# Web Server Management Checklist

1st Hour and On…

### First things First...

* **Change given password for Server admin**

|  |
| --- |
| passwd |

New Password:

New Password: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

New Password: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

New Password: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

New Password: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* **Try to figure out what distro is running**

|  |  |
| --- | --- |
| cat /etc/\*-release  -- OR --  lsb\_release -a  -- OR -- | uname -a  -- OR --  cat /proc/version |

* **Figure out what tools are already installed (what you’ve got to work with)**

|  |
| --- |
| dpkg -l  -- OR --  rpm -qa  -- OR --  pgk\_info |

* **Backup /etc and /var**

|  |
| --- |
| cp -r /etc ~  cp -r /var ~ |

* **See what ports are “LISTEN”ing**

|  |
| --- |
| netstat -tulpn  -- OR --  netstat -na | grep -i LISTEN (Free BSD | Unix) |

If netstat is not installed, try lsof:

|  |
| --- |
| lsof -i  -- OR --  sockstat -l (Free BSD) |

**Write those ports down and save ‘em for later**

* **What’s the Server’s IP Address?**

|  |
| --- |
| ifconfig |

Internal IP: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* **Is SSH running? Shut it down (for now…)**
* **Do a quick check of the common directories (figure out any weird file organization)**
* **Check what services/processes are running**

|  |
| --- |
| top -- OR -- htop  ps aux | less (all running processes)  service --status-all \  -- OR -- | (all services)  systemctl list-unit-files /  chkconfig --list |

* **Setup gray log forwarding to a specific machine**

|  |
| --- |
| ls -a /var/log  More info on syslog needed... |

* **Check groups and user names**

|  |
| --- |
| cat /etc/passwd  cat /etc/group |

* **Put up a firewall**

|  |
| --- |
| # **iptables:**  # if using RHEL/Fedora/CentOS, edit /etc/sysconfig/iptables-config:  # make sure -> IPTABLES\_MODULES\_UNLOAD = no  iptables -P INPUT DROP # by default, drop all incoming connections  iptables -P FORWARD DROP # same for forwarded connections  iptables -P OUTPUT ACCEPT # allow outgoing connections  iptables -L -n -v # status  iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT # eg: allow HTTP  ... continue for all necessary services …  service iptables restart # restart the firewall when ready |

### Time to Harden Apache

#### Hardening the Apache Web Server

**Important File Paths**

|  |  |
| --- | --- |
| /var/www/html OR /var/www | Document Root Directory |
| /etc/httpd/conf/httpd.conf (RHEL, CentOS, Fedora)  /etc/apache2/apache2.conf (Debian) | Main Configuration File |
| /var/log/httpd/access\_log OR /var/log/httpd/error\_log | Access and Error Logs for the Web Server |
| /etc/apache2/conf-available/phpmyadmin.conf | Main file for PHPMyAdmin (change path) |

**Always use the command** httpd -t OR apachectl -t **to check the config file settings and syntax after any change**

**Gives all virtual host IP, name, configuration location:** apachectl -t -D DUMP\_VHOSTS

* **Backup the original config file**

|  |
| --- |
| cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.origin  -- OR --  cp /etc/apache2/apache2.conf /etc/apache2/apache2.conf.origin |

* **Create a non-privileged account that runs the Apache service**

|  |
| --- |
| groupadd http-web  useradd -d /var/www/ -g http-web -s /bin/nologin http-web  chown -R apache:apache /opt/apache # switch apache install dir to new user |

* **Secure Config File Settings**

|  |
| --- |
| # change these lines in the config file  ServerTokens **Prod**  ServerSignature **Off**  # ...  <Directory ...>  Options **None** # disables directory browsing  AllowOverride **None** # only allow root to change server settings  **Deny from all**  </Directory>  # ...  **<LimitExcept GET POST HEAD>**  **deny from all** # limit HTTP Requests to only a select few  **</LimitExcept>**  # ...  **FileETag None** # disable Etag header vulnerability  # ...  User **http-web** # tell apache to use the new apache  Group **http-web** # user and group as control  # ...  **TraceEnable off** # deters Cross Site Tracing attacks  Timeout **60** # lower DoS success rate  # ...  # custom logging information  LogFormat “%h %l %u %t **%{sessionID}C** \”%r\” %>s %b **%T**” common  # ...  **RewriteEngine On** # \  **RewriteCond %{THE\_REQUEST} !HTTP/1.1$** # allow only HTTP 1.1  **RewriteRule .\* - [F]** # /  # ...  **#**LoadModule dav\_module modules/mod\_dav.so  **#**LoadModule dav\_fs\_module modules/mod\_dav\_fs.so  **#**Include conf/extra/httpd-dav.conf  # ...  **#**LoadModule info\_module modules/mod\_info.so  # ...  **Header edit Set-Cookie ^(.\*)$ $1;HttpOnly;Secure** # protect the cookies  **Header always append X-Frame-Options SAMEORIGIN** # prevent clickjacking  **Header set X-XSS-Protection “1;mode=block”** # protect from XSS  **# Don’t forget to restart Apache after every config change!** |

* **Ensure that the apache user is running the apache service**

|  |
| --- |
| ps -ef | grep http |

* **Protect apache binary and conf files from insider viewing (just in case)**

|  |
| --- |
| chmod -R 750 /opt/apache/bin /opt/apache/conf |