# Identification des rootkits

Les rootkits sur les serveurs Linux, les ordinateurs de bureau ou les ordinateurs portables sont de plus en plus une menace.

Si on souhaite **vérifier si des rootkits sont présents ou non sur un système** et de s’en débarrasser, on doit, dans un premier temps, **analyser le système**.

L'un des **meilleurs outils pour rechercher des rootkits sur Linux est Tiger**.   
Lorsqu'il est exécuté, il **crée un rapport de sécurité complet du système Lin**ux qui indique où se trouvent les problèmes (y compris les rootkits).

## Installation de Tiger

Pour **installer Tiger** …  
**>> sudo apt install tiger**

## Recherche de rootkits

Tiger est une **application automatique**.   
Il n'a **pas d'options ou de commutateurs uniques** que les utilisateurs peuvent utiliser dans la ligne de commande.   
Tiger **ne peut rechercher un rootkit particulier car il n’exécute qu’une analyse complète**.

Chaque fois que le programme s'exécute, il analyse de nombreux types de menaces de sécurité sur le système ...

* Fichiers de mots de passe Linux ;
* Fichiers .rhost ;
* Fchiers .netrc ;
* ttytab, securetty et fichiers de configuration de connexion ;
* Paramètres du chemin (*path*) Bash ;
* Vérifications des rootkits ;
* Entrées de démarrage de Cron ;
* Fichiers de configuration SSH ;
* Processus d'écoute ;
* Fichiers de configuration FTP.

**Remarque** …  
Tiger **ne peut être exécuté que par l’utilisateur root**.

Pour **démarrer une recherche** …  
**>>** **sudo** **tiger**

Tiger s'exécute et permet de suivre le processus d'audit.   
Il **affichera ce qu'il balaie et comment il interagit avec le système Linux**.

### Sortie typique d’une recherche

**Tiger UN\*X security checking system**

**Developed by Texas A&M University, 1994**

**Updated by the Advanced Research Corporation, 1999-2002**

**Further updated by Javier Fernandez-Sanguino, 2001-2018**

**Contributions by Francisco Manuel Garcia Claramonte, 2009-2010**

**Covered by the GNU General Public License (GPL)**

**Configuring...**

**Will try to check using config for 'unknown' running Linux 4.19.0-17-amd64...**

**--CONFIG-- [con005c] Using configuration files for Linux 4.19.0-17-amd64. Using**

**configuration files for generic Linux 4.**

**Tiger security scripts \*\*\* 3.2.4rc1, 2018.02.10.20.30 \*\*\***

**13:03> Beginning security report for debian-cli.**

**13:03> Starting file systems scans in background...**

**13:03> Checking password files...**

**13:03> Checking group files...**

**13:03> Checking user accounts...**

**13:03> Checking .rhosts files...**

**13:03> Checking .netrc files...**

**13:03> Checking ttytab, securetty, and login configuration files...**

**13:03> Checking PATH settings...**

**13:03> Checking anonymous ftp setup...**

**13:03> Checking mail aliases...**

**13:03> Checking cron entries...**

**13:03> Checking 'services' configuration...**

**13:04> Checking NFS export entries...**

**13:04> Checking permissions and ownership of system files...**

**13:04> Checking for indications of break-in...**

**13:04> Performing rootkit checks...**

**13:04> Performing system specific checks...**

**13:07> Performing root directory checks...**

**13:07> Checking for secure backup devices...**

**13:07> Checking for the presence of log files...**

**13:07> Checking for the setting of user's umask...**

**13:07> Checking for listening processes...**

**13:07> Checking SSHD's configuration...**

**13:07> Checking the printers control file...**

**13:07> Checking ftpusers configuration...**

**13:07> Checking NTP configuration...**

**13:07> Waiting for filesystems scans to complete...**

**13:07> Filesystems scans completed...**

**13:07> Performing check of embedded pathnames...**

**13:08> Security report completed for debian-cli.**

**Security report is in `/var/log/tiger/security.report.debian-cli.210731-13:03'.**

## Affichage des journaux

Pour déterminer si loge un rootkit sur un système Linux, il faut **consulter afficher le rapport de sécurité**.

Pour **consulter un rapport de sécurité**, on doit accéder au **répertoire /var/log/tiger** et …  
**>>** **sudo less security.report.xxx.xxx-xx:xx  
>>** **sudo less security.report.debian-cli.210731-13:03**