Apache Web server (Installation, Security and Hardening) – Version :3 (Last Update: 9th January 2016)

The following packages should require to install a web server:-

apt-get update
apt-get install ssh
apt-cache policy apache2 (On Debian based OS)
apt-get install apache2 (On Debian based OS)
apt-get install mysql mysql-server mysql-client (On Debian based OS)
apt-get install php5 libapache2-mod-auth-mysql php5-mysql (On Debian based OS)
Among of these packages, no need to install additional or extra packages!!

Before we apply these changes in your web server, we should have some basics of the Apache server.

1. Document root Directory: **/var/www/html** or **/var/www**
2. Main Configuration file: **/etc/httpd/conf/httpd.conf** (RHEL/CentOS/Fedora) and **/etc/apache/apache2.conf** (Debian/Ubuntu).
3. Default HTTP Port: **80** TCP
4. Default HTTPS Port: **443** TCP
5. Test your Configuration file settings and syntax: **httpd -t**
6. Access Log files of Web Server: **/var/log/httpd/access_log**
7. Error Log files of Web Server: **/var/log/httpd/error_log**

Apache hardening below:

For Ubuntu:

---

cd /etc/apache2/
chown 0 . apache2.conf ports.conf conf-available sites-available
chgrp 0 . apache2.conf ports.conf conf-available sites-available
chmod 755 . apache2.conf ports.conf conf-available sites-available

cd /var/log
chown 0 . apache2
chgrp 0 . apache2
chmod 755 . apache2

cd */usr/sbin/*
chown 0 . apache2 apache2ctl
chgrp 0 . apache2 apache2ctl
chmod 755 . apache2 apache2ctl

For CentOS

---

cd */etc/httpd/conf/*
chown 0 . httpd.conf
chgrp 0 . httpd.conf
chmod 755 . httpd.conf

cd /var/log
chown 0 . httpd
chgrp 0 . httpd
chmod 755 . httpd

cd */usr/sbin/*
chown 0 . apache2 apache2ctl
chgrp 0 . apache2 apache2ctl
chmod 755 . apache2 apache2ctl

Module enable: vi /etc/httpd/conf.d/modsecurity.conf
SecRuleEngine On

A. Disabled "SELINUX" for both Centos and Debian, but another additional security rule "appormor" it also should be off and uninstall the package!!

B. Increase the "ip_conntrack_max" from /proc/sys/net/ipv4/netfilter/ location and write it to rc.local file (Calculation: Physical memory Like, 32G will be 3200M x 16) is maximum!!

C. Hide Apache Version and OS Identity from Errors >>

vim /etc/apache/apache2.conf (Debian/Ubuntu)

ServerSignature Off
ServerTokens Prod

service apache2 restart (Debian/Ubuntu)

D. Disable Directory Listing >>

We can **turn off** directory listing by using **Options directive** in configuration file for a specific directory. For that we need to make an entry in **httpd.conf** or **apache2.conf** file

<Directory /var/www/html>
Options -Indexes
</Directory

E. Disable Unnecessary Modules (For apache and php)

It's always good to minor the chances of being a victim of any **web attack**. So it's recommended to disable all those **modules** that are not in use currently. You can list all the compiled modules of web server, using following command.

grep LoadModule /etc/httpd/conf/httpd.conf

```
# have to place corresponding `LoadModule' lines at this location so the
# LoadModule foo_module modules/mod_foo.so
LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule auth_digest_module modules/mod_auth_digest.so
LoadModule authn_file_module modules/mod_authn_file.so
LoadModule authn_alias_module modules/mod_authn_alias.so
LoadModule authn_anon_module modules/mod_authn_anon.so
LoadModule authn_dbm_module modules/mod_authn_dbm.so
LoadModule authn_default_module modules/mod_authn_default.so
LoadModule authz_host_module modules/mod_authz_host.so
LoadModule authz_user_module modules/mod_authz_user.so
LoadModule authz_owner_module modules/mod_authz_owner.so
LoadModule authz_groupfile_module modules/mod_authz_groupfile.so
LoadModule authz_dbm_module modules/mod_authz_dbm.so
LoadModule authz_default_module modules/mod_authz_default.so
LoadModule ldap_module modules/mod_ldap.so
LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
LoadModule include_module modules/mod_include.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule logio_module modules/mod_logio.so
LoadModule env_module modules/mod_env.so
```

LoadModule ext_filter_module modules/mod_ext_filter.so
....

Above is the list of modules that are enabled by default but often not needed: **mod_imap**, **mod_include**, **mod_info**, **mod_userdir**, **mod_autoindex**. To disable the particular module, you can insert a "**#**" at the beginning of that line and restart the service.

F. Run Apache as a separate User and Group:-

With a default installation **Apache** runs its process with user **nobody** or **daemon**. For security reasons it is recommended to run **Apache** in its own **non-privileged** account. For example: **http-web**.

```
# groupadd http-web
# useradd -d /var/www/ -g http-web -s /bin/nologin http-web

User http-web
Group http-web
```

G. Use Allow and Deny to Restrict access to Directories:-

We can restrict access to directories with "**Allow**" and "**Deny**" options in **httpd.conf** or apache.conf file. Here in this example, we'll be securing **root directory**, for that by setting the following in the **httpd.conf** or apache.conf file.

```
<Directory />
  Options None
  Order deny,allow
  Deny from all
</Directory>
```

H. Use mod_security and mod_evasive Modules to Secure Apache

Where **mod_security** works as a **firewall** for our web applications and allows us to **monitor traffic** on a real time basis. It also helps us to protect our websites or web server from **brute force attacks**. You can simply install **mod_security** on your server with the help of your default package installers.

apt-get install mod_security mod_evasive

```
$ sudo apt-get install libapache2-modsecurity
$ sudo a2enmod mod-security
$ sudo /etc/init.d/apache2 force-reload
```

mod_evasive works very efficiently, it takes one request to process and processes it very well. It prevents **DDOS attacks** from doing as much damage. This feature of **mod_evasive** enables it to handle the **HTTP brute force** and **Dos** or **DDos** attack. This module detects attacks with three methods.

1. If so many requests come to a same page in a few times per second.
2. If any child process trying to make more than **50** concurrent requests.
3. If any **IP** still trying to make new requests when its temporarily **blacklisted**.

mod_evasive can be installed directly from the source. Here, we have an Installation and setup guide of these modules which will help you to set up these Apache modules in your Linux box.

I. Disable Apache's following of Symbolic Links

By default **Apache** follows **symlinks**, we can **turn off** this feature with **FollowSymLinks** with **Options directive**. And to do so we need to make the following entry in main configuration file.

Options –FollowSymLinks

And, if any particular **user** or **website** need **FollowSymLinks** enable, we can simply write a rule in "**.htaccess**" file from that website.

Enable symbolic links
Options +FollowSymLinks

Note: To enable rewrite rules inside "**.htaccess**" file "**AllowOverride All**" should be present in the main configuration globally.

J. Turn off Server Side Includes and CGI Execution

We can **turn off** server side includes (**mod_include**) and **CGI** execution if not needed and to do so we need to modify main configuration file.

Options -Includes
Options –ExecCGI

We can do this for a particular directory too with Directory tag. Here In this example, we are **turning off** Includes and Cgi file executions for "**/var/www/html/web1**" directory.

<Directory "/var/www/html/web1">
Options -Includes -ExecCGI
</Directory>

K. Remove the unnecessary user from the /etc/password file!!

L. Disable the unnecessary service from startup (Like, portmap, rpc.stade, rpcbind, sysstat, cups etc.)

M. Partition Tables structure:-

Root size >> 50 GB
Var size >> maximum

If the webserver include with MYSQL, then the partition tables

Root size >> 50GB
Var size >> Maximum (GB)
Tmp size >> 40-50GB
Swap >> Double of physical memory
Boot >> 1 GB

Optional,
Home size >> As per HDD size
Usr size >> As per size (Max.25GB)

Version:3 (9th January 2016)
In Hosts file:-

Inside hosts file, database server's IP address entry should be required