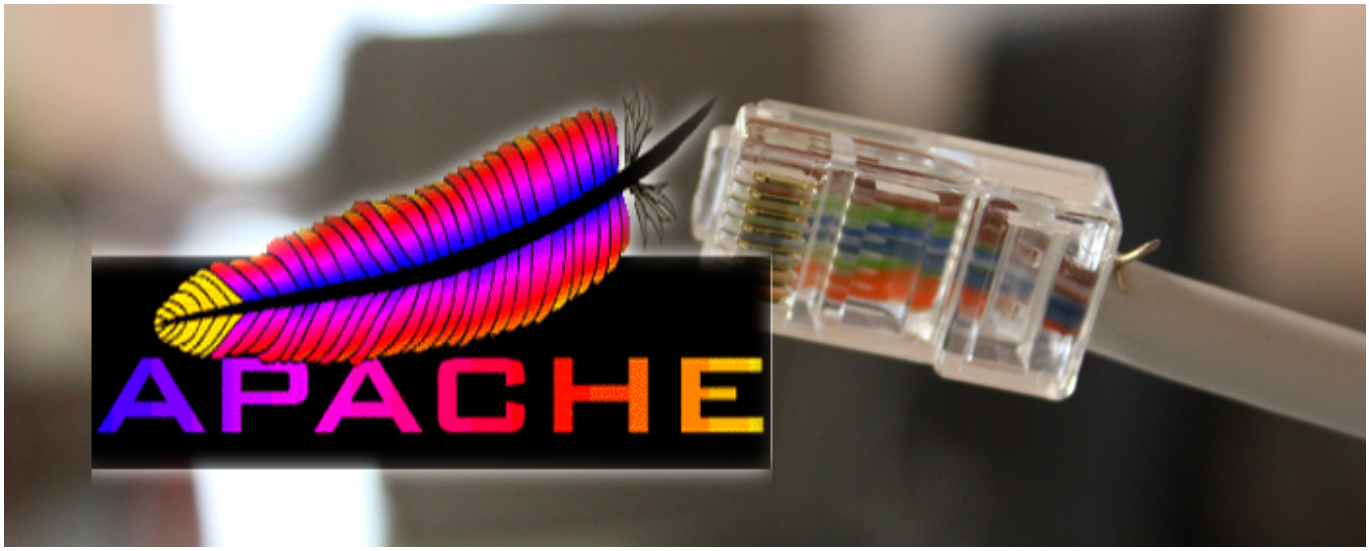
Introduction à Apache et Sécurisation de votre accés Web #GMSI19 R

by tontonfred - mercredi, février 01, 2017

http://www.tontonfred.net/blog/?p=1401



Pour notre TD : Attention (Adapter en fonction de la version du Debian)

Pour une version 9.X de Debian prendre la ISO du DVD1 pour avoir l'interface graphique de base afin de pouvoir paramétrer le navigateur et pouvoir traverser le proxy du Cesi.

Installer nano

```
apt-get install nano
```

Sources.list a modifier pour une 9.X

```
deb http://deb.debian.org/debian stretch main
deb-src http://deb.debian.org/debian stretch main

deb http://deb.debian.org/debian-security/ stretch/updates main
deb-src http://deb.debian.org/debian-security/ stretch/updates main
```

```
deb http://deb.debian.org/debian stretch-updates main
deb-src http://deb.debian.org/debian stretch-updates main
deb http://deb.debian.org/debian stretch main contrib non-free
deb-src http://deb.debian.org/debian stretch main contrib non-free

deb http://deb.debian.org/debian-
security/ stretch/updates main contrib non-free
deb-src http://deb.debian.org/debian-
security/ stretch/updates main contrib non-free

deb http://deb.debian.org/debian stretch-updates main contrib non-free
deb-src http://deb.debian.org/debian stretch-updates main contrib non-
free
```

Charger les modifs du sources.list

```
apt-get update
```

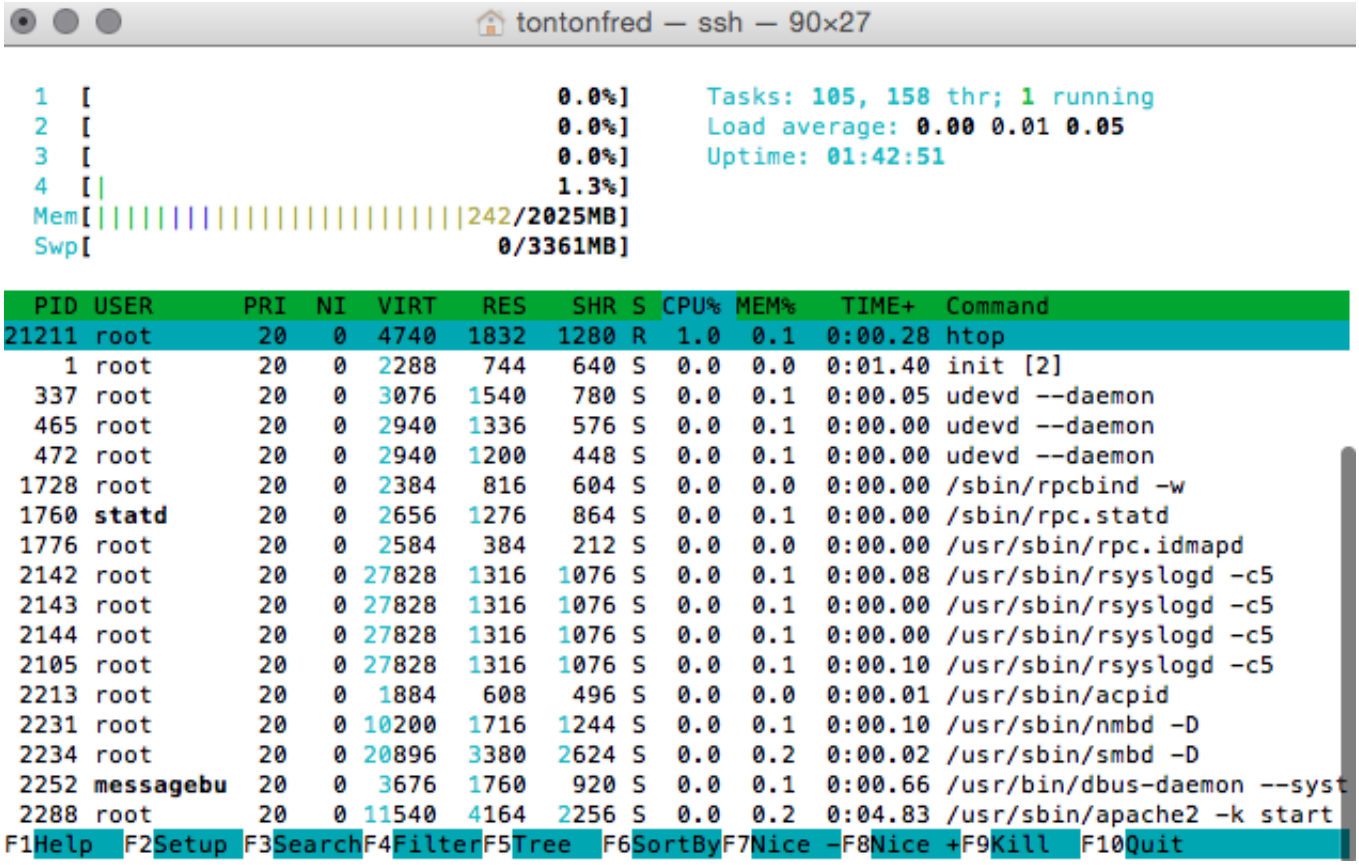
Mise en place EtcKeeper

```
apt-get install etckeeper
```

Outils pour surveiller votre serveur WEB

Installez htop (plus sympa que top)

```
apt-get install htop
```



install pour la suite des différents TD

```
apt-get install mysql-client mysql-
server openssl rkhunter binutils clamav
```

Install pour la suite des différents TD

```
apt-get install apache2 apache2.2-common apache2-doc apache2-mpm-worke
r libapache2-mod-fastcgi php5-fpm php-apc apache2-utils libexpat1 ssl-
```

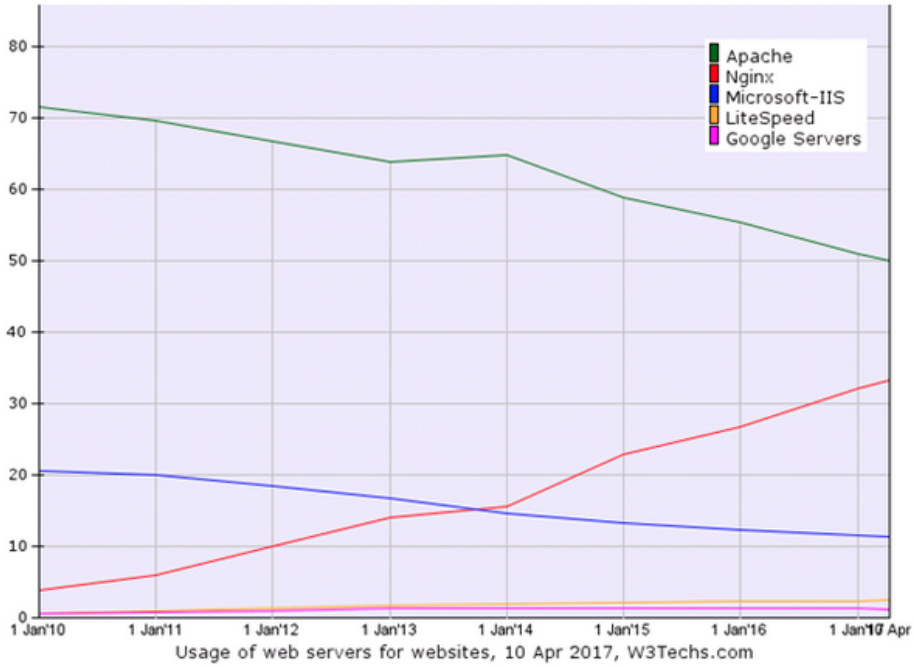
```
cert php5 php5-common php5-gd php5-mysql php5-imap php5-cli php5-cgi l
ibapache2-mod-fcgid apache2-suexec php-pear php-auth php5-mcrypt mcryp
t php5-imagick imagemagick libapache2-mod-python php5-curl php5-intl
php5-pspell php5-recode php5-snmp php5-sqlite php5-tidy php5-xmlrpc ph
p5-xsl
```

Installer Glances

```
apt-get install glances

####pour lancer glances#####
glances
```

Apache est un serveur http libre, c'est un des serveurs http les plus utilisé sur Internet



Part de Marché Serveur Web 2017

Apache est conçu pour prendre en charge de nombreux modules lui donnant des fonctionnalités supplémentaires : interprétation du langage Perl, PHP, Python et Ruby, serveur proxy, Common Gateway Interface, Server Side Includes, réécriture d'URL, négociation de contenu, protocoles de communication additionnels, etc. Néanmoins, il est à noter que l'existence de nombreux modules Apache complexifie la configuration du serveur web. En effet, les bonnes pratiques recommandent de ne charger que les modules utiles : de nombreuses failles de sécurité affectant uniquement les modules d'Apache sont régulièrement découvertes.

On trouvera une documentation complète sur apache (en anglais) sur le site suivant : *http://httpd.apache.org/docs/*.

Redémarrer Apache

```
 service apache2 restart
#######ou###############
/etc/init.d/apache2 restart
```

Tester la syntaxe pour éviter de planter Apache

```
apache2ctl -t
#en prod évite de planter Apache si erreur de Syntaxe
```

Redémarre Apache en Prod sans perturber les visiteurs

```
apache2ctl graceful
```

Vérifier que apache tourne

```
ps -ef|grep apache
```

INFO IMPORTANTE

```
Pour simuler des noms de domaine pensez à modifier le fichier hosts de
 votre poste client
```

La con?guration globale d'apache s'e?ectue par modi?cation du ?chier de con?guration */etc/apache2/apache2.conf*.

Hôtes Virtuels

Cette méthode est la plus utilisée et la plus conseillée. Elle tend même à devenir un standard. Il s'agit simplement d'associer plusieurs **noms DNS** à une seule adresse IP.

dans **/etc/apache2/sites-available** se trouve un fichier nommé *default.*..

il ressemble a ceci:

Exemple de Virtualhost

```
<VirtualHost *:80>
 ServerAdmin votre-mail@monsite1.fr
 ServerName monsite1.fr
 ServerAlias www.monsite1.fr

 DocumentRoot /var/www/monsite1
 <Directory />
  Options FollowSymLinks
  AllowOverride None
 </Directory>
 <Directory /var/www/monsite1>
  Options Indexes FollowSymLinks MultiViews
  AllowOverride None
  Order allow,deny
  allow from all
 </Directory>

 ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
 <Directory "/usr/lib/cgi-bin">
  AllowOverride None
  Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
  Order allow,deny
  Allow from all
 </Directory>

 ErrorLog /var/log/apache2/error.log

 # Possible values include: debug, info, notice, warn, error, crit,
 # alert, emerg.
 LogLevel warn

 CustomLog /var/log/apache2/access.log combined

    Alias /doc/ "/usr/share/doc/"
```

```
    <Directory "/usr/share/doc/">
        Options Indexes MultiViews FollowSymLinks
        AllowOverride None
        Order deny,allow
        Deny from all
        Allow from 127.0.0.0/255.0.0.0 ::1/128
    </Directory>

</VirtualHost>
```

Ceci fait, enregistrez le fichier sous le nom **monsite1.conf** puis modifiez-le en mettant cette fois **monsite2** à la place de **monsite1**, puis ré-enregistrez sous le nom de **monsite2.conf**.

Pour terminer, il vous suffit de créer des liens des deux fichiers nouvellement créés dans le sites-available à l'aide d'un script des fichiers créés auparavant dans le dossier **/etc/apache2/sites-enabled**. Pour ce faire, une commande a été faite spécialement :

créer les liens dans sites-available

```
a2ensite monsite1.conf
a2ensite monsite2.conf

etc..
```

Rédémarrer ensuite les services comme vu au dessus ..

Par exemple pour vérifier les dernières IP qui ont visité votre site web vous pouvez faire un petit tail

Et Voila !!!!!!!!!

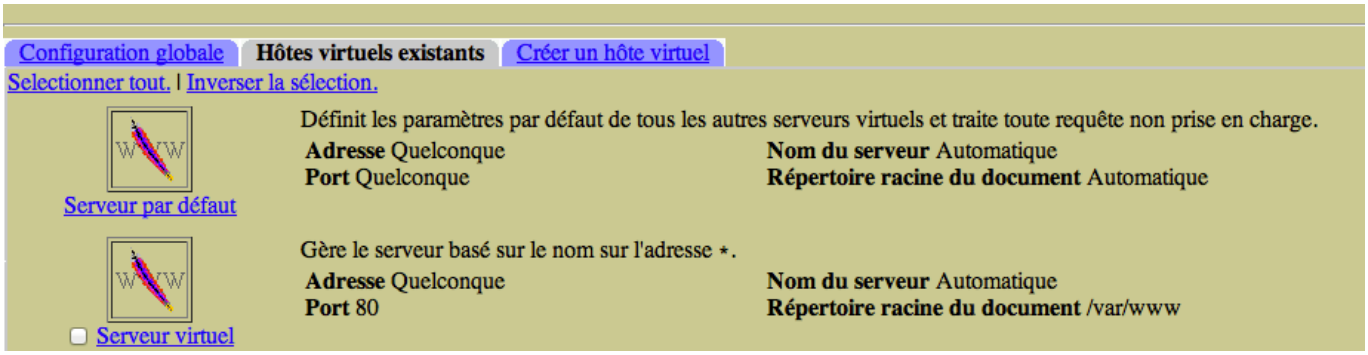
Un version plus user friendly ici avec Webmin

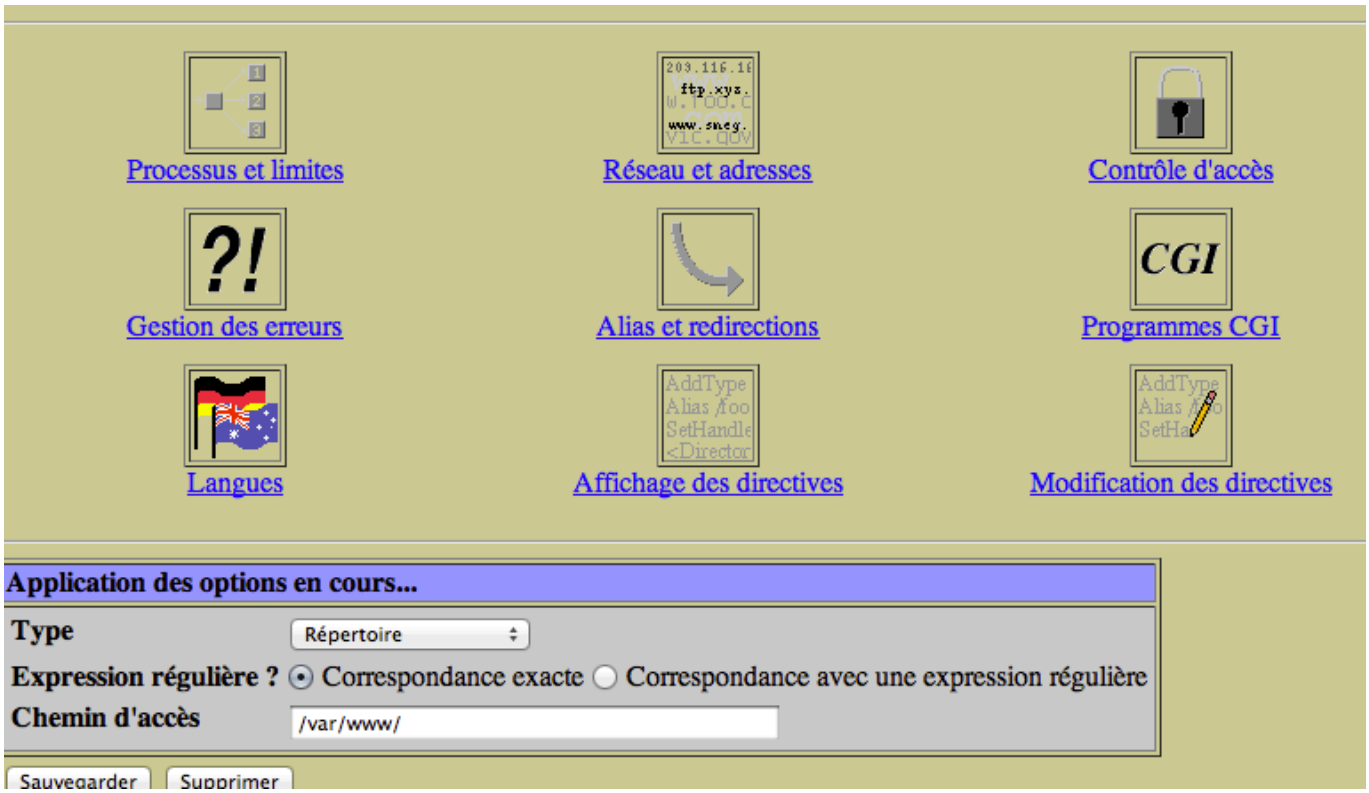
Installation de Webmin

Install de Webmin

```
dpkg -i webmin_de la version que tu as_all.deb
######ensuite#######
#####Corrigez les erreurs avec####
apt-get install -f
```

Apache dans Webmin





Pour aller plus loin :

Sécuriser Apache et son serveur

Tout d'abord Retour sur SSH qui va permettre d'accéder à votre serveur pour l'administrer. Merci a Alsacreation pour la personnalisation des scripts..

Configuration SSH

Afin de sécuriser l'accès SSH au serveur, éditons le fichier **/etc/ssh/sshd_config**. Nous allons changer le port de connexion par défaut pour éviter quelques attaques par bruteforce sur le port 22, qui est bien connu pour héberger ce service. N'oubliez pas de préciser ce nouveau port (dans Putty ou en ligne de commande ssh sous Linux) à la prochaine connexion.

vi /etc/ssh/sshd_config

```
Port 2222                   # Changer le port par défaut
PermitRootLogin no          # Ne pas permettre de login en root
Protocol 2                  # Protocole v2
AllowUsers dew              # N'autoriser qu'un utilisateur précis
```

Redémarrez le service SSH après ces modifications :

/etc/init.d/ssh restart

Alerte login Root

Vous pouvez éditer le fichier **/root/.bashrc** qui est exécuté au démarrage d'une sesion root pour envoyer un e-mail de notification. De cette façon, vous serez prévenu lorsqu'un login est effectué.

vi /root/.bashrc

Ajoutez la ligne (en modifiant l'adresse e-mail de destination) :

```
echo 'Accès Shell Root le ' `date` `who` | mail -s `hostname` Shell Ro
ot de `who | cut -d"(" -f2 | cut -d")" -f1` monitoring@test.com
```

Profitons-en pour un peu de personnalisation esthétique avec ces lignes :

```
alias ls='ls $LS_OPTIONS --color=auto'
alias ll='ls $LS_OPTIONS -al --color=auto'
alias vi='vim'
```

Mise en place d'un Firewall *(source alsacreations)*

vi /etc/init.d/firewall

```
#!/bin/sh

# Vider les tables actuelles
```

```
iptables -t filter -F

# Vider les règles personnelles
iptables -t filter -X

# Interdire toute connexion entrante et sortante
iptables -t filter -P INPUT DROP
iptables -t filter -P FORWARD DROP
iptables -t filter -P OUTPUT DROP

# ---

# Ne pas casser les connexions etablies
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

# Autoriser loopback
iptables -t filter -A INPUT -i lo -j ACCEPT
iptables -t filter -A OUTPUT -o lo -j ACCEPT

# ICMP (Ping)
iptables -t filter -A INPUT -p icmp -j ACCEPT
iptables -t filter -A OUTPUT -p icmp -j ACCEPT

# ---

# SSH In
iptables -t filter -A INPUT -p tcp --dport 2222 -j ACCEPT

# SSH Out
iptables -t filter -A OUTPUT -p tcp --dport 2222 -j ACCEPT

# DNS In/Out
iptables -t filter -A OUTPUT -p tcp --dport 53 -j ACCEPT
iptables -t filter -A OUTPUT -p udp --dport 53 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 53 -j ACCEPT
iptables -t filter -A INPUT -p udp --dport 53 -j ACCEPT

# NTP Out
iptables -t filter -A OUTPUT -p udp --dport 123 -j ACCEPT
```

Si vous hébergez un sevreur web (Apache) :

```
# HTTP + HTTPS Out
```

```
iptables -t filter -A OUTPUT -p tcp --dport 80 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 443 -j ACCEPT

# HTTP + HTTPS In
iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 8443 -j ACCEPT
```

Si vous hébergez un serveur FTP :

```
# FTP Out
iptables -t filter -A OUTPUT -p tcp --dport 20:21 -j ACCEPT

# FTP In
modprobe ip_conntrack_ftp # ligne facultative avec les serveurs OVH
iptables -t filter -A INPUT -p tcp --dport 20:21 -j ACCEPT
iptables -t filter -A INPUT -m state --state ESTABLISHED,RELATED -j AC
CEPT
```

Si vous hébergez un serveur de mail avec SMTP, POP3 et IMAP :

```
# Mail SMTP:25
iptables -t filter -A INPUT -p tcp --dport 25 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 25 -j ACCEPT

# Mail POP3:110
iptables -t filter -A INPUT -p tcp --dport 110 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 110 -j ACCEPT

# Mail IMAP:143
iptables -t filter -A INPUT -p tcp --dport 143 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 143 -j ACCEPT

# Mail POP3S:995
iptables -t filter -A INPUT -p tcp --dport 995 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 995 -j ACCEPT
```

N’oubliez pas de tester vos régles !!! Exemples, elles pourraient vous empêcher d’accéder à votre accés ssh si elles sont trop restrictives.

N’oubliez pas non plus de redémarrer le sevice firewall aprés les modifs..

##

IPtables / Netfilter

IPtables (associé à Netfilter) est un des meilleurs firewalls pour Linux, et certainement le plus répandu. Vous pourrez trouver de nombreux scripts de configuration à son sujet. En voici un, à adapter à votre configuration. A tout instant, utilisez la commande iptables -L -v pour lister les règles en place.

Celles-ci portent sur 3 chaînes : INPUT (en entrée), FORWARD (dans le cas d’un routage réseau) et OUPUT (en sortie). Les actions à entreprendre sont *ACCEPT* (accepter le paquet), *DROP* (le jeter), *QUEUE* et *RETURN*.

Arguments utilisés :

- i : interface d’entrée (input)
- i : interface de sortie (output)
- t : table (par défaut *filter* contenant les chaînes INPUT, FORWARD, OUTPUT)
- j : règle à appliquer (Jump)
- A : ajoute la règle à la fin de la chaîne (Append)
- I : insère la règle au début de la chaîne (Insert)
- R : remplace une règle dans la chaîne (Replace)
- D : efface une règle (Delete)
- F : efface toutes les règles (Flush)
- X : efface la chaîne
- P : règle par défaut (Policy)
- lo : localhost (ou 127.0.0.1, machine locale)

##

Fail2ban

Fail2ban est un script surveillant les accès réseau grâce aux logs des serveurs. Lorsqu’il détecte des erreurs d’authentification répétées, il prend des contre-mesures en bannissant l’adresse IP grâce à **iptables**. Cela permet d’éviter nombre d’attaques *bruteforce* et/ou par dictionnaire.

Installation

apt-get install fail2ban

Configuration

vi /etc/fail2ban/fail2ban.conf

loglevel
: Niveau de détail des logs (défaut 3)

logtarget = /var/log/fail2ban.log
: Chemin vers le fichier de log (description des actions entreprises par fail2ban)

Les services à monitorer sont stockés dans **jail.conf**. Il est recommandé d'en effectuer une copie nommée **jail.local** qui sera automatiquement utilisée à la place du fichier exemple.

cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

vi /etc/fail2ban/jail.local

Quelques paramètres globaux :

ignoreip = 127.0.0.1
: Liste des adresses IP de confiance à ignorer par fail2ban

bantime = 600
: Temps de ban en secondes

maxretry = 3
: Nombre d'essais autorisés pour une connexion avant d'être banni

destmail monitoring@test.com
: Adresse e-mail destinataire des notifications

action
: Action à entreprendre en cas de détection positive (voir dans /etc/fail2ban/action.d/)

Chaque section possède ses propres paramètres qui prennent le pas sur les globaux s'ils sont mentionnés :

enabled
: Monitoring activé (true) ou non (false)

maxretry, bantime, ignoreip, destmail
: Voir ci-dessus

port
: Port IP concerné

logpath
: Fichier de log à analyser pour détecter des anomalies

filter
: Filtre utilisé pour l'analyser du log

Les filtres par défaut sont stockés dans **/etc/fail2ban/filter.d**. Ils contiennent en général une instruction **failregex** suivie d'une expression régulière matchant la détection d'une authentification erronée. Par exemple pour le service Courier :

```
failregex = LOGIN FAILED, ip=[<HOST>]$
```

Note : Celle-ci peut être précisée directement dans **jail.local** à la section appropriée pour prendre le pas sur la directive **filter**.

Modifiez les ports le cas échéant dans la section *ssh* si vous avez suivi la recommandation ci-dessus…

```
enabled = true
port    = 2222
```

Après modification de la configuration, n'oubliez pas de redémarrer fail2ban : /etc/init.d/fail2ban restart

Rkhunter

Rootkit Hunter est un programme de détection de rootkits. Vous pouvez l'installer grâce à :

apt-get install rkhunter

Il procédera à des détections journalières anti-rootkits et enverra des notifications par e-mail si nécessaire. Il est conseillé de l'installer très tôt car il calcule l'empreinte MD5 des programmes installés afin de détecter d'éventuels changements. Editez **/etc/default/rkhunter** pour indiquer l'adresse de notification et l'exécution journalière :

vi /etc/default/rkhunter

```
REPORT_EMAIL="monitoring@test.com"
CRON_DAILY_RUN="yes"
```

En cas de fausses détections positives sur des répertoires ou fichiers existants et sains, éditez **/etc/rkhunter.conf** pour les ajouter à la liste des éléments autorisés.

vi /etc/rkhunter.conf

```
ALLOWHIDDENDIR=/dev/.udev
ALLOWHIDDENDIR=/dev/.static
```

Vous pouvez également utiliser **chkrootkit** qui est un équivalent.

Empêcher l’accès aux sous dossiers

Bloquer l’accès à *PhpMyAdmin* par exemple.

Sur un reverse proxy

```
/etc/apache2/apache2.conf
RewriteCond %{THE_REQUEST} /phpmyadmin/
RewriteRule ^.*$ - [G,L]
```

Via le .htaccess

Renvoie un code 403.

```
RewriteRule ^phpMyAdmin - [F]
```

Empêcher l’accès à la racine de apache

```
/etc/apache2/sites-available/default
et /etc/apache2/sites-available/default-ssl
<Directory /var/www/>
                Options -Indexes FollowSymLinks MultiViews
                AllowOverride All
                Order allow,deny
                deny from all
</Directory>
```

Désactiver le listage des répertoires

Changer *« Indexes »* en *« -Indexes »*.

```
/etc/apache2/sites-available/default
/etc/apache2/sites-available/default-ssl
et les configurations des vhosts
```

Attribuer les permissions correctement

```
cd /var/www
chown www-monsite:www-monsite -R *
find . -type f -exec chmod 644 {} \;
find . -type d -exec chmod 755 {} \;
```

installer wordpress

```
apt-get install wordpress curl mysql-server
```

Créer le site

```
# nano /etc/apache2/sites-available/wp
```

Ajouter ceci au fichier wp

```
Alias /wp/wp-content /var/lib/wordpress/wp-content
        Alias /wp /usr/share/wordpress
        <Directory /usr/share/wordpress>
            Options FollowSymLinks
            AllowOverride Limit Options FileInfo
            DirectoryIndex index.php
            Order allow,deny
            Allow from all
```

```
        </Directory>
        <Directory /var/lib/wordpress/wp-content>
            Options FollowSymLinks
            Order allow,deny
            Allow from all
        </Directory>
```

rendre actif le site

```
a2ensite wp
```

relancer le service

```
service apache2 reload
#####ou#####@
service apache2 restart
```

creer le fichier config-dev.php

```
nano /etc/wordpress/config-dev.php
```

ajouter ce code au fichier

```
<?php
define('DB_NAME', 'wordpress');
define('DB_USER', 'wordpress');
define('DB_PASSWORD', 'password');
define('DB_HOST', 'localhost');
define('WP_CONTENT_DIR', '/var/lib/wordpress/wp-content');
?>
```

creer un fichier de config pour sql

```
nano ~/wp.sql
```

adapter pour le fichier

```
CREATE DATABASE wordpress;
GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP,ALTER
ON wordpress.*
TO wordpress@localhost
IDENTIFIED BY 'password';
FLUSH PRIVILEGES;
```

créer la base

```
cat ~/wp.sql | mysql --defaults-extra-file=/etc/mysql/debian.cnf
```

Envoyer l'article en PDF

PDF generated by Kalin's PDF Creation Station