Steps for Apache & Server Hardening

1. **Recommend version of LAMP** 
   1. Apache 2.2.24
   2. Php 5.5.15
   3. Phpmyadmin 4.2.8
   4. MySql 5.6.12
   5. Apache version 2.2.29 (latest version)

Download link <http://archive.apache.org/dist/httpd/httpd-2.2.29.tar.gz>

* 1. **Following points are achieved in this document** 
     1. Mod\_ssl module needs to be installed
     2. In httpd.conf file following values to be set

                 ServerSignature Off

                 ServerTokens Prod

* + 1. In /etc/php.ini file

expose\_php=off

* + 1. Disable FTP services
    2. Disable SMTP services
    3. Disable SNMP services.
    4. Disable ICMP redirect.
    5. Disable Weak ciphers.
    6. Disable HTTP Trace method.
    7. Disable Web directory browsing.

1. **Install mod\_ssl**

Yum install mod\_ssl

1. **Edit apache/httpd.conf in /**

Cd etc/http/conf/httpd.conf

Vi http.conf

**Find and set the following values**

ServerSignature Off

ServerTokens Prod

1. **DISABLE HTTP TRACKING METHODS**

To turn off track and trace methods globally on the server add the following line:

vim /etc/httpd/conf/httpd.conf

TraceEnable Off

1. **DISABLE WEB DIRECTORY BROWSING**

Open vi editor and edit file /etc/apache/httpd.conf

find the line that looks as follows:

**Options Includes Indexes FollowSymLinks MultiViews**

Then remove word Indexes and save the file. The line should look like this one:

**Options Includes FollowSymLinks MultiViews**

**Disabling specific Apache Modules**

To check which apache modules are loaded run the command -

For CentOS-

**httpd -M**

For Windows

**httpd –t –D DUMP\_MODULES**

For Ubuntu

**apachectl -t -D DUMP\_MODULES**

Disable the following apache modules -

* mod\_cgid
* mod\_status
* mod\_dav
* mod\_rewrit
* mod\_deflate
* mod\_load\_config

Disable the Apache Default Welcome Page by commenting/Deleting the line in httpd.conf -

**include ./conf.d/\***

1. **Edit php.ini**

Vi /et/php.ini

Find and change the following

Expose\_php=off

1. **Disable FTP Services**

Service vsftpd stop

Chkconfig vsftod off

1. **Disable ICMP Redirect**

You need to edit the file /etc/sysctl.conf

#For IPv4

net.ipv4.conf.all.accept\_redirects = 1

net.ipv4.conf.all.send\_redirects = 1

#For Ipv6

net.ipv6.conf.all.accept\_redirects = 1

net.ipv6.conf.all.send\_redirects = 1

1. **Disable SMTP(In our case postfix is installed)**

To check which service is used for mail

**telnet localhost 25**

**dicovered postfix not smtp**

**Turn off Postfix**

Service postfix stop

Chkconfig postfix off

1. **DISABLE SNMP**

service snmpd stop

chkconfig snmpd off

1. **DISABLE WEAK CYPHERS**

open /etc/httpd/conf.d/ssl.conf

make following entry under SSL CIPHER SUITE

SSLProtocol -ALL +SSLv3 +TLSv1

SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:!LOW:!SSLv2:!EXPORT

Port Hardening

iptables -L -n –v

iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT

iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -m state --state NEW -p tcp --dport 8080 -j ACCEPT

iptables -A INPUT -m state --state NEW -p tcp --dport 443 -j ACCEPT

iptables -I INPUT -p tcp --dport 3306 -j ACCEPT

iptables -A INPUT -m state --state NEW -p udp --dport 123 -j ACCEPT

iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

service iptables save

service iptables restart

service iptables stop  
service iptables start  
service iptables restart

iptables -n -L -v --line-numbers

iptables -L -n –v

**#3: Delete Firewall Rules**

To display line number along with other information for existing rules, enter:  
# iptables -L INPUT -n --line-numbers  
# iptables -L OUTPUT -n --line-numbers  
# iptables -L OUTPUT -n --line-numbers | less  
# iptables -L OUTPUT -n --line-numbers | grep 202.54.1.1  
You will get the list of IP. Look at the number on the left, then use number to delete it. For example delete line number 4, enter:  
# iptables -D INPUT 4  
OR find source IP 202.54.1.1 and delete from rule:  
# iptables -D INPUT -s 202.54.1.1 -j DROP