuration Settings), SC-39 (Process Isolation)
**ANSSI :** R28 — Partitionnement du système de fichiers

**DESCRIPTION :**
Les options de montage restrictives sur /tmp empêchent la création de fichiers de périphérique (nodev), l'exécution de programmes avec des permissions élevées (nosuid) et l'exécution directe de binaires (noexec). Ces trois options combinées constituent une protection essentielle contre l'exploitation de la partition temporaire.

```
# Vérifier le montage
findmnt --kernel /tmp | grep -E 'nodev|nosuid|noexec'
```

**AUDIT :**

- **Fichier :** `/etc/fstab ou /etc/systemd/system/tmp.mount`
- **Valeur attendue :** Options : nodev,nosuid,noexec

```
# Modifier /etc/fstab pour /tmp
# tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime,size=2G 0 0
sudo mount -o remount,nodev,nosuid,noexec /tmp

# Ou modifier /etc/systemd/system/tmp.mount
# [Mount]
# Options=mode=1777,strictatime,nosuid,nodev,noexec,size=2G
```

**VALEUR PAR DÉFAUT :**
Non configuré par défaut — nécessite un partitionnement manuel lors de l'installation
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.2.3 *Vérifier l'existence d'une partition séparée pour /var*

**Profil :** Niveau 2 (L2) — Serveur
**MITRE ATT&CK :** T1499.001 (Endpoint Denial of Service)
**NIST SP 800-53 :** CM-6 (Configuration Settings), SC-39 (Process Isolation)
**ANSSI :** R28 — Partitionnement du système de fichiers

**DESCRIPTION :**
La partition /var contient des données variables telles que les journaux système, les files d'attente de courrier et les caches. Un utilisateur ou un processus malveillant pourrait remplir /var et provoquer un déni de service. Une partition séparée pour /var protège le système de fichiers racine.

```
# Vérifier le montage
findmnt --kernel /var
```

**AUDIT :**

- **Fichier :** `/var`
- **Valeur attendue :** Une ligne montrant /var comme point de montage séparé

```
# /var doit être configuré lors de l'installation
# Ajouter dans /etc/fstab si partition existante :
# /dev/sdXN /var ext4 defaults,nosuid,nodev 0 2
```

**VALEUR PAR DÉFAUT :**
Non configuré par défaut — nécessite un partitionnement manuel lors de l'installation
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.2.4 *Vérifier l'existence d'une partition séparée pour /var/tmp*

**Profil :** Niveau 2 (L2) — Serveur
**MITRE ATT&CK :** T1499.001 (Endpoint Denial of Service)
**NIST SP 800-53 :** CM-6 (Configuration Settings), SC-39 (Process Isolation)
**ANSSI :** R28 — Partitionnement du système de fichiers

**DESCRIPTION :**
La partition /var/tmp est utilisée pour stocker des fichiers temporaires qui doivent persister entre les redémarrages. Comme /tmp, elle doit être isolée sur une partition séparée avec des options de montage restrictives pour empêcher l'exploitation.

```
# Vérifier le montage
findmnt --kernel /var/tmp
```

**AUDIT :**

- **Fichier :** `/var/tmp`
- **Valeur attendue :** Une ligne montrant /var/tmp comme point de montage séparé avec nodev,nosuid,noexec

```
# Ajouter dans /etc/fstab :
# /dev/sdXN /var/tmp ext4 defaults,nosuid,nodev,noexec 0 2
# Ou lier à /tmp :
# sudo mount --bind /tmp /var/tmp
```

**VALEUR PAR DÉFAUT :**
Non configuré par défaut — nécessite un partitionnement manuel lors de l'installation
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.2.5 *Vérifier l'existence d'une partition séparée pour /var/log*

**Profil :** Niveau 2 (L2) — Serveur
**MITRE ATT&CK :** T1070.002 (Indicator Removal: Clear Linux or Mac System Logs)
**NIST SP 800-53 :** CM-6 (Configuration Settings), SC-39 (Process Isolation)
**ANSSI :** R28 — Partitionnement du système de fichiers

**DESCRIPTION :**
Les journaux système sont critiques pour la détection d'incidents. Une partition séparée pour /var/log protège les journaux contre le remplissage du système de fichiers racine et vice-versa. Elle permet aussi d'appliquer des politiques de rétention spécifiques.

```
# Vérifier le montage
findmnt --kernel /var/log
```

**AUDIT :**

- **Fichier :** `/var/log`
- **Valeur attendue :** Une ligne montrant /var/log comme point de montage séparé

```
# /var/log doit être configuré lors de l'installation
# Ajouter dans /etc/fstab :
# /dev/sdXN /var/log ext4 defaults,nosuid,nodev,noexec 0 2
```

**VALEUR PAR DÉFAUT :**
Non configuré par défaut — nécessite un partitionnement manuel lors de l'installation
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.2.6 *Vérifier l'existence d'une partition séparée pour /var/log/audit*

**Profil :** Niveau 2 (L2) — Serveur
**MITRE ATT&CK :** T1070.002 (Indicator Removal: Clear Linux or Mac System Logs)
**NIST SP 800-53 :** CM-6 (Configuration Settings), SC-39 (Process Isolation)
**ANSSI :** R28 — Partitionnement du système de fichiers
**DESCRIPTION :**
Les journaux d'audit (auditd) sont essentiels pour la traçabilité des actions de sécurité. Une partition séparée pour /var/log/audit garantit que les journaux d'audit ne sont pas affectés par le remplissage d'autres journaux et protège l'intégrité des preuves forensiques.

```
# Vérifier le montage
findmnt --kernel /var/log/audit
```

**AUDIT :**

- **Fichier :** `/var/log/audit`
- **Valeur attendue :** Une ligne montrant /var/log/audit comme point de montage séparé

```
# /var/log/audit doit être configuré lors de l'installation
# Ajouter dans /etc/fstab :
# /dev/sdXN /var/log/audit ext4 defaults,nosuid,nodev,noexec 0 2
```

**VALEUR PAR DÉFAUT :**
Non configuré par défaut — nécessite un partitionnement manuel lors de l'installation
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.2.7 *Vérifier l'existence d'une partition séparée pour /home*

**Profil :** Niveau 2 (L2) — Serveur
**MITRE ATT&CK :** T1499.001 (Endpoint Denial of Service)
**NIST SP 800-53 :** CM-6 (Configuration Settings), SC-39 (Process Isolation)
**ANSSI :** R28 — Partitionnement du système de fichiers
**DESCRIPTION :**
La partition /home contient les répertoires personnels des utilisateurs. L'isolation de /home sur une partition séparée empêche les utilisateurs de remplir le système de fichiers racine et permet d'appliquer des options de montage restrictives telles que nodev et nosuid.

```
# Vérifier le montage
findmnt --kernel /home
```

**AUDIT :**

- **Fichier :** `/home`
- **Valeur attendue :** Une ligne montrant /home comme point de montage séparé avec nodev,nosuid

```
# /home doit être configuré lors de l'installation
# Ajouter dans /etc/fstab :
# /dev/sdXN /home ext4 defaults,nosuid,nodev 0 2
```

**VALEUR PAR DÉFAUT :**
Non configuré par défaut — nécessite un partitionnement manuel lors de l'installation
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.2.8 *Vérifier les options nodev, nosuid sur /home*

**Profil :** Niveau 2 (L2) — Serveur
**MITRE ATT&CK :** T1036.005 (Masquerading: Match Legitimate Name)
**NIST SP 800-53 :** CM-6 (Configuration Settings), SC-39 (Process Isolation)
**ANSSI :** R28 — Partitionnement du système de fichiers
**DESCRIPTION :**
L'option nodev empêche la création de fichiers de périphérique dans /home, tandis que nosuid empêche l'exécution de programmes avec des permissions SUID/SGID. Ces options réduisent le risque d'élévation de privilèges depuis les répertoires utilisateurs.

```
# Vérifier le montage
findmnt --kernel /home | grep -E 'nodev|nosuid'
```

**AUDIT :**

- **Fichier :** `/etc/fstab`
- **Valeur attendue :** Options : nodev,nosuid

```
# Modifier /etc/fstab pour /home
# /dev/sdXN /home ext4 defaults,nosuid,nodev 0 2
sudo mount -o remount,nodev,nosuid /home
```

**VALEUR PAR DÉFAUT :**
Non configuré par défaut — nécessite un partitionnement manuel lors de l'installation
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.2.9 *Vérifier les options nodev, nosuid, noexec sur /dev/shm*

**Profil :** Niveau 2 (L2) — Serveur
**MITRE ATT&CK :** T1055.009 (Process Injection: Proc Memory)
**NIST SP 800-53 :** CM-6 (Configuration Settings), SC-39 (Process Isolation)
**ANSSI :** R28 — Partitionnement du système de fichiers

**DESCRIPTION :**
Le système de fichiers /dev/shm (mémoire partagée) est souvent exploité par les attaquants pour stocker et exécuter du code malveillant car il réside en mémoire. L'application des options nodev, nosuid et noexec sur /dev/shm est une mesure de sécurité critique qui empêche l'exécution de code depuis la mémoire partagée.

```
# Vérifier le montage
findmnt --kernel /dev/shm | grep -E 'nodev|nosuid|noexec'
```

**AUDIT :**

- **Fichier :** `/etc/fstab`
- **Valeur attendue :** Options : nodev,nosuid,noexec

```
# Ajouter ou modifier dans /etc/fstab :
tmpfs /dev/shm tmpfs defaults,nodev,nosuid,noexec 0 0
sudo mount -o remount,nodev,nosuid,noexec /dev/shm
```

**VALEUR PAR DÉFAUT :**
Non configuré par défaut — nécessite un partitionnement manuel lors de l'installation
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.3.1 *Vérifier que le mot de passe du chargeur de démarrage GRUB est configuré*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1542.003 (Pre-OS Boot: Bootkit)
**NIST SP 800-53 :** SI-7 (Software, Firmware, and Information Integrity)
**ANSSI :** R5 — Protection du chargeur de démarrage

**DESCRIPTION :**
Le chargeur de démarrage GRUB permet de modifier les paramètres de démarrage du noyau, ce qui peut être exploité pour obtenir un accès root en mode mono-utilisateur ou pour démarrer avec des paramètres dangereux (init=/bin/bash). Un mot de passe GRUB empêche les modifications non autorisées du menu de démarrage.

```
sudo grep -E '^set superusers' /boot/grub/grub.cfg 2>/dev/null
sudo grep -E '^password_pbkdf2' /boot/grub/grub.cfg 2>/dev/null
```

**AUDIT :**

- **Fichier :** `/boot/grub/grub.cfg, /etc/grub.d/40_custom`
- **Valeur attendue :** `Présence de 'set superusers' et 'password_pbkdf2'`

```
# Générer le hash du mot de passe GRUB
sudo grub-mkpasswd-pbkdf2
# Copier le hash généré

# Ajouter dans /etc/grub.d/40_custom :
cat << 'EOF' | sudo tee -a /etc/grub.d/40_custom
set superusers="grubadmin"
password_pbkdf2 grubadmin grub.pbkdf2.sha512.10000.<HASH>
EOF

# Mettre à jour GRUB
sudo update-grub
```

**VALEUR PAR DÉFAUT :**
Non configuré par défaut sur Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.3.2 *Vérifier les permissions du fichier de configuration GRUB*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1542.003 (Pre-OS Boot: Bootkit)
**NIST SP 800-53 :** SI-7 (Software, Firmware, and Information Integrity)
**ANSSI :** R5 — Protection du chargeur de démarrage
**DESCRIPTION :**
Le fichier /boot/grub/grub.cfg contient la configuration du chargeur de démarrage, y compris les mots de passe hashés. Les permissions doivent être restrictives (600 ou plus strict) et le propriétaire doit être root:root pour empêcher tout utilisateur non privilégié de lire ou modifier la configuration de démarrage.

```
stat -c '%a %U %G' /boot/grub/grub.cfg
```

**AUDIT :**

- **Fichier :** `/boot/grub/grub.cfg`
- **Valeur attendue :** `Permissions : 600, Propriétaire : root:root`

```
sudo chown root:root /boot/grub/grub.cfg
sudo chmod 600 /boot/grub/grub.cfg
```

**VALEUR PAR DÉFAUT :**
Non configuré par défaut sur Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.3.3 *Vérifier que l'authentification est requise pour le mode mono-utilisateur (single user)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1548.001 (Abuse Elevation Control: Setuid and Setgid)
**NIST SP 800-53 :** SI-7 (Software, Firmware, and Information Integrity)
**ANSSI :** R5 — Protection du chargeur de démarrage
**DESCRIPTION :**
Le mode mono-utilisateur (single user mode / recovery mode) donne un accès root sans authentification par défaut. Il est impératif de configurer un mot de passe root pour empêcher l'accès non autorisé via le mode de récupération. Un attaquant ayant un accès physique pourrait sinon obtenir un shell root.

```
sudo grep -E '^root:\$' /etc/shadow | cut -d: -f2 | head -c 3
```

**AUDIT :**

- **Fichier :** `/etc/shadow`
- **Valeur attendue :** `Le champ mot de passe de root ne doit pas être vide ou contenir '!' ou '*'`

```
# Définir un mot de passe root fort
sudo passwd root

# Vérifier que le service rescue requiert l'authentification
sudo systemctl show rescue.service | grep ExecStart
```

**VALEUR PAR DÉFAUT :**
Non configuré par défaut sur Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.3.4 *Vérifier que Secure Boot est activé (si UEFI)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1542.003 (Pre-OS Boot: Bootkit)
**NIST SP 800-53 :** SI-7 (Software, Firmware, and Information Integrity)
**ANSSI :** R5 — Protection du chargeur de démarrage
**DESCRIPTION :**
Secure Boot est une fonctionnalité UEFI qui vérifie la signature cryptographique du chargeur de démarrage et du noyau avant leur exécution. Cela empêche le chargement de code non signé ou modifié au niveau du démarrage, protégeant contre les rootkits et bootkits. Secure Boot doit être activé sur tous les serveurs UEFI.

```
mokutil --sb-state 2>/dev/null || echo 'mokutil non disponible'
# Alternative
dmesg | grep -i 'secure boot'
```

**AUDIT :**

- **Fichier :** `Firmware UEFI`
- **Valeur attendue :** `SecureBoot enabled`

```
# Secure Boot s'active dans le firmware UEFI/BIOS
# 1. Redémarrer le serveur et accéder au firmware UEFI
# 2. Activer Secure Boot dans les paramètres de sécurité
# 3. S'assurer que les clés Microsoft sont inscrites
# Sur Ubuntu, installer shim-signed :
sudo apt install shim-signed grub-efi-amd64-signed linux-signed-generic
```

**VALEUR PAR DÉFAUT :**
Non configuré par défaut sur Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.4.1 *Vérifier que AppArmor est installé*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1068 (Exploitation for Privilege Escalation)
**NIST SP 800-53 :** AC-3 (Access Enforcement), AC-6 (Least Privilege)
**ANSSI :** R4 — Activer et configurer le contrôle d'accès obligatoire

**DESCRIPTION :**
AppArmor est le système de contrôle d'accès obligatoire (MAC — Mandatory Access Control) par défaut sur Ubuntu. Il confine les applications dans des profils de sécurité qui restreignent leurs capacités (accès fichiers, réseau, capabilities). AppArmor est essentiel pour limiter les dégâts en cas de compromission d'un service.

```
dpkg -l | grep -E '^ii.*apparmor\b'
apt list --installed 2>/dev/null | grep apparmor
```

**AUDIT :**

- **Fichier / Composant :** `apparmor, apparmor-utils`
- **Valeur attendue :** `Les paquets apparmor et apparmor-utils doivent être installés`

```
sudo apt update && sudo apt install -y apparmor apparmor-utils apparmor-profiles
```

**VALEUR PAR DÉFAUT :**
AppArmor est installé et activé par défaut sur Ubuntu 24.04 LTS, la plupart des profils sont en mode enforce
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.4.2 *Vérifier que AppArmor est activé dans la configuration du chargeur de démarrage*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1068 (Exploitation for Privilege Escalation)
**NIST SP 800-53 :** AC-3 (Access Enforcement), AC-6 (Least Privilege)
**ANSSI :** R4 — Activer et configurer le contrôle d'accès obligatoire

**DESCRIPTION :**
AppArmor doit être activé au niveau du noyau via les paramètres de démarrage GRUB. Les paramètres apparmor=1 et security=apparmor doivent être présents dans la ligne de commande du noyau. Sans ces paramètres, AppArmor ne sera pas actif même s'il est installé.

```
grep -E 'apparmor=1|security=apparmor' /proc/cmdline
```

**AUDIT :**

- **Fichier / Composant :** `/etc/default/grub`
- **Valeur attendue :** `GRUB_CMDLINE_LINUX contient 'apparmor=1 security=apparmor'`

```
# Modifier /etc/default/grub
sudo sed -i 's/^GRUB_CMDLINE_LINUX="/GRUB_CMDLINE_LINUX="apparmor=1 security=apparmor /' /etc/default/grub
sudo update-grub
# Redémarrer le serveur pour appliquer
```

**VALEUR PAR DÉFAUT :**
AppArmor est installé et activé par défaut sur Ubuntu 24.04 LTS, la plupart des profils sont en mode enforce
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.4.3 *Vérifier que tous les profils AppArmor sont en mode enforce ou complain*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1068 (Exploitation for Privilege Escalation)
**NIST SP 800-53 :** AC-3 (Access Enforcement), AC-6 (Least Privilege)
**ANSSI :** R4 — Activer et configurer le contrôle d'accès obligatoire

**DESCRIPTION :**
Les profils AppArmor définissent les permissions de chaque application confinée. En mode 'enforce', les violations sont bloquées et journalisées. En mode 'complain', les violations sont uniquement journalisées. L'objectif est d'avoir tous les profils en mode enforce. Aucun profil ne doit être en mode 'unconfined'.

```
sudo apparmor_status
# Ou
sudo aa-status --json 2>/dev/null | python3 -m json.tool
```

**AUDIT :**

- **Fichier / Composant :** `Profils AppArmor`
- **Valeur attendue :** `0 profils en mode unconfined, maximum de profils en mode enforce`

```
# Passer tous les profils en mode enforce
sudo aa-enforce /etc/apparmor.d/*

# Vérifier le statut
sudo aa-status

# Pour un profil spécifique en mode complain (debug) :
# sudo aa-complain /etc/apparmor.d/<profil>
```

**VALEUR PAR DÉFAUT :**
AppArmor est installé et activé par défaut sur Ubuntu 24.04 LTS, la plupart des profils sont en mode enforce
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.4.4 *Vérifier qu'aucun profil AppArmor n'est déchargé (unconfined)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1068 (Exploitation for Privilege Escalation)
**NIST SP 800-53 :** AC-3 (Access Enforcement), AC-6 (Least Privilege)
**ANSSI :** R4 — Activer et configurer le contrôle d'accès obligatoire

**DESCRIPTION :**
Un processus 'unconfined' n'est soumis à aucune restriction AppArmor. Tous les processus qui disposent d'un profil AppArmor doivent être en mode enforce ou complain. Les processus critiques sans profil doivent faire l'objet d'un profil personnalisé.

```
sudo aa-status | grep -c 'processes are unconfined'
sudo aa-unconfined --paranoid 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `Profils AppArmor`
- **Valeur attendue :** `0 processus unconfined (ou minimum possible)`

```
# Identifier les processus non confinés
sudo aa-unconfined

# Créer un profil pour un processus non confiné
sudo aa-genprof /chemin/vers/programme
# Suivre les instructions interactives

# Activer le nouveau profil
sudo aa-enforce /etc/apparmor.d/<nouveau_profil>
```

**VALEUR PAR DÉFAUT :**
AppArmor est installé et activé par défaut sur Ubuntu 24.04 LTS, la plupart des profils sont en mode enforce

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 1.5.1 *Vérifier que les mises à jour de sécurité sont installées*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1190 (Exploit Public-Facing Application)
**NIST SP 800-53 :** CM-6 (Configuration Settings)
**ANSSI :** R1 — Maintenir le système à jour

**DESCRIPTION :**
Les correctifs de sécurité doivent être appliqués en temps opportun pour protéger le système contre les vulnérabilités connues. Ubuntu 24.04 LTS utilise APT et le dépôt security.ubuntu.com pour les mises à jour de sécurité. Un retard dans l'application des correctifs expose le serveur aux exploits publics.

```
sudo apt update && apt list --upgradable 2>/dev/null | grep -i security
# Nombre de mises à jour de sécurité en attente
sudo unattended-upgrade --dry-run -d 2>/dev/null | grep 'Checking' | wc -l
```

**AUDIT :**

- **Fichier / Composant :** `/etc/apt/sources.list.d/ubuntu.sources`
- **Valeur attendue :** `Aucune mise à jour de sécurité en attente`

```
# Installer toutes les mises à jour de sécurité
sudo apt update
sudo apt upgrade -y

# Installer uniquement les mises à jour de sécurité
sudo unattended-upgrade -d

# Vérifier la date de dernière mise à jour
ls -la /var/log/apt/history.log
```

**VALEUR PAR DÉFAUT :**
Variable selon l'installation Ubuntu 24.04 LTS

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 1.5.2 *Vérifier que les dépôts de paquets sont configurés et authentifiés (GPG)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1195.002 (Supply Chain Compromise: Software Supply Chain)
**NIST SP 800-53 :** CM-6 (Configuration Settings)
**ANSSI :** R1 — Maintenir le système à jour

**DESCRIPTION :**
Les dépôts de paquets doivent être configurés avec des sources officielles et authentifiés par des clés GPG pour garantir l'intégrité et l'authenticité des paquets installés. L'utilisation de dépôts non signés ou de sources tierces non vérifiées constitue un risque de compromission de la chaîne d'approvisionnement.

```
apt-key list 2>/dev/null
grep -r 'deb ' /etc/apt/sources.list /etc/apt/sources.list.d/ 2>/dev/null | grep -v '^#'
apt-config dump | grep -i 'AllowUnauthenticated'
```

**AUDIT :**

- **Fichier / Composant :** `/etc/apt/sources.list, /etc/apt/sources.list.d/`
- **Valeur attendue :** `Tous les dépôts doivent utiliser des clés GPG valides, AllowUnauthenticated=false`

```
# Vérifier les clés GPG
apt-key list

# S'assurer que les dépôts non authentifiés sont refusés
echo 'APT::Get::AllowUnauthenticated "false";' | sudo tee /etc/apt/apt.conf.d/99auth
echo 'Acquire::AllowInsecureRepositories "false";' | sudo tee -a /etc/apt/apt.conf.d/99auth
```

**VALEUR PAR DÉFAUT :**
Variable selon l'installation Ubuntu 24.04 LTS

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 1.5.3 *Vérifier que AIDE (Advanced Intrusion Detection Environment) est installé*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1565.001 (Data Manipulation: Stored Data Manipulation)
**NIST SP 800-53 :** SI-7 (Software, Firmware, and Information Integrity)
**ANSSI :** R67 — Mettre en place un contrôle d'intégrité des fichiers

**DESCRIPTION :**
AIDE est un outil de vérification d'intégrité des fichiers qui compare l'état actuel du système de fichiers avec une base de référence. Il détecte toute modification non autorisée des fichiers système critiques, des binaires et des fichiers de configuration. AIDE est essentiel pour détecter les rootkits et les modifications malveillantes.

```
dpkg -l | grep -E '^ii.*aide\b'
aide --version 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `aide, aide-common`
- **Valeur attendue :** `Le paquet aide doit être installé`

```
# Installer AIDE
sudo apt install -y aide aide-common

# Initialiser la base de données AIDE
sudo aideinit
# Copier la base de données
sudo cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db

# Configurer la vérification quotidienne via cron
echo '0 5 * * * root /usr/bin/aide.wrapper --config /etc/aide/aide.conf --check' | sudo tee /etc/cron.d/aide
```

**VALEUR PAR DÉFAUT :**
Variable selon l'installation Ubuntu 24.04 LTS

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 1.5.4 *Vérifier que la vérification d'intégrité AIDE est planifiée*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1565.001 (Data Manipulation: Stored Data Manipulation)
**NIST SP 800-53 :** SI-7 (Software, Firmware, and Information Integrity)
**ANSSI :** R67 — Mettre en place un contrôle d'intégrité des fichiers

**DESCRIPTION :**
La vérification d'intégrité AIDE doit être exécutée régulièrement (au minimum quotidiennement) pour détecter rapidement les modifications non autorisées. Un cron job ou un timer systemd doit être configuré pour automatiser cette vérification. Les résultats doivent être envoyés à un système de journalisation centralisé.

```
sudo crontab -u root -l 2>/dev/null | grep aide
systemctl is-enabled aidecheck.timer 2>/dev/null
systemctl is-enabled aidecheck.service 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `/etc/cron.d/aide ou aidecheck.timer`
- **Valeur attendue :** `Une entrée cron ou un timer systemd planifiant aide --check`

```
# Option 1 : Cron job
echo '0 5 * * * root /usr/bin/aide.wrapper --config /etc/aide/aide.conf --check' | sudo tee /etc/cron.d/aide

# Option 2 : Timer systemd
sudo systemctl enable aidecheck.timer
sudo systemctl start aidecheck.timer
```

**VALEUR PAR DÉFAUT :**
Variable selon l'installation Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.5.5 *Vérifier que les privilèges de core dump sont restreints*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1003.007 (OS Credential Dumping: Proc Filesystem)
**NIST SP 800-53 :** SI-16 (Memory Protection)
**ANSSI :** R14 — Durcissement du noyau Linux

**DESCRIPTION :**
Les core dumps contiennent une image mémoire du processus au moment du crash, pouvant inclure des informations sensibles telles que des mots de passe, des clés de chiffrement ou des données confidentielles. La restriction des core dumps empêche la fuite d'informations sensibles et réduit la surface d'attaque.

```
grep -E '^\*.*hard.*core' /etc/security/limits.conf /etc/security/limits.d/*.conf 2>/dev/null
sysctl fs.suid_dumpable
grep -r 'Storage=none' /etc/systemd/coredump.conf /etc/systemd/coredump.conf.d/ 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `/etc/security/limits.conf, /etc/sysctl.d/, /etc/systemd/coredump.conf`
- **Valeur attendue :** `'* hard core 0', fs.suid_dumpable=0, Storage=none`

```
# Désactiver les core dumps
echo '* hard core 0' | sudo tee -a /etc/security/limits.conf

# Configurer sysctl
echo 'fs.suid_dumpable = 0' | sudo tee /etc/sysctl.d/50-coredump.conf
sudo sysctl -w fs.suid_dumpable=0

# Configurer systemd
sudo mkdir -p /etc/systemd/coredump.conf.d
cat << EOF | sudo tee /etc/systemd/coredump.conf.d/disable.conf
[Coredump]
Storage=none
ProcessSizeMax=0
EOF
sudo systemctl daemon-reload
```

**VALEUR PAR DÉFAUT :**
Variable selon l'installation Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.5.6 *Vérifier que la randomisation de l'espace d'adressage (ASLR) est activée*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1055 (Process Injection)
**NIST SP 800-53 :** SI-16 (Memory Protection)
**ANSSI :** R14 — Durcissement du noyau Linux

**DESCRIPTION :**
L'ASLR (Address Space Layout Randomization) randomise l'emplacement mémoire des bibliothèques, de la pile, du tas et du code exécutable. Cela rend l'exploitation de vulnérabilités de type buffer overflow significativement plus difficile. La valeur 2 active la randomisation complète.

```
sysctl kernel.randomize_va_space
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/`
- **Valeur attendue :** `kernel.randomize_va_space = 2`

```
echo 'kernel.randomize_va_space = 2' | sudo tee /etc/sysctl.d/50-aslr.conf
sudo sysctl -w kernel.randomize_va_space=2
```

**VALEUR PAR DÉFAUT :**
Variable selon l'installation Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.5.7 *Vérifier que le support de la fonctionnalité ptrace est restreint*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1055.008 (Process Injection: Ptrace System Calls)
**NIST SP 800-53 :** SI-16 (Memory Protection)
**ANSSI :** R14 — Durcissement du noyau Linux

**DESCRIPTION :**
La fonctionnalité ptrace permet à un processus de surveiller et contrôler l'exécution d'un autre processus. Un attaquant peut utiliser ptrace pour injecter du code malveillant dans un processus en cours d'exécution. La restriction de ptrace à 1 (processus enfants uniquement) limite ce vecteur d'attaque.

```
sysctl kernel.yama.ptrace_scope
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/`
- **Valeur attendue :** `kernel.yama.ptrace_scope = 1 (ou plus restrictif : 2 ou 3)`

```
echo 'kernel.yama.ptrace_scope = 1' | sudo tee /etc/sysctl.d/50-ptrace.conf
sudo sysctl -w kernel.yama.ptrace_scope=1
# Valeurs possibles :
# 0 = pas de restriction (dangereux)
# 1 = processus enfants uniquement (recommandé)
# 2 = admin uniquement (CAP_SYS_PTRACE)
# 3 = totalement désactivé
```

**VALEUR PAR DÉFAUT :**
Variable selon l'installation Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.5.8 *Vérifier que la bannière d'avertissement pré-connexion est configurée (/etc/issue)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1082 (System Information Discovery)
**NIST SP 800-53 :** AC-8 (System Use Notification)
**ANSSI :** R6 — Afficher une bannière d'avertissement

**DESCRIPTION :**
Le fichier /etc/issue affiche un message avant l'invite de connexion sur les consoles locales. Ce message doit contenir un avertissement légal indiquant que l'accès est réservé aux utilisateurs autorisés et que toute activité est surveillée. Il ne doit pas contenir d'informations système (\m, \r, \s, \v).

```
cat /etc/issue
```

**AUDIT :**

- **Fichier / Composant :** `/etc/issue`
- **Valeur attendue :** `Message d'avertissement sans informations système (\m, \r, \s, \v)`

```
cat << 'EOF' | sudo tee /etc/issue
************************************************************
*                   AVERTISSEMENT                          *
*  L'accès à ce système est réservé aux utilisateurs       *
*  autorisés. Toute activité est surveillée et enregistrée. *
*  Tout accès non autorisé sera poursuivi conformément     *
*  à la législation en vigueur.                            *
************************************************************
EOF
```

**VALEUR PAR DÉFAUT :**
Variable selon l'installation Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.5.9 *Vérifier que la bannière d'avertissement réseau est configurée (/etc/issue.net)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1082 (System Information Discovery)
**NIST SP 800-53 :** AC-8 (System Use Notification)
**ANSSI :** R6 — Afficher une bannière d'avertissement

**DESCRIPTION :**
Le fichier /etc/issue.net est affiché pour les connexions réseau (SSH, telnet). Comme /etc/issue, il doit contenir un message d'avertissement légal et ne pas divulguer d'informations système. Ce message est utilisé par le paramètre SSH Banner.

```
cat /etc/issue.net
```

**AUDIT :**

- **Fichier / Composant :** `/etc/issue.net`
- **Valeur attendue :** `Message d'avertissement sans informations système`

```
cat << 'EOF' | sudo tee /etc/issue.net
************************************************************
*                   AVERTISSEMENT                          *
*  L'accès à ce système est réservé aux utilisateurs       *
*  autorisés. Toute activité est surveillée et enregistrée. *
*  Tout accès non autorisé sera poursuivi conformément     *
*  à la législation en vigueur.                            *
************************************************************
EOF
```

**VALEUR PAR DÉFAUT :**
Variable selon l'installation Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.5.10 *Vérifier les permissions du fichier /etc/motd*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1082 (System Information Discovery)
**NIST SP 800-53 :** AC-8 (System Use Notification)
**ANSSI :** R6 — Afficher une bannière d'avertissement
**DESCRIPTION :**
Le fichier /etc/motd (Message of the Day) est affiché après une connexion réussie. Il ne doit pas contenir d'informations sensibles sur le système et ses permissions doivent être restrictives pour empêcher les utilisateurs non privilégiés de le modifier.

```
stat -c '%a %U %G' /etc/motd 2>/dev/null || echo 'Fichier non trouvé'
```

**AUDIT :**

- **Fichier / Composant :** `/etc/motd`
- **Valeur attendue :** `Permissions : 644, Propriétaire : root:root`

```
sudo chown root:root /etc/motd 2>/dev/null
sudo chmod 644 /etc/motd 2>/dev/null
# Supprimer les informations système du motd
sudo chmod -x /etc/update-motd.d/* 2>/dev/null
```

**VALEUR PAR DÉFAUT :**
Variable selon l'installation Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.5.11 *Vérifier les permissions du fichier /etc/issue*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1082 (System Information Discovery)
**NIST SP 800-53 :** AC-8 (System Use Notification)
**ANSSI :** R6 — Afficher une bannière d'avertissement
**DESCRIPTION :**
Les permissions du fichier /etc/issue doivent garantir que seul root peut modifier le message d'avertissement pré-connexion. Des permissions trop permissives permettraient à un attaquant de modifier ou supprimer le message d'avertissement légal.

```
stat -c '%a %U %G' /etc/issue
```

**AUDIT :**

- **Fichier / Composant :** `/etc/issue`
- **Valeur attendue :** `Permissions : 644, Propriétaire : root:root`

```
sudo chown root:root /etc/issue
sudo chmod 644 /etc/issue
```

**VALEUR PAR DÉFAUT :**
Variable selon l'installation Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.5.12 *Vérifier les permissions du fichier /etc/issue.net*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1082 (System Information Discovery)
**NIST SP 800-53 :** AC-8 (System Use Notification)
**ANSSI :** R6 — Afficher une bannière d'avertissement
**DESCRIPTION :**
Les permissions du fichier /etc/issue.net doivent garantir que seul root peut modifier le message d'avertissement réseau. Ce fichier est particulièrement important car il est affiché aux connexions distantes.

```
stat -c '%a %U %G' /etc/issue.net
```

**AUDIT :**

- **Fichier / Composant :** `/etc/issue.net`
- **Valeur attendue :** `Permissions : 644, Propriétaire : root:root`

```
sudo chown root:root /etc/issue.net
sudo chmod 644 /etc/issue.net
```

**VALEUR PAR DÉFAUT :**
Variable selon l'installation Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 1.5.13 *Vérifier que le gestionnaire d'affichage GDM est absent ou sécurisé*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1078.001 (Valid Accounts: Default Accounts)
**NIST SP 800-53 :** CM-6 (Configuration Settings)
**ANSSI :** R1 — Maintenir le système à jour

**DESCRIPTION :**
Sur un serveur, aucun environnement graphique ne devrait être installé. Si GDM (GNOME Display Manager) est présent, il doit être sécurisé : bannière configurée, verrouillage automatique, désactivation de la liste des utilisateurs, et désactivation du login automatique. Idéalement, GDM et GNOME doivent être supprimés.

```
dpkg -l | grep -E 'gdm3|gnome-shell|xorg' | head -5
systemctl get-default
```

**AUDIT :**

- **Fichier / Composant :** `Environnement graphique`
- **Valeur attendue :** `Aucun environnement graphique installé, default target = multi-user.target`

```
# Vérifier et supprimer l'environnement graphique si présent
sudo systemctl set-default multi-user.target
sudo apt purge -y gdm3 gnome-shell ubuntu-desktop 2>/dev/null
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Variable selon l'installation Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

## 2.0 — SERVICES RÉSEAU ET DÉMONS

### 2.1.1 *Vérifier que le service xinetd n'est pas installé*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1203 (Exploitation for Client Execution)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
xinetd (Extended Internet Services Daemon) est un super-démon qui écoute les connexions réseau et lance les services configurés à la demande. Il est considéré comme obsolète et insécurisé car il ne supporte pas les mécanismes de sécurité modernes. xinetd ne doit pas être installé sur un serveur Ubuntu 24.04.

```
dpkg -l | grep xinetd
systemctl is-enabled xinetd 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `xinetd`
- **Valeur attendue :** `Le paquet ne doit pas être installé`

```
sudo apt purge -y xinetd
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut sur Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.2 *Vérifier que le service openbsd-inetd n'est pas installé*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1203 (Exploitation for Client Execution)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
openbsd-inetd est un autre super-démon réseau qui, comme xinetd, lance des services à la demande. Il est obsolète et constitue un risque de sécurité. Les services modernes utilisent systemd pour la gestion des sockets et des services.

```
dpkg -l | grep openbsd-inetd
systemctl is-enabled inetd 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `openbsd-inetd`
- **Valeur attendue :** `Le paquet ne doit pas être installé`

```
sudo apt purge -y openbsd-inetd
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut sur Ubuntu 24.04 LTS
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.3 *Vérifier que le service avahi-daemon n'est pas installé ou est désactivé*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1557 (Adversary-in-the-Middle)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
Avahi est une implémentation de mDNS/DNS-SD (Zeroconf) qui permet la découverte automatique de services sur le réseau local. Sur un serveur, cette fonctionnalité est rarement nécessaire et expose le système à des attaques de type man-in-the-middle et d'empoisonnement DNS. Avahi doit être désactivé ou supprimé.

```
dpkg -l | grep avahi-daemon
systemctl is-enabled avahi-daemon 2>/dev/null
ss -tlnp | grep avahi
```

**AUDIT :**

- **Fichier / Composant :** `avahi-daemon`
- **Valeur attendue :** `Le service ne doit pas être actif ni installé`

```
sudo systemctl stop avahi-daemon
sudo systemctl disable avahi-daemon
sudo apt purge -y avahi-daemon
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Peut être installé par défaut selon le profil d'installation

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 2.1.4 *Vérifier que le service CUPS n'est pas installé (sauf si nécessaire)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1210 (Exploitation of Remote Services)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
CUPS (Common UNIX Printing System) est le système d'impression standard. Sur un serveur qui ne gère pas d'impression, CUPS représente une surface d'attaque inutile avec un historique de vulnérabilités critiques (CVE). Le service doit être supprimé si l'impression n'est pas requise.

```
dpkg -l | grep cups
systemctl is-enabled cups 2>/dev/null
ss -tlnp | grep ':631'
```

**AUDIT :**

- **Fichier / Composant :** `cups, cups-daemon`
- **Valeur attendue :** `Le service ne doit pas être installé sur un serveur`

```
sudo systemctl stop cups
sudo systemctl disable cups
sudo apt purge -y cups cups-daemon cups-server-common
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut en mode serveur

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 2.1.5 *Vérifier que le serveur DHCP n'est pas installé (sauf si requis)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1557.002 (DHCP Spoofing)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
Le serveur DHCP (isc-dhcp-server ou kea-dhcp4-server) attribue automatiquement des adresses IP aux clients réseau. Un serveur DHCP non autorisé peut être exploité pour des attaques de type DHCP spoofing, permettant la redirection du trafic réseau. Ce service ne doit être installé que sur les serveurs désignés comme serveurs DHCP.

```
dpkg -l | grep -E 'isc-dhcp-server|kea-dhcp'
systemctl is-enabled isc-dhcp-server 2>/dev/null
systemctl is-enabled kea-dhcp4-server 2>/dev/null
ss -ulnp | grep ':67'
```

**AUDIT :**

- **Fichier / Composant :** `isc-dhcp-server, kea-dhcp4-server`
- **Valeur attendue :** `Non installé sauf si le serveur est un serveur DHCP dédié`

```
sudo systemctl stop isc-dhcp-server 2>/dev/null
sudo systemctl disable isc-dhcp-server 2>/dev/null
sudo apt purge -y isc-dhcp-server 2>/dev/null
sudo apt purge -y kea-dhcp4-server 2>/dev/null
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.6 *Vérifier que le serveur LDAP (slapd) n'est pas installé (sauf si requis)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1210 (Exploitation of Remote Services)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
slapd (OpenLDAP Server Daemon) est le serveur d'annuaire LDAP. Un serveur LDAP expose des informations d'annuaire sensibles et peut être ciblé pour des attaques d'énumération d'utilisateurs ou d'injection LDAP. Ce service ne doit être installé que sur les serveurs d'annuaire dédiés.

```
dpkg -l | grep slapd
systemctl is-enabled slapd 2>/dev/null
ss -tlnp | grep ':389\|:636'
```

**AUDIT :**

- **Fichier / Composant :** `slapd`
- **Valeur attendue :** `Non installé sauf si serveur LDAP dédié`

```
sudo systemctl stop slapd 2>/dev/null
sudo systemctl disable slapd 2>/dev/null
sudo apt purge -y slapd
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.7 *Vérifier que le serveur NFS n'est pas installé (sauf si requis)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1021.002 (Remote Services: SMB/Windows Admin Shares)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
NFS (Network File System) permet le partage de fichiers entre systèmes Unix/Linux. Le protocole NFS, particulièrement les versions anciennes, présente des vulnérabilités connues et peut exposer des données sensibles. Le serveur NFS ne doit être activé que si le partage de fichiers est strictement nécessaire.

```
dpkg -l | grep nfs-kernel-server
systemctl is-enabled nfs-server 2>/dev/null
ss -tlnp | grep ':2049'
```

**AUDIT :**

- **Fichier / Composant :** `nfs-kernel-server`
- **Valeur attendue :** `Non installé sauf si serveur NFS dédié`

```
sudo systemctl stop nfs-server 2>/dev/null
sudo systemctl disable nfs-server 2>/dev/null
sudo apt purge -y nfs-kernel-server
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 2.1.8 *Vérifier que rpcbind n'est pas installé ou est masqué*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1210 (Exploitation of Remote Services)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
rpcbind convertit les numéros de programme RPC en adresses réseau. Il est nécessaire pour NFS et d'autres services RPC. En l'absence de services RPC, rpcbind doit être désactivé car il peut fournir des informations sur les services actifs à un attaquant.

```
dpkg -l | grep rpcbind
systemctl is-enabled rpcbind 2>/dev/null
systemctl is-enabled rpcbind.socket 2>/dev/null
ss -tlnp | grep ':111'
```

**AUDIT :**

- **Fichier / Composant :** `rpcbind`
- **Valeur attendue :** `Non installé ou masqué si NFS n'est pas utilisé`

```
sudo systemctl stop rpcbind rpcbind.socket
sudo systemctl disable rpcbind rpcbind.socket
sudo systemctl mask rpcbind rpcbind.socket
sudo apt purge -y rpcbind 2>/dev/null
```

**VALEUR PAR DÉFAUT :**
Peut être installé comme dépendance

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 2.1.9 *Vérifier que le serveur DNS (bind9) n'est pas installé (sauf si requis)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1584.002 (Compromise Infrastructure: DNS Server)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
BIND9 est le serveur DNS le plus utilisé. Un serveur DNS mal configuré peut être exploité pour des attaques d'amplification DNS, d'empoisonnement de cache ou de fuite d'informations de zone. Ce service ne doit être installé que sur les serveurs DNS dédiés.

```
dpkg -l | grep bind9
systemctl is-enabled named 2>/dev/null
systemctl is-enabled bind9 2>/dev/null
ss -tulnp | grep ':53'
```

**AUDIT :**

- **Fichier / Composant :** `bind9`
- **Valeur attendue :** `Non installé sauf si serveur DNS dédié`

```
sudo systemctl stop bind9 2>/dev/null
sudo systemctl disable bind9 2>/dev/null
sudo apt purge -y bind9
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.10 *Vérifier que le serveur FTP (vsftpd) n'est pas installé*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1071.002 (Application Layer Protocol: File Transfer Protocols)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
FTP (File Transfer Protocol) transmet les identifiants et les données en clair sur le réseau. Ce protocole est intrinsèquement insécurisé et doit être remplacé par SFTP (SSH File Transfer Protocol) ou SCP. Aucun serveur FTP ne doit être installé sur un serveur Ubuntu sécurisé.

```
dpkg -l | grep -E 'vsftpd|proftpd|pure-ftpd'
systemctl is-enabled vsftpd 2>/dev/null
ss -tlnp | grep ':21'
```

**AUDIT :**

- **Fichier / Composant :** `vsftpd, proftpd, pure-ftpd`
- **Valeur attendue :** `Aucun serveur FTP ne doit être installé`

```
sudo systemctl stop vsftpd 2>/dev/null
sudo systemctl disable vsftpd 2>/dev/null
sudo apt purge -y vsftpd proftpd pure-ftpd 2>/dev/null
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.11 *Vérifier que le serveur HTTP (Apache/Nginx) n'est pas installé (sauf si requis)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1190 (Exploit Public-Facing Application)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
Les serveurs web (Apache2, Nginx) sont des cibles fréquentes d'attaques. Un serveur web ne doit être installé que si le rôle du serveur l'exige. Si un serveur web est nécessaire, il doit être durci conformément aux recommandations de la section 10 de cette checklist.

```
dpkg -l | grep -E 'apache2|nginx'
systemctl is-enabled apache2 2>/dev/null
systemctl is-enabled nginx 2>/dev/null
ss -tlnp | grep -E ':80|:443'
```

**AUDIT :**

- **Fichier / Composant :** `apache2, nginx`
- **Valeur attendue :** `Non installé sauf si serveur web dédié`

```
sudo systemctl stop apache2 nginx 2>/dev/null
sudo systemctl disable apache2 nginx 2>/dev/null
sudo apt purge -y apache2 nginx 2>/dev/null
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut en mode serveur
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.12 *Vérifier que le serveur Samba n'est pas installé (sauf si requis)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1021.002 (Remote Services: SMB/Windows Admin Shares)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
Samba fournit le partage de fichiers et d'imprimantes compatibles Windows via le protocole SMB/CIFS. Le protocole SMB a un historique de vulnérabilités critiques (EternalBlue, WannaCry). Samba ne doit être installé que si l'interopérabilité avec des clients Windows est strictement nécessaire.

```
dpkg -l | grep -E 'samba\b'
systemctl is-enabled smbd 2>/dev/null
systemctl is-enabled nmbd 2>/dev/null
ss -tlnp | grep -E ':139|:445'
```

**AUDIT :**

- **Fichier / Composant :** `samba`
- **Valeur attendue :** `Non installé sauf si partage SMB nécessaire`

```
sudo systemctl stop smbd nmbd 2>/dev/null
sudo systemctl disable smbd nmbd 2>/dev/null
sudo apt purge -y samba samba-common
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.13 *Vérifier que le proxy Squid n'est pas installé (sauf si requis)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1090 (Proxy)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
Squid est un serveur proxy cache web. Un proxy mal configuré peut être utilisé comme relais pour des attaques ou pour contourner les contrôles de sécurité réseau. Ce service ne doit être installé que sur les serveurs proxy dédiés et correctement configuré.

```
dpkg -l | grep squid
systemctl is-enabled squid 2>/dev/null
ss -tlnp | grep ':3128'
```

**AUDIT :**

- **Fichier / Composant :** `squid`
- **Valeur attendue :** `Non installé sauf si serveur proxy dédié`

```
sudo systemctl stop squid 2>/dev/null
sudo systemctl disable squid 2>/dev/null
sudo apt purge -y squid
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 2.1.14 *Vérifier que le serveur SNMP n'est pas installé (sauf si requis)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1602.001 (Data from Configuration Repository: SNMP)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
SNMP (Simple Network Management Protocol) est utilisé pour la supervision réseau. Les versions SNMPv1 et SNMPv2c transmettent les community strings en clair. Si SNMP est nécessaire, seul SNMPv3 avec authentification et chiffrement doit être utilisé.

```
dpkg -l | grep snmpd
systemctl is-enabled snmpd 2>/dev/null
ss -ulnp | grep ':161'
```

**AUDIT :**

- **Fichier / Composant :** `snmpd`
- **Valeur attendue :** `Non installé ou uniquement SNMPv3 configuré`

```
sudo systemctl stop snmpd 2>/dev/null
sudo systemctl disable snmpd 2>/dev/null
sudo apt purge -y snmpd
sudo apt autoremove -y
# Si SNMPv3 requis, configurer avec authentification et chiffrement
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 2.1.15 *Vérifier que le serveur de messagerie est en mode local uniquement*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1071.003 (Application Layer Protocol: Mail Protocols)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
Le serveur de messagerie (MTA — Mail Transfer Agent) tel que Postfix ne doit écouter que sur l'interface locale (127.0.0.1) si le serveur n'est pas un relais de messagerie. Un MTA écoutant sur toutes les interfaces peut être exploité comme relais de spam ou pour des attaques par injection de courrier.

```
ss -tlnp | grep ':25'
postconf inet_interfaces 2>/dev/null
cat /etc/postfix/main.cf 2>/dev/null | grep inet_interfaces
```

**AUDIT :**

- **Fichier / Composant :** `/etc/postfix/main.cf`
- **Valeur attendue :** `inet_interfaces = loopback-only ou inet_interfaces = 127.0.0.1`

```
# Configurer Postfix en mode local uniquement
sudo postconf -e 'inet_interfaces = loopback-only'
sudo systemctl restart postfix

# Ou supprimer Postfix si non nécessaire
# sudo apt purge -y postfix
```

**VALEUR PAR DÉFAUT :**
Postfix peut être installé par défaut, inet_interfaces = all

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 2.1.16 *Vérifier que rsync n'est pas installé ou est correctement configuré*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1105 (Ingress Tool Transfer)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
rsync est un outil de synchronisation de fichiers qui peut fonctionner en mode démon. Le démon rsync écoute sur le port 873 et peut exposer des fichiers sensibles si mal configuré. Le service rsync doit être désactivé s'il n'est pas nécessaire.

```
dpkg -l | grep rsync
systemctl is-enabled rsync 2>/dev/null
ss -tlnp | grep ':873'
```

**AUDIT :**

- **Fichier / Composant :** `rsync`
- **Valeur attendue :** `Le service rsync (démon) ne doit pas être actif`

```
sudo systemctl stop rsync 2>/dev/null
sudo systemctl disable rsync 2>/dev/null
sudo systemctl mask rsync
```

**VALEUR PAR DÉFAUT :**
rsync est installé mais le démon n'est pas activé par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 2.1.17 *Vérifier que le service NIS (ypserv) n'est pas installé*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1557 (Adversary-in-the-Middle)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
NIS (Network Information Service, anciennement Yellow Pages) est un protocole d'authentification réseau obsolète et intrinsèquement insécurisé. NIS transmet les informations d'authentification en clair et est vulnérable à de nombreuses attaques. Il doit être remplacé par LDAP/Kerberos.

```
dpkg -l | grep -E 'nis\b|ypserv'
systemctl is-enabled ypserv 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `nis, ypserv`
- **Valeur attendue :** `Non installé`

```
sudo apt purge -y nis ypserv 2>/dev/null
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 2.1.18 *Vérifier que le client rsh n'est pas installé*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1021.004 (Remote Services: SSH)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
Les clients rsh (remote shell), rlogin et rcp sont des protocoles d'accès distant obsolètes qui transmettent tout le trafic (y compris les mots de passe) en clair. Ces outils doivent être remplacés par SSH, SCP et SFTP.

```
dpkg -l | grep -E 'rsh-client|rsh-redone-client'
which rsh rlogin rcp 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `rsh-client`
- **Valeur attendue :** `Non installé`

```
sudo apt purge -y rsh-client rsh-redone-client 2>/dev/null
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.19 *Vérifier que le client talk n'est pas installé*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1071 (Application Layer Protocol)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
talk est un protocole de communication en temps réel obsolète. Le client et le serveur talk transmettent les données en clair et sont rarement utilisés sur les serveurs modernes. Ils doivent être supprimés pour réduire la surface d'attaque.

```
dpkg -l | grep talk
which talk 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `talk, talkd`
- **Valeur attendue :** `Non installé`

```
sudo apt purge -y talk talkd 2>/dev/null
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.20 *Vérifier que le client telnet n'est pas installé*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1021.004 (Remote Services: SSH)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
Le client telnet transmet toutes les données, y compris les identifiants, en texte clair sur le réseau. Il doit être remplacé par SSH pour toute connexion distante. La présence du client telnet sur un serveur peut indiquer des pratiques d'administration insécurisées.

```
dpkg -l | grep telnet
which telnet 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `telnet`
- **Valeur attendue :** `Non installé`

```
sudo apt purge -y telnet
sudo apt autoremove -y
# Utiliser SSH à la place
```

**VALEUR PAR DÉFAUT :**
Peut être installé par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.21 *Vérifier que le client LDAP n'est pas installé (sauf si requis)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1018 (Remote System Discovery)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
Le client LDAP (ldap-utils) peut être utilisé pour interroger des annuaires LDAP. Sur un serveur qui n'a pas besoin d'intégration LDAP, le client doit être supprimé pour empêcher les attaques d'énumération et réduire la surface d'attaque.

```
dpkg -l | grep ldap-utils
```

**AUDIT :**

- **Fichier / Composant :** `ldap-utils`
- **Valeur attendue :** `Non installé sauf si intégration LDAP requise`

```
sudo apt purge -y ldap-utils 2>/dev/null
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.22 *Vérifier que la synchronisation horaire (chrony ou systemd-timesyncd) est configurée*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1070.006 (Indicator Removal: Timestomp)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
La synchronisation horaire est critique pour la corrélation des journaux de sécurité, la validité des certificats TLS et l'authentification Kerberos. Ubuntu 24.04 utilise systemd-timesyncd par défaut, mais chrony est recommandé pour les serveurs car il offre une meilleure précision et plus d'options de configuration.

```
systemctl is-enabled systemd-timesyncd chrony 2>/dev/null
timedatectl status
chronyc tracking 2>/dev/null || timedatectl show-timesync 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `/etc/chrony/chrony.conf ou /etc/systemd/timesyncd.conf`
- **Valeur attendue :** `Service actif et synchronisé avec des serveurs NTP fiables`

```
# Option recommandée : chrony
sudo apt install -y chrony
sudo systemctl enable chrony
sudo systemctl start chrony

# Configurer les serveurs NTP dans /etc/chrony/chrony.conf :
# pool ntp.ubuntu.com iburst maxsources 4
# pool 0.ubuntu.pool.ntp.org iburst maxsources 1
# pool 1.ubuntu.pool.ntp.org iburst maxsources 1

sudo systemctl restart chrony
chronyc tracking
```

**VALEUR PAR DÉFAUT :**
systemd-timesyncd est activé par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.23 *Vérifier que chrony/NTP est configuré avec des sources autorisées uniquement*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1557 (Adversary-in-the-Middle)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
Les sources NTP doivent être des serveurs de confiance pour empêcher les attaques de type NTP amplification ou de manipulation horaire. L'utilisation de pools NTP publics non vérifiés peut exposer le système à des attaques temporelles qui affectent la validité des certificats et la corrélation des journaux.

```
grep -E '^(server|pool)' /etc/chrony/chrony.conf 2>/dev/null
grep -E '^NTP=' /etc/systemd/timesyncd.conf 2>/dev/null
chronyc sources 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `/etc/chrony/chrony.conf`
- **Valeur attendue :** `Serveurs NTP de confiance configurés (ex: ntp.ubuntu.com, pool.ntp.org)`

```
# Éditer /etc/chrony/chrony.conf
sudo cat << EOF > /etc/chrony/chrony.conf
pool ntp.ubuntu.com iburst maxsources 4
pool 0.ubuntu.pool.ntp.org iburst maxsources 2
keyfile /etc/chrony/chrony.keys
driftfile /var/lib/chrony/chrony.drift
logdir /var/log/chrony
maxupdateskew 100.0
rtcsync
makestep 1 3
EOF
sudo systemctl restart chrony
```

**VALEUR PAR DÉFAUT :**
Pools NTP Ubuntu configurés par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.24 *Vérifier que chrony s'exécute en tant qu'utilisateur non privilégié*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1068 (Exploitation for Privilege Escalation)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
Le démon chrony doit s'exécuter sous un compte utilisateur non privilégié dédié (_chrony) pour limiter l'impact d'une éventuelle compromission du service. Cela applique le principe du moindre privilège à la synchronisation horaire.

```
ps -ef | grep chronyd | grep -v grep
grep '^user' /etc/chrony/chrony.conf 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `/etc/chrony/chrony.conf`
- **Valeur attendue :** `chronyd s'exécute en tant que _chrony`

```
# Vérifier que chrony s'exécute en tant que _chrony
# Le fichier de service systemd devrait contenir User=_chrony
systemctl show chronyd | grep -i user
```

**VALEUR PAR DÉFAUT :**
chrony s'exécute en tant que _chrony par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.25 *Vérifier que le client NFS n'est pas installé (sauf si requis)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1021.002 (Remote Services: SMB/Windows Admin Shares)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
Le client NFS (nfs-common) permet de monter des partages NFS distants. Si le serveur n'a pas besoin d'accéder à des partages NFS, le client doit être supprimé pour réduire la surface d'attaque et empêcher le montage de partages malveillants.

```
dpkg -l | grep nfs-common
```

**AUDIT :**

- **Fichier / Composant :** `nfs-common`
- **Valeur attendue :** `Non installé sauf si montage NFS requis`

```
sudo apt purge -y nfs-common
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Peut être installé comme dépendance
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.26 *Vérifier que le client Samba (smbclient/cifs-utils) n'est pas installé (sauf si requis)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1021.002 (Remote Services: SMB/Windows Admin Shares)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
Les utilitaires client Samba (smbclient, cifs-utils) permettent d'accéder aux partages SMB/CIFS. Sur un serveur qui n'a pas besoin d'accéder aux partages Windows, ces paquets doivent être supprimés pour réduire la surface d'attaque.

```
dpkg -l | grep -E 'smbclient|cifs-utils'
```

**AUDIT :**

- **Fichier / Composant :** `smbclient, cifs-utils`
- **Valeur attendue :** `Non installé sauf si accès SMB requis`

```
sudo apt purge -y smbclient cifs-utils 2>/dev/null
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.27 *Vérifier que le service dnsmasq n'est pas installé (sauf si requis)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1584.002 (Compromise Infrastructure: DNS Server)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
dnsmasq est un serveur DNS/DHCP léger souvent utilisé pour le cache DNS et le service DHCP sur les petits réseaux. Sur un serveur de production, dnsmasq peut entrer en conflit avec systemd-resolved et présente des risques de sécurité si mal configuré.

```
dpkg -l | grep dnsmasq
systemctl is-enabled dnsmasq 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `dnsmasq`
- **Valeur attendue :** `Non installé sauf si explicitement requis`

```
sudo systemctl stop dnsmasq 2>/dev/null
sudo systemctl disable dnsmasq 2>/dev/null
sudo apt purge -y dnsmasq dnsmasq-base 2>/dev/null
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut sur le serveur
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 2.1.28 *Vérifier que le service de base de données (MySQL/PostgreSQL/MariaDB) est sécurisé ou absent*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1190 (Exploit Public-Facing Application)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
Les serveurs de base de données sont des cibles de haute valeur pour les attaquants. Si un SGBD est installé, il doit être correctement durci (suppression des bases de test, désactivation des accès distants non nécessaires, utilisation de mots de passe forts). S'il n'est pas nécessaire, il doit être supprimé.

```
dpkg -l | grep -E 'mysql-server|mariadb-server|postgresql'
systemctl is-enabled mysql 2>/dev/null
systemctl is-enabled mariadb 2>/dev/null
systemctl is-enabled postgresql 2>/dev/null
ss -tlnp | grep -E ':3306|:5432'
```

**AUDIT :**

- **Fichier / Composant :** `mysql-server, mariadb-server, postgresql`
- **Valeur attendue :** `Non installé ou correctement durci`

```
# Si MySQL est installé et requis :
sudo mysql_secure_installation

# Si non requis :
sudo apt purge -y mysql-server mariadb-server postgresql 2>/dev/null
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 2.1.29 *Vérifier qu'aucun service en écoute non autorisé n'est présent*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1046 (Network Service Discovery)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
Chaque port en écoute sur le serveur représente un point d'entrée potentiel pour un attaquant. Un audit régulier des services en écoute permet de détecter les services non autorisés ou les portes dérobées. Seuls les services strictement nécessaires doivent écouter sur des interfaces réseau.

```
ss -tlnp
ss -ulnp
# Liste complète des ports en écoute
ss -tulnp | grep LISTEN
# Comparer avec la liste des services autorisés
```

**AUDIT :**

- **Fichier / Composant :** `Tous les ports en écoute`
- **Valeur attendue :** `Seuls les ports autorisés doivent être en écoute`

```
# Identifier et arrêter les services non autorisés
# Pour chaque service non autorisé :
sudo systemctl stop <service_name>
sudo systemctl disable <service_name>
sudo systemctl mask <service_name>

# Vérifier après correction
ss -tulnp | grep LISTEN
```

**VALEUR PAR DÉFAUT :**
Variable selon les paquets installés

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 2.1.30 *Vérifier que le service snapd est désactivé (si les snaps ne sont pas utilisés)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1072 (Software Deployment Tools)
**NIST SP 800-53 :** CM-7 (Least Functionality)
**ANSSI :** R17 — Réduire la surface réseau

**DESCRIPTION :**
snapd est le service qui gère les paquets Snap sur Ubuntu. Si les paquets Snap ne sont pas utilisés, snapd doit être désactivé pour réduire la surface d'attaque et la consommation de ressources. Note : la désactivation de snapd empêchera l'installation de paquets Snap.

```
systemctl is-enabled snapd 2>/dev/null
systemctl is-active snapd 2>/dev/null
snap list 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `snapd`
- **Valeur attendue :** `Désactivé si les snaps ne sont pas utilisés`

```
# Supprimer tous les snaps installés
for snap in $(snap list 2>/dev/null | awk 'NR>1{print $1}'); do
  sudo snap remove --purge "$snap"
done

# Désactiver et supprimer snapd
sudo systemctl stop snapd snapd.socket
sudo systemctl disable snapd snapd.socket
sudo systemctl mask snapd
sudo apt purge -y snapd
sudo rm -rf /snap /var/snap /var/lib/snapd /var/cache/snapd
```

**VALEUR PAR DÉFAUT :**
snapd est installé et activé par défaut sur Ubuntu 24.04
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

## 3.0 — CONFIGURATION RÉSEAU ET PARE-FEU

### 3.1.1 *Désactiver le transfert de paquets IPv4 (IP forwarding)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1557 (Adversary-in-the-Middle)
**NIST SP 800-53 :** SC-7 (Boundary Protection)
**ANSSI :** R12 — Durcissement de la pile réseau

**DESCRIPTION :**
Le transfert de paquets IP (IP forwarding) permet au serveur de router les paquets entre interfaces réseau. Sauf si le serveur est configuré comme routeur ou passerelle, cette fonctionnalité doit être désactivée pour empêcher le détournement de trafic réseau et les attaques man-in-the-middle.

```
sysctl net.ipv4.ip_forward
grep -r 'net.ipv4.ip_forward' /etc/sysctl.conf /etc/sysctl.d/ 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/60-network-hardening.conf`
- **Valeur attendue :** `net.ipv4.ip_forward = 0`

```
echo 'net.ipv4.ip_forward = 0' | sudo tee /etc/sysctl.d/60-network-hardening.conf
sudo sysctl -w net.ipv4.ip_forward=0
sudo sysctl -w net.ipv4.route.flush=1
```

**VALEUR PAR DÉFAUT :**
net.ipv4.ip_forward = 0 (par défaut)
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.1.2 *Désactiver le transfert de paquets IPv6*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1557 (Adversary-in-the-Middle)
**NIST SP 800-53 :** SC-7 (Boundary Protection)
**ANSSI :** R12 — Durcissement de la pile réseau

**DESCRIPTION :**
Comme pour IPv4, le transfert IPv6 doit être désactivé sauf si le serveur est un routeur IPv6. Le transfert IPv6 actif peut être exploité pour des attaques de routage malveillant dans un environnement dual-stack.

```
sysctl net.ipv6.conf.all.forwarding
grep -r 'net.ipv6.conf.all.forwarding' /etc/sysctl.conf /etc/sysctl.d/ 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/60-network-hardening.conf`
- **Valeur attendue :** `net.ipv6.conf.all.forwarding = 0`

```
echo 'net.ipv6.conf.all.forwarding = 0' | sudo tee -a /etc/sysctl.d/60-network-hardening.conf
sudo sysctl -w net.ipv6.conf.all.forwarding=0
sudo sysctl -w net.ipv6.route.flush=1
```

**VALEUR PAR DÉFAUT :**
net.ipv6.conf.all.forwarding = 0 (par défaut)
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.1.3 *Vérifier que les redirections ICMP ne sont pas acceptées (IPv4)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1557.001 (LLMNR/NBT-NS Poisoning and SMB Relay)
**NIST SP 800-53 :** SC-7 (Boundary Protection)
**ANSSI :** R12 — Durcissement de la pile réseau

**DESCRIPTION :**
Les redirections ICMP permettent à un routeur d'informer un hôte d'une meilleure route. Un attaquant peut envoyer de fausses redirections ICMP pour détourner le trafic réseau. La désactivation des redirections ICMP empêche ces attaques de routage malveillant.

```
sysctl net.ipv4.conf.all.accept_redirects
sysctl net.ipv4.conf.default.accept_redirects
grep -r 'accept_redirects' /etc/sysctl.conf /etc/sysctl.d/ 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/60-network-hardening.conf`
- **Valeur attendue :** `net.ipv4.conf.all.accept_redirects = 0, net.ipv4.conf.default.accept_redirects = 0`

```
cat << EOF | sudo tee -a /etc/sysctl.d/60-network-hardening.conf
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
EOF
sudo sysctl -w net.ipv4.conf.all.accept_redirects=0
sudo sysctl -w net.ipv4.conf.default.accept_redirects=0
```

**VALEUR PAR DÉFAUT :**
Activé par défaut (valeur 1)
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.1.4 *Vérifier que les redirections ICMP ne sont pas envoyées*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1557 (Adversary-in-the-Middle)
**NIST SP 800-53 :** SC-7 (Boundary Protection)
**ANSSI :** R12 — Durcissement de la pile réseau

**DESCRIPTION :**
Un serveur ne doit pas envoyer de redirections ICMP car cela peut être exploité pour manipuler les tables de routage des hôtes du réseau. Seuls les routeurs légitimes devraient envoyer des redirections ICMP.

```
sysctl net.ipv4.conf.all.send_redirects
sysctl net.ipv4.conf.default.send_redirects
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/60-network-hardening.conf`
- **Valeur attendue :** `net.ipv4.conf.all.send_redirects = 0, net.ipv4.conf.default.send_redirects = 0`

```
cat << EOF | sudo tee -a /etc/sysctl.d/60-network-hardening.conf
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
EOF
sudo sysctl -w net.ipv4.conf.all.send_redirects=0
sudo sysctl -w net.ipv4.conf.default.send_redirects=0
```

**VALEUR PAR DÉFAUT :**
Activé par défaut (valeur 1)
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.1.5 *Vérifier que le source routing est désactivé (IPv4)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1557 (Adversary-in-the-Middle)
**NIST SP 800-53 :** SC-7 (Boundary Protection)
**ANSSI :** R12 — Durcissement de la pile réseau

**DESCRIPTION :**
Le source routing permet à un paquet de spécifier sa propre route à travers le réseau, contournant les tables de routage normales. Un attaquant peut utiliser le source routing pour diriger le trafic à travers un hôte malveillant. Cette fonctionnalité doit être désactivée.

```
sysctl net.ipv4.conf.all.accept_source_route
sysctl net.ipv4.conf.default.accept_source_route
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/60-network-hardening.conf`
- **Valeur attendue :** `net.ipv4.conf.all.accept_source_route = 0`

```
cat << EOF | sudo tee -a /etc/sysctl.d/60-network-hardening.conf
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
EOF
sudo sysctl -w net.ipv4.conf.all.accept_source_route=0
sudo sysctl -w net.ipv4.conf.default.accept_source_route=0
```

**VALEUR PAR DÉFAUT :**
Désactivé par défaut (valeur 0) sur Ubuntu 24.04

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 3.1.6 *Vérifier que le source routing est désactivé (IPv6)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1557 (Adversary-in-the-Middle)
**NIST SP 800-53 :** SC-7 (Boundary Protection)
**ANSSI :** R12 — Durcissement de la pile réseau

**DESCRIPTION :**
Comme pour IPv4, le source routing IPv6 permet aux paquets de spécifier leur propre route. Cette fonctionnalité doit être désactivée pour les mêmes raisons de sécurité que pour IPv4.

```
sysctl net.ipv6.conf.all.accept_source_route
sysctl net.ipv6.conf.default.accept_source_route
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/60-network-hardening.conf`
- **Valeur attendue :** `net.ipv6.conf.all.accept_source_route = 0`

```
cat << EOF | sudo tee -a /etc/sysctl.d/60-network-hardening.conf
net.ipv6.conf.all.accept_source_route = 0
net.ipv6.conf.default.accept_source_route = 0
EOF
sudo sysctl -w net.ipv6.conf.all.accept_source_route=0
sudo sysctl -w net.ipv6.conf.default.accept_source_route=0
```

**VALEUR PAR DÉFAUT :**
Désactivé par défaut (valeur 0)

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 3.1.7 *Activer la validation de la source par chemin inverse (Reverse Path Filtering)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1557 (Adversary-in-the-Middle)
**NIST SP 800-53 :** SC-7 (Boundary Protection)
**ANSSI :** R12 — Durcissement de la pile réseau
**DESCRIPTION :**
Le Reverse Path Filtering (rp_filter) vérifie que l'adresse source de chaque paquet entrant est accessible via l'interface sur laquelle il a été reçu. Cela empêche les attaques par usurpation d'adresse IP (IP spoofing). La valeur 1 (strict) est recommandée.

```
sysctl net.ipv4.conf.all.rp_filter
sysctl net.ipv4.conf.default.rp_filter
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/60-network-hardening.conf`
- **Valeur attendue :** `net.ipv4.conf.all.rp_filter = 1, net.ipv4.conf.default.rp_filter = 1`

```
cat << EOF | sudo tee -a /etc/sysctl.d/60-network-hardening.conf
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
EOF
sudo sysctl -w net.ipv4.conf.all.rp_filter=1
sudo sysctl -w net.ipv4.conf.default.rp_filter=1
```

**VALEUR PAR DÉFAUT :**
rp_filter = 2 (loose) par défaut sur Ubuntu 24.04
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.1.8 *Activer la journalisation des paquets suspects (martians)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1040 (Network Sniffing)
**NIST SP 800-53 :** SC-7 (Boundary Protection)
**ANSSI :** R12 — Durcissement de la pile réseau
**DESCRIPTION :**
La journalisation des paquets martiens (paquets avec des adresses source impossibles) aide à détecter les tentatives d'usurpation d'adresse IP et les anomalies réseau. Ces journaux sont essentiels pour l'analyse forensique et la détection d'intrusion.

```
sysctl net.ipv4.conf.all.log_martians
sysctl net.ipv4.conf.default.log_martians
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/60-network-hardening.conf`
- **Valeur attendue :** `net.ipv4.conf.all.log_martians = 1`

```
cat << EOF | sudo tee -a /etc/sysctl.d/60-network-hardening.conf
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
EOF
sudo sysctl -w net.ipv4.conf.all.log_martians=1
sudo sysctl -w net.ipv4.conf.default.log_martians=1
```

**VALEUR PAR DÉFAUT :**
Désactivé par défaut (valeur 0)
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.1.9 *Activer les SYN cookies TCP*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1498.001 (Network Denial of Service: Direct Network Flood)
**NIST SP 800-53 :** SC-7 (Boundary Protection)
**ANSSI :** R12 — Durcissement de la pile réseau
**DESCRIPTION :**
Les SYN cookies permettent au noyau de gérer les connexions TCP semi-ouvertes sans allouer de ressources, protégeant contre les attaques SYN flood. Lorsque la file d'attente SYN est pleine, le serveur utilise des cookies cryptographiques au lieu de conserver l'état de chaque connexion en attente.

```
sysctl net.ipv4.tcp_syncookies
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/60-network-hardening.conf`
- **Valeur attendue :** `net.ipv4.tcp_syncookies = 1`

```
echo 'net.ipv4.tcp_syncookies = 1' | sudo tee -a /etc/sysctl.d/60-network-hardening.conf
sudo sysctl -w net.ipv4.tcp_syncookies=1
```

**VALEUR PAR DÉFAUT :**
Activé par défaut (valeur 1) sur Ubuntu 24.04
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.1.10 *Désactiver les réponses ICMP Broadcast (Smurf protection)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1498 (Network Denial of Service)
**NIST SP 800-53 :** SC-7 (Boundary Protection)
**ANSSI :** R12 — Durcissement de la pile réseau

**DESCRIPTION :**
La réponse aux requêtes ICMP echo envoyées à l'adresse broadcast peut être exploitée dans les attaques Smurf, où un attaquant envoie des paquets ICMP avec une adresse source usurpée à l'adresse broadcast, provoquant un déni de service sur la victime.

```
sysctl net.ipv4.icmp_echo_ignore_broadcasts
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/60-network-hardening.conf`
- **Valeur attendue :** `net.ipv4.icmp_echo_ignore_broadcasts = 1`

```
echo 'net.ipv4.icmp_echo_ignore_broadcasts = 1' | sudo tee -a /etc/sysctl.d/60-network-hardening.conf
sudo sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
```

**VALEUR PAR DÉFAUT :**
Activé par défaut (valeur 1)
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.1.11 *Ignorer les messages ICMP bogus error responses*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1498 (Network Denial of Service)
**NIST SP 800-53 :** SC-7 (Boundary Protection)
**ANSSI :** R12 — Durcissement de la pile réseau

**DESCRIPTION :**
Les réponses ICMP erronées (bogus) peuvent être utilisées pour des attaques de déni de service ou pour perturber les communications réseau. L'activation de icmp_ignore_bogus_error_responses empêche la journalisation excessive de ces messages erronés.

```
sysctl net.ipv4.icmp_ignore_bogus_error_responses
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/60-network-hardening.conf`
- **Valeur attendue :** `net.ipv4.icmp_ignore_bogus_error_responses = 1`

```
echo 'net.ipv4.icmp_ignore_bogus_error_responses = 1' | sudo tee -a /etc/sysctl.d/60-network-hardening.conf
sudo sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1
```

**VALEUR PAR DÉFAUT :**
Activé par défaut (valeur 1)
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.1.12 *Désactiver les redirections ICMP sécurisées*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1557 (Adversary-in-the-Middle)
**NIST SP 800-53 :** SC-7 (Boundary Protection)
**ANSSI :** R12 — Durcissement de la pile réseau

**DESCRIPTION :**
Les redirections ICMP sécurisées (secure_redirects) sont des redirections provenant de passerelles par défaut. Même si elles sont considérées plus sûres que les redirections standard, elles peuvent toujours être exploitées pour manipuler les tables de routage.

```
sysctl net.ipv4.conf.all.secure_redirects
sysctl net.ipv4.conf.default.secure_redirects
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/60-network-hardening.conf`
- **Valeur attendue :** `net.ipv4.conf.all.secure_redirects = 0`

```
cat << EOF | sudo tee -a /etc/sysctl.d/60-network-hardening.conf
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
EOF
sudo sysctl -w net.ipv4.conf.all.secure_redirects=0
sudo sysctl -w net.ipv4.conf.default.secure_redirects=0
```

**VALEUR PAR DÉFAUT :**
Activé par défaut (valeur 1)
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.1.13 *Désactiver les redirections ICMP IPv6*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1557 (Adversary-in-the-Middle)
**NIST SP 800-53 :** SC-7 (Boundary Protection)
**ANSSI :** R12 — Durcissement de la pile réseau

**DESCRIPTION :**
Les redirections ICMP IPv6 peuvent être exploitées pour détourner le trafic dans un réseau IPv6. La désactivation des redirections IPv6 est nécessaire pour compléter la protection du routage réseau.

```
sysctl net.ipv6.conf.all.accept_redirects
sysctl net.ipv6.conf.default.accept_redirects
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/60-network-hardening.conf`
- **Valeur attendue :** `net.ipv6.conf.all.accept_redirects = 0`

```
cat << EOF | sudo tee -a /etc/sysctl.d/60-network-hardening.conf
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0
EOF
sudo sysctl -w net.ipv6.conf.all.accept_redirects=0
sudo sysctl -w net.ipv6.conf.default.accept_redirects=0
```

**VALEUR PAR DÉFAUT :**
Activé par défaut (valeur 1)
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.1.14 *Désactiver les annonces de routeur IPv6*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1557 (Adversary-in-the-Middle)
**NIST SP 800-53 :** SC-7 (Boundary Protection)
**ANSSI :** R12 — Durcissement de la pile réseau

**DESCRIPTION :**
L'acceptation des annonces de routeur IPv6 (Router Advertisements) peut permettre à un attaquant de se faire passer pour un routeur IPv6 légitime (attaque de type rogue router advertisement). Sur un serveur avec une configuration réseau statique, cette fonctionnalité doit être désactivée.

```
sysctl net.ipv6.conf.all.accept_ra
sysctl net.ipv6.conf.default.accept_ra
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/60-network-hardening.conf`
- **Valeur attendue :** `net.ipv6.conf.all.accept_ra = 0`

```
cat << EOF | sudo tee -a /etc/sysctl.d/60-network-hardening.conf
net.ipv6.conf.all.accept_ra = 0
net.ipv6.conf.default.accept_ra = 0
EOF
sudo sysctl -w net.ipv6.conf.all.accept_ra=0
sudo sysctl -w net.ipv6.conf.default.accept_ra=0
```

**VALEUR PAR DÉFAUT :**
Activé par défaut (valeur 1) — peut être nécessaire pour SLAAC
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.1.15 *Désactiver IPv6 si non utilisé*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1095 (Non-Application Layer Protocol)
**NIST SP 800-53 :** SC-7 (Boundary Protection)
**ANSSI :** R12 — Durcissement de la pile réseau

**DESCRIPTION :**
Si IPv6 n'est pas utilisé dans l'infrastructure réseau, il doit être complètement désactivé pour éliminer un vecteur d'attaque potentiel. IPv6 peut être exploité pour contourner les règles de pare-feu IPv4 si les règles IPv6 ne sont pas correctement configurées.

```
ip -6 addr show
sysctl net.ipv6.conf.all.disable_ipv6
grep -r 'ipv6.disable' /proc/cmdline
```

**AUDIT :**

- **Fichier / Composant :** `/etc/sysctl.d/60-network-hardening.conf ou /etc/default/grub`
- **Valeur attendue :** `net.ipv6.conf.all.disable_ipv6 = 1 (si IPv6 non utilisé)`

```
# Option 1 : Via sysctl
cat << EOF | sudo tee /etc/sysctl.d/60-disable-ipv6.conf
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
EOF
sudo sysctl --system

# Option 2 : Via GRUB (plus fiable)
# Ajouter ipv6.disable=1 dans GRUB_CMDLINE_LINUX de /etc/default/grub
sudo update-grub
```

**VALEUR PAR DÉFAUT :**
IPv6 est activé par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.2.1 *Vérifier que ufw (Uncomplicated Firewall) est installé*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1046 (Network Service Discovery)
**NIST SP 800-53 :** SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)
**ANSSI :** R12 — Configurer un pare-feu local

**DESCRIPTION :**
ufw est l'interface de gestion simplifiée du pare-feu iptables/nftables sur Ubuntu. Il fournit une couche d'abstraction qui facilite la création et la gestion des règles de filtrage. ufw doit être installé comme couche de gestion du pare-feu.

```
dpkg -l | grep ufw
ufw version 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `ufw`
- **Valeur attendue :** `Le paquet ufw doit être installé`

```
sudo apt install -y ufw
```

**VALEUR PAR DÉFAUT :**
ufw est installé par défaut sur Ubuntu 24.04

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.2.2 *Vérifier que le service iptables-persistent n'est pas installé avec ufw*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1562.004 (Impair Defenses: Disable or Modify System Firewall)
**NIST SP 800-53 :** SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)
**ANSSI :** R12 — Configurer un pare-feu local

**DESCRIPTION :**
iptables-persistent et ufw ne doivent pas être utilisés simultanément car ils peuvent entrer en conflit. Si ufw est choisi comme solution de pare-feu, iptables-persistent doit être supprimé pour éviter les conflits de règles.

```
dpkg -l | grep iptables-persistent
```

**AUDIT :**

- **Fichier / Composant :** `iptables-persistent`
- **Valeur attendue :** `Non installé si ufw est utilisé`

```
sudo apt purge -y iptables-persistent netfilter-persistent 2>/dev/null
sudo apt autoremove -y
```

**VALEUR PAR DÉFAUT :**
Non installé par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.2.3 *Vérifier que ufw est activé et en cours d'exécution*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1562.004 (Impair Defenses: Disable or Modify System Firewall)
**NIST SP 800-53 :** SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)
**ANSSI :** R12 — Configurer un pare-feu local

**DESCRIPTION :**
Le pare-feu ufw doit être activé et en cours d'exécution pour protéger le serveur. Un pare-feu inactif laisse tous les ports ouverts et exposés. La politique par défaut doit être de refuser tout trafic entrant non explicitement autorisé.

```
sudo ufw status verbose
systemctl is-enabled ufw
```

**AUDIT :**

- **Fichier / Composant :** `ufw`
- **Valeur attendue :** `Status: active, Default: deny (incoming), allow (outgoing)`

```
# Configurer la politique par défaut
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw default deny routed

# Autoriser SSH avant d'activer (pour ne pas perdre l'accès)
sudo ufw allow ssh

# Activer ufw
sudo ufw --force enable
sudo systemctl enable ufw
```

**VALEUR PAR DÉFAUT :**
ufw est installé mais désactivé par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.2.4 *Vérifier que la politique par défaut de ufw refuse le trafic entrant*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1190 (Exploit Public-Facing Application)
**NIST SP 800-53 :** SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)
**ANSSI :** R12 — Configurer un pare-feu local

**DESCRIPTION :**
La politique par défaut du pare-feu doit être 'deny' pour le trafic entrant, ce qui signifie que tout trafic non explicitement autorisé par une règle est bloqué. Cette approche de liste blanche (whitelist) est la seule approche de sécurité acceptable pour un pare-feu.

```
sudo ufw status verbose | grep 'Default:'
sudo ufw show raw | head -20
```

**AUDIT :**

- **Fichier / Composant :** `ufw`
- **Valeur attendue :** `Default: deny (incoming), allow (outgoing)`

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw default deny routed
```

**VALEUR PAR DÉFAUT :**
deny incoming par défaut (quand ufw est activé)
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.2.5 *Vérifier que les règles ufw sont configurées pour les services autorisés*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1046 (Network Service Discovery)
**NIST SP 800-53 :** SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)
**ANSSI :** R12 — Configurer un pare-feu local

**DESCRIPTION :**
Chaque service réseau nécessaire doit avoir une règle de pare-feu explicite. Les règles doivent être aussi restrictives que possible, en limitant l'accès par adresse IP source et port de destination. La documentation des règles est essentielle pour l'audit.

```
sudo ufw status numbered
sudo ufw show added
```

**AUDIT :**

- **Fichier / Composant :** `ufw`
- **Valeur attendue :** `Seuls les services nécessaires sont autorisés (SSH minimum)`

```
# Exemple de règles pour un serveur web
sudo ufw allow from any to any port 22 proto tcp comment 'SSH'
sudo ufw allow from any to any port 80 proto tcp comment 'HTTP'
sudo ufw allow from any to any port 443 proto tcp comment 'HTTPS'

# Règle restrictive par IP source
sudo ufw allow from 192.168.1.0/24 to any port 22 proto tcp comment 'SSH LAN'
```

**VALEUR PAR DÉFAUT :**
Aucune règle configurée par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.2.6 *Vérifier que les règles de pare-feu pour le trafic de loopback sont configurées*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1090.001 (Proxy: Internal Proxy)
**NIST SP 800-53 :** SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)
**ANSSI :** R12 — Configurer un pare-feu local

**DESCRIPTION :**
Le trafic de l'interface loopback (127.0.0.1/lo) doit être autorisé car de nombreux services communiquent via localhost. Cependant, le trafic entrant avec une adresse source 127.0.0.0/8 sur une interface autre que lo doit être bloqué pour empêcher l'usurpation d'adresse loopback.

```
sudo ufw status verbose | grep -E '127|lo|Anywhere'
sudo iptables -L INPUT -v -n | grep lo
sudo iptables -L OUTPUT -v -n | grep lo
```

**AUDIT :**

- **Fichier / Composant :** `ufw / iptables`
- **Valeur attendue :** `Trafic loopback autorisé entrant et sortant, paquets 127.0.0.0/8 sur interfaces non-lo bloqués`

```
sudo ufw allow in on lo
sudo ufw allow out on lo
sudo ufw deny in from 127.0.0.0/8
sudo ufw deny in from ::1
```

**VALEUR PAR DÉFAUT :**
Non configuré par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.2.7 *Vérifier que la journalisation du pare-feu ufw est activée*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1562.004 (Impair Defenses: Disable or Modify System Firewall)
**NIST SP 800-53 :** SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)
**ANSSI :** R12 — Configurer un pare-feu local

**DESCRIPTION :**
La journalisation du pare-feu est essentielle pour détecter les tentatives d'intrusion et les anomalies réseau. Les journaux du pare-feu fournissent des preuves forensiques précieuses et alimentent les systèmes SIEM pour la corrélation d'événements de sécurité.

```
sudo ufw status verbose | grep Logging
grep -r 'LOGLEVEL' /etc/ufw/ufw.conf
```

**AUDIT :**

- **Fichier / Composant :** `/etc/ufw/ufw.conf`
- **Valeur attendue :** `Logging: on (medium ou high)`

```
sudo ufw logging medium
# Niveaux disponibles : off, low, medium, high, full
# 'medium' journalise les paquets bloqués et les connexions autorisées
# 'high' journalise également les paquets avec rate limiting
```

**VALEUR PAR DÉFAUT :**
Logging désactivé par défaut
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.2.8 *Vérifier que nftables est installé comme backend de ufw*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1562.004 (Impair Defenses: Disable or Modify System Firewall)
**NIST SP 800-53 :** SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)
**ANSSI :** R12 — Configurer un pare-feu local

**DESCRIPTION :**
nftables est le successeur d'iptables et fournit un cadre de filtrage de paquets plus performant et plus flexible. Ubuntu 24.04 utilise nftables comme backend par défaut pour ufw. La présence de nftables assure la compatibilité et les performances du pare-feu.

```
dpkg -l | grep nftables
nft list tables 2>/dev/null
grep -i 'ipt_backend' /etc/default/ufw
```

**AUDIT :**

- **Fichier / Composant :** `/etc/default/ufw`
- **Valeur attendue :** `IPT_BACKEND=nftables`

```
sudo apt install -y nftables
# Configurer ufw pour utiliser nftables
sudo sed -i 's/IPT_BACKEND=iptables/IPT_BACKEND=nftables/' /etc/default/ufw
```

**VALEUR PAR DÉFAUT :**
nftables est le backend par défaut sur Ubuntu 24.04
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.2.9 *Désactiver le protocole DCCP*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1095 (Non-Application Layer Protocol)
**NIST SP 800-53 :** SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)
**ANSSI :** R12 — Configurer un pare-feu local

**DESCRIPTION :**
Le protocole DCCP (Datagram Congestion Control Protocol) est rarement utilisé et peut représenter une surface d'attaque. La désactivation des protocoles réseau inutilisés fait partie de la stratégie de minimisation de la surface d'attaque du noyau.

```
modprobe -n -v dccp 2>/dev/null | grep -E '(install|/bin/(true|false))'
lsmod | grep dccp
```

**AUDIT :**

- **Fichier / Composant :** `/etc/modprobe.d/dccp.conf`
- **Valeur attendue :** `install /bin/false`

```
echo 'install dccp /bin/false' | sudo tee /etc/modprobe.d/dccp.conf
echo 'blacklist dccp' | sudo tee -a /etc/modprobe.d/dccp.conf
```

**VALEUR PAR DÉFAUT :**
Module disponible mais non chargé
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.2.10 *Désactiver le protocole SCTP*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1095 (Non-Application Layer Protocol)
**NIST SP 800-53 :** SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)
**ANSSI :** R12 — Configurer un pare-feu local

**DESCRIPTION :**
Le protocole SCTP (Stream Control Transmission Protocol) est utilisé principalement dans les réseaux de télécommunication. Sur un serveur standard, ce protocole n'est pas nécessaire et doit être désactivé pour réduire la surface d'attaque.

```
modprobe -n -v sctp 2>/dev/null | grep -E '(install|/bin/(true|false))'
lsmod | grep sctp
```

**AUDIT :**

- **Fichier / Composant :** `/etc/modprobe.d/sctp.conf`
- **Valeur attendue :** `install /bin/false`

```
echo 'install sctp /bin/false' | sudo tee /etc/modprobe.d/sctp.conf
echo 'blacklist sctp' | sudo tee -a /etc/modprobe.d/sctp.conf
```

**VALEUR PAR DÉFAUT :**
Module disponible mais non chargé
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.2.11 *Désactiver le protocole RDS*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1095 (Non-Application Layer Protocol)
**NIST SP 800-53 :** SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)
**ANSSI :** R12 — Configurer un pare-feu local

**DESCRIPTION :**
Le protocole RDS (Reliable Datagram Sockets) est un protocole de transport conçu pour les clusters Oracle. Il n'est pas nécessaire sur les serveurs standard et peut être désactivé pour réduire la surface d'attaque du noyau.

```
modprobe -n -v rds 2>/dev/null | grep -E '(install|/bin/(true|false))'
lsmod | grep rds
```

**AUDIT :**

- **Fichier / Composant :** `/etc/modprobe.d/rds.conf`
- **Valeur attendue :** `install /bin/false`

```
echo 'install rds /bin/false' | sudo tee /etc/modprobe.d/rds.conf
echo 'blacklist rds' | sudo tee -a /etc/modprobe.d/rds.conf
```

**VALEUR PAR DÉFAUT :**
Module disponible mais non chargé
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.2.12 *Désactiver le protocole TIPC*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1095 (Non-Application Layer Protocol)
**NIST SP 800-53 :** SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)
**ANSSI :** R12 — Configurer un pare-feu local

**DESCRIPTION :**
Le protocole TIPC (Transparent Inter-Process Communication) est utilisé pour la communication inter-nœuds dans les clusters. Sur un serveur non clusterisé, ce protocole n'est pas nécessaire et doit être désactivé.

```
modprobe -n -v tipc 2>/dev/null | grep -E '(install|/bin/(true|false))'
lsmod | grep tipc
```

**AUDIT :**

- **Fichier / Composant :** `/etc/modprobe.d/tipc.conf`
- **Valeur attendue :** `install /bin/false`

```
echo 'install tipc /bin/false' | sudo tee /etc/modprobe.d/tipc.conf
echo 'blacklist tipc' | sudo tee -a /etc/modprobe.d/tipc.conf
```

**VALEUR PAR DÉFAUT :**
Module disponible mais non chargé
**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A
**Commentaire de l'auditeur :** _____

### 3.2.13 *Désactiver les interfaces sans fil (Wi-Fi)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1200 (Hardware Additions)
**NIST SP 800-53 :** SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)
**ANSSI :** R12 — Configurer un pare-feu local

**DESCRIPTION :**
Les interfaces sans fil sur un serveur représentent un risque de sécurité majeur car elles permettent des attaques sans accès physique au câblage réseau. Sur un serveur, toutes les interfaces sans fil doivent être désactivées sauf si explicitement requises et sécurisées.

```
ip link show | grep -i wlan
iwconfig 2>/dev/null
nmcli radio wifi 2>/dev/null
rfkill list all 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `Interfaces réseau`
- **Valeur attendue :** `Aucune interface sans fil active`

```
# Désactiver le Wi-Fi
sudo rfkill block wifi 2>/dev/null
sudo nmcli radio wifi off 2>/dev/null

# Désactiver les modules sans fil
echo 'install cfg80211 /bin/false' | sudo tee /etc/modprobe.d/disable-wireless.conf
echo 'install mac80211 /bin/false' | sudo tee -a /etc/modprobe.d/disable-wireless.conf
echo 'install iwlwifi /bin/false' | sudo tee -a /etc/modprobe.d/disable-wireless.conf
```

**VALEUR PAR DÉFAUT :**
Le Wi-Fi peut être activé si du matériel sans fil est détecté

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 3.2.14 *Vérifier la configuration de TCP Wrappers (hosts.allow / hosts.deny)*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1046 (Network Service Discovery)
**NIST SP 800-53 :** SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)
**ANSSI :** R12 — Configurer un pare-feu local

**DESCRIPTION :**
TCP Wrappers fournit une couche de filtrage d'accès réseau au niveau applicatif via les fichiers /etc/hosts.allow et /etc/hosts.deny. Bien que remplacé par le pare-feu pour le filtrage principal, TCP Wrappers fournit une défense en profondeur supplémentaire pour les services qui le supportent.

```
cat /etc/hosts.allow 2>/dev/null
cat /etc/hosts.deny 2>/dev/null
ldd /usr/sbin/sshd | grep libwrap 2>/dev/null
```

**AUDIT :**

- **Fichier / Composant :** `/etc/hosts.allow, /etc/hosts.deny`
- **Valeur attendue :** `hosts.deny contient 'ALL: ALL' et hosts.allow liste les accès autorisés`

```
# Politique restrictive : tout bloquer par défaut
echo 'ALL: ALL' | sudo tee /etc/hosts.deny

# Autoriser les accès nécessaires
echo 'sshd: 192.168.1.0/24' | sudo tee /etc/hosts.allow
echo 'sshd: 10.0.0.0/8' | sudo tee -a /etc/hosts.allow
```

**VALEUR PAR DÉFAUT :**
hosts.allow et hosts.deny sont vides par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 3.2.15 *Vérifier qu'aucune règle de pare-feu en double ou contradictoire n'existe*

**Profil :** Niveau 1 (L1) — Serveur
**MITRE ATT&CK :** T1562.004 (Impair Defenses: Disable or Modify System Firewall)
**NIST SP 800-53 :** SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)
**ANSSI :** R12 — Configurer un pare-feu local

**DESCRIPTION :**
Les règles de pare-feu en double ou contradictoires peuvent créer des failles de sécurité ou rendre le pare-feu inefficace. Un audit régulier des règles de pare-feu est nécessaire pour maintenir une politique de filtrage cohérente et optimale.

```
sudo ufw status numbered
sudo iptables -L -n --line-numbers 2>/dev/null | head -50
sudo ip6tables -L -n --line-numbers 2>/dev/null | head -50
sudo nft list ruleset 2>/dev/null | head -50
```

**AUDIT :**

- **Fichier / Composant :** `Règles de pare-feu`
- **Valeur attendue :** `Aucune règle en double, aucune contradiction, politique cohérente`

```
# Examiner les règles et supprimer les doublons
sudo ufw status numbered
# Supprimer une règle par son numéro
sudo ufw delete <numéro>

# Réinitialiser si nécessaire
# sudo ufw reset
```

**VALEUR PAR DÉFAUT :**
Aucune règle configurée par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

## 4.0 — PARE-FEU UFW/NFTABLES

### 4.1.1 *Vérifier qu'UFW est installé et activé*

**MITRE ATT&CK :** T1562.004 (Impair Defenses: Disable or Modify System Firewall)

**DESCRIPTION :**

UFW (Uncomplicated Firewall) est l'interface recommandée pour gérer les règles de pare-feu sur Ubuntu. Il doit être installé, activé et configuré pour filtrer le trafic réseau entrant et sortant selon les besoins de l'organisation.

```
sudo ufw status verbose
systemctl is-enabled ufw
dpkg -s ufw | grep -E '^Status|^Version'
```

**REMÉDIATION :**

1. Installer UFW si nécessaire :

```
sudo apt update && sudo apt install ufw
```

**REMÉDIATION :**

1. Activer UFW :

```
sudo ufw enable
sudo systemctl enable ufw
```

**VALEUR PAR DÉFAUT :**

UFW installé mais inactif sur Ubuntu 24.04 LTS

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 4.1.2 *Configurer la politique par défaut UFW (deny incoming, allow outgoing)*

**MITRE ATT&CK :** T1090 (Proxy)

**DESCRIPTION :**

La politique par défaut d'UFW doit être configurée pour refuser tout le trafic entrant non autorisé et permettre le trafic sortant. Cette approche 'deny by default' réduit la surface d'attaque en ne permettant que les connexions explicitement autorisées.

```
sudo ufw status verbose | grep -E 'Default:'
```

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw default deny forward
```

**VALEUR PAR DÉFAUT :**

Policies par défaut non restrictives

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 4.1.3 *Autoriser uniquement les services réseau nécessaires dans UFW*

**MITRE ATT&CK :** T1046 (Network Service Discovery)

**DESCRIPTION :**

Seuls les services réseau requis pour les fonctions métier doivent être autorisés par le pare-feu. Chaque règle d'autorisation doit être justifiée et documentée. Les services non nécessaires exposent des surfaces d'attaque supplémentaires.

```
sudo ufw status numbered
sudo ss -tuln | grep LISTEN
sudo netstat -tuln 2>/dev/null | grep LISTEN
```

```
# Exemple : autoriser SSH depuis un réseau spécifique
sudo ufw allow from 192.168.1.0/24 to any port 22

# Autoriser HTTP/HTTPS
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp

# Supprimer les règles inutiles
sudo ufw delete <numéro_règle>
```

**VALEUR PAR DÉFAUT :**

Aucune règle d'autorisation configurée

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 4.1.4 *Vérifier la journalisation UFW*

**MITRE ATT&CK :** T1562.006 (Impair Defenses: Indicator Blocking)

**DESCRIPTION :**

La journalisation UFW doit être activée pour permettre la surveillance des tentatives de connexion et la détection d'activités suspectes. Les logs doivent être configurés à un niveau approprié et régulièrement analysés.

```
sudo ufw status verbose | grep -i logging
grep -E '^[[:space:]]*LOGLEVEL=' /etc/ufw/ufw.conf
tail -20 /var/log/ufw.log 2>/dev/null
```

```
# Activer la journalisation (niveau low recommandé)
sudo ufw logging on
sudo ufw logging low

# Configuration avancée dans /etc/ufw/ufw.conf
sudo sed -i 's/^LOGLEVEL=.*/LOGLEVEL=low/' /etc/ufw/ufw.conf
```

**VALEUR PAR DÉFAUT :**

Journalisation désactivée

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 4.2.1 *Vérifier la configuration nftables comme backend*

**MITRE ATT&CK :** T1562.004 (Impair Defenses: Disable or Modify System Firewall)

**DESCRIPTION :**

nftables est le framework de filtrage réseau moderne du noyau Linux, remplaçant iptables. UFW peut utiliser nftables comme backend pour améliorer les performances et la gestion des règles. La configuration doit être vérifiée pour s'assurer de la cohérence.

```
sudo nft list tables
sudo nft list ruleset | head -20
cat /etc/ufw/ufw.conf | grep -i backend
```

```
# Configurer UFW pour utiliser nftables
sudo sed -i 's/^IPT_BACKEND=.*/IPT_BACKEND=nftables/' /etc/ufw/ufw.conf

# Redémarrer UFW
sudo ufw reload
```

**VALEUR PAR DÉFAUT :**

Backend iptables par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 4.2.2 *Configurer des règles de limitation de débit (rate limiting)*

**MITRE ATT&CK :** T1499 (Endpoint Denial of Service)

**DESCRIPTION :**

Les règles de limitation de débit protègent contre les attaques par déni de service et les tentatives de brute force. UFW permet de configurer des limites sur les connexions par seconde pour certains services critiques comme SSH.

```
sudo ufw status | grep -i limit
sudo nft list ruleset | grep -A5 -B5 limit 2>/dev/null
```

```
# Limiter les connexions SSH (6 tentatives par 30 secondes)
sudo ufw limit ssh

# Ou pour un port spécifique
sudo ufw limit 22/tcp

# Vérifier la règle
sudo ufw status numbered
```

**VALEUR PAR DÉFAUT :**

Aucune limitation configurée

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 4.3.1 *Bloquer les adresses IP et réseaux malveillants*

**MITRE ATT&CK :** T1071 (Application Layer Protocol)

**DESCRIPTION :**

Le pare-feu doit être configuré pour bloquer automatiquement les adresses IP et réseaux connus comme malveillants. Cette protection proactive réduit les risques d'intrusion et d'attaques automatisées.

```
sudo ufw status | grep -E 'DENY|REJECT'
grep -c 'DENY' /etc/ufw/user.rules 2>/dev/null
```

```
# Bloquer des réseaux suspects (exemple)
sudo ufw deny from 10.0.0.0/8
sudo ufw deny from 169.254.0.0/16
sudo ufw deny from 224.0.0.0/3

# Bloquer une IP spécifique
sudo ufw deny from 192.0.2.1
```

**VALEUR PAR DÉFAUT :**

Aucun blocage proactif configuré

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 4.3.2 *Configurer des règles de sortie restrictives*

**MITRE ATT&CK :** T1041 (Exfiltration Over C2 Channel)

**DESCRIPTION :**

Le trafic sortant doit être filtré pour empêcher l'exfiltration de données et les communications non autorisées vers l'extérieur. Seuls les protocoles et destinations nécessaires doivent être autorisés en sortie.

```
sudo ufw status | grep -i out
cat /etc/ufw/user6.rules | grep OUTPUT 2>/dev/null
```

```
# Changer la politique par défaut sortante (après configuration des règles nécessaires)
# sudo ufw default deny outgoing

# Autoriser uniquement le trafic nécessaire
sudo ufw allow out 53    # DNS
sudo ufw allow out 80    # HTTP
sudo ufw allow out 443   # HTTPS
sudo ufw allow out 123   # NTP
```

**VALEUR PAR DÉFAUT :**

Trafic sortant autorisé par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 4.4.1 *Vérifier la protection contre l'IP spoofing*

**MITRE ATT&CK :** T1557 (Adversary-in-the-Middle)

**DESCRIPTION :**

La protection contre l'IP spoofing empêche les attaques où un attaquant usurpe l'adresse IP d'une source de confiance. Cette protection doit être activée au niveau du noyau et renforcée par les règles de pare-feu.

```
sysctl net.ipv4.conf.all.rp_filter
sysctl net.ipv4.conf.default.rp_filter
grep -r 'rp_filter' /etc/sysctl.conf /etc/sysctl.d/ 2>/dev/null
```

```
# Activer la protection rp_filter
echo 'net.ipv4.conf.all.rp_filter = 1' | sudo tee -a /etc/sysctl.d/60-netipv4_sysctl.conf
echo 'net.ipv4.conf.default.rp_filter = 1' | sudo tee -a /etc/sysctl.d/60-netipv4_sysctl.conf

# Appliquer immédiatement
sudo sysctl -p /etc/sysctl.d/60-netipv4_sysctl.conf
```

**VALEUR PAR DÉFAUT :**

rp_filter peut être désactivé selon la distribution

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 4.4.2 *Configurer la protection DDoS basique*

**MITRE ATT&CK :** T1499 (Endpoint Denial of Service)

**DESCRIPTION :**

Des mécanismes de protection basique contre les attaques DDoS doivent être configurés au niveau du pare-feu et du noyau. Cela inclut la limitation des connexions simultanées et la protection contre les attaques SYN flood.

```
sysctl net.ipv4.tcp_syncookies
sysctl net.ipv4.tcp_max_syn_backlog
sysctl net.netfilter.nf_conntrack_max
```

```
# Activer SYN cookies
echo 'net.ipv4.tcp_syncookies = 1' | sudo tee -a /etc/sysctl.d/60-netipv4_sysctl.conf

# Augmenter la taille du backlog SYN
echo 'net.ipv4.tcp_max_syn_backlog = 2048' | sudo tee -a /etc/sysctl.d/60-netipv4_sysctl.conf

# Limiter les connexions avec UFW
sudo ufw limit ssh
```

**VALEUR PAR DÉFAUT :**

Protection DDoS basique non optimisée

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 4.5.1 *Vérifier l'intégration avec fail2ban*

**MITRE ATT&CK :** T1110 (Brute Force)

**DESCRIPTION :**

fail2ban doit être intégré avec UFW pour bloquer automatiquement les adresses IP qui effectuent des tentatives d'attaque répétées. Cette intégration fournit une protection proactive contre les attaques par brute force.

```
systemctl is-active fail2ban
sudo fail2ban-client status
grep -i ufw /etc/fail2ban/jail.conf /etc/fail2ban/jail.local 2>/dev/null
```

```
# Installer fail2ban
sudo apt update && sudo apt install fail2ban

# Configurer pour UFW
sudo tee /etc/fail2ban/jail.local << 'EOF'
[DEFAULT]
banaction = ufw

[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 3600
EOF

sudo systemctl enable fail2ban
sudo systemctl start fail2ban
```

**VALEUR PAR DÉFAUT :**

fail2ban non installé par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 4.5.2 *Tester et valider les règles de pare-feu*

**MITRE ATT&CK :** T1562.004 (Impair Defenses: Disable or Modify System Firewall)

**DESCRIPTION :**

Les règles de pare-feu doivent être régulièrement testées pour s'assurer qu'elles fonctionnent comme prévu. Des tests de connectivité et de blocage doivent être effectués pour valider la configuration.

```
sudo ufw status numbered
nmap localhost -p 1-65535 2>/dev/null | grep -E 'open|filtered' | head -10
sudo ss -tuln | grep LISTEN
```

```
# Tests de connectivité (depuis un autre système)
# nmap -sS <ip_serveur> -p 22,80,443
# telnet <ip_serveur> 22

# Vérifier les logs
sudo tail -f /var/log/ufw.log &
# Effectuer des tests de connexion puis stopper le tail
```

**VALEUR PAR DÉFAUT :**

Aucune procédure de test systématique

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 4.6.1 *Documenter les règles de pare-feu et leur justification*

**MITRE ATT&CK :** T1562.004 (Impair Defenses: Disable or Modify System Firewall)

**DESCRIPTION :**

Chaque règle de pare-feu doit être documentée avec sa justification métier, la date de création, et les critères de révision. Cette documentation facilite la maintenance et l'audit des règles de sécurité.

```
sudo ufw status numbered
# Vérifier l'existence d'une documentation des règles
ls -la /etc/ufw/ | grep -E 'doc|readme'
```

```
# Créer un fichier de documentation
sudo tee /etc/ufw/rules-documentation.txt << 'EOF'
# UFW Rules Documentation
# Created: $(date)
# Maintainer: IT Security Team

Rule 1: Allow SSH from management network
- Justification: Administrative access required
- Source: 192.168.1.0/24
- Review: Quarterly

Rule 2: Allow HTTP/HTTPS for web service
- Justification: Public web server
- Ports: 80, 443
- Review: Monthly
EOF
```

**VALEUR PAR DÉFAUT :**

Aucune documentation standardisée

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 4.6.2 *Configurer la sauvegarde automatique des règles UFW*

**MITRE ATT&CK :** T1485 (Data Destruction)

**DESCRIPTION :**

Les règles de pare-feu doivent être sauvegardées automatiquement pour permettre une restauration rapide en cas de problème. La sauvegarde doit inclure tous les fichiers de configuration UFW et être stockée de manière sécurisée.

```
ls -la /etc/ufw/
crontab -l | grep -i ufw
ls -la /var/backups/ | grep -i ufw
```

```
# Créer un script de sauvegarde
sudo tee /usr/local/bin/backup-ufw.sh << 'EOF'
BACKUP_DIR="/var/backups/ufw"
DATE=$(date +%Y%m%d-%H%M%S)

mkdir -p $BACKUP_DIR
tar czf $BACKUP_DIR/ufw-backup-$DATE.tar.gz /etc/ufw/
find $BACKUP_DIR -name "ufw-backup-*.tar.gz" -mtime +30 -delete
EOF

sudo chmod +x /usr/local/bin/backup-ufw.sh

# Programmer la sauvegarde quotidienne
echo "0 2 * * * /usr/local/bin/backup-ufw.sh" | sudo crontab -
```

**VALEUR PAR DÉFAUT :**

Aucune sauvegarde automatique configurée

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

## 5.0 — JOURNALISATION & AUDIT

### 5.1.1 *Vérifier que rsyslog est installé et configuré*

**MITRE ATT&CK :** T1562.006 (Impair Defenses: Indicator Blocking)

**DESCRIPTION :**

Le service rsyslog doit être installé et configuré pour centraliser la collecte des journaux système. Une journalisation appropriée est essentielle pour la surveillance de sécurité, la détection d'incidents et la conformité réglementaire.

```
dpkg -s rsyslog | grep Status
systemctl is-enabled rsyslog
systemctl is-active rsyslog
ls -la /etc/rsyslog.conf
```

```
# Installer rsyslog si nécessaire
sudo apt update && sudo apt install rsyslog

# Activer et démarrer le service
sudo systemctl enable rsyslog
sudo systemctl start rsyslog
```

**VALEUR PAR DÉFAUT :**

rsyslog installé et activé par défaut sur Ubuntu 24.04 LTS

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 5.1.2 *Configurer la journalisation centralisée avec un serveur distant*

**MITRE ATT&CK :** T1070.002 (Indicator Removal on Host: Clear Linux or Mac System Logs)

**DESCRIPTION :**

Les journaux doivent être envoyés vers un serveur de journalisation centralisé pour éviter leur perte en cas de compromission du système local. Cette centralisation améliore la surveillance et l'analyse de sécurité.

```
grep -E '^\*\.\*' /etc/rsyslog.conf
grep -E '@' /etc/rsyslog.conf /etc/rsyslog.d/*.conf 2>/dev/null
ss -tuln | grep :514
```

```
# Configurer l'envoi vers un serveur syslog distant
echo '*.* @@log-server.domain.com:514' | sudo tee -a /etc/rsyslog.conf

# Ou pour UDP (moins sûr)
# echo '*.* @log-server.domain.com:514' | sudo tee -a /etc/rsyslog.conf

sudo systemctl restart rsyslog
```

**VALEUR PAR DÉFAUT :**

Journalisation locale uniquement

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 5.1.3 *Configurer la rotation et la rétention des journaux*

**MITRE ATT&CK :** T1070.002 (Indicator Removal on Host: Clear Linux or Mac System Logs)

**DESCRIPTION :**

La rotation automatique des journaux doit être configurée pour éviter la saturation de l'espace disque tout en conservant suffisamment d'historique pour l'analyse de sécurité et la conformité réglementaire.

```
ls -la /etc/logrotate.d/rsyslog
cat /etc/logrotate.d/rsyslog
logrotate -d /etc/logrotate.d/rsyslog
```

```
# Configurer la rotation des logs rsyslog
sudo tee /etc/logrotate.d/rsyslog << 'EOF'
/var/log/syslog
/var/log/mail.info
/var/log/mail.warn
/var/log/mail.err
/var/log/mail.log
/var/log/daemon.log
/var/log/kern.log
/var/log/auth.log
/var/log/user.log
/var/log/lpr.log
/var/log/cron.log
/var/log/debug
/var/log/messages
{
    rotate 52
    weekly
    missingok
    notifempty
    compress
    delaycompress
    sharedscripts
    postrotate
        /usr/lib/rsyslog/rsyslog-rotate
    endscript
}
EOF
```

**VALEUR PAR DÉFAUT :**

Rotation basique configurée

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 5.2.1 *Installer et configurer auditd*

**MITRE ATT&CK :** T1562.006 (Impair Defenses: Indicator Blocking)

**DESCRIPTION :**

Le démon auditd doit être installé et configuré pour enregistrer les événements de sécurité critiques du système. L'audit permet de détecter les activités malveillantes et de maintenir la traçabilité des actions administratives.

```
dpkg -s auditd | grep Status
systemctl is-enabled auditd
systemctl is-active auditd
auditctl -s
```

```
# Installer auditd
sudo apt update && sudo apt install auditd audispd-plugins

# Activer et démarrer auditd
sudo systemctl enable auditd
sudo systemctl start auditd
```

**VALEUR PAR DÉFAUT :**

auditd non installé par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 5.2.2 *Configurer les règles d'audit pour les fichiers sensibles*

**MITRE ATT&CK :** T1562.006 (Impair Defenses: Indicator Blocking)

**DESCRIPTION :**

Des règles d'audit spécifiques doivent être configurées pour surveiller l'accès et la modification des fichiers sensibles comme /etc/passwd, /etc/shadow, et les fichiers de configuration système critiques.

```
auditctl -l | grep -E '/etc/passwd|/etc/shadow|/etc/group'
cat /etc/audit/audit.rules | grep -E '/etc/passwd|/etc/shadow'
```

```
# Ajouter les règles d'audit pour les fichiers sensibles
sudo tee -a /etc/audit/audit.rules << 'EOF'
# Surveillance des fichiers de comptes utilisateurs
-w /etc/passwd -p wa -k passwd_changes
-w /etc/shadow -p wa -k shadow_changes
-w /etc/group -p wa -k group_changes
-w /etc/gshadow -p wa -k gshadow_changes
-w /etc/security/opasswd -p wa -k opasswd_changes

# Surveillance des fichiers de configuration réseau
-w /etc/network/interfaces -p wa -k network_changes
-w /etc/hosts -p wa -k hosts_changes
-w /etc/hostname -p wa -k hostname_changes

# Surveillance des configurations système critiques
-w /etc/sudoers -p wa -k sudoers_changes
-w /etc/sudoers.d/ -p wa -k sudoers_changes
EOF

sudo service auditd restart
```

**VALEUR PAR DÉFAUT :**

Aucune règle d'audit configurée

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 5.2.3 *Configurer l'audit des commandes privilégiées*

**MITRE ATT&CK :** T1548 (Abuse Elevation Control Mechanism)

**DESCRIPTION :**

Toutes les commandes exécutées avec des privilèges élevés (sudo, su, setuid) doivent être auditées. Cette surveillance permet de détecter les abus de privilèges et les tentatives d'élévation non autorisées.

```
find /usr/bin /usr/sbin /bin /sbin -perm -4000 -type f | head -10
auditctl -l | grep -E 'sudo|su'
grep -E 'sudo|su' /etc/audit/audit.rules
```

```
# Audit des commandes sudo et su
sudo tee -a /etc/audit/audit.rules << 'EOF'
# Surveillance des commandes privilégiées
-w /usr/bin/sudo -p x -k sudo_commands
-w /bin/su -p x -k su_commands
-w /usr/bin/su -p x -k su_commands

# Audit des binaires setuid
-a always,exit -F arch=b64 -S execve -F euid=0 -F auid>=1000 -F auid!=4294967295 -k privileged_commands
-a always,exit -F arch=b32 -S execve -F euid=0 -F auid>=1000 -F auid!=4294967295 -k privileged_commands
EOF

sudo service auditd restart
```

**VALEUR PAR DÉFAUT :**

Commandes privilégiées non auditées

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 5.2.4 *Configurer l'audit des modifications de temps système*

**MITRE ATT&CK :** T1070.006 (Indicator Removal on Host: Timestomp)

**DESCRIPTION :**

Les modifications de l'heure système doivent être auditées car elles peuvent être utilisées pour masquer des activités malveillantes ou contourner les mécanismes de sécurité basés sur le temps.

```
auditctl -l | grep -E 'time|clock'
grep -E 'time|clock' /etc/audit/audit.rules
```

```
# Audit des modifications de temps
sudo tee -a /etc/audit/audit.rules << 'EOF'
# Surveillance des modifications de temps système
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time_change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time_change
-a always,exit -F arch=b64 -S clock_settime -k time_change
-a always,exit -F arch=b32 -S clock_settime -k time_change
-w /etc/localtime -p wa -k time_change
EOF

sudo service auditd restart
```

**VALEUR PAR DÉFAUT :**

Modifications de temps non auditées

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 5.3.1 *Configurer l'audit des connexions et authentifications*

**MITRE ATT&CK :** T1078 (Valid Accounts)

**DESCRIPTION :**

Toutes les tentatives de connexion et d'authentification doivent être enregistrées pour permettre la détection des tentatives d'accès non autorisées et l'analyse des patterns de connexion suspects.

```
grep -E 'session|login' /etc/audit/audit.rules
tail -20 /var/log/auth.log
auditctl -l | grep -E 'session|login'
```

```
# Audit des sessions et authentifications
sudo tee -a /etc/audit/audit.rules << 'EOF'
# Surveillance des sessions utilisateur
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p wa -k logins

# Surveillance des modifications PAM
-w /etc/pam.d/ -p wa -k pam_changes
-w /etc/security/limits.conf -p wa -k pam_changes
EOF

sudo service auditd restart
```

**VALEUR PAR DÉFAUT :**

Authentifications partiellement loggées

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 5.3.2 *Configurer l'immutabilité des règles d'audit*

**MITRE ATT&CK :** T1562.006 (Impair Defenses: Indicator Blocking)

**DESCRIPTION :**

Les règles d'audit doivent être rendues immutables pour empêcher leur modification par des attaquants. Une fois immutables, les règles ne peuvent plus être modifiées jusqu'au redémarrage du système.

```
auditctl -s | grep enabled
tail -5 /etc/audit/audit.rules | grep -e '-e 2'
```

```
# Ajouter la règle d'immutabilité à la fin du fichier
echo '-e 2' | sudo tee -a /etc/audit/audit.rules

# Redémarrer auditd pour appliquer
sudo service auditd restart
```

**VALEUR PAR DÉFAUT :**

Règles d'audit modifiables

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 5.4.1 *Configurer la surveillance des montages et démontages*

**MITRE ATT&CK :** T1005 (Data from Local System)

**DESCRIPTION :**

Les opérations de montage et démontage de systèmes de fichiers doivent être auditées car elles peuvent indiquer des tentatives d'accès à des données non autorisées ou l'introduction de supports amovibles malveillants.

```
auditctl -l | grep -E 'mount|umount'
grep -E 'mount|umount' /etc/audit/audit.rules
```

```
# Audit des opérations de montage
sudo tee -a /etc/audit/audit.rules << 'EOF'
# Surveillance des montages et démontages
-a always,exit -F arch=b64 -S mount -k mounts
-a always,exit -F arch=b32 -S mount -k mounts
-a always,exit -F arch=b64 -S umount2 -k mounts
-a always,exit -F arch=b32 -S umount -S umount2 -k mounts
EOF

sudo service auditd restart
```

**VALEUR PAR DÉFAUT :**

Montages non audités

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 5.4.2 *Configurer l'audit des suppressions de fichiers*

**MITRE ATT&CK :** T1070.004 (Indicator Removal on Host: File Deletion)

**DESCRIPTION :**

Les suppressions de fichiers doivent être auditées pour détecter les tentatives de destruction de preuves ou les suppressions accidentelles de données critiques.

```
auditctl -l | grep -E 'unlink|rename'
grep -E 'unlink|rename' /etc/audit/audit.rules
```

```
# Audit des suppressions de fichiers
sudo tee -a /etc/audit/audit.rules << 'EOF'
# Surveillance des suppressions et renommages
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -k delete
EOF

sudo service auditd restart
```

**VALEUR PAR DÉFAUT :**

Suppressions non auditées

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 5.5.1 *Configurer la protection des fichiers de logs*

**MITRE ATT&CK :** T1070 (Indicator Removal on Host)

**DESCRIPTION :**

Les fichiers de journaux doivent être protégés contre la modification et la suppression non autorisées. Des permissions appropriées et des mécanismes de protection d'intégrité doivent être mis en place.

```
ls -la /var/log/ | head -10
stat /var/log/auth.log
find /var/log -type f -perm /o+w
```

```
# Sécuriser les permissions des logs
sudo find /var/log -type f -exec chmod g-wx,o-rwx {} +
sudo find /var/log -type d -exec chmod g-w,o-rwx {} +

# Définir l'owner approprié
sudo chown -R root:adm /var/log/

# Protéger spécifiquement certains logs critiques
sudo chmod 600 /var/log/auth.log
sudo chmod 600 /var/log/secure 2>/dev/null || true
```

**VALEUR PAR DÉFAUT :**

Permissions par défaut potentiellement trop permissives

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 5.5.2 *Configurer la surveillance en temps réel des logs*

**MITRE ATT&CK :** T1562.006 (Impair Defenses: Indicator Blocking)

**DESCRIPTION :**

Une surveillance en temps réel des logs critiques doit être mise en place pour détecter rapidement les incidents de sécurité. Des alertes automatiques doivent être configurées pour les événements suspects.

```
systemctl is-active rsyslog
ps aux | grep -E 'logwatch|logcheck'
crontab -l | grep -E 'logwatch|logcheck'
```

```
# Installer logwatch pour la surveillance
sudo apt update && sudo apt install logwatch

# Configurer logwatch pour les rapports quotidiens
sudo sed -i 's/^Output = .*/Output = mail/' /usr/share/logwatch/default.conf/logwatch.conf
sudo sed -i 's/^Format = .*/Format = html/' /usr/share/logwatch/default.conf/logwatch.conf
sudo sed -i 's/^Detail = .*/Detail = Med/' /usr/share/logwatch/default.conf/logwatch.conf

# Programmer l'exécution quotidienne
echo '0 1 * * * /usr/sbin/logwatch --output mail --mailto admin@domain.com' | sudo tee -a /etc/cron.daily/00logwatch
```

**VALEUR PAR DÉFAUT :**

Aucune surveillance automatique configurée

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 5.6.1 *Configurer la rétention à long terme des logs d'audit*

**MITRE ATT&CK :** T1070 (Indicator Removal on Host)

**DESCRIPTION :**

Les logs d'audit doivent être conservés pendant une durée suffisante pour répondre aux exigences réglementaires et permettre les investigations de sécurité. Un système d'archivage sécurisé doit être mis en place.

```
grep 'max_log_file' /etc/audit/auditd.conf
grep 'num_logs' /etc/audit/auditd.conf
df -h /var/log/audit/
```

```
# Configurer la rétention des logs d'audit
sudo sed -i 's/^max_log_file = .*/max_log_file = 100/' /etc/audit/auditd.conf
sudo sed -i 's/^num_logs = .*/num_logs = 10/' /etc/audit/auditd.conf
sudo sed -i 's/^max_log_file_action = .*/max_log_file_action = rotate/' /etc/audit/auditd.conf

# Créer un script d'archivage
sudo tee /usr/local/bin/archive-audit-logs.sh << 'EOF'
ARCHIVE_DIR="/var/log/audit/archive"
mkdir -p $ARCHIVE_DIR
find /var/log/audit/ -name "audit.log.*" -mtime +30 -exec gzip {} \;
find /var/log/audit/ -name "audit.log.*.gz" -mtime +90 -exec mv {} $ARCHIVE_DIR/ \;
EOF

sudo chmod +x /usr/local/bin/archive-audit-logs.sh
```

**VALEUR PAR DÉFAUT :**

Rétention limitée des logs d'audit

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

## 6.0 — GESTION DES COMPTES

### 6.1.1 *Définir l'expiration par défaut des comptes utilisateurs*

**MITRE ATT&CK :** T1078.003 (Valid Accounts: Local Accounts)

**DESCRIPTION :**

Les comptes utilisateurs doivent avoir une date d'expiration définie pour éviter l'accumulation de comptes dormants qui pourraient être compromis. Cette mesure réduit la surface d'attaque en désactivant automatiquement les comptes inutilisés.

```
grep INACTIVE /etc/default/useradd
grep EXPIRE /etc/default/useradd
chage -l root | grep 'Account expires'
```

```
# Définir l'inactivité par défaut (30 jours après expiration du mot de passe)
sudo sed -i 's/^INACTIVE=.*/INACTIVE=30/' /etc/default/useradd

# Ou si la ligne n'existe pas
echo 'INACTIVE=30' | sudo tee -a /etc/default/useradd

# Appliquer aux comptes existants si nécessaire
# sudo chage -I 30 username
```

**VALEUR PAR DÉFAUT :**

INACTIVE=-1 (pas d'expiration automatique)

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 6.1.2 *Configurer l'âge minimum des mots de passe par défaut*

**MITRE ATT&CK :** T1110.001 (Brute Force: Password Guessing)

**DESCRIPTION :**

Un âge minimum pour les mots de passe doit être configuré pour empêcher les utilisateurs de changer rapidement leur mot de passe pour revenir à l'ancien. Cette mesure renforce l'efficacité des politiques de rotation des mots de passe.

```
grep PASS_MIN_DAYS /etc/login.defs
chage -l root | grep 'Minimum number of days'
```

```
# Définir l'âge minimum à 1 jour
sudo sed -i 's/^PASS_MIN_DAYS.*/PASS_MIN_DAYS 1/' /etc/login.defs

# Appliquer aux comptes existants
for user in $(getent passwd | awk -F: '$3 >= 1000 && $3 < 65534 {print $1}'); do
    sudo chage -m 1 $user
done
```

**VALEUR PAR DÉFAUT :**

PASS_MIN_DAYS 0

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 6.1.3 *Configurer l'âge maximum des mots de passe*

**MITRE ATT&CK :** T1110 (Brute Force)

**DESCRIPTION :**

Les mots de passe doivent expirer après une période définie pour réduire le risque d'utilisation prolongée de mots de passe compromis. L'âge maximum doit être équilibré entre sécurité et utilisabilité.

```
grep PASS_MAX_DAYS /etc/login.defs
chage -l root | grep 'Maximum number of days'
```

```
# Définir l'âge maximum à 90 jours
sudo sed -i 's/^PASS_MAX_DAYS.*/PASS_MAX_DAYS 90/' /etc/login.defs

# Appliquer aux comptes existants
for user in $(getent passwd | awk -F: '$3 >= 1000 && $3 < 65534 {print $1}'); do
    sudo chage -M 90 $user
done
```

**VALEUR PAR DÉFAUT :**

PASS_MAX_DAYS 99999

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 6.1.4 *Configurer l'avertissement d'expiration des mots de passe*

**MITRE ATT&CK :** T1078 (Valid Accounts)

**DESCRIPTION :**

Les utilisateurs doivent être avertis avant l'expiration de leur mot de passe pour éviter le verrouillage de compte et encourager le renouvellement proactif des mots de passe.

```
grep PASS_WARN_AGE /etc/login.defs
chage -l root | grep 'Number of days of warning'
```

```
# Configurer l'avertissement 7 jours avant expiration
sudo sed -i 's/^PASS_WARN_AGE.*/PASS_WARN_AGE 7/' /etc/login.defs

# Appliquer aux comptes existants
for user in $(getent passwd | awk -F: '$3 >= 1000 && $3 < 65534 {print $1}'); do
    sudo chage -W 7 $user
done
```

**VALEUR PAR DÉFAUT :**

PASS_WARN_AGE 7

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 6.2.1 *Verrouiller les comptes système inutilisés*

**MITRE ATT&CK :** T1078.003 (Valid Accounts: Local Accounts)

**DESCRIPTION :**

Les comptes système non utilisés doivent être verrouillés ou supprimés pour réduire la surface d'attaque. Ces comptes peuvent être exploités par des attaquants pour obtenir un accès initial au système.

```
awk -F: '($3 < 1000) {print $1 " : " $7}' /etc/passwd
grep -E '^[^:]*:[^!*]' /etc/shadow | cut -d: -f1
```

```
# Verrouiller les comptes système avec shell
for user in games news uucp proxy www-data backup list irc gnats; do
    if getent passwd $user > /dev/null; then
        sudo usermod -L -s /usr/sbin/nologin $user 2>/dev/null
    fi
done

# Vérifier que root est le seul compte avec UID 0
awk -F: '($3 == 0) { print $1 }' /etc/passwd
```

**VALEUR PAR DÉFAUT :**

Comptes système avec shells actifs

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 6.2.2 *Vérifier l'unicité des UID utilisateurs*

**MITRE ATT&CK :** T1078.003 (Valid Accounts: Local Accounts)

**DESCRIPTION :**

Chaque utilisateur doit avoir un UID unique pour assurer une identification et une autorisation correctes. Des UID dupliqués peuvent conduire à des privilèges non intentionnels et des problèmes de sécurité.

```
cut -f3 -d":" /etc/passwd | sort -n | uniq -c | awk '$1 > 1 {print $2}'
awk -F":" '{print $3}' /etc/passwd | sort | uniq -d
```

```
# Script pour détecter les UID dupliqués
echo "Recherche d'UID dupliqués..."
cut -f3 -d":" /etc/passwd | sort -n | uniq -c | while read count uid; do
    if [ $count -gt 1 ]; then
        echo "UID dupliqué trouvé: $uid"
        awk -F":" -v uid="$uid" '$3 == uid {print "  - Utilisateur: " $1}' /etc/passwd
    fi
done

# Corriger manuellement les UID dupliqués avec usermod
# sudo usermod -u <nouveau_uid> <nom_utilisateur>
```

**VALEUR PAR DÉFAUT :**

UIDs généralement uniques sur installation propre

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 6.2.3 *Vérifier l'unicité des GID groupes*

**MITRE ATT&CK :** T1078.003 (Valid Accounts: Local Accounts)

**DESCRIPTION :**

Chaque groupe doit avoir un GID unique pour assurer une gestion correcte des permissions. Des GID dupliqués peuvent créer des conflits de permissions et des vulnérabilités de sécurité.

```
cut -f3 -d":" /etc/group | sort -n | uniq -c | awk '$1 > 1 {print $2}'
awk -F":" '{print $3}' /etc/group | sort | uniq -d
```

```
# Script pour détecter les GID dupliqués
echo "Recherche de GID dupliqués..."
cut -f3 -d":" /etc/group | sort -n | uniq -c | while read count gid; do
    if [ $count -gt 1 ]; then
        echo "GID dupliqué trouvé: $gid"
        awk -F":" -v gid="$gid" '$3 == gid {print "  - Groupe: " $1}' /etc/group
    fi
done

# Corriger manuellement les GID dupliqués avec groupmod
# sudo groupmod -g <nouveau_gid> <nom_groupe>
```

**VALEUR PAR DÉFAUT :**

GIDs généralement uniques sur installation propre

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 6.3.1 *Vérifier l'existence des répertoires home des utilisateurs*

**MITRE ATT&CK :** T1083 (File and Directory Discovery)

**DESCRIPTION :**

Tous les utilisateurs définis dans /etc/passwd doivent avoir un répertoire home existant et accessible. Les répertoires manquants peuvent indiquer des problèmes de configuration ou des comptes corrompus.

```
awk -F: '($3 >= 1000) && ($1 != "nobody") {print $1 " : " $6}' /etc/passwd | while IFS=':' read user home; do
    if [ ! -d "$home" ]; then
        echo "Répertoire home manquant pour $user: $home"
    fi
done
```

```
# Créer les répertoires home manquants
awk -F: '($3 >= 1000) && ($1 != "nobody") {print $1 " " $6}' /etc/passwd | while read user home; do
    if [ ! -d "$home" ]; then
        sudo mkdir -p "$home"
        sudo chown $user:$user "$home"
        sudo chmod 750 "$home"

        # Copier les fichiers de squelette si nécessaire
        sudo cp -r /etc/skel/. "$home/"
        sudo chown -R $user:$user "$home"
    fi
done
```

**VALEUR PAR DÉFAUT :**

Répertoires home créés à la création du compte

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 6.3.2 *Vérifier les permissions des répertoires home*

**MITRE ATT&CK :** T1083 (File and Directory Discovery)

**DESCRIPTION :**

Les répertoires home des utilisateurs doivent avoir des permissions appropriées pour empêcher l'accès non autorisé aux fichiers personnels. Les permissions trop permissives exposent les données sensibles des utilisateurs.

```
awk -F: '($3 >= 1000) && ($1 != "nobody") {print $6}' /etc/passwd | while read home; do
    if [ -d "$home" ]; then
        ls -ld "$home"
    fi
done
```

```
# Corriger les permissions des répertoires home
awk -F: '($3 >= 1000) && ($1 != "nobody") {print $1 " " $6}' /etc/passwd | while read user home; do
    if [ -d "$home" ]; then
        # Retirer les permissions pour group et other
        sudo chmod g-w,o-rwx "$home"

        # S'assurer que l'utilisateur est propriétaire
        sudo chown $user:$user "$home"
    fi
done
```

**VALEUR PAR DÉFAUT :**

Permissions 755 par défaut (trop permissives)

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 6.4.1 *Vérifier les fichiers .netrc dans les répertoires home*

**MITRE ATT&CK :** T1552.001 (Unsecured Credentials: Credentials In Files)

**DESCRIPTION :**

Les fichiers .netrc contiennent des identifiants en clair et présentent un risque de sécurité. Ils doivent être supprimés ou sécurisés avec des permissions appropriées s'ils sont nécessaires.

```
find /home -name ".netrc" -type f 2>/dev/null
awk -F: '($3 >= 1000) && ($1 != "nobody") {print $6}' /etc/passwd | while read home; do
    if [ -f "$home/.netrc" ]; then
        ls -la "$home/.netrc"
    fi
done
```

```
# Supprimer ou sécuriser les fichiers .netrc
find /home -name ".netrc" -type f 2>/dev/null | while read netrc_file; do
    echo "Fichier .netrc trouvé: $netrc_file"

    # Option 1: Supprimer (recommandé)
    # sudo rm "$netrc_file"

    # Option 2: Sécuriser si nécessaire
    sudo chmod 600 "$netrc_file"

    # Avertir le propriétaire
    owner=$(stat -c %U "$netrc_file")
    echo "ATTENTION: $owner a un fichier .netrc avec des identifiants en clair"
done
```

**VALEUR PAR DÉFAUT :**

Pas de fichiers .netrc par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 6.4.2 *Vérifier les fichiers .rhosts dans les répertoires home*

**MITRE ATT&CK :** T1021.004 (Remote Services: SSH)

**DESCRIPTION :**

Les fichiers .rhosts permettent l'authentification sans mot de passe et présentent un risque de sécurité majeur. Ils doivent être supprimés car ils peuvent être exploités pour des accès non autorisés.

```
find /home -name ".rhosts" -type f 2>/dev/null
awk -F: '($3 >= 1000) && ($1 != "nobody") {print $6}' /etc/passwd | while read home; do
    if [ -f "$home/.rhosts" ]; then
        ls -la "$home/.rhosts"
    fi
done
```

```
# Supprimer tous les fichiers .rhosts
find /home -name ".rhosts" -type f -delete 2>/dev/null

# Rechercher aussi dans les répertoires système
find /root -name ".rhosts" -type f -delete 2>/dev/null

# Vérifier la suppression
find /home /root -name ".rhosts" -type f 2>/dev/null
```

**VALEUR PAR DÉFAUT :**

Pas de fichiers .rhosts par défaut

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 6.5.1 *Auditer les groupes dans /etc/passwd vs /etc/group*

**MITRE ATT&CK :** T1078 (Valid Accounts)

**DESCRIPTION :**

Tous les groupes référencés dans /etc/passwd doivent exister dans /etc/group. Les références vers des groupes inexistants peuvent causer des problèmes de permissions et de sécurité.

```
for group in $(awk -F: '{print $4}' /etc/passwd | sort -u); do
    if ! getent group $group >/dev/null; then
        echo "Groupe manquant: $group"
    fi
done
```

```
# Créer les groupes manquants ou corriger les références
for group in $(awk -F: '{print $4}' /etc/passwd | sort -u); do
    if ! getent group $group >/dev/null; then
        echo "Création du groupe manquant: $group"
        sudo groupadd -g $group $group 2>/dev/null || echo "Erreur lors de la création du groupe $group"
    fi
done

# Vérifier les utilisateurs affectés par des groupes manquants
awk -F: '{print $1 " : " $4}' /etc/passwd | while IFS=':' read user gid; do
    if ! getent group $gid >/dev/null; then
        echo "Utilisateur $user référence le groupe inexistant $gid"
    fi
done
```

**VALEUR PAR DÉFAUT :**

Cohérence généralement maintenue sur installation propre

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 6.5.2 *Vérifier l'absence de comptes avec des mots de passe vides*

**MITRE ATT&CK :** T1078.003 (Valid Accounts: Local Accounts)

**DESCRIPTION :**

Aucun compte ne doit avoir un mot de passe vide. Les mots de passe vides permettent un accès non autorisé immédiat au système et représentent une vulnérabilité critique.

```
awk -F: '($2 == "") {print $1}' /etc/shadow
getent shadow | awk -F: '($2 == "") {print $1}'
```

```
# Identifier et verrouiller les comptes avec mots de passe vides
awk -F: '($2 == "") {print $1}' /etc/shadow | while read user; do
    echo "ATTENTION: Utilisateur $user a un mot de passe vide"

    # Verrouiller le compte immédiatement
    sudo usermod -L $user

    # Forcer la définition d'un mot de passe au prochain login
    sudo chage -d 0 $user
done

# Vérifier qu'aucun compte n'a de mot de passe vide
if awk -F: '($2 == "") {print $1}' /etc/shadow | grep -q .; then
    echo "ERREUR: Des comptes avec mots de passe vides existent encore"
else
    echo "OK: Aucun compte avec mot de passe vide détecté"
fi
```

**VALEUR PAR DÉFAUT :**

Mots de passe requis lors de la création de comptes

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 6.6.1 *Configurer la politique de verrouillage de compte*

**MITRE ATT&CK :** T1110 (Brute Force)

**DESCRIPTION :**

Une politique de verrouillage automatique des comptes doit être configurée pour protéger contre les attaques par brute force. Le verrouillage doit être temporaire et permettre le déverrouillage administratif.

```
grep pam_faillock /etc/pam.d/common-auth
grep pam_faillock /etc/pam.d/common-account
cat /etc/security/faillock.conf 2>/dev/null
```

```
# Installer et configurer pam_faillock
sudo apt update && sudo apt install libpam-modules

# Configurer faillock dans common-auth
sudo sed -i '/^auth.*pam_unix.so/i auth required pam_faillock.so preauth' /etc/pam.d/common-auth
sudo sed -i '/^auth.*pam_unix.so/a auth [default=die] pam_faillock.so authfail' /etc/pam.d/common-auth

# Configurer faillock dans common-account
sudo sed -i '/^account.*pam_unix.so/i account required pam_faillock.so' /etc/pam.d/common-account

# Créer la configuration faillock
sudo tee /etc/security/faillock.conf << 'EOF'
# Politique de verrouillage de comptes
deny = 5
fail_interval = 900
unlock_time = 900
even_deny_root
root_unlock_time = 300
EOF
```

**VALEUR PAR DÉFAUT :**

Pas de politique de verrouillage configurée

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 6.6.2 *Surveiller et auditer les connexions utilisateurs*

**MITRE ATT&CK :** T1078 (Valid Accounts)

**DESCRIPTION :**

Toutes les connexions utilisateurs doivent être surveillées et auditées pour détecter les accès non autorisés et les patterns de connexion suspects. Un historique des connexions doit être maintenu.

```
last -n 20
lastlog | head -20
who -a
grep -i 'session opened' /var/log/auth.log | tail -10
```

```
# Configurer la journalisation des connexions
echo 'session required pam_lastlog.so showfailed' | sudo tee -a /etc/pam.d/common-session

# Script de surveillance des connexions
sudo tee /usr/local/bin/monitor-logins.sh << 'EOF'
LOG_FILE="/var/log/login-monitor.log"

# Analyser les connexions des dernières 24h
echo "$(date): Analyse des connexions" >> $LOG_FILE
last -s -24hours | grep -v 'wtmp begins' >> $LOG_FILE

# Détecter les connexions suspectes (horaires inhabituels, IPs étrangères)
grep "$(date +%b' '%d)" /var/log/auth.log | grep 'session opened' | while read line; do
    if echo $line | grep -E '(0[0-5]:|2[2-3]:)' >/dev/null; then
        echo "Connexion hors heures détectée: $line" >> $LOG_FILE
    fi
done
EOF

sudo chmod +x /usr/local/bin/monitor-logins.sh

# Programmer l'exécution quotidienne
echo '0 6 * * * /usr/local/bin/monitor-logins.sh' | sudo tee -a /etc/crontab
```

**VALEUR PAR DÉFAUT :**

Journalisation basique des connexions

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

## 7.0 — AUTHENTIFICATION PAM

### 7.1.1 *Configurer la politique de complexité des mots de passe avec pam_pwquality*

**MITRE ATT&CK :** T1110.001 (Brute Force: Password Guessing)

**DESCRIPTION :**

Le module pam_pwquality doit être configuré pour imposer des mots de passe complexes et résistants aux attaques. Cette politique doit équilibrer sécurité et utilisabilité pour encourager l'adoption de mots de passe forts.

```
grep pam_pwquality /etc/pam.d/common-password
cat /etc/security/pwquality.conf | grep -v '^#' | grep -v '^$'
```

```
# Installer pam_pwquality si nécessaire
sudo apt update && sudo apt install libpam-pwquality

# Configurer pam_pwquality dans common-password
sudo sed -i 's/^password.*pam_unix.so.*/password requisite pam_pwquality.so retry=3
password [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass sha512/' /etc/pam.d/common-password

# Configurer la politique de complexité
sudo tee /etc/security/pwquality.conf << 'EOF'
# Politique de complexité des mots de passe
minlen = 12
minclass = 3
maxrepeat = 2
dcredit = -1
ucredit = -1
lcredit = -1
ocredit = -1
difok = 3
gecoscheck = 1
badwords = password 123456 qwerty admin root
dictcheck = 1
usercheck = 1
enforcing = 1
EOF
```

**VALEUR PAR DÉFAUT :**

Politique de complexité minimale

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 7.1.2 *Configurer l'historique des mots de passe avec pam_pwhistory*

**MITRE ATT&CK :** T1110 (Brute Force)

**DESCRIPTION :**

Le module pam_pwhistory doit empêcher la réutilisation des anciens mots de passe pour éviter les cycles de mots de passe faibles. Un historique de 12-24 mots de passe précédents doit être maintenu.

```
grep pam_pwhistory /etc/pam.d/common-password
ls -la /etc/security/opasswd
```

```
# Configurer pam_pwhistory
sudo sed -i '/pam_pwquality.so/a password required pam_pwhistory.so remember=12 use_authtok' /etc/pam.d/common-password

# Créer le fichier d'historique avec les bonnes permissions
sudo touch /etc/security/opasswd
sudo chmod 600 /etc/security/opasswd
sudo chown root:root /etc/security/opasswd
```

**VALEUR PAR DÉFAUT :**

Pas d'historique de mots de passe configuré

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 7.2.1 *Configurer les délais de verrouillage avec pam_faillock*

**MITRE ATT&CK :** T1110 (Brute Force)

**DESCRIPTION :**

Le module pam_faillock doit être configuré pour verrouiller temporairement les comptes après plusieurs tentatives d'authentification échouées. Cette protection est essentielle contre les attaques par brute force.

```
grep pam_faillock /etc/pam.d/common-auth
grep pam_faillock /etc/pam.d/common-account
cat /etc/security/faillock.conf
```

```
# Configuration avancée de faillock
sudo tee /etc/security/faillock.conf << 'EOF'
# Configuration détaillée du verrouillage de comptes
audit
silent
no_log_info
local_users_only
deny = 5
fail_interval = 900
unlock_time = 900
even_deny_root
root_unlock_time = 300
admin_group = wheel
EOF

# Vérifier la configuration dans PAM
grep -q 'pam_faillock.so preauth' /etc/pam.d/common-auth ||     sudo sed -i '/^auth.*pam_unix.so/i auth required pam_faillock.so pr
```

**VALEUR PAR DÉFAUT :**

Pas de verrouillage automatique configuré

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 7.2.2 *Configurer pam_tally2 comme protection supplémentaire*

**MITRE ATT&CK :** T1110 (Brute Force)

**DESCRIPTION :**

En complément de pam_faillock, pam_tally2 peut fournir une protection additionnelle contre les attaques par brute force avec des fonctionnalités de comptage et de reset des tentatives.

```
grep pam_tally2 /etc/pam.d/common-auth 2>/dev/null
grep pam_tally2 /etc/pam.d/common-account 2>/dev/null
```

```
# Note: pam_tally2 est dépréciée, utiliser pam_faillock à la place
# Cette configuration est montrée pour la compatibilité legacy

# Si pam_tally2 doit être utilisée (non recommandé)
# sudo sed -i '/^auth.*pam_unix.so/i auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900' /etc/pam.d/common-
# sudo sed -i '/^account.*pam_unix.so/i account required pam_tally2.so' /etc/pam.d/common-account

echo "RECOMMANDATION: Utiliser pam_faillock au lieu de pam_tally2"
```

**VALEUR PAR DÉFAUT :**

pam_tally2 non configuré (dépréciée)

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 7.3.1 *Configurer les limites de ressources avec pam_limits*

**MITRE ATT&CK :** T1499 (Endpoint Denial of Service)

**DESCRIPTION :**

Le module pam_limits doit être configuré pour prévenir les attaques de déni de service en limitant les ressources système utilisables par chaque utilisateur ou groupe.

```
grep pam_limits /etc/pam.d/common-session
cat /etc/security/limits.conf | grep -v '^#' | grep -v '^$'
ls -la /etc/security/limits.d/
```

```
# Activer pam_limits dans PAM
grep -q 'pam_limits.so' /etc/pam.d/common-session ||     echo 'session required pam_limits.so' | sudo tee -a /etc/pam.d/common-sess

# Configurer les limites de ressources
sudo tee /etc/security/limits.d/90-security.conf << 'EOF'
# Limites de sécurité pour prévenir les attaques DoS

# Limites pour les utilisateurs normaux
*               soft    nproc           1024
*               hard    nproc           2048
*               soft    nofile          1024
*               hard    nofile          4096
*               soft    fsize           102400
*               hard    fsize           204800
*               soft    cpu             60
*               hard    cpu             120

# Limites spécifiques pour root
root            soft    nproc           unlimited
root            hard    nproc           unlimited
root            soft    nofile          unlimited
root            hard    nofile          unlimited

# Limites pour les services système
@users          hard    core            0
@users          soft    maxlogins       4
EOF
```

**VALEUR PAR DÉFAUT :**

Limites système par défaut généralement permissives

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 7.4.1 *Configurer pam_wheel pour restreindre l'accès su*

**MITRE ATT&CK :** T1548.003 (Abuse Elevation Control Mechanism: Sudo and Sudo Caching)

**DESCRIPTION :**

Le module pam_wheel doit être configuré pour restreindre l'utilisation de la commande su aux seuls membres du groupe wheel, réduisant ainsi les risques d'élévation de privilèges non autorisée.

```
grep pam_wheel /etc/pam.d/su
getent group wheel
id root | grep wheel
```

```
# Créer le groupe wheel s'il n'existe pas
sudo groupadd wheel 2>/dev/null || echo "Groupe wheel existe déjà"

# Ajouter root au groupe wheel
sudo usermod -aG wheel root

# Configurer pam_wheel dans su
sudo sed -i 's/^#.*auth.*required.*pam_wheel.so.*/auth required pam_wheel.so use_uid/' /etc/pam.d/su

# Ou ajouter la ligne si elle n'existe pas
grep -q 'pam_wheel.so' /etc/pam.d/su ||     sudo sed -i '/^auth.*sufficient.*pam_rootok.so/a auth required pam_wheel.so use_uid' /e
```

**VALEUR PAR DÉFAUT :**

su accessible à tous les utilisateurs

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐N/A

**Commentaire de l'auditeur :** _____

### 7.4.2 *Configurer les restrictions de temps avec pam_time*

**MITRE ATT&CK :** T1078 (Valid Accounts)

**DESCRIPTION :**

Le module pam_time peut être utilisé pour restreindre les connexions selon des plages horaires spécifiques, ajoutant une couche de sécurité temporelle aux accès utilisateurs.

```
grep pam_time /etc/pam.d/common-account
cat /etc/security/time.conf | grep -v '^#' | grep -v '^$'
```

```
# Activer pam_time
echo 'account required pam_time.so' | sudo tee -a /etc/pam.d/common-account

# Configurer les restrictions temporelles
sudo tee /etc/security/time.conf << 'EOF'
# Restrictions temporelles pour les connexions

# Exemple: utilisateurs normaux seulement en heures de bureau
services:*;*;users;Mo0800-1800|Tu0800-1800|We0800-1800|Th0800-1800|Fr0800-1800

# Admin toujours autorisé (exemple)
# services:*;*;wheel;Al0000-2400

# SSH restreint la nuit pour les utilisateurs normaux
EOF
```

**VALEUR PAR DÉFAUT :**

Aucune restriction temporelle configurée

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 7.5.1 *Configurer l'authentification à deux facteurs avec pam_google_authenticator*

**MITRE ATT&CK :** T1078 (Valid Accounts)

**DESCRIPTION :**

L'authentification à deux facteurs (2FA) avec Google Authenticator ajoute une couche de sécurité supplémentaire en requérant un code temporaire en plus du mot de passe traditionnel.

```
dpkg -l | grep google-authenticator
grep pam_google_authenticator /etc/pam.d/sshd 2>/dev/null
```

```
# Installer Google Authenticator PAM
sudo apt update && sudo apt install libpam-google-authenticator

# Configurer pour SSH (optionnel, nécessite configuration utilisateur)
# sudo sed -i 's/^@include common-auth/auth required pam_google_authenticator.so
@include common-auth/' /etc/pam.d/sshd

# Configuration dans sshd_config (si activé)
# sudo sed -i 's/^ChallengeResponseAuthentication no/ChallengeResponseAuthentication yes/' /etc/ssh/sshd_config
# sudo sed -i 's/^AuthenticationMethods.*/AuthenticationMethods publickey,keyboard-interactive/' /etc/ssh/sshd_config

echo "CONFIGURATION MANUELLE REQUISE:"
echo "1. Chaque utilisateur doit exécuter: google-authenticator"
echo "2. Configurer l'application mobile"
echo "3. Ajuster /etc/pam.d/sshd selon les besoins"
```

**VALEUR PAR DÉFAUT :**

2FA non configuré

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

### 7.6.1 *Auditer et nettoyer la configuration PAM*

**MITRE ATT&CK :** T1556.003 (Modify Authentication Process: Pluggable Authentication Modules)

**DESCRIPTION :**

La configuration PAM doit être régulièrement auditée pour identifier les modules inutiles, les configurations obsolètes ou les vulnérabilités potentielles. Une documentation des modules actifs doit être maintenue.

```
find /etc/pam.d -type f -exec grep -l 'auth\|account\|password\|session' {} \;
ls -la /etc/pam.d/ | wc -l
pam-auth-update --package
```

```
# Script d'audit de la configuration PAM
sudo tee /usr/local/bin/audit-pam.sh << 'EOF'
echo "=== AUDIT PAM - $(date) ==="

echo "
1. Fichiers de configuration PAM:"
ls -la /etc/pam.d/ | grep -v total

echo "
2. Modules PAM utilisés:"
grep -h '^[^#]' /etc/pam.d/* | grep -E 'pam_[a-z_]+\.so' |     sed 's/.*pam_\([a-z_]*\)\.so.*/pam_/' | sort | uniq -c | sort -nr

echo "
3. Modules potentiellement dangereux:"
grep -r 'pam_permit\|pam_rootok' /etc/pam.d/ 2>/dev/null || echo "Aucun module dangereux détecté"

echo "
4. Configuration de sécurité critique:"
echo "  - Faillock:"
grep -c pam_faillock /etc/pam.d/common-auth
echo "  - Pwquality:"
grep -c pam_pwquality /etc/pam.d/common-password
echo "  - Limits:"
grep -c pam_limits /etc/pam.d/common-session

echo "
5. Fichiers de configuration modifiés récemment:"
find /etc/pam.d -type f -mtime -7 -ls
EOF

sudo chmod +x /usr/local/bin/audit-pam.sh

# Exécuter l'audit
sudo /usr/local/bin/audit-pam.sh
```

**VALEUR PAR DÉFAUT :**

Configuration PAM de base Ubuntu

**Résultat :** ☐ ✅ Conforme ☐ ❌ Non conforme ☐ ⚠️ Partiel ☐ N/A

**Commentaire de l'auditeur :** _____

# Section 8 — POLITIQUES DE MOT DE PASSE

## 8.0 — POLITIQUES DE MOT DE PASSE

### 8.1.1 *Configurer la longueur minimale des mots de passe*

**MITRE ATT&CK :** T1110.001 (Brute Force: Password Guessing)

**DESCRIPTION :**

Une longueur minimale de mot de passe doit être imposée pour résister aux attaques par force brute. La longueur recommandée est de 12 caractères minimum pour équilibrer sécurité et utilisabilité.

```
grep minlen /etc/security/pwquality.conf
grep PASS_MIN_LEN /etc/login.defs
```

```
sudo sed -i 's/^# minlen = 8/minlen = 12/' /etc/security/pwquality.conf
sudo sed -i 's/^PASS_MIN_LEN.*/PASS_MIN_LEN 12/' /etc/login.defs
```

**VALEUR PAR DÉFAUT :**

8 caractères

### 8.1.2 *Imposer la complexité des mots de passe*

**MITRE ATT&CK :** T1110.001 (Brute Force: Password Guessing)

**DESCRIPTION :**

Les mots de passe doivent contenir différents types de caractères pour augmenter leur entropie et résister aux attaques par dictionnaire.

```
grep -E '^(d|u|l|o)credit' /etc/security/pwquality.conf
```

```
sudo tee -a /etc/security/pwquality.conf << 'EOF'
dcredit = -1
ucredit = -1
lcredit = -1
ocredit = -1
minclass = 3
EOF
```

**VALEUR PAR DÉFAUT :**

Complexité basique

### 8.2.1 *Configurer l'historique des mots de passe*

**MITRE ATT&CK :** T1110 (Brute Force)

**DESCRIPTION :**

Empêcher la réutilisation des 12 derniers mots de passe pour éviter les cycles de mots de passe faibles.

```
grep remember /etc/pam.d/common-password
```

```
sudo sed -i '/pam_unix.so/s/$/ remember=12/' /etc/pam.d/common-password
```

**VALEUR PAR DÉFAUT :**

Pas d'historique

### 8.3.1 *Bloquer les mots de passe communs*

**MITRE ATT&CK :** T1110.001 (Brute Force: Password Guessing)

**DESCRIPTION :**

Empêcher l'utilisation de mots de passe couramment utilisés et facilement devinables.

```
grep dictcheck /etc/security/pwquality.conf
grep badwords /etc/security/pwquality.conf
```

```
sudo sed -i 's/# dictcheck = 1/dictcheck = 1/' /etc/security/pwquality.conf
echo 'badwords = password 123456 qwerty admin root' | sudo tee -a /etc/security/pwquality.conf
```

**VALEUR PAR DÉFAUT :**

Vérification dictionnaire désactivée

## 9.0 — PERMISSIONS FICHIERS

### 9.1.1 *Vérifier les permissions des fichiers système critiques*

**MITRE ATT&CK :** T1078 (Valid Accounts)

**DESCRIPTION :**

Les fichiers système critiques doivent avoir des permissions appropriées pour empêcher les modifications non autorisées.

```
stat /etc/passwd /etc/shadow /etc/group /etc/gshadow
```

```
sudo chmod 644 /etc/passwd
sudo chmod 640 /etc/shadow
sudo chmod 644 /etc/group
sudo chmod 640 /etc/gshadow
sudo chown root:root /etc/passwd /etc/group
sudo chown root:shadow /etc/shadow /etc/gshadow
```

**VALEUR PAR DÉFAUT :**

Permissions correctes sur installation propre

### 9.1.2 *Auditer les fichiers avec permissions SUID/SGID*

**MITRE ATT&CK :** T1548.001 (Abuse Elevation Control Mechanism: Setuid and Setgid)

**DESCRIPTION :**

Les fichiers SUID/SGID doivent être régulièrement auditées car ils peuvent être exploités pour l'élévation de privilèges.

```
find / -perm -4000 -type f 2>/dev/null | head -20
find / -perm -2000 -type f 2>/dev/null | head -20
```

```
# Créer une liste de référence des fichiers SUID/SGID légitimes
find / -perm -4000 -o -perm -2000 -type f 2>/dev/null | sort > /var/log/suid-sgid-files.baseline
# Comparer régulièrement avec cette baseline
```

**VALEUR PAR DÉFAUT :**

Fichiers SUID/SGID système standards

### 9.2.1 *Sécuriser les répertoires world-writable*

**MITRE ATT&CK :** T1222 (File and Directory Permissions Modification)

**DESCRIPTION :**

Les répertoires world-writable doivent avoir le sticky bit pour empêcher les utilisateurs de supprimer les fichiers d'autres utilisateurs.

```
find / -type d -perm -002 ! -perm -1000 2>/dev/null
```

```
find / -type d -perm -002 ! -perm -1000 -exec chmod +t {} \; 2>/dev/null
```

**VALEUR PAR DÉFAUT :**

/tmp et /var/tmp ont généralement le sticky bit

## 10.0 — INTÉGRITÉ SYSTÈME

### 10.1.1 *Installer et configurer AIDE*

**MITRE ATT&CK :** T1565 (Data Manipulation)

**DESCRIPTION :**

AIDE (Advanced Intrusion Detection Environment) doit être installé pour surveiller l'intégrité des fichiers système et détecter les modifications non autorisées.

```
dpkg -l aide
ls -la /var/lib/aide/
```

```
sudo apt update && sudo apt install aide
sudo aideinit
sudo mv /var/lib/aide/aide.db.new /var/lib/aide/aide.db
```

**VALEUR PAR DÉFAUT :**

AIDE non installé par défaut

### 10.1.2 *Configurer la vérification régulière d'intégrité*

**MITRE ATT&CK :** T1070 (Indicator Removal on Host)

**DESCRIPTION :**

Des vérifications automatiques d'intégrité doivent être programmées pour détecter rapidement les compromissions système.

```
crontab -l | grep aide
cat /etc/cron.d/aide 2>/dev/null
```

```
echo '0 5 * * * /usr/bin/aide --check' | sudo tee /etc/cron.d/aide-check
sudo chmod 644 /etc/cron.d/aide-check
```

**VALEUR PAR DÉFAUT :**

Pas de vérification automatique configurée

## 11.0 — SSH

### 11.1.1 *Configurer SSH Protocol 2 uniquement*

**MITRE ATT&CK :** T1021.004 (Remote Services: SSH)

**DESCRIPTION :**

SSH doit être configuré pour utiliser uniquement le protocole version 2, qui est plus sécurisé que la version 1.

```
sshd -T | grep protocol
grep -i protocol /etc/ssh/sshd_config
```

```
sudo sed -i 's/^#Protocol.*/Protocol 2/' /etc/ssh/sshd_config
sudo systemctl reload sshd
```

**VALEUR PAR DÉFAUT :**

Protocol 2 par défaut sur Ubuntu 24.04

### 11.1.2 *Désactiver l'authentification par mot de passe root SSH*

**MITRE ATT&CK :** T1078.003 (Valid Accounts: Local Accounts)

**DESCRIPTION :**

L'authentification SSH directe en tant que root doit être désactivée pour forcer l'utilisation de comptes nominatifs et sudo.

```
sshd -T | grep permitrootlogin
grep -i PermitRootLogin /etc/ssh/sshd_config
```

```
sudo sed -i 's/^#PermitRootLogin.*/PermitRootLogin no/' /etc/ssh/sshd_config
sudo sed -i 's/^PermitRootLogin.*/PermitRootLogin no/' /etc/ssh/sshd_config
sudo systemctl reload sshd
```

**VALEUR PAR DÉFAUT :**

PermitRootLogin prohibit-password

### 11.2.1 *Configurer des algorithmes de chiffrement forts*

**MITRE ATT&CK :** T1021.004 (Remote Services: SSH)

**DESCRIPTION :**

SSH doit être configuré pour utiliser uniquement des algorithmes de chiffrement, MAC et échange de clés cryptographiquement sûrs.

```
sshd -T | grep -E 'ciphers|macs|kexalgorithms'
```

```
sudo tee -a /etc/ssh/sshd_config << 'EOF'
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
MACs hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512
KexAlgorithms curve25519-sha256@libssh.org,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512
EOF
sudo systemctl reload sshd
```

**VALEUR PAR DÉFAUT :**

Configuration par défaut incluant algorithmes faibles

### 11.3.1 *Configurer l'authentification par clés SSH uniquement*

**MITRE ATT&CK :** T1021.004 (Remote Services: SSH)

**DESCRIPTION :**

L'authentification par clés SSH est plus sécurisée que les mots de passe et doit être privilégiée ou imposée.

```
sshd -T | grep passwordauthentication
sshd -T | grep pubkeyauthentication
```

```
sudo sed -i 's/^#PasswordAuthentication.*/PasswordAuthentication no/' /etc/ssh/sshd_config
sudo sed -i 's/^#PubkeyAuthentication.*/PubkeyAuthentication yes/' /etc/ssh/sshd_config
sudo systemctl reload sshd
```

**VALEUR PAR DÉFAUT :**

Authentification par mot de passe activée

### 11.4.1 *Limiter les utilisateurs et groupes SSH*

**MITRE ATT&CK :** T1078 (Valid Accounts)

**DESCRIPTION :**

L'accès SSH doit être limité aux seuls utilisateurs et groupes autorisés pour réduire la surface d'attaque.

```
sshd -T | grep -E 'allowusers|allowgroups|denyusers|denygroups'
```

```
echo 'AllowGroups sshusers sudo' | sudo tee -a /etc/ssh/sshd_config
sudo groupadd sshusers 2>/dev/null
sudo systemctl reload sshd
```

**VALEUR PAR DÉFAUT :**

Tous les utilisateurs autorisés

### 11.5.1 *Configurer des timeouts et limites de connexion SSH*

**MITRE ATT&CK :** T1021.004 (Remote Services: SSH)

**DESCRIPTION :**

Des timeouts et limites doivent être configurés pour prévenir les connexions SSH inutilisées et les attaques par brute force.

```
sshd -T | grep -E 'clientaliveinterval|clientalivecountmax|maxauthtries|maxstartups'
```

```
sudo tee -a /etc/ssh/sshd_config << 'EOF'
ClientAliveInterval 300
ClientAliveCountMax 3
MaxAuthTries 3
MaxStartups 10:30:60
LoginGraceTime 60
EOF
sudo systemctl reload sshd
```

**VALEUR PAR DÉFAUT :**

Timeouts par défaut permissifs

## 12.0 — SUDO & ÉLÉVATION DE PRIVILÈGES

### 12.1.1 *Configurer sudoers avec visudo uniquement*

**MITRE ATT&CK :** T1548.003 (Abuse Elevation Control Mechanism: Sudo and Sudo Caching)

**DESCRIPTION :**

Le fichier sudoers doit être édité uniquement avec visudo pour éviter les erreurs de syntaxe qui pourraient verrouiller l'accès administrateur.

```
sudo visudo -c
ls -la /etc/sudoers*
```

```
# Toujours utiliser visudo pour éditer
sudo visudo
# Vérifier la syntaxe
sudo visudo -c
```

**VALEUR PAR DÉFAUT :**

Configuration sudoers basique correcte

### 12.1.2 *Configurer le timeout sudo approprié*

**MITRE ATT&CK :** T1548.003 (Abuse Elevation Control Mechanism: Sudo and Sudo Caching)

**DESCRIPTION :**

Le timeout sudo doit être configuré pour équilibrer sécurité et utilisabilité, généralement entre 5-15 minutes.

```
sudo grep -E 'timestamp_timeout|passwd_timeout' /etc/sudoers /etc/sudoers.d/*
```

```
echo 'Defaults timestamp_timeout=10' | sudo tee /etc/sudoers.d/timeout
echo 'Defaults passwd_timeout=1' | sudo tee -a /etc/sudoers.d/timeout
```

**VALEUR PAR DÉFAUT :**

15 minutes par défaut

### 12.2.1 *Activer la journalisation sudo*

**MITRE ATT&CK :** T1548.003 (Abuse Elevation Control Mechanism: Sudo and Sudo Caching)

**DESCRIPTION :**

Toutes les commandes sudo doivent être journalisées pour l'audit de sécurité et la traçabilité des actions administratives.

```
grep -E 'log_input|log_output|logfile' /etc/sudoers /etc/sudoers.d/* 2>/dev/null
```

```
sudo tee /etc/sudoers.d/logging << 'EOF'
Defaults logfile=/var/log/sudo.log
Defaults log_input, log_output
Defaults iolog_dir=/var/log/sudo-io
EOF
sudo mkdir -p /var/log/sudo-io
```

**VALEUR PAR DÉFAUT :**

Journalisation basique via syslog

## 13.0 — APPARMOR & MAC

### 13.1.1 *Vérifier qu'AppArmor est installé et activé*

**MITRE ATT&CK :** T1055 (Process Injection)

**DESCRIPTION :**

AppArmor doit être installé et activé pour fournir un contrôle d'accès obligatoire (MAC) et limiter les capacités des processus.

```
dpkg -l apparmor
systemctl is-active apparmor
aa-status
```

```
sudo apt update && sudo apt install apparmor apparmor-utils
sudo systemctl enable apparmor
sudo systemctl start apparmor
```

**VALEUR PAR DÉFAUT :**

AppArmor installé et activé sur Ubuntu 24.04

### 13.1.2 *Configurer les profils AppArmor en mode enforce*

**MITRE ATT&CK :** T1055 (Process Injection)

**DESCRIPTION :**

Les profils AppArmor doivent être en mode enforce pour bloquer effectivement les actions non autorisées, pas seulement les journaliser.

```
aa-status | grep 'profiles are in enforce mode'
aa-status | grep 'profiles are in complain mode'
```

```
# Passer les profils en mode enforce
sudo aa-enforce /etc/apparmor.d/*
# Ou pour des profils spécifiques
# sudo aa-enforce /etc/apparmor.d/usr.bin.firefox
```

**VALEUR PAR DÉFAUT :**

Profils en mode enforce par défaut

## 14.0 — CONTENEURS & VIRTUALISATION

### 14.1.1 *Sécuriser Docker si installé*

**MITRE ATT&CK :** T1611 (Escape to Host)

**DESCRIPTION :**

Si Docker est installé, il doit être sécurisé selon les meilleures pratiques pour éviter l'évasion de conteneurs.

```
systemctl is-active docker 2>/dev/null
docker version 2>/dev/null
```

```
# Sécuriser le démon Docker
sudo tee /etc/docker/daemon.json << 'EOF'
{
  "icc": false,
  "userns-remap": "default",
  "live-restore": true,
  "userland-proxy": false,
  "no-new-privileges": true
}
EOF
sudo systemctl reload docker
```

**VALEUR PAR DÉFAUT :**

Docker non installé par défaut

## 15.0 — MISES À JOUR & PATCHS

### 15.1.1 *Configurer les mises à jour automatiques de sécurité*

**MITRE ATT&CK :** T1068 (Exploitation for Privilege Escalation)

**DESCRIPTION :**

Les mises à jour de sécurité doivent être installées automatiquement pour corriger rapidement les vulnérabilités connues.

```
dpkg -l unattended-upgrades
cat /etc/apt/apt.conf.d/20auto-upgrades
```

```
sudo apt update && sudo apt install unattended-upgrades
sudo dpkg-reconfigure -plow unattended-upgrades
echo 'Unattended-Upgrade::Automatic-Reboot "true";' | sudo tee -a /etc/apt/apt.conf.d/50unattended-upgrades
```

**VALEUR PAR DÉFAUT :**

Mises à jour manuelles

### 15.2.1 *Vérifier l'intégrité des paquets APT*

**MITRE ATT&CK :** T1195 (Supply Chain Compromise)

**DESCRIPTION :**

L'intégrité des paquets APT doit être vérifiée via les signatures GPG pour éviter l'installation de logiciels compromis.

```
apt-config dump | grep -E 'APT::Get::(AllowUnauthenticated|AllowDowngradeToInsecureRepositories)'
```

```
echo 'APT::Get::AllowUnauthenticated "false";' | sudo tee /etc/apt/apt.conf.d/99security
```

**VALEUR PAR DÉFAUT :**

Vérification activée par défaut

## 16.0 — CRYPTOGRAPHIE & CHIFFREMENT

### 16.1.1 *Configurer des algorithmes cryptographiques forts système*

**MITRE ATT&CK :** T1600 (Weaken Encryption)

**DESCRIPTION :**

Le système doit être configuré pour utiliser uniquement des algorithmes cryptographiques approuvés et sûrs.

```
update-crypto-policies --show
grep -r 'LEGACY' /etc/crypto-policies/ 2>/dev/null
```

```
# Sur Ubuntu, configurer via system-wide crypto policies si disponible
# Ou configurer individuellement chaque service
sudo sed -i 's/DEFAULT@SECLEVEL=1/DEFAULT@SECLEVEL=2/' /etc/ssl/openssl.cnf
```

**VALEUR PAR DÉFAUT :**

Niveau de sécurité standard

## 17.0 — SÉCURITÉ KERNEL

### 17.1.1 *Configurer les paramètres kernel de sécurité*

**MITRE ATT&CK :** T1068 (Exploitation for Privilege Escalation)

**DESCRIPTION :**

Les paramètres du noyau doivent être durcis pour améliorer la sécurité système et prévenir certaines classes d'attaques.

```
sysctl kernel.dmesg_restrict
sysctl kernel.kptr_restrict
sysctl kernel.yama.ptrace_scope
```

```
sudo tee /etc/sysctl.d/99-security.conf << 'EOF'
kernel.dmesg_restrict = 1
kernel.kptr_restrict = 2
kernel.yama.ptrace_scope = 1
kernel.kexec_load_disabled = 1
net.core.bpf_jit_harden = 2
EOF
sudo sysctl -p /etc/sysctl.d/99-security.conf
```

**VALEUR PAR DÉFAUT :**

Paramètres par défaut moins restrictifs

## 18.0 — CONFORMITÉ & GOUVERNANCE

### 18.1.1 *Documenter la configuration de sécurité*

**MITRE ATT&CK :** N/A

**DESCRIPTION :**

Toute la configuration de sécurité doit être documentée pour faciliter la maintenance, l'audit et la conformité réglementaire.

```
ls -la /etc/security/docs/ 2>/dev/null
find /etc -name "*.conf" -mtime -30 | wc -l
```

```
sudo mkdir -p /etc/security/docs
sudo tee /etc/security/docs/README.md << 'EOF'
# Documentation de Sécurité Ubuntu 24.04

## Configurations appliquées
- Date: $(date)
- Auditeur: [Nom]
- Référentiel: CIS Ubuntu 24.04 LTS

## Modifications principales
[À documenter]
EOF
```

**VALEUR PAR DÉFAUT :**

Documentation minimale

### 18.2.1 *Planifier les audits de sécurité réguliers*

**MITRE ATT&CK :** N/A

**DESCRIPTION :**

Des audits de sécurité réguliers doivent être planifiés pour maintenir le niveau de sécurité et détecter les dérives de configuration.

```
crontab -l | grep -E 'audit|security|check'
ls -la /etc/cron.d/ | grep security
```

```
sudo tee /usr/local/bin/security-audit.sh << 'EOF'
# Audit de sécurité automatique
DATE=$(date +%Y%m%d-%H%M%S)
LOGFILE="/var/log/security-audit-$DATE.log"

echo "=== AUDIT SÉCURITÉ - $DATE ===" > $LOGFILE
echo "1. Vérification des comptes:" >> $LOGFILE
awk -F: '($3 >= 1000) {print $1}' /etc/passwd >> $LOGFILE

echo "2. Processus en écoute:" >> $LOGFILE
ss -tuln >> $LOGFILE

echo "3. Dernières connexions:" >> $LOGFILE
last -n 10 >> $LOGFILE
EOF

sudo chmod +x /usr/local/bin/security-audit.sh
echo '0 2 * * 1 /usr/local/bin/security-audit.sh' | sudo tee /etc/cron.d/security-audit
```

**VALEUR PAR DÉFAUT :**

Pas d'audit automatique configuré

## RÉCAPITULATIF PAR SECTION

## RÉSUMÉ EXÉCUTIF

### Score de Conformité Global

- **Contrôles Critiques (🔴)** : 51/285 (18%) - Sécurité minimale requise
- **Contrôles Importants (🟠)** : 138/285 (48%) - Durcissement recommandé
- **Contrôles Recommandés (🟡)** : 82/285 (29%) - Optimisation sécuritaire
- **Contrôles Optionnels (🟢)** : 14/285 (5%) - Amélioration continue

### Top 3 des Risques Critiques

1. **Gestion des Comptes et Authentification** - Impact: Accès administrateur non autorisé
2. **Configuration Réseau et Pare-feu** - Impact: Intrusion réseau et exfiltration
3. **Journalisation et Détection** - Impact: Activités malveillantes persistantes

## MAPPINGS DE CONFORMITÉ

### NIST SP 800-53 Rev5

- **AC (Access Control)** : S6, S7, S11, S12
- **AU (Audit)** : S5
- **SC (System Protection)** : S3, S4, S11, S16, S17
- **SI (System Integrity)** : S10, S15, S17

### ISO 27001:2022

- **A.9 - Contrôle d'accès** : S6, S7, S11, S12
- **A.12 - Sécurité d'exploitation** : S2, S3, S4, S15
- **A.18 - Conformité** : S5, S18

### MITRE ATT&CK Coverage

- **Initial Access** : T1078, T1133 → S6, S7, S11
- **Privilege Escalation** : T1068, T1548 → S6, S9, S12, S17
- **Defense Evasion** : T1055, T1562 → S5, S10, S13

## Annexe : Checklist (177 controles)

| # | Recommandation | Niveau | Oui | Non | N/A |
|---|---|---|---|---|---|
| **Section 1 — CONFIGURATION INITIALE ET SYSTÈME DE FICHIERS** | | | | | |
| **1.1.1** | Désactiver le montage du système de fichiers cramfs | ● | ☐ | ☐ | ☐ |
| **1.1.2** | Désactiver le montage du système de fichiers squashfs | ● | ☐ | ☐ | ☐ |
| **1.1.3** | Désactiver le montage du système de fichiers udf | ● | ☐ | ☐ | ☐ |
| **1.1.4** | Désactiver le montage du système de fichiers freevxfs | ● | ☐ | ☐ | ☐ |
| **1.1.5** | Désactiver le montage du système de fichiers jffs2 | ● | ☐ | ☐ | ☐ |
| **1.1.6** | Désactiver le montage du système de fichiers hfs | ● | ☐ | ☐ | ☐ |
| **1.1.7** | Désactiver le montage du système de fichiers hfsplus | ● | ☐ | ☐ | ☐ |
| **1.1.8** | Désactiver le montage du système de fichiers usb-storage | ● | ☐ | ☐ | ☐ |
| **1.2.1** | Vérifier l'existence d'une partition séparée pour /tmp | ● | ☐ | ☐ | ☐ |
| **1.2.2** | Vérifier les options nodev, nosuid, noexec sur /tmp | ● | ☐ | ☐ | ☐ |
| **1.2.3** | Vérifier l'existence d'une partition séparée pour /var | ● | ☐ | ☐ | ☐ |
| **1.2.4** | Vérifier l'existence d'une partition séparée pour /var/tmp | ● | ☐ | ☐ | ☐ |
| **1.2.5** | Vérifier l'existence d'une partition séparée pour /var/log | ● | ☐ | ☐ | ☐ |
| **1.2.6** | Vérifier l'existence d'une partition séparée pour /var/log/audit | ● | ☐ | ☐ | ☐ |
| **1.2.7** | Vérifier l'existence d'une partition séparée pour /home | ● | ☐ | ☐ | ☐ |
| **1.2.8** | Vérifier les options nodev, nosuid sur /home | ● | ☐ | ☐ | ☐ |
| **1.2.9** | Vérifier les options nodev, nosuid, noexec sur /dev/shm | ● | ☐ | ☐ | ☐ |
| **1.3.1** | Vérifier que le mot de passe du chargeur de démarrage GRUB est configuré | ● | ☐ | ☐ | ☐ |
| **1.3.2** | Vérifier les permissions du fichier de configuration GRUB | ● | ☐ | ☐ | ☐ |
| **1.3.3** | Vérifier que l'authentification est requise pour le mode mono-utilisateur (single user) | ● | ☐ | ☐ | ☐ |
| **1.3.4** | Vérifier que Secure Boot est activé (si UEFI) | ● | ☐ | ☐ | ☐ |
| **1.4.1** | Vérifier que AppArmor est installé | ● | ☐ | ☐ | ☐ |
| **1.4.2** | Vérifier que AppArmor est activé dans la configuration du chargeur de démarrage | ● | ☐ | ☐ | ☐ |
| **1.4.3** | Vérifier que tous les profils AppArmor sont en mode enforce ou complain | ● | ☐ | ☐ | ☐ |
| **1.4.4** | Vérifier qu'aucun profil AppArmor n'est déchargé (unconfined) | ● | ☐ | ☐ | ☐ |
| **1.5.1** | Vérifier que les mises à jour de sécurité sont installées | ● | ☐ | ☐ | ☐ |
| **1.5.2** | Vérifier que les dépôts de paquets sont configurés et authentifiés (GPG) | ● | ☐ | ☐ | ☐ |
| **1.5.3** | Vérifier que AIDE (Advanced Intrusion Detection Environment) est installé | ● | ☐ | ☐ | ☐ |
| **1.5.4** | Vérifier que la vérification d'intégrité AIDE est planifiée | ● | ☐ | ☐ | ☐ |
| **1.5.5** | Vérifier que les privilèges de core dump sont restreints | ● | ☐ | ☐ | ☐ |
| **1.5.6** | Vérifier que la randomisation de l'espace d'adressage (ASLR) est activée | ● | ☐ | ☐ | ☐ |
| **1.5.7** | Vérifier que le support de la fonctionnalité ptrace est restreint | ● | ☐ | ☐ | ☐ |
| **1.5.8** | Vérifier que la bannière d'avertissement pré-connexion est configurée (/etc/issue) | ● | ☐ | ☐ | ☐ |
| **1.5.9** | Vérifier que la bannière d'avertissement réseau est configurée (/etc/issue.net) | ● | ☐ | ☐ | ☐ |
| **1.5.10** | Vérifier les permissions du fichier /etc/motd | ● | ☐ | ☐ | ☐ |
| **1.5.11** | Vérifier les permissions du fichier /etc/issue | ● | ☐ | ☐ | ☐ |
| **1.5.12** | Vérifier les permissions du fichier /etc/issue.net | ● | ☐ | ☐ | ☐ |
| **1.5.13** | Vérifier que le gestionnaire d'affichage GDM est absent ou sécurisé | ● | ☐ | ☐ | ☐ |
| **Section 2 — SERVICES RÉSEAU ET DÉMONS** | | | | | |
| **2.1.1** | Vérifier que le service xinetd n'est pas installé | ● | ☐ | ☐ | ☐ |
| **2.1.2** | Vérifier que le service openbsd-inetd n'est pas installé | ● | ☐ | ☐ | ☐ |
| **2.1.3** | Vérifier que le service avahi-daemon n'est pas installé ou est désactivé | ● | ☐ | ☐ | ☐ |
| **2.1.4** | Vérifier que le service CUPS n'est pas installé (sauf si nécessaire) | ● | ☐ | ☐ | ☐ |
| **2.1.5** | Vérifier que le serveur DHCP n'est pas installé (sauf si requis) | ● | ☐ | ☐ | ☐ |
| **2.1.6** | Vérifier que le serveur LDAP (slapd) n'est pas installé (sauf si requis) | ● | ☐ | ☐ | ☐ |
| **2.1.7** | Vérifier que le serveur NFS n'est pas installé (sauf si requis) | ● | ☐ | ☐ | ☐ |
| **2.1.8** | Vérifier que rpcbind n'est pas installé ou est masqué | ● | ☐ | ☐ | ☐ |
| **2.1.9** | Vérifier que le serveur DNS (bind9) n'est pas installé (sauf si requis) | ● | ☐ | ☐ | ☐ |
| **2.1.10** | Vérifier que le serveur FTP (vsftpd) n'est pas installé | ● | ☐ | ☐ | ☐ |
| **2.1.11** | Vérifier que le serveur HTTP (Apache/Nginx) n'est pas installé (sauf si requis) | ● | ☐ | ☐ | ☐ |
| **2.1.12** | Vérifier que le serveur Samba n'est pas installé (sauf si requis) | ● | ☐ | ☐ | ☐ |
| **2.1.13** | Vérifier que le proxy Squid n'est pas installé (sauf si requis) | ● | ☐ | ☐ | ☐ |
| **2.1.14** | Vérifier que le serveur SNMP n'est pas installé (sauf si requis) | ● | ☐ | ☐ | ☐ |
| **2.1.15** | Vérifier que le serveur de messagerie est en mode local uniquement | ● | ☐ | ☐ | ☐ |

| # | Recommandation | Niveau | Oui | Non | N/A |
|---|---|---|---|---|---|
| **2.1.16** | Vérifier que rsync n'est pas installé ou est correctement configuré | ● | ☐ | ☐ | ☐ |
| **2.1.17** | Vérifier que le service NIS (ypserv) n'est pas installé | ● | ☐ | ☐ | ☐ |
| **2.1.18** | Vérifier que le client rsh n'est pas installé | ● | ☐ | ☐ | ☐ |
| **2.1.19** | Vérifier que le client talk n'est pas installé | ● | ☐ | ☐ | ☐ |
| **2.1.20** | Vérifier que le client telnet n'est pas installé | ● | ☐ | ☐ | ☐ |
| **2.1.21** | Vérifier que le client LDAP n'est pas installé (sauf si requis) | ● | ☐ | ☐ | ☐ |
| **2.1.22** | Vérifier que la synchronisation horaire (chrony ou systemd-timesyncd) est configurée | ● | ☐ | ☐ | ☐ |
| **2.1.23** | Vérifier que chrony/NTP est configuré avec des sources autorisées uniquement | ● | ☐ | ☐ | ☐ |
| **2.1.24** | Vérifier que chrony s'exécute en tant qu'utilisateur non privilégié | ● | ☐ | ☐ | ☐ |
| **2.1.25** | Vérifier que le client NFS n'est pas installé (sauf si requis) | ● | ☐ | ☐ | ☐ |
| **2.1.26** | Vérifier que le client Samba (smbclient/cifs-utils) n'est pas installé (sauf si requis) | ● | ☐ | ☐ | ☐ |
| **2.1.27** | Vérifier que le service dnsmasq n'est pas installé (sauf si requis) | ● | ☐ | ☐ | ☐ |
| **2.1.28** | Vérifier que le service de base de données (MySQL/PostgreSQL/MariaDB) est sécurisé ou absent | ● | ☐ | ☐ | ☐ |
| **2.1.29** | Vérifier qu'aucun service en écoute non autorisé n'est présent | ● | ☐ | ☐ | ☐ |
| **2.1.30** | Vérifier que le service snapd est désactivé (si les snaps ne sont pas utilisés) | ● | ☐ | ☐ | ☐ |
| **Section 3 — CONFIGURATION RÉSEAU ET PARE-FEU** | | | | | |
| **3.1.1** | Désactiver le transfert de paquets IPv4 (IP forwarding) | ● | ☐ | ☐ | ☐ |
| **3.1.2** | Désactiver le transfert de paquets IPv6 | ● | ☐ | ☐ | ☐ |
| **3.1.3** | Vérifier que les redirections ICMP ne sont pas acceptées (IPv4) | ● | ☐ | ☐ | ☐ |
| **3.1.4** | Vérifier que les redirections ICMP ne sont pas envoyées | ● | ☐ | ☐ | ☐ |
| **3.1.5** | Vérifier que le source routing est désactivé (IPv4) | ● | ☐ | ☐ | ☐ |
| **3.1.6** | Vérifier que le source routing est désactivé (IPv6) | ● | ☐ | ☐ | ☐ |
| **3.1.7** | Activer la validation de la source par chemin inverse (Reverse Path Filtering) | ● | ☐ | ☐ | ☐ |
| **3.1.8** | Activer la journalisation des paquets suspects (martians) | ● | ☐ | ☐ | ☐ |
| **3.1.9** | Activer les SYN cookies TCP | ● | ☐ | ☐ | ☐ |
| **3.1.10** | Désactiver les réponses ICMP Broadcast (Smurf protection) | ● | ☐ | ☐ | ☐ |
| **3.1.11** | Ignorer les messages ICMP bogus error responses | ● | ☐ | ☐ | ☐ |
| **3.1.12** | Désactiver les redirections ICMP sécurisées | ● | ☐ | ☐ | ☐ |
| **3.1.13** | Désactiver les redirections ICMP IPv6 | ● | ☐ | ☐ | ☐ |
| **3.1.14** | Désactiver les annonces de routeur IPv6 | ● | ☐ | ☐ | ☐ |
| **3.1.15** | Désactiver IPv6 si non utilisé | ● | ☐ | ☐ | ☐ |
| **3.2.1** | Vérifier que ufw (Uncomplicated Firewall) est installé | ● | ☐ | ☐ | ☐ |
| **3.2.2** | Vérifier que le service iptables-persistent n'est pas installé avec ufw | ● | ☐ | ☐ | ☐ |
| **3.2.3** | Vérifier que ufw est activé et en cours d'exécution | ● | ☐ | ☐ | ☐ |
| **3.2.4** | Vérifier que la politique par défaut de ufw refuse le trafic entrant | ● | ☐ | ☐ | ☐ |
| **3.2.5** | Vérifier que les règles ufw sont configurées pour les services autorisés | ● | ☐ | ☐ | ☐ |
| **3.2.6** | Vérifier que les règles de pare-feu pour le trafic de loopback sont configurées | ● | ☐ | ☐ | ☐ |
| **3.2.7** | Vérifier que la journalisation du pare-feu ufw est activée | ● | ☐ | ☐ | ☐ |
| **3.2.8** | Vérifier que nftables est installé comme backend de ufw | ● | ☐ | ☐ | ☐ |
| **3.2.9** | Désactiver le protocole DCCP | ● | ☐ | ☐ | ☐ |
| **3.2.10** | Désactiver le protocole SCTP | ● | ☐ | ☐ | ☐ |
| **3.2.11** | Désactiver le protocole RDS | ● | ☐ | ☐ | ☐ |
| **3.2.12** | Désactiver le protocole TIPC | ● | ☐ | ☐ | ☐ |
| **3.2.13** | Désactiver les interfaces sans fil (Wi-Fi) | ● | ☐ | ☐ | ☐ |
| **3.2.14** | Vérifier la configuration de TCP Wrappers (hosts.allow / hosts.deny) | ● | ☐ | ☐ | ☐ |
| **3.2.15** | Vérifier qu'aucune règle de pare-feu en double ou contradictoire n'existe | ● | ☐ | ☐ | ☐ |
| **Section 4 — PARE-FEU UFW/NFTABLES** | | | | | |
| **4.1.1** | Vérifier qu'UFW est installé et activé | ● | ☐ | ☐ | ☐ |
| **4.1.2** | Configurer la politique par défaut UFW (deny incoming, allow outgoing) | ● | ☐ | ☐ | ☐ |
| **4.1.3** | Autoriser uniquement les services réseau nécessaires dans UFW | ● | ☐ | ☐ | ☐ |
| **4.1.4** | Vérifier la journalisation UFW | ● | ☐ | ☐ | ☐ |
| **4.2.1** | Vérifier la configuration nftables comme backend | ● | ☐ | ☐ | ☐ |
| **4.2.2** | Configurer des règles de limitation de débit (rate limiting) | ● | ☐ | ☐ | ☐ |
| **4.3.1** | Bloquer les adresses IP et réseaux malveillants | ● | ☐ | ☐ | ☐ |
| **4.3.2** | Configurer des règles de sortie restrictives | ● | ☐ | ☐ | ☐ |
| **4.4.1** | Vérifier la protection contre l'IP spoofing | ● | ☐ | ☐ | ☐ |
| **4.4.2** | Configurer la protection DDoS basique | ● | ☐ | ☐ | ☐ |
| **4.5.1** | Vérifier l'intégration avec fail2ban | ● | ☐ | ☐ | ☐ |
| **4.5.2** | Tester et valider les règles de pare-feu | ● | ☐ | ☐ | ☐ |

| # | Recommandation | Niveau | Oui | Non | N/A |
|---|---|---|---|---|---|
| **4.6.1** | Documenter les règles de pare-feu et leur justification | ● | ☐ | ☐ | ☐ |
| **4.6.2** | Configurer la sauvegarde automatique des règles UFW | ● | ☐ | ☐ | ☐ |
| **Section 5 — JOURNALISATION & AUDIT** | | | | | |
| **5.1.1** | Vérifier que rsyslog est installé et configuré | ● | ☐ | ☐ | ☐ |
| **5.1.2** | Configurer la journalisation centralisée avec un serveur distant | ● | ☐ | ☐ | ☐ |
| **5.1.3** | Configurer la rotation et la rétention des journaux | ● | ☐ | ☐ | ☐ |
| **5.2.1** | Installer et configurer auditd | ● | ☐ | ☐ | ☐ |
| **5.2.2** | Configurer les règles d'audit pour les fichiers sensibles | ● | ☐ | ☐ | ☐ |
| **5.2.3** | Configurer l'audit des commandes privilégiées | ● | ☐ | ☐ | ☐ |
| **5.2.4** | Configurer l'audit des modifications de temps système | ● | ☐ | ☐ | ☐ |
| **5.3.1** | Configurer l'audit des connexions et authentifications | ● | ☐ | ☐ | ☐ |
| **5.3.2** | Configurer l'immutabilité des règles d'audit | ● | ☐ | ☐ | ☐ |
| **5.4.1** | Configurer la surveillance des montages et démontages | ● | ☐ | ☐ | ☐ |
| **5.4.2** | Configurer l'audit des suppressions de fichiers | ● | ☐ | ☐ | ☐ |
| **5.5.1** | Configurer la protection des fichiers de logs | ● | ☐ | ☐ | ☐ |
| **5.5.2** | Configurer la surveillance en temps réel des logs | ● | ☐ | ☐ | ☐ |
| **5.6.1** | Configurer la rétention à long terme des logs d'audit | ● | ☐ | ☐ | ☐ |
| **Section 6 — GESTION DES COMPTES** | | | | | |
| **6.1.1** | Définir l'expiration par défaut des comptes utilisateurs | ● | ☐ | ☐ | ☐ |
| **6.1.2** | Configurer l'âge minimum des mots de passe par défaut | ● | ☐ | ☐ | ☐ |
| **6.1.3** | Configurer l'âge maximum des mots de passe | ● | ☐ | ☐ | ☐ |
| **6.1.4** | Configurer l'avertissement d'expiration des mots de passe | ● | ☐ | ☐ | ☐ |
| **6.2.1** | Verrouiller les comptes système inutilisés | ● | ☐ | ☐ | ☐ |
| **6.2.2** | Vérifier l'unicité des UID utilisateurs | ● | ☐ | ☐ | ☐ |
| **6.2.3** | Vérifier l'unicité des GID groupes | ● | ☐ | ☐ | ☐ |
| **6.3.1** | Vérifier l'existence des répertoires home des utilisateurs | ● | ☐ | ☐ | ☐ |
| **6.3.2** | Vérifier les permissions des répertoires home | ● | ☐ | ☐ | ☐ |
| **6.4.1** | Vérifier les fichiers .netrc dans les répertoires home | ● | ☐ | ☐ | ☐ |
| **6.4.2** | Vérifier les fichiers .rhosts dans les répertoires home | ● | ☐ | ☐ | ☐ |
| **6.5.1** | Auditer les groupes dans /etc/passwd vs /etc/group | ● | ☐ | ☐ | ☐ |
| **6.5.2** | Vérifier l'absence de comptes avec des mots de passe vides | ● | ☐ | ☐ | ☐ |
| **6.6.1** | Configurer la politique de verrouillage de compte | ● | ☐ | ☐ | ☐ |
| **6.6.2** | Surveiller et auditer les connexions utilisateurs | ● | ☐ | ☐ | ☐ |
| **Section 7 — AUTHENTIFICATION PAM** | | | | | |
| **7.1.1** | Configurer la politique de complexité des mots de passe avec pam_pwquality | ● | ☐ | ☐ | ☐ |
| **7.1.2** | Configurer l'historique des mots de passe avec pam_pwhistory | ● | ☐ | ☐ | ☐ |
| **7.2.1** | Configurer les délais de verrouillage avec pam_faillock | ● | ☐ | ☐ | ☐ |
| **7.2.2** | Configurer pam_tally2 comme protection supplémentaire | ● | ☐ | ☐ | ☐ |
| **7.3.1** | Configurer les limites de ressources avec pam_limits | ● | ☐ | ☐ | ☐ |
| **7.4.1** | Configurer pam_wheel pour restreindre l'accès su | ● | ☐ | ☐ | ☐ |
| **7.4.2** | Configurer les restrictions de temps avec pam_time | ● | ☐ | ☐ | ☐ |
| **7.5.1** | Configurer l'authentification à deux facteurs avec pam_google_authenticator | ● | ☐ | ☐ | ☐ |
| **7.6.1** | Auditer et nettoyer la configuration PAM | ● | ☐ | ☐ | ☐ |
| **Section 8 — POLITIQUES DE MOT DE PASSE** | | | | | |
| **8.1.1** | Configurer la longueur minimale des mots de passe | ● | ☐ | ☐ | ☐ |
| **8.1.2** | Imposer la complexité des mots de passe | ● | ☐ | ☐ | ☐ |
| **8.2.1** | Configurer l'historique des mots de passe | ● | ☐ | ☐ | ☐ |
| **8.3.1** | Bloquer les mots de passe communs | ● | ☐ | ☐ | ☐ |
| **Section 9 — PERMISSIONS FICHIERS** | | | | | |
| **9.1.1** | Vérifier les permissions des fichiers système critiques | ● | ☐ | ☐ | ☐ |
| **9.1.2** | Auditer les fichiers avec permissions SUID/SGID | ● | ☐ | ☐ | ☐ |
| **9.2.1** | Sécuriser les répertoires world-writable | ● | ☐ | ☐ | ☐ |
| **Section 10 — INTÉGRITÉ SYSTÈME** | | | | | |
| **10.1.1** | Installer et configurer AIDE | ● | ☐ | ☐ | ☐ |
| **10.1.2** | Configurer la vérification régulière d'intégrité | ● | ☐ | ☐ | ☐ |
| **Section 11 — SSH** | | | | | |
| **11.1.1** | Configurer SSH Protocol 2 uniquement | ● | ☐ | ☐ | ☐ |

| # | Recommandation | Niveau | Oui | Non | N/A |
|---|---|---|---|---|---|
| **11.1.2** | Désactiver l'authentification par mot de passe root SSH | ● | ☐ | ☐ | ☐ |
| **11.2.1** | Configurer des algorithmes de chiffrement forts | ● | ☐ | ☐ | ☐ |
| **11.3.1** | Configurer l'authentification par clés SSH uniquement | ● | ☐ | ☐ | ☐ |
| **11.4.1** | Limiter les utilisateurs et groupes SSH | ● | ☐ | ☐ | ☐ |
| **11.5.1** | Configurer des timeouts et limites de connexion SSH | ● | ☐ | ☐ | ☐ |
| **Section 12 — SUDO & ÉLÉVATION DE PRIVILÈGES** | | | | | |
| **12.1.1** | Configurer sudoers avec visudo uniquement | ● | ☐ | ☐ | ☐ |
| **12.1.2** | Configurer le timeout sudo approprié | ● | ☐ | ☐ | ☐ |
| **12.2.1** | Activer la journalisation sudo | ● | ☐ | ☐ | ☐ |
| **Section 13 — APPARMOR & MAC** | | | | | |
| **13.1.1** | Vérifier qu'AppArmor est installé et activé | ● | ☐ | ☐ | ☐ |
| **13.1.2** | Configurer les profils AppArmor en mode enforce | ● | ☐ | ☐ | ☐ |
| **Section 14 — CONTENEURS & VIRTUALISATION** | | | | | |
| **14.1.1** | Sécuriser Docker si installé | ● | ☐ | ☐ | ☐ |
| **Section 15 — MISES À JOUR & PATCHS** | | | | | |
| **15.1.1** | Configurer les mises à jour automatiques de sécurité | ● | ☐ | ☐ | ☐ |
| **15.2.1** | Vérifier l'intégrité des paquets APT | ● | ☐ | ☐ | ☐ |
| **Section 16 — CRYPTOGRAPHIE & CHIFFREMENT** | | | | | |
| **16.1.1** | Configurer des algorithmes cryptographiques forts système | ● | ☐ | ☐ | ☐ |
| **Section 17 — SÉCURITÉ KERNEL** | | | | | |
| **17.1.1** | Configurer les paramètres kernel de sécurité | ● | ☐ | ☐ | ☐ |
| **Section 18 — CONFORMITÉ & GOUVERNANCE** | | | | | |
| **18.1.1** | Documenter la configuration de sécurité | ● | ☐ | ☐ | ☐ |
| **18.2.1** | Planifier les audits de sécurité réguliers | ● | ☐ | ☐ | ☐ |