Ce document est offert par
http://www.jmrenouard.fr/

Manuel Pratique de sécurité sous Linux

Version 1.5

12 décembre 2011

Le présent document détaille les procédures de sécurisation type lors d'une installation de serveur Linux.

Rédigé par :
Jean-Marie Renouard
http://jmrenouard.fr

Vérifié par :
Jean-Marie Renouard
http://jmrenouard.fr

Approuvé par :
Jean-Marie Renouard
http://jmrenouard.fr

1 Version

Version	Date	Auteur	Description
1.0	24/04/2006	Jean-Marie Renouard	Version initiale
1.1	21/06/2008	Jean-Marie Renouard	Amélioration du document Ajout de la partie sur l'installation Changement de licence
1.2	22/08/2008	Jean-Marie Renouard	Mise à jour de la syntaxe et corrections orthographiques
1.3	23/02/2009	Jean-Marie Renouard	Mise à jour des conseils autour de l'identité des intervenants sur les serveurs
1.4	09/03/2009	Jean-Marie Renouard	Mises à jour multiples et ajout d'illustrations
1.5	12/11/2011	Jean-Marie Renouard	Mises à jour

2 MENTIONS LEGALES

3 Table des matières

4 Introduction

4.1 Objet du document

Le présent document spécifie techniquement les procédures de sécurisation d'un serveur Linux Red Hat lors d'un déploiement d'un service sur Internet ou dans le cas d'un partage d'application avec un partenaire extérieur.

4.2 Contexte du document

Ce document a été rédigé pour système de la famille Red Hat et fonctionne sur les systèmes suivants:

- Red Hat 3.xx
- Red Hat 4.xx
- Red Hat 5.xx
- Centos 4.xx
- Centos 5.xx
- Fedora Core XX

Cependant il doit fonctionner correctement sans trop de difficultés sur l'ensemble des serveurs utilisant un système de packaging de type RPM.

L'ensemble de des préconisations ne sont pas uniquement valables pour systèmes compatibles Red Hat et peuvent servir de base pour toutes variantes de Linux comme Debian, Mandriva, Slackware, Gentoo, Ubuntu, ...

4.3 Références documentaires

4.4 Typologie

Exemple	Descritpion
# ifconfiq	Appel de la commande « ifconfig » lors d'une connexion super-utilisateur (root)

$ ls	Appel de la commande « ls » lors d'une connexion utilisateur (autre que root)

`1.txt`
`2.txt`
`toto`
`foo`
`bazr`
	Résultats affichés à l'appel d'un script shell

4.5 Glossaire

Item	Description

5 Considérations globales de sécurité.

L'ensemble de ces préconisations a pour but d'augmenter la sécurité, des interventions et du suivi des applications sur les plateformes Linux. L'application ou la non application reste à la discrétion de chacun. 123Solution ne peut pas être tenu responsable de la mauvaise application des préconisations de ce document.

6 Mises à jour de sécurité et distribution maintenue

La sécurité d'une distribution dépend de 2 éléments importants :

1. Le cycle de vie de la distribution;
2. La fréquence des mises à jour de votre système.

L'utilisation d'une distribution ayant un contrat de maintenance longue durée « long term maintenance » est importante car en effet, une application déployée en production à pour but de fonctionner plus de 3 à 4 mois et donc dans ce contexte nécessite un environnement système stable et maintenable durant un temps suffisant permettant sa mise à jour régulière et la planification de migration vers une version de distribution plus récente dans des conditions acceptable et non contraignante (**« effet fin de course »**)

6.1 Procédure de mise à jour intégrale de la distribution

Procédure sur Red Hat 5.xx et Fedora Core 3+

 # yum -y upgrade

. . .

Procédure sur les variantes de Debian/Ubuntu

 # apt-get upgrade

. . .

Procédure sur Red Hat 4-

 # up2date -uf

. . .

6.2 Réflexion de gestion applicative sur distribution en fin de vie

Il est important d'anticiper la migration vers des systèmes Linux et des versions de distribution ayant un cycle de vie permettant de rester serein dans un espace de temps suffisant afin de pouvoir garantir un nombre de correctifs de sécurité permettant de garantir de **« ne ne pas subir l'effet passoire »**

7 Topologie d'installation

7.1 Installation minimum

Les serveurs de production doivent être installés a minima.
Nous ne devons donc pas trouver sur un serveur de production les applications suivantes:

- Compilateur
- Serveur non nécessaire
- Serveur X
- Tout environnement graphique dernière génération

7.2 Retrait de toutes les documentations et applications non nécessaires

Pour enfin permettre une sécurité optimum sur le serveur de production, nous conseillons de retirer l'ensemble des applications qui ne sont pas strictement nécessaires au fonctionnement des applications qu'il héberge.

Les applications à proscrire en priorité sur un serveur de production sont les suivantes :

- Tous les compilateurs de code;
- Tous les langages de scripts non nécessaires;
- Toutes les applications de communication : mail, jabber, irc.
- Tous les outils de configuration système.
- Toutes documentations.

7.3 Effet « simple is beautiful »

Les systèmes ayant peu de programme installé sont toujours moins vulnérables car en effet les failles de sécurité potentielles concernent forcement moins d'applications sur votre serveur.
De plus, les installations minimalistes installent toujours des programmes fondamentaux et qui dit fondamental dit technologie mature, stable et donc très faiblement vulnérable.
Le fait de ne pas installer d'application serveur permets de ne pas ouvrir de service sur le serveur qui n'ont rien à y faire (serveur de Mail, rsync, Portmap, ...)

8 Compte à droits restreints

Pour l'ensemble des opérations, il est impératif d'utiliser un compte ayant des droits restreints pour plusieurs raisons :

- Pas besoin des droits d'un super administrateur pour effectuer des opérations non critiques.
- Besoins importants de traçabilité des opérations effectuées sur le serveur avec les droits du super utilisateur.
- Sécurisation et limitation des impacts de commandes tapées trop rapidement.
- Sécurisation des accès qui peuvent être réalisées sur un compte non privilégié.

8.1 Restrictions des accès SSH

Pour éviter des accès en tant que super utilisateur sur les plateformes de l'application, il est possible de restreindre l'accès au utilisateur non privilégié.

Il est possible d'interdire simplement les connexions root par SSH. Dans de nombreux cas, cela suffit largement à sécuriser le serveur.

Dans le fichier **/etc/ssh/sshd_config,** positionnez explicitement :

$ vim /etc/ssh/sshd_config

```
...
PermitRootLogin no

...
```

8.2 Mise en place du mécanisme d'usurpation

Cette technique permet de sécuriser l'ensemble des opérations effectuées en tant que super utilisateur.

8.2.1 Mise en place pour un utilisateur spécifique

 # adduser admin

```
# visudo
# User alias specification
User_Alias STAFF=admin

# User privilege specification
root ALL=(ALL) ALL
STAFF ALL=(ALL) NOPASSWD:ALL
```

8.2.2 Mise en place pour un groupe spécifique

 # visudo

```
%wheel ALL=(ALL) NOPASSWD:ALL
```

 # gpasswd -a admin wheel

8.2.3 Test la mise en place

 # su – admin
$ sudo mount /mnt/usbdisk

Si l'opération de montage d'une clé USB fonctionne alors le mécanisme d'usurpation est opérationnel.

8.2.4 Test de la présence des logs des actions

Ces traces contiennent l'ensemble des commandes concernant les opérations effectuées en tant que super utilisateur :

$ sudo cat /var/log/secure

```
Mar  7 16:42:21 localhost sshd[2807]: Accepted password for jmrenouard from
10.194.60.94 port 4087 ssh2
Mar  7 16:43:10 localhost sshd[2886]: Accepted password for jmrenouard from
10.194.60.94 port 4088 ssh2
Mar  7 16:43:30 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/bin/chmod -R 644 .ssh
Mar  7 16:44:01 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/bin/chown -R jmrenouard: .ss
Mar  7 16:44:03 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/bin/chown -R jmrenouard: .ssh/
Mar  7 16:44:18 localhost sshd[2974]: Accepted password for jmrenouard from
10.194.60.94 port 4089 ssh2
Mar  7 16:44:34 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/bin/chmod -R 644 .ssh
Mar  7 16:44:46 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/bin/chown -R jmrenouard: .ssh/authorized_keys
Mar  7 16:46:48 localhost sshd[3096]: Accepted publickey for jmrenouard from
10.194.60.94 port 4090 ssh2
Mar  8 11:10:39 localhost sshd[2291]: Accepted publickey for jmrenouard from
10.194.60.94 port 1538 ssh2
Mar  8 11:36:47 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/usr/bin/yum update
Mar  8 11:37:47 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/usr/bin/cpan install Template
Mar  8 11:43:24 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/usr/bin/cpan install XML::RSS
Mar  8 11:45:25 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/usr/bin/cpan install Digest::SHA
Mar  8 11:45:55 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/usr/bin/cpan install Digest::SHA
Mar  8 11:47:25 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/usr/bin/cpan install XML::DOM
Mar  8 11:47:30 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/usr/bin/cpan notest install XML::DOM
Mar  8 11:47:40 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/usr/bin/cpan force install XML::DOM
Mar  8 11:47:49 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/usr/bin/cpan force install XML::DOM
```

```
Mar  8 11:47:58 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/usr/bin/cpan
Mar  8 11:48:37 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/usr/bin/cpan install Digest::SHA
Mar  8 11:48:56 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/usr/bin/cpan install Template
Mar  8 14:07:50 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/usr/bin/myisamchk -c -v -u /var/lib/mysql/crl/*
Mar  8 14:07:58 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/usr/bin/myisamchk -c -v -u /var/lib/mysql/crl
Mar  8 14:08:06 localhost sudo: jmrenouard : TTY=pts/0 ; PWD=/home/jmrenouard ;
USER=root ; COMMAND=/usr/bin/myisamchk -c -v -u /var/lib/mysql/crl/*
```

8.3 Suppression du droits de connexion pour le super utilisateur

Pour finir de la configuration d'accès sécurisé au serveur et que des utilisateurs ont le droit usurper l'identité du super utilisateur, il suffit d'interdire la connexion du super utilisateur lui-même sur la plateforme.
Cette technique évite les attaques de type "brute force ssh attack" courant sur Internet.

Le fichier **/etc/passwd** doit contenir un astérisque en 2ème champ pour interdire tout mot de passe pour l'utilisateur root.
$ vim root /etc/passwd

```
 root:*:…
```

8.4 Choix des mots de passes de qualité pour le super-utilisateur et l'ensemble des comptes privilégiés

Il est impératif de sécuriser l'ensemble des utilisateurs avec un mot de passe de grande qualité. Ceci est d'autant plus vrai que le compte peut usurper les droits du super-utilisateur.

Voici donc un lien vers une application en ligne capable de valider le niveau de sécurité de votre mot de passe :

http://www.microsoft.com/protect/yourself/password/checker.mspx

9 Mise en place d'utilitaire de sécurité

9.1 Utilitaire d'analyse de log

Un analyseur de log permet de connaître au niveau système d'état général du serveur. Le rapport peut et doit être envoyer par email soit en local ou à une adresse externe d'un exploitant.

Ce rapport indique les grandes lignes de l'état du serveur.

Le programme logwatch est idéal pour ce genre de tâche
$ sudo yum -y install logwatch

L'analyse des traces a lieu une fois par jour et un mail est envoyé à l'utilisateur root du serveur.

Cet outil peut être configuré pour permettre en avant les erreurs au niveau des applications.

$ sudo /usr/share/logwatch/scripts/logwatch.pl --print

9.2 Mise sous surveillance des disques avec SMART

La mise sous surveillance des disques est une opération permettant de prévenir des crash de disque. En effet, la mise sous surveillance des disques peut être simplement réalisée par le protocole SMART fonctionnant sur l'ensemble des disques durs IDE/ATA/SCSI.

$ df
```
Filesystem    Type    Size  Used Avail Use% Mounted on
/dev/sda1     ext3     16G  2.0G   14G  13% /
/dev/sdb1     ext3     17G  306M   16G   2% /home
none         tmpfs    502M     0  502M   0% /dev/shm
```

$ cat /etc/smartd.conf
```
/dev/sda -a
/dev/sdb -a
```

9.2.1 Activation du protocole SMART

$ sudo service smartd restart
$ sudo chkconfig –level=12345 smartd on

$ sudo smartctl –a /dev/sda1
$ sudo smartctl –a /dev/sdb1

```
# Lancement d'un test court
```
$ sudo smartctl –t short /dev/sdb1
…
$ sudo smartctl --smart=on --offlineauto=on --saveauto=on /dev/sdb1
```
smartctl version 5.1-11 Copyright (C) 2002-3 Bruce Allen
Home page is http://smartmontools.sourceforge.net/

Informational Exceptions (SMART) enabled
Temperature warning enabled
$  sudo smartctl --smart=on --offlineauto=on --saveauto=on  /dev/sda1
```

```
smartctl version 5.1-11 Copyright (C) 2002-3 Bruce Allen
Home page is http://smartmontools.sourceforge.net/

Informational Exceptions (SMART) enabled
Temperature warning enabled
…
```

9.3 Mise sous surveillance de modification de certains répertoires

Un analyseur de modification permet de mettre en évidence des modifications survenues sur un répertoire sur le serveur. Cela permet d'attendre 2 objectifs majeurs :

- La prévention des erreurs non volontaires par exemple dans le répertoire de configuration.
- La prévention des installations de chevaux de troie dans le répertoire des binaires par exemple.

9.3.1 Utilitaire de surveillance des altérations de répertoire :afick

$ sudo vim /etc/afick.conf

```
…
```

$ sudo rpm -ivh afick-2.1.noarch.rpm

```
#Validation de la configuration
```
$ sudo afick -C -c /etc/afick.conf

```
# config file /etc/afick.conf ok

$  sudo afick -u -c /etc/afick.conf
# Afick (2.19) update at 2011/11/10 15:54:33 with options (/etc/afick.conf):
# database:=/var/lib/afick/afick
# history:=/var/lib/afick/history
# archive:=/var/lib/afick/archive
# report_url:=stdout
# running_files:=1
# timing:=1
# exclude_suffix:= log LOG html htm HTM txt TXT xml
# max_checksum_size:=10000000
# last run on 2006/03/08 15:52:01 with afick version 2.8-2
new file : /var/lib/afick/afick.ctr
new file : /var/lib/afick/afick.dir
new file : /var/lib/afick/afick.pag
changed file : /etc/afick.conf

# detailed changes
new file : /var/lib/afick/afick.ctr
        inode_date               : Wed Mar  8 15:52:52 2006
new file : /var/lib/afick/afick.dir
        inode_date               : Wed Mar  8 15:54:33 2006
new file : /var/lib/afick/afick.pag
        inode_date               : Wed Mar  8 15:55:09 2006
changed file : /etc/afick.conf
        md5                      : Lb1Xd1ropZoWs3eFLlxmSQ
rjgzjzvyE9Th1W2Liv7L7w
        inode                    : 228985       229196
        filesize                 : 4386 4387
```

```
        mtime                     : Wed Mar  8 15:52:00 2006     Wed Mar  8
15:54:16 2006
        ctime                     : Wed Mar  8 15:52:00 2006     Wed Mar  8
15:54:16 2006

# Hash database updated successfully : 34930 files scanned, 4 changed (new : 3;
delete : 0; changed : 1; dangling : 6; exclude_suffix : 90; exclude_prefix : 0;
exclude_re : 0; degraded : 4)
# ###################################################################
# MD5 hash of /var/lib/afick/afick => StOLSBHwHP2xJ9Jvis/RAQ

# user time : 21.86; system time : 4.28; real time : 37

#Second lancement
$ sudo afick -u -c /etc/afick.conf
# Afick (2.8-2) update at 2006/03/08 15:56:40 with options (/etc/afick.conf):
# database:=/var/lib/afick/afick
# history:=/var/lib/afick/history
# archive:=/var/lib/afick/archive
# report_url:=stdout
# running_files:=1
# timing:=1
# exclude_suffix:= log LOG html htm HTM txt TXT xml
# max_checksum_size:=10000000
# last run on 2006/03/08 15:54:33 with afick version 2.8-2


# Hash database updated successfully : 34930 files scanned, 0 changed (new : 0;
delete : 0; changed : 0; dangling : 6; exclude_suffix : 90; exclude_prefix : 0;
exclude_re : 0; degraded : 4)
# ###################################################################
# MD5 hash of /var/lib/afick/afick => StOLSBHwHP2xJ9Jvis/RAQ

# user time : 21.48; system time : 3.64; real time : 27
..
```

9.4 Mise en place d'un audit automatique de la présence de rootkit

Chkrootkit est un utilitaire de validation de la non présence de rootkits sur une machine. Un rootkit étant un programme binaire substituant un utilitaire du système pour permettre l'usurpation frauduleuse de droits.

$ sudo tar xzvf chkrootkit.tar.gz

```
chkrootkit-0.49
chkrootkit-0.49/ifpromisc.c
chkrootkit-0.49/COPYRIGHT
chkrootkit-0.49/chkdirs.c
chkrootkit-0.49/check_wtmpx.c
chkrootkit-0.49/chkrootkit.lsm
chkrootkit-0.49/Makefile
chkrootkit-0.49/ACKNOWLEDGMENTS
chkrootkit-0.49/README.chkwtmp
chkrootkit-0.49/chklastlog.c
chkrootkit-0.49/chkrootkit
chkrootkit-0.49/chkutmp.c
chkrootkit-0.49/chkwtmp.c
chkrootkit-0.49/README
```

```
chkrootkit-0.49/README.chklastlog
chkrootkit-0.49/strings.c
chkrootkit-0.49/chkproc.c
```

$ sudo cd chkrootkit-0.49

$ sudo make

$ sudo ./chkrootkit

…

Bien sûr, il est évident que la compilation peut être réalisée sur une autre machine afin d'éviter l'installation d'un compilateur sur la plateforme de production.
Il faut cependant prendre un peu de recul vis-à-vis de cette technologie en effet, ce logiciel n'a pas été mis à jour depuis août 2009

9.5 Configuration d'un pare-feu local et d'un détecteur d'attaque réseau

Un pare-feu local sur les frontaux peut-être installe pour éviter toutes connections sur le serveur en dehors des ports http(80), HTTPS(443), SSH(22).

$ sudo iptables –L

$ sudo iptables-save

```
# Generated by iptables-save v1.2.8 on Wed Mar  8 16:31:18 2006
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [25400502:18548269096]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp -m icmp --icmp-type 255 -j ACCEPT
-A RH-Firewall-1-INPUT -p esp -j ACCEPT
-A RH-Firewall-1-INPUT -p ah -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Wed Mar  8 16:31:18 2006
```

Un utilitaire de configuration de pare-feu existe sous Red Hat : redhat-config-security-gui
Attention, sans la consultation des fichiers de configuration, il est difficile de connaître l'intégralité des règles de filtrage comme par exemple les règles de redirection de port.

9.5.1 Mise en place de réaction automatique aux connexions non autorisées

Il est possible avec un utilitaire comme portsentry de suivre l'ensemble des tentatives de connexions sur un serveur, de les tracer et d'y apporter une réponse automatique (blocage du port, effet miroir, …)

$ sudo rpm -ivh portsentry-1.2-2.i386.rpm

$ sudo vim /etc/portsentry/portsentry.conf

…

$ sudo service portsentry start

$ sudo chkconfig –level=12345 portsentry on

9.6 Restriction des connexions au serveur X

Pour éviter des prises de main à distance sur le serveur X au cas où les équipes d'exploitation souhaitent pouvoir se connecter via une interface graphique, il est possible de limiter les connexions depuis le serveur lui-même.

9.7 Mise en place du suivi standard

L'activation des serveurs **snmpd** et **snmptrapd** provenant du paquet RPM **net-snmp** permettent de réaliser une démarche de suivi de performances et des d'indicateurs principaux au niveau système, applicatif et réseau.

Les fichiers de configuration sont respectivement **/etc/snmpd.conf** et **/etc/snmptrad.conf.**

$ sudo service snmpd restart

$ sudo service snmptrapd restart

$ sudo chkconfig –level=12345 snmpd on

$ sudo chkconfig –level=12345 snmptrapd on

10 Gestion du document

Adresser toute remarque sur ce document au responsable de sa gestion:

Jean-Marie Renouard jmrenouard@123solution.fr