Installing the pre-reqs on CentOS and RedHat (old pre v1.3.1)

Open-AudIT should be installed on 64bit systems only. You might try it on a 32bit system, but this will not be supported going forward.

These installation instructions and scripts have been tested on CentOS 6.3. Other versions *may* work. If you do install on another version and need to make alterations, please contribute this back to the community so others can also benefit.

The below commands should be run as the root user.

All items in CAPITALS should be substituted with actual specific values.

Make sure your server is up to date.

```
yum update
```

There are a few variables you should note down (they will be used later on).

HOSTNAME

```
uname -n
```

TIMEZONE

This should match a valid time zone for PHP. You can check which time zones PHP supports at http://www.php.net/manual/en/timezones.php

```
cat /etc/sysconfig/clock | grep ZONE | cut -d"\"" -f2
```

Install the various prerequisite packages.

You will need an external repo to install some items, so we'll set that up now.

```
rpm -Uvh http://download.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
```

Install MySQL

```
yum -y install mysql mysql-server

chkconfig --levels 235 mysqld on

service mysqld start
```

When the `mysqld` service starts you will likely see a reminder about setting a database root password; if you do it immediately make sure that you note down the password for later. Alternatively you can leave the database without password until you configure Open-Audit.

Install Apache

```
yum -y install httpd

chkconfig --levels 235 httpd on

service httpd start
```

Install the other required packages

```
yum -y install nano php php-cli php-mysql php-ldap php-mbstring php-mcrypt php-snmp php-xml nmap zip curl wget
sshpass screen samba-client
```

We also need to install winexe. It is not in repositiories, but available for most distributions via the SuSe Build Server. Go to the URL http://download.opensuse.org/repositories/home:/ahajda:/winexe/ and download the relevant package for your distribution. Install it using "yum install PACKAGENAME" and you should be good to go.

Open-AudIT uses Nmap for discovery, sshpass for Linux auditing and screen / samba-client / winexe for Windows auditing.

Discovery will not work without these packages installed.

Disable SELinux

```
sed -i -e 's/SELINUX=/#SELINUX=/g' /etc/selinux/config

echo "SELINUX=disabled" >> /etc/selinux/config

setenforce 0
```

Configure IPTables

```
 sed -i 's/\*filter$/*filter\n-A INPUT -m state --state NEW -p tcp --dport 443 -j ACCEPT/' /etc/sysconfig
/iptables
 sed -i 's/\*filter$/*filter\n-A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT/' /etc/sysconfig
/iptables
/etc/init.d/iptables restart
```

Configure PHP (substituting $TIMEZONE from above).

```
sed -i -e 's/memory_limit/;memory_limit/g' /etc/php.ini

echo "memory_limit = 512M" >> /etc/php.ini

sed -i -e 's/max_execution_time/;max_execution_time/g' /etc/php.ini

echo "max_execution_time = 300" >> /etc/php.ini

sed -i -e 's/max_input_time/;max_input_time/g' /etc/php.ini

echo "max_input_time = 600" >> /etc/php.ini

sed -i -e 's/error_reporting/;error_reporting/g' /etc/php.ini

echo "error_reporting = E_ALL" >> /etc/php.ini

sed -i -e 's/display_errors/;display_errors/g' /etc/php.ini

echo "display_errors = On" >> /etc/php.ini

sed -i -e 's/upload_max_filesize/;upload_max_filesize/g' /etc/php.ini

echo "upload_max_filesize = 10M" >> /etc/php.ini

# Get a valid dat/time string from http://www.php.net/manual/en/timezones.php

sed -i -e 's/date.timezone/;date.timezone/g' /etc/php.ini

echo "date.timezone = $TIMEZONE" >> /etc/php.ini
```

Set the server name (substituting $HOSTNAME from above) and shell (used for scripts) for Apache and restart

```
echo "ServerName $HOSTNAME" >> /etc/httpd/conf/httpd.conf

chsh -s /bin/bash apache

service httpd restart
```

Set the SUID for the nmap binary (so we can use the apache front end to run scripts which call nmap).

NOTE - This command will likely need to be re-run if Nmap is upgraded.

```
chmod u+s /usr/bin/nmap
```