#!/bin/bash

# a simple script to uninstall ossec (tested on debian)

# Author: Han The Thanh <h a n t h e t h a n h @ g m a i l . c o m>

# Public domain.

# this script has been tested on debian; it should also work on other linux

# systems but I have not tested. If you want to be careful and need to see what

# would be done without executing any real action, uncomment the following line:

# dryrun="echo "

set -e

. /etc/ossec-init.conf

dirs="$DIRECTORY"

files=`ls /etc/init.d/ossec /etc/rc[0-9S].d/[SK][0-9][0-9]ossec`

users=`egrep '^ossec' /etc/passwd | sed 's/:.\*//'`

groups=`egrep '^ossec' /etc/group | sed 's/:.\*//'`

deluser=`which deluser` || true

if [ -z "$deluser" ]; then

deluser="userdel"

fi

delgroup=`which delgroup` || true

if [ -z "$delgroup" ]; then

delgroup="groupdel"

fi

echo ""

echo "I am going to remove the following:"

echo ""

echo ">>> Files:"

for f in $files; do

ls -l $f

done

echo ""

echo ">>> Directory:"

for f in $dirs; do

ls -ld $f

done

echo ""

echo ">>> Users:"

echo $users

echo ""

echo ">>> Group:"

echo $groups

echo ""

echo "If you have not backed up your config file(s), they will be lost forever!"

read -p "Is this want you want (yes/no)? "

if [ "$REPLY" = "yes" ]; then

$dryrun /etc/init.d/ossec stop

$dryrun rm -f $files

$dryrun rm -rf $dirs

for u in $users; do

$dryrun $deluser $u

done

for g in $groups; do

$dryrun $delgroup $g

done

fi