


Titre de Votre Tuto

- Objet : Outil de sécurisation lynis
- Version lynis : ~~2.7.5-1~~ Version à voir
- [en-chantier-a-tester-a-placer](#)
- Niveau requis : avisé
- Commentaires : *Tuto à l'état de projet.* 
- Débutant, à savoir : [Utiliser GNU/Linux en ligne de commande, tout commence là !](#) 😊

Introduction

Lynis est un outil d'audit en logiciel libre pour le raffermissement de sécurité des systèmes basés sur AIX, FreeBSD, HP-UX, Linux, macOS, NetBSD, OpenBSD, Solaris et autres dérivés d'Unix ou de type POSIX. Il assiste les administrateurs systèmes et les professionnels de la sécurité dans la tâche d'examen rapide (scan) d'un système et de ses défenses de sécurité, ceci dans un but de durcissement (en anglais *system hardening*). L'outil a été créé par Michael Boelen, l'auteur original de rkhunter ainsi que par plusieurs autres contributeurs spéciaux et traducteurs. Lynis est publié sous Licence publique générale GNU version 3.

- Plus d'information : [notice wikipédia de lynis](#)
- Site de la société commerciale CISOFY qui crée et maintient l'outil lynis et assiste les utilisateurs : [Lien externe](#)

But du tuto

Il s'agit de se passer des conseils de la société CISOFY qui basculent de plus en plus des logs vers le site de la société et du gratuit au payant. Public visé : Les utilisateurs d'ordinateurs individuels qui sont prêts à réfléchir pour évaluer les risques et implanter des solutions pour les diminuer. Les administrateurs systèmes et les gestionnaires de serveurs devraient pouvoir utiliser lynis sans assistance.

Installation

Installation du paquet debian lynis, ceci après une installation d'une debian ~~bulleyes~~ (version à voir) avec un environnement de bureau. Comme lynis est un outil de sécurité, la première chose qui le fera tiquer, c'est votre système non-à jour ! Pour éviter cela, mettez-le à jour avant suivant vos choix et préférences :

Soit une mise à jour très conservatrice :

```
aptitude update && aptitude safe-upgrade && aptitude install lynis
```

ou

```
apt update && apt upgrade && apt install lynis
```

Soit une mise à jour plus souple et plus évolutive :

```
aptitude update && aptitude full-upgrade && aptitude install lynis
```

ou

```
apt update && apt full-upgrade && apt install lynis
```

Une autre méthode (hors du paquet debian et plus à jour) existe à base d'un fichier sources.list additionnel et d'épinglage (*pinning*), mais elle apporte une complexité qui ne sert pratiquement à rien, voire même est contre-productive si entre-temps CISOFY a encore basculé des messages d'erreurs du gratuit vers le payant.

Utilisation

À faire

Ceci d'après les messages de log de lynis lancés par :

```
lynis audit system
```

From:

<http://debian-facile.org/> - **Documentation - Wiki**

Permanent link:

<http://debian-facile.org/utilisateurs:gilles:tutos:outil-de-securisation-lynis>



Last update: **08/06/2020 13:48**