

Protection sur Ubuntu 14.04LTS

Logiciels de sécurité pour Ubuntu

Wulfk

30/04/2015



LES OUTILS DISPONIBLES

DÉFINITION D'UN ROOTKIT

Un rootkit est un programme qui maintient un accès frauduleux à un système informatique et cela le plus discrètement possible, leur détection est difficile, parfois même impossible tant que le système d'exploitation fonctionne. Certains rootkits résistent même au formatage car ils peuvent s'introduire directement dans le BIOS. Ils existent sous Linux depuis longtemps (car le noyau est ouvert et modulaire).

Un Webkit quant à lui permet de prendre l'accès d'une machine via une faille puis par port http et de prendre l'accès sur le système.

Il existe néanmoins des programmes pour les détecter, nous allons les voir ci-dessous.

Source : [Rootkit – Documentation Ubuntu Francophone](#)

LA SÉCURITÉ SUR UBUNTU

Avec seulement **1,52%** d'utilisateurs d'une distribution Linux (Source [NetMarketShare](#) , **1,91%** sur [StatCounter](#)), **les stations de travail ne sont pas la cible des pirates informatiques. Néanmoins, les machines Linux sont souvent des serveurs ce qui en fait des cibles de choix !**

Ubuntu possède tout de même un Firewall intégré de base ([UFW](#)), il n'est pas actif par défaut. Il s'utilise via un terminal, mais pour faciliter son utilisation il est possible d'y adjoindre une interface graphique (**GUI = Graphic User Interface**) : [Gufw](#) via la logithèque Ubuntu.

De base Ubuntu ne dispose pas d'Antivirus, et à vrai dire on peut même sans passer, mais il y a tout de même possibilité d'installer [ClamAv](#), avec comme interface graphique [ClamTk](#)

Anti-malwares

On dispose de quelques outils d'analyses qui s'utilisent via un terminal il n'existe pas d'interface graphique (GUI):

- **Chkrootkit** (installation via paquet **.deb**)
- **Rkhunter** (installation via paquet **.deb**)
- **Lynis** (outil le plus récent, permet d'exécuter un audit de sécurité du système)

Protection du système

On dispose de l'outil **AppArmor** (installation via le terminal ou paquet **.deb**)

Analyse vulnérabilité du système

On dispose de 2 outils :

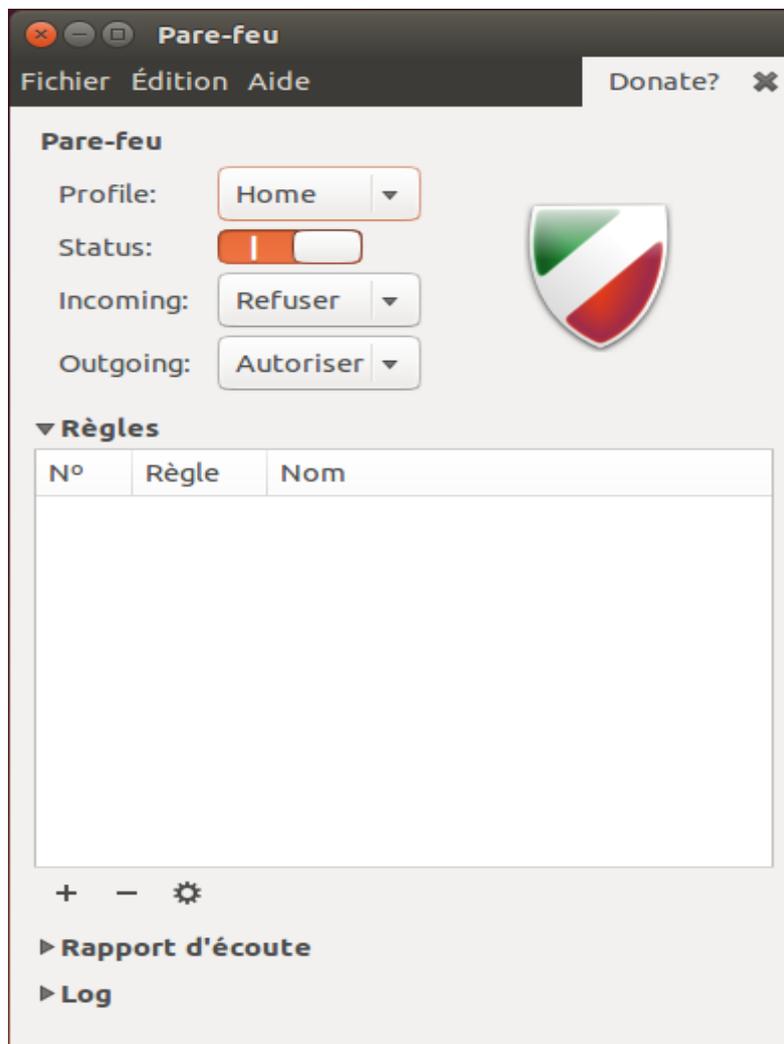
- **Nessus** (Scanner de vulnérabilité)
- **OpenVAS** (Scanner de vulnérabilité libre basé sur Nessus)

GUFW (INTERFACE GRAPHIQUE POUR UFW)



L'interface graphique pour le [Firewall UFW](#) d'Ubuntu s'installe via la Logithèque Ubuntu, **UFW** n'est pas activé par défaut. Une fois l'installation effectuée pour activer l'interface et de fait le Firewall on le lance via le Dash d'Unity ou via son icône dans la barre Unity, puis on clique sur le bouton **Status**.

Votre mot de passe vous sera demandé, car seul un administrateur peut débloquer le Firewall



D'autres paramètres sont disponibles dans l'interface, se reporter à la [documentation Ubuntu sur Gufw](#) pour peaufiner vos réglages.

CLAMAV ET CLAMTK



Clam AntiVirus (ClamAv) est un antivirus GPL pour UNIX qui s'utilise de base dans un terminal, mais on peut lui adjoindre une interface (GUI) **ClamTk** celle-ci est disponible via un paquet **.deb**.

La mise à jour de la base de données de ClamAv peut s'effectuer manuellement via le lien suivant :

<https://launchpad.net/~ubuntu-security-proposed/+archive/ubuntu/ppa/+build/6764309>



Pour avoir la dernière version de **ClamTk** cliquer sur le lien suivant : **Download ClamTk** il vous reste plus qu'à lancer le paquet **.deb** pour effectuer l'installation qui s'effectuera via la Logithèque Ubuntu.

Une fois l'interface installée, lancé là via le Dash d'Unity ou son icône dans la barre Unity.



Sécurité sur Ubuntu 14.04LTS

Il vous reste plus qu'à effectuer vos réglages

CHKROOTKIT

Chkrootkit est un **scanner Anti-rootkit**, qui s'utilise via un terminal.

Vérifie que les fichiers exécutables du système n'ont pas été modifiés, que la carte réseau n'est pas en mode "promiscuous" et que des vers [LKM](#) (Loadable Kernel Module) ne sont pas présents.

Source : [Rootkit - Documentation Ubuntu Francophone](#)

La documentation Ubuntu francophone ([paragraphe 1.2](#)) renvoi sur le site officiel en Anglais : <http://www.chkrootkit.org/>

Celui-ci ne propose pas de paquet **debian** pour l'installation, il faut passer par la page [Ubuntu](#) pour pouvoir télécharger le fichier **.deb** **version 0.49** pour **Ubuntu 14.04 (Trusty Tar)** sélectionner votre version en fonction de votre système (32 ou 64Bits) ou cliquer sur un des liens si dessous :

- [chkrootkit 0.49-4.1ubuntu1 amd64.deb](#) (374.1 KiB)
- [chkrootkit 0.49-4.1ubuntu1 i386.deb](#) (352.7 KiB)

En passant par un paquet **debian** et donc par la Logithèque Ubuntu, on dispose en Anglais d'un peu plus d'explication sur les actions de Chkrootkit, comme le montre la capture d'écran si dessous :



Détecteur de rootkit
chkrootkit
★★★★☆ (4 évaluations)

Veillez installer « chkrootkit » à partir des dépôts officiels. N'installez ce fichier que si vous avez confiance en son origine.

The chkrootkit security scanner searches the local system for signs that it is infected with a 'rootkit'. Rootkits are set of programs and hacks designed to take control of a target machine by using known security flaws.

Types that chkrootkit can identify are listed on the project's home page.

Please note that where chkrootkit detects no intrusions, this does not guarantee that the system is uncompromised. In addition to running chkrootkit, more specific tests should always be performed.

[Site Web des Développeurs](#)

Version chkrootkit 0.49-4.1ubuntu1
Taille totale 293,5 ko à télécharger, 921,6 ko une fois installé
Licence Libre

Liste des commandes de Chkrootkit via la commande suivante :

```
sudo chkrootkit -h
```

Sécurité sur Ubuntu 14.04LTS

```
ghost@ghost-VirtualBox: ~
Fichier Édition Affichage Rechercher Terminal Aide
ghost@ghost-VirtualBox:~$ sudo chkrootkit -h
[sudo] password for ghost:
Usage: /usr/sbin/chkrootkit [options] [test ...]
Options:
    -h          show this help and exit
    -V          show version information and exit
    -l          show available tests and exit
    -d          debug
    -q          quiet mode
    -x          expert mode
    -e          exclude known false positive files/dirs, quoted,
               space separated, READ WARNING IN README
    -r dir      use dir as the root directory
    -p dir1:dir2:dirN path for the external commands used by chkrootkit
    -n          skip NFS mounted dirs
ghost@ghost-VirtualBox:~$
```

RKHUNTER



Rkhunter (pour Rootkit Hunter) est une alternative, voir un complément de **Chkrootkit**. Il s'utilise aussi via un terminal. ([Rkhunter – Documentation Ubuntu Francophone](#))



Rootkit, backdoor, sniffer and exploit scanner

rkhunter
★★★★☆ (5 évaluations)

Veillez installer « rkhunter » à partir des dépôts officiels. N'installez ce fichier que si vous avez confiance en son origine.

Rootkit Hunter scans systems for known and unknown rootkits, backdoors, sniffers and exploits.

It checks for:

- MD5 hash changes;
- files commonly created by rootkits;
- executables with anomalous file permissions;
- suspicious strings in kernel modules;
- hidden files in system directories; and can optionally scan within files. Using rkhunter alone does not guarantee that a system is not compromised. Running additional tests, such as chkrootkit, is recommended.

[Site Web des Développeurs](#)

Version	rkhunter 1.4.0-3
Taille totale	4,0 Mo à télécharger, 17,7 Mo une fois installé
Licence	Libre
Mises à jour	Inconnu

Sécurité sur Ubuntu 14.04LTS

Contrôle notamment que les fichiers n'ont pas été modifiés en comparant les hash avec une base de données en ligne. Source : [Rootkit \(paragraphe 1.1\) - Documentation Ubuntu Francophone](#)

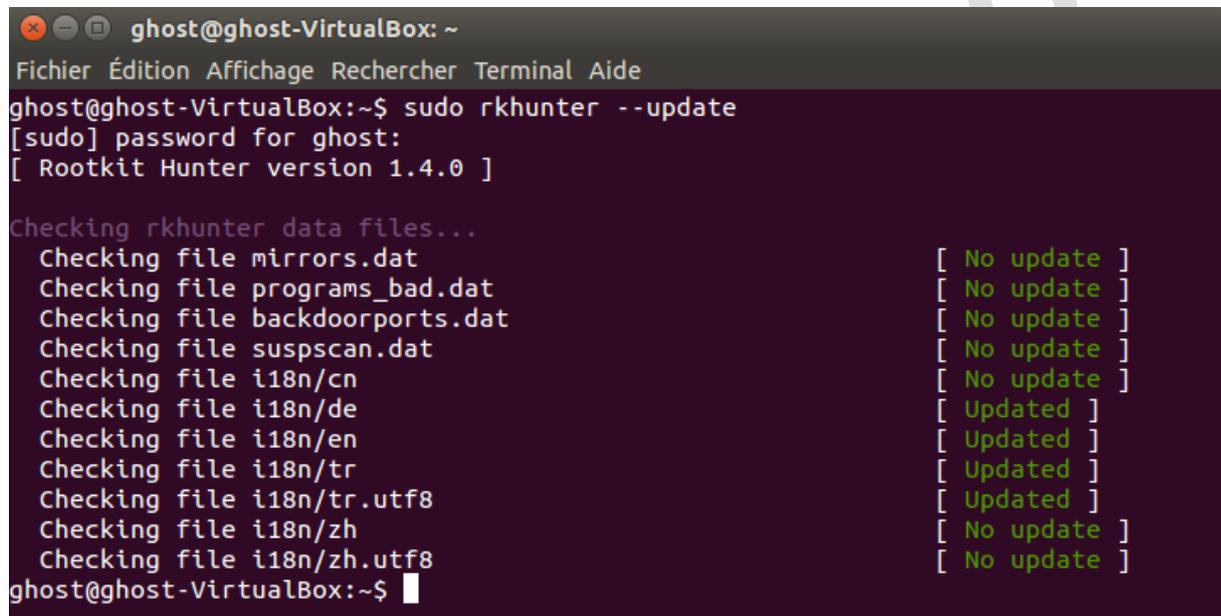
Site officiel : [The Rootkit Hunter Project](#)

Le téléchargement du fichier **deb**ian, s'effectue via le lien suivant : [rkhunter 1.4.0-3 all.deb](#) (205.9 KiB)

Installation en effectuant un double clic sur le fichier qui ouvre la Logithèque Ubuntu (image ci-dessus)

Avant la première utilisation effectuer la mise à jour via la commande suivante :

```
sudo rkhunter --update
```



```
ghost@ghost-VirtualBox: ~
Fichier Édition Affichage Rechercher Terminal Aide
ghost@ghost-VirtualBox:~$ sudo rkhunter --update
[sudo] password for ghost:
[ Rootkit Hunter version 1.4.0 ]

Checking rkhunter data files...
  Checking file mirrors.dat           [ No update ]
  Checking file programs_bad.dat      [ No update ]
  Checking file backdoorports.dat     [ No update ]
  Checking file suspscan.dat          [ No update ]
  Checking file i18n/cn                [ No update ]
  Checking file i18n/de                [ Updated ]
  Checking file i18n/en                [ Updated ]
  Checking file i18n/tr                [ Updated ]
  Checking file i18n/tr.utf8          [ Updated ]
  Checking file i18n/zh                [ No update ]
  Checking file i18n/zh.utf8          [ No update ]
ghost@ghost-VirtualBox:~$
```

Avant toute chose, nous allons maintenant configurer notre anti-rootkit convenablement. Pour cela, on va d'abord réaliser une sauvegarde du fichier de configuration initiale

```
cp /etc/rkhunter.conf /etc/rkhunter.conf.bak
```

Maintenant, on peut utiliser notre éditeur de texte Gedit pour ajuster la configuration de Rkhunter en fonction de nos besoins.

```
sudo gedit /etc/rkhunter.conf
```

On cherche dans ce fichier la ligne suivante pour la modifier en ajoutant l'adresse mail sur laquelle vous recevrez les rapports générés quotidiennement et/ou les alertes transmises par Rkhunter :

MAIL-ON-WARNING=[Utilisateur@VotreNomDeDomaine.extension](#)

Par défaut, Rkhunter stocke ses fichiers de logs dans le répertoire **/var/log/rkhunter.log/**, si vous souhaitez les déplacer, vous pouvez modifier la ligne suivante :

LOGFILE=[/var/log/rkhunter.log](#)

Sécurité sur Ubuntu 14.04LTS

Vous pouvez à présent lancer votre première analyse en spécifiant par exemple un **rapport uniquement sur les avertissements** via la ligne de commande suivante :

```
sudo rkhunter --checkall --report-warning-only
```

La commande suivante :

```
sudo rkhunter -propupd
```

Permet de créer la première base de données qui sera utilisée pour les futurs scans. Il faut donc être sûr que le système est sain à ce moment précis et avant de créer la base qui sera utilisé pour les prochains scans.

Pour que Rkhunter s'exécute automatiquement sans intervention il faut créer un script lié à une tâche **crontab**

Création d'un script comme l'exemple suivant à adaptez celons vos besoin :

```
#!/bin/sh
source /etc/profile
rkhunter --update && rkhunter --check
```

Enregistrer le dans **/home/login/Documents** sous le nom **auto-rkhunter.sh**

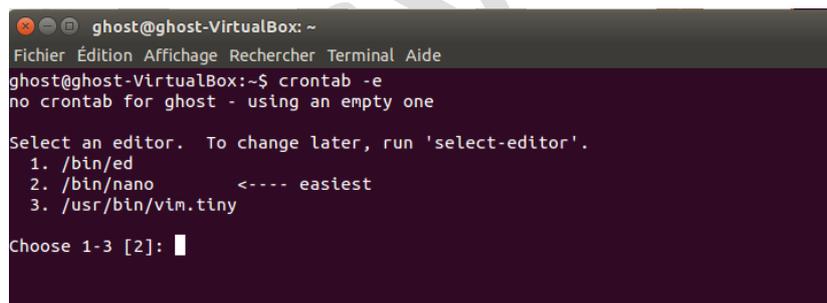
Remplacer **login** par votre nom d'utilisateur

Le rendre exécutable avec la commande suivante dans un terminal :

```
chmod +x auto-rkhunter.sh
```

Puis créer votre tâche cron en éditant le fichier crontab via la commande :

```
crontab -e
```



```
ghost@ghost-VirtualBox: ~
Fichier Édition Affichage Rechercher Terminal Aide
ghost@ghost-VirtualBox:~$ crontab -e
no crontab for ghost - using an empty one

Select an editor. To change later, run 'select-editor'.
 1. /bin/ed
 2. /bin/nano <---- easiest
 3. /usr/bin/vim.tiny

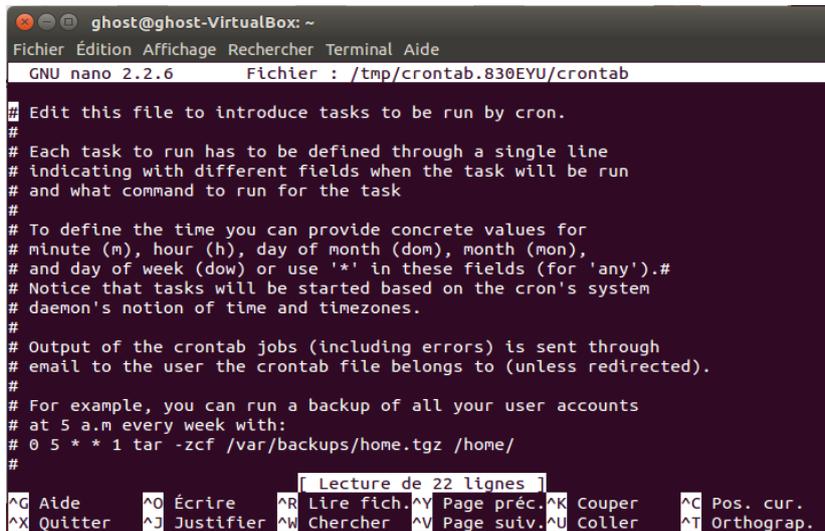
Choose 1-3 [2]:
```

Choisir l'option 2 (l'éditeur **nano**) et saisissez votre tâche cron, comme dans l'exemple suivant :

```
00 20 * * * /home/login/Documents/auto-rkhunter.sh
```

À adapter celons vos propres critères

Sécurité sur Ubuntu 14.04LTS



```
ghost@ghost-VirtualBox: ~
Fichier Édition Affichage Rechercher Terminal Aide
GNU nano 2.2.6 Fichier : /tmp/crontab.830EYU/crontab
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
^G Aide      ^O Écrire    ^R Lire fich.^Y Page préc.^K Couper    ^C Pos. cur.
^X Quitter   ^J Justifier ^W Chercher  ^V Page suiv.^U Coller   ^T Orthograp.
```

Finaliser en enregistrant par la combinaison de touche **CTRL+X** et valider la sauvegarde par **OUI**

LYNIS

Lynis est un outil d'analyse plus récent que **CHKROOTKIT** et **RKHUNTER**, il permet d'effectuer un audit de sécurité de votre système via un terminal.

Contrôle notamment le pare-feu, que les certificats SSL ne sont pas périmés, l'intégrité des fichiers.

Source : [Rootkit \(paragraphe 1.3\) - Documentation Ubuntu Francophone](#)

Il existe sur la page Ubuntu [lynis 1.3.9-1 all.deb](#) (92.8 KiB) pour **Ubuntu 14.04 (Trusty Thar)** qui s'installe via un paquet **.deb** et dispose d'un lanceur dans la barre Unity.



Utilitaire d'audit Lynis
security auditing tool for Unix based systems
★★★★☆ (2 évaluations)

Veillez installer « lynis » à partir des dépôts officiels. N'installez ce fichier que si vous avez confiance en son origine. Installer

Lynis is an auditing tool for Unix. It scans the system configuration and creates an overview of system information and security issues usable by professional auditors.

It can assist in automated audits.

Lynis can be used in addition to other software, like security scanners, system benchmarking and fine-tuning tools.

[Site Web des Développeurs](#)

Version: lynis 1.3.9-1
Taille totale: 95,0 ko à télécharger, 725,0 ko une fois installé
Licence: Libre

Mais ce n'est pas la dernière version disponible comme l'indique la capture d'écran ci-dessous.

Sécurité sur Ubuntu 14.04LTS

```
- Checking profile file (/etc/lynis/default.prf)...
- Program update status... [ WARNING ]

=====
Notice: Lynis update available
Current version : 139 Latest version : 200
Please update to the latest version for new features, bug fixes, tests
and baselines.
=====

[ Press [ENTER] to continue, or [CTRL]+C to stop ]
```

Pour avoir la dernière version (**2.1.0**) il faut aller sur le site de [l'éditeur CISOFY](#) pour télécharger l'archive **.tar.gz**
Pour l'installation suivre le guide en ligne : [Get Started with Lynis – Installation Guide](#)
Vous pouvez aussi [utiliser Lynis sans installation](#)

Cette version ne dispose malheureusement pas d'un lanceur dans la barre Unity, il faut lancer l'audit de sécurité via un terminal avec les commandes suivantes :

```
cd /usr/local/lynis
./lynis
```

Contrairement à la référence de l'archive télécharger (2.1.0) la version qui s'affiche dans le terminal est la 2.1.1

```
[ Lynis 2.1.1 ]

#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

Copyright 2007-2015 - CISOfy, https://cisofy.com
Enterprise support and plugins available via CISOfy
#####

[+] Initializing program
-----

#####
#
# NON-PRIVILEGED SCAN MODE
#
#####

NOTES:
-----
* Some tests will be skipped (as they require root permissions)
```

Différents [paramètres](#) peuvent être associés à la commande :

```
./lynis
```

Bien qu'en Anglais [la documentation Lynis](#) est bien construite et relativement simple à comprendre.

Je n'ai pas essayé, mais il est peut-être possible de créer un lanceur pour cette version afin de l'intégrer dans la barre Unity.

Sécurité sur Ubuntu 14.04LTS

APPARMOR

(Tiré du *Guide de sécurisation pour Ubuntu 14.04*)

Les distributions Linux sont en majorité équipées de Firefox comme navigateur web, ce qui fait de Firefox une cible de choix pour tout service de renseignement soucieux d'infecter GNU/Linux (faille Oday dans Tor Browser, etc)

Pour empêcher qu'un exploit Oday ciblant Firefox ne fasse des dégâts considérables, il faut sécuriser Firefox avec le logiciel **AppArmor**.

AppArmor est un logiciel libre qui permet de limiter l'exécution et l'accès des programmes au système.
<https://fr.wikipedia.org/wiki/AppArmor>

Par défaut, AppArmor ne protège pas Firefox (incompréhensible), pour le constater faites l'expérience suivante : ouvrez avec Firefox un fichier sensible, par exemple le fichier **gfxblacklist.txt**

Ce fichier est situé dans le système de fichier **/boot/grub**, c'est la partition non-chiffrée d'amorçage qui permet le déchiffrement du disque dur lors du démarrage de l'ordinateur. Si Firefox peut y accéder alors un attaquant qui exploite Firefox peut y accéder aussi, il peut modifier la partition **/boot** et y installer un keylogger qui va enregistrer le mot de passe de chiffrement disque lors du démarrage.

Un attaquant exploitant Firefox peut aussi compromettre le système avec un trojan ou n'importe quel virus made in NSA.

Pour protéger le système vous devez sécuriser Firefox avec AppArmor

Ouvrez un terminal et installez AppArmor :

```
sudo apt-get install apparmor-utils apparmor-profiles apparmor-notify
```

Ou via des paquets **.deb** :

[apparmor_2.8.95~2430-0ubuntu5_amd64.deb](#) (311.3 KiB)

[apparmor-utils_2.8.95~2430-0ubuntu5_amd64.deb](#) (51.5 KiB)

[apparmor-profiles_2.8.95~2430-0ubuntu5_all.deb](#) (32.5 KiB)

[apparmor-notify_2.8.95~2430-0ubuntu5_all.deb](#) (11.3 KiB)

[apparmor_2.8.95~2430-0ubuntu5_i386.deb](#) (320.6 KiB)

[apparmor-utils_2.8.95~2430-0ubuntu5_i386.deb](#) (51.5 KiB)

Il faut passer le profil de Firefox en mode "enforce"

```
sudo aa-status | grep firefox
sudo aa-enforce /etc/apparmor.d/usr.bin.firefox
sudo aa-status | grep firefox
```

Les binaires Firefox sont désormais en mode "enforce"

Sécurité sur Ubuntu 14.04LTS

Vous devez redémarrer pour appliquer les changements. Vérifiez si Firefox est bien en mode "*enforce*" en essayant à nouveau d'ouvrir un fichier sensible. On obtient une notification indiquant que **AppArmor a bloqué Firefox** lorsque celui-ci a tenté d'ouvrir un fichier dont il n'a pas les droits d'accès...



Si la notification vous dérange vous pouvez la désactiver en utilisant la commande suivante :

```
sudo gedit /etc/apparmor/notify.conf
```

```
# set to 'yes' to enable AppArmor DENIED notifications  
show_notifications="no"
```

Redémarrer le PC pour la prise en compte

Vous pouvez ajouter d'autres processus et binaires en mode "*enforce*" pour diminuer les risques de compromission.

<https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/AppArmorProfiles>

Ouvrez un terminal et vérifiez l'état des profils :

```
sudo apparmor_status
```

Sécurité sur Ubuntu 14.04LTS

```
apparmor module is loaded.
46 profiles are loaded.
22 profiles are in enforce mode.
  /sbin/dhclient
  /usr/bin/evince
  /usr/bin/evince-previewer
  /usr/bin/evince-previewer//sanitized_helper
  /usr/bin/evince-thumbnailer
  /usr/bin/evince-thumbnailer//sanitized_helper
  /usr/bin/evince//sanitized_helper
  /usr/lib/NetworkManager/nm-dhcp-client.action
  /usr/lib/chromium-browser/chromium-browser//browser_java
  /usr/lib/chromium-browser/chromium-browser//browser_openjdk
  /usr/lib/chromium-browser/chromium-browser//sanitized_helper
  /usr/lib/connman/scripts/dhclient-script
  /usr/lib/cups/backend/cups-pdf
  /usr/lib/firefox/firefox{,*[^s][^h]}
  /usr/lib/firefox/firefox{,*[^s][^h]}//browser_java
  /usr/lib/firefox/firefox{,*[^s][^h]}//browser_openjdk
  /usr/lib/firefox/firefox{,*[^s][^h]}//sanitized_helper
  /usr/lib/lightdm/lightdm-guest-session
  /usr/lib/lightdm/lightdm-guest-session//chromium
  /usr/sbin/cups-browsed
  /usr/sbin/cupsd
  /usr/sbin/tcpdump
24 profiles are in complain mode.
  /sbin/klogd
  /sbin/syslog-ng
  /sbin/syslogd
  /usr/lib/chromium-browser/chromium-browser
  /usr/lib/chromium-browser/chromium-browser//chromium_browser_sandbox
  /usr/lib/chromium-browser/chromium-browser//lsb_release
  /usr/lib/chromium-browser/chromium-browser//xdgsettings
  /usr/lib/dovecot/deliver
  /usr/lib/dovecot/dovecot-auth
  /usr/lib/dovecot/imap
  /usr/lib/dovecot/imap-login
  /usr/lib/dovecot/managesieve-login
  /usr/lib/dovecot/pop3
  /usr/lib/dovecot/pop3-login
  /usr/sbin/avahi-daemon
  /usr/sbin/dnsmasq
  /usr/sbin/dovecot
  /usr/sbin/identd
  /usr/sbin/mdnsd
  /usr/sbin/nmbd
  /usr/sbin/nscd
  /usr/sbin/smbd
  /usr/{sbin/traceroute,bin/traceroute.db}
  /{usr/,}bin/ping
7 processes have profiles defined.
4 processes are in enforce mode.
  /sbin/dhclient (958)
  /usr/sbin/cups-browsed (1180)
  /usr/sbin/cupsd (1819)
  /usr/sbin/cupsd (1822)
0 processes are in complain mode.
3 processes are unconfined but have a profile defined.
  /usr/sbin/avahi-daemon (733)
  /usr/sbin/avahi-daemon (735)
  /usr/sbin/dnsmasq (1226)
```

Sécurité sur Ubuntu 14.04LTS

Passez les profils critiques en mode "enforce" les profils d'AppArmor sont localisés dans **/etc/apparmor.d**

```
sudo aa-enforce /etc/apparmor.d/usr.sbin.avahi-daemon
sudo aa-enforce /etc/apparmor.d/usr.sbin.dnsmasq
sudo aa-enforce /etc/apparmor.d/usr.sbin.mdnssd
sudo aa-enforce /etc/apparmor.d/usr.sbin.smbd
```

NESSUS



Nessus est un outil de sécurité informatique.

Il signale les faiblesses potentielles ou avérées du matériel testé (machines, équipement réseau).

Nessus est devenu un logiciel propriétaire à partir de la version 3. Cependant, il est resté gratuit pour usage non commercial. Un fork libre a été créé :

Plus d'infos ici : [Nessus - Documentation Ubuntu Francophone](#)

OPENVAS



Un fork libre de **Nessus**

Tout comme **Nessus**, il signale les faiblesses potentielles ou avérées du matériel testé (machines, équipement réseau).

OpenVAS est capable de scanner un équipement (machine ou matériel réseau), un ensemble d'équipements (à partir d'un fichier ou d'une plage IP) ou encore un réseau entier.

Plus d'infos ici : [OpenVAS - Documentation Ubuntu Francophone](#)

Voilà ça devrait suffire pour une utilisation raisonnablement sûre de votre système.

Ce tutoriel est fini, vous disposez à présent de 6 outils pour protéger et analyser la sécurité sur Ubuntu.

Ce tutoriel est aussi disponible au format PDF