11/02/2026

# Documentation d’installation et utilisation de Lynis

Version 1.1

Lyes Mouhoun

# Table des matières

Lyes Mouhoun

# Introduction : Qu'est-ce que Lynis ?

Lynis est un outil d'audit de sécurité, de gestion de la conformité et de durcissement open-source, reconnu par l'industrie et spécialement conçu pour les systèmes basés sur UNIX (Linux, macOS…).

Que fait-il exactement ?

Contrairement aux scanners de vulnérabilités traditionnels qui sondent un système depuis l'extérieur (via le réseau), Lynis s'exécute de manière privilégiée et locale directement sur l'hôte. Il effectue une auscultation approfondie de l'architecture interne du système en analysant :

- Les fichiers de configuration système et réseau.
- Les règles de pare-feu et le routage.
- La gestion des identités, des accès et les permissions des fichiers critiques.
- Les services actifs, les démons et les paquets logiciels installés.

Quel est son objectif principal ?
L'objectif de Lynis est d'évaluer de manière proactive la posture de sécurité d'un serveur avant qu'il ne soit compromis.
À l'issue de son exécution, il ne se contente pas de lister les problèmes ; il fournit un plan d'action concret. Son but est de :

1. Détecter les erreurs de configuration, les logiciels obsolètes ou les failles de sécurité potentielles.
2. Fournir des recommandations d'experts (suggestions de durcissement) pour corriger chaque vulnérabilité identifiée.
3. Mesurer le niveau de sécurité via un indicateur clair (l'Index de durcissement) afin d'assurer un suivi dans le temps.
4. Faciliter la conformité avec les standards de sécurité internationaux .

Lyes Mouhoun

# 1. *Prérequis et Installation*

Cette méthode d'installation via GitHub permet de s'assurer de disposer de la version la plus récente de Lynis, souvent plus à jour que celle présente dans les dépôts officiels des distributions.
Note importante : Si Lynis est déjà installé via un gestionnaire de paquets (APT, DNF, etc.), il est impératif de le désinstaller au préalable afin d'éviter tout conflit.
Installation de Git
Si votre serveur (VPS ou machine dédiée) est fraîchement installé, Git peut être manquant. Installez-le selon votre distribution :
Pour Ubuntu / Debian :
*sudo apt install git*
Pour Linux:
*sudo dnf install git*
Clonage et préparation de Lynis
Récupérez la dernière version directement depuis le dépôt officiel :
git clone https://github.com/CISOfy/lynis
Il est fortement recommandé d'exécuter Lynis avec les privilèges root. Pour éviter les avertissements de sécurité et garantir que l'outil ait les droits nécessaires pour analyser le système en profondeur, modifiez le propriétaire du dossier :
*sudo chown -R 0:0 lynis*
*cd lynis*
Vérifiez ensuite que l'installation s'est bien déroulée en consultant la version :
*sudo ./lynis --version*

---

# 2. *Documentation et Commandes de Base*

Lynis intègre sa propre documentation en ligne de commande. Depuis le répertoire lynis, vous pouvez explorer ses capacités :

- Afficher toutes les commandes disponibles :

*sudo ./lynis show commands*


- Obtenir de l'aide sur une commande spécifique :

*sudo ./lynis show help [commande]*

- Explorer les catégories avancées :

*sudo ./lynis show options  # Affiche toutes les options d'audit*
*sudo ./lynis show tests  # Liste tous les tests disponibles*
*sudo ./lynis show debug  # Affiche les commandes de débogage*

# 3. Exécution du Premier Audit

Pour lancer une analyse de sécurité complète de votre système, exécutez la commande d'audit principal (assurez-vous d'être dans le répertoire lynis) :
*sudo ./lynis audit system*
Note : Le processus de scan peut prendre plusieurs minutes en fonction des ressources et de la configuration du système.

---

# 4. Analyse des Résultats de l'Audit

À l'issue de l'analyse, Lynis génère un rapport détaillé comprenant un Index de durcissement (Hardening index) — un score permettant d'évaluer le niveau de sécurité global du serveur.
Les retours sont classés en trois catégories :

- Avertissements (WARNINGS) : Problèmes critiques nécessitant une attention immédiate (ex: paquets vulnérables, pare-feu inactif, problèmes de synchronisation temporelle NTP).
- Suggestions (SUGGESTIONS) : Recommandations pour améliorer la sécurité non critiques (ex: durcissement SSH, installation de Fail2ban, surveillance d'intégrité des fichiers).
- Informations (Informational) : État général des composants du système (services en cours d'exécution, configuration).

Chaque avertissement ou suggestion est accompagné de :

1. Un identifiant unique (ex: [PKGS-7392]).
2. Une description concise du problème.
3. Un lien vers la documentation officielle pour sa résolution.

```
Lynis security scan details:

Hardening index : 61 [############        ]
Tests performed : 255
Plugins enabled : 1

Components:
- Firewall               [V]
- Malware scanner        [X]

Scan mode:
Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

Lynis modules:
- Compliance status      [?]
- Security audit         [V]
- Vulnerability scan     [V]

Files:
- Test and debug information      : /var/log/lynis.log
- Report data                     : /var/log/lynis-report.dat
```

Fichiers de reporting :

- Journal complet d'exécution : */var/log/lynis.log*
- Rapport de données : */var/log/lynis-report.dat*

---

# 5. Configuration et Remédiation : Exemple de

Lyes Mouhoun

# *Durcissement SSH*

L'objectif post-audit est d'augmenter votre Index de durcissement en corrigeant les points soulevés. Prenons l'exemple des recommandations classiques concernant le service OpenSSH.
Lynis remonte souvent ces suggestions :

```
OpenSSH option: PermitRootLogin                    [ SUGGESTION ]
OpenSSH option: MaxAuthTries                       [ SUGGESTION ]
OpenSSH option: MaxSessions                        [ SUGGESTION ]
OpenSSH option: LogLevel                           [ SUGGESTION ]
OpenSSH option: AllowTcpForwarding                 [ SUGGESTION ]
OpenSSH option: X11Forwarding                      [ SUGGESTION ]
OpenSSH option: AllowAgentForwarding               [ SUGGESTION ]
```

comment Implémenter des correctifs ?:

```
  Suggestions (49):
  ------------------------------

  * This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
      https://cisofy.com/lynis/controls/LYNIS/

  * Consider hardening system services [BOOT-5264]
    - Details  : Run '/usr/bin/systemd-analyze security SERVICE' for each service
      https://cisofy.com/lynis/controls/BOOT-5264/

  * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
      https://cisofy.com/lynis/controls/KRNL-5820/

  * Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]
      https://cisofy.com/lynis/controls/AUTH-9229/

  * Configure password hashing rounds in /etc/login.defs [AUTH-9230]
      https://cisofy.com/lynis/controls/AUTH-9230/

  * Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
      https://cisofy.com/lynis/controls/AUTH-9262/

  * When possible set expire dates for all password protected accounts [AUTH-9282]
      https://cisofy.com/lynis/controls/AUTH-9282/

  * Configure minimum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/lynis/controls/AUTH-9286/

  * Configure maximum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/lynis/controls/AUTH-9286/
```

Éditez le fichier de configuration SSH (généralement situé dans */etc/ssh/sshd_config)* et appliquez les modifications suivantes :

1. Désactiver la connexion root directe (assurez-vous d'avoir un utilisateur avec les droits sudo au préalable) :

```
PermitRootLogin no
```

2. Limiter les tentatives et les sessions simultanées (protection contre la force brute) :

```
OpenSSH option: MaxAuthTries                                [ SUGGESTION ]
OpenSSH option: MaxSessions                                 [ SUGGESTION ]
```

```
MaxAuthTries 4       # Default is 6, which allows too many attempts
MaxSessions 2        # Default is 10, which is usually unnecessary
```

3) Augmenter la verbosité des journaux (meilleure traçabilité) :

```
OpenSSH option: LogLevel                                    [ SUGGESTION ]
```

```
LogLevel VERBOSE
```

*LogLevel VERBOSE*

3. Désactiver les transferts inutiles (limite la surface d'attaque) :

```
OpenSSH option: AllowTcpForwarding                          [ SUGGESTION ]
OpenSSH option: X11Forwarding                               [ SUGGESTION ]
OpenSSH option: AllowAgentForwarding                        [ SUGGESTION ]
```

```
AllowTcpForwarding no
X11Forwarding no
AllowAgentForwarding no
```

*AllowTcpForwarding no*
*X11Forwarding no*
*AllowAgentForwarding no*

Validation et Redémarrage
Avant d'appliquer les modifications, validez la syntaxe de votre configuration pour éviter de vous bloquer hors du serveur :
*sudo sshd -t*
Si aucune erreur n'est retournée, redémarrez le service :
*sudo systemctl restart sshd*

Conseil de sécurité : Maintenez toujours votre session SSH actuelle ouverte. Ouvrez un nouveau terminal et testez la connexion avec vos nouveaux paramètres. Ne fermez votre session initiale qu'après avoir validé que le nouvel accès fonctionne.
Une fois ces modifications appliquées, relancez un audit (sudo ./lynis audit system). Vous constaterez que votre Index de durcissement a augmenté.

# *6. Conclusion*

Lynis est un outil puissant pour auditer et maintenir le niveau de sécurité des serveurs Linux. La méthode consiste en une amélioration continue : analysez les avertissements critiques en priorité, implémentez les suggestions par lots de configuration (comme démontré avec SSH), et ré-exécutez des audits réguliers pour mesurer vos progrès.