#!/bin/bash

#ensure root path integrity

echo -e "\e[36m---------ensure root path integrity---------\e[0m"

if [ "`echo $PATH | grep :: `" != "" ]; then

echo "Empty Directory in PATH (::)"

fi

if [ "`echo $PATH | grep :$`" != "" ]; then

echo "Trailing : in PATH"

fi

p=`echo $PATH | sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`

set -- $p

while [ "$1" != "" ]; do

if [ "$1" = "." ]; then

echo "PATH contains ."

shift

continue

fi

if [ -d $1 ]; then

dirperm=`ls -ldH $1 | cut -f1 -d" "`

if [ `echo $dirperm | cut -c6 ` != "-" ]; then

echo "Group Write permission set on directory $1"

fi

if [ `echo $dirperm | cut -c9 ` != "-" ]; then

echo "Other Write permission set on directory $1"

fi

dirown=`ls -ldH $1 | awk '{print $3}'`

if [ "$dirown" != "root" ] ; then

echo $1 is not owned by root

fi

else

echo $1 is not a directory

fi

shift

done

#ensure all users' home directories exist

echo -e "\e[36m---------ensure all users' home directories exist---------\e[0m"

cat /etc/passwd | egrep -v '^(root|halt|sync|shutdown)' | awk -F: '($7 != "/usr/sbin/nologin" && $7 != "/bin/false") {print $1 " " $6 }' | while read user dir; do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist."

fi

done

#ensure users' home directories permissions are 750 or more restrictive

echo -e "\e[36m---------check user home directory permissions---------\e[0m"

cat /etc/passwd | egrep -v '^(root|halt|sync|shutdown)' | awk -F: '($7 != "/usr/sbin/nologin" && $7 != "/bin/false") {print $1 " " $6 }' | while read user dir; do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist."

else

dirperm=`ls -ld $dir | cut -f1 -d" "`

if [ `echo $dirperm | cut -c6` != "-" ]; then

echo "Group Write permission set on the home directory ($dir) of user $user"

fi

if [ `echo $dirperm | cut -c8` != "-" ]; then

echo "Other Read permission set on the home directory ($dir) of user $user"

fi

if [ `echo $dirperm | cut -c9` != "-" ]; then

echo "Other Write permission set on the home directory ($dir) of user $user"

fi

if [ `echo $dirperm | cut -c10` != "-" ]; then

echo "Other Execute permission set on the home directory ($dir) of user $user"

fi

fi

done

#ensure users own their home directories

echo -e "\e[36m---------check users own their home directories---------\e[0m"

cat /etc/passwd | egrep -v '^(root|halt|sync|shutdown)' | awk -F: '($7 != "/usr/sbin/nologin" && $7 != "/bin/false") {print $1 " " $6 }' | while read user dir;do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist."

else

owner=$(stat -L -c "%U" "$dir")

if [ "$owner" != "$user" ]; then

echo "The home directory ($dir) of user $user is owned by $owner."

fi

fi

done

#ensure users' dot files are not group or world writable

echo -e "\e[36m---------ensure users' dot files are not group or world writable---------\e[0m"

cat /etc/passwd | egrep -v '^(root|halt|sync|shutdown)' | awk -F: '($7 != "/usr/sbin/nologin" && $7 != "/bin/false") {print $1 " " $6 }' | while read user dir; do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist."

else

for file in $dir/.[A-Za-z0-9]\*; do

if [ ! -h "$file" -a -f "$file" ]; then

fileperm=`ls -ld $file | cut -f1 -d" "`

if [ `echo $fileperm | cut -c6` != "-" ]; then

echo "Group Write permission set on file $file"

fi

if [ `echo $fileperm | cut -c9` != "-" ]; then

echo "Other Write permission set on file $file"

fi

fi

done

fi

done

#ensure no users have .forward files

echo -e "\e[36m---------ensure no users have .forward files---------\e[0m"

cat /etc/passwd | egrep -v '^(root|halt|sync|shutdown)' | awk -F: '($7 != "/usr/sbin/nologin" && $7 != "/bin/false") {print $1 " " $6 }' | while read user dir;do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist."

else

if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then

echo ".forward file $dir/.forward exists"

fi

fi

done

#ensure users' dot files are not group or world writable

echo -e "\e[36m---------ensure users' dot files are not group or world writable---------\e[0m"

cat /etc/passwd | egrep -v '^(root|halt|sync|shutdown)' | awk -F: '($7 != "/usr/sbin/nologin" && $7 != "/bin/false") {print $1 " " $6 }' | while read user dir;do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist."

else

for file in $dir/.[A-Za-z0-9]\*; do

if [ ! -h "$file" -a -f "$file" ]; then

fileperm=`ls -ld $file | cut -f1 -d" "`

if [ `echo $fileperm | cut -c6` != "-" ]; then

echo "Group Write permission set on file $file"

fi

if [ `echo $fileperm | cut -c9` != "-" ]; then

echo "Other Write permission set on file $file"

fi

fi

done

fi

done

#ensure no users have .forward files

echo -e "\e[36m---------ensure no users have .forward files---------\e[0m"

cat /etc/passwd | egrep -v '^(root|halt|sync|shutdown)' | awk -F: '($7 != "/usr/sbin/nologin" && $7 != "bin/false") {print $1 " " $6 }' | while read user dir;do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist."

else

if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then

echo ".forward file $dir/.forward exists"

fi

fi

done

#ensure no users have .netrc files

echo -e "\e[36m---------ensure no users have .netrc files---------\e[0m"

cat /etc/passwd | egrep -v '^(root|halt|sync|shutdown)' | awk -F: '($7 != "/usr/sbin/nologin" && $7 != "/bin/false") {print $1 " " $6 }' | while read user dir;do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist."

else

if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then

echo ".netrc file $dir/.netrc exists"

fi

fi

done

#ensure users' .netrc files are not group or world accessible

echo -e "\e[36m---------ensure users' .netrc files are not group or world accessible---------\e[0m"

cat /etc/passwd | egrep -v '^(root|halt|sync|shutdown)' | awk -F: '($7 != "/usr/sbin/nologin" && $7 != "/bin/false") {print $1 " " $6 }' | while read user dir;do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist."

else

for file in $dir/.netrc; do

if [ ! -h "$file" -a -f "$file" ]; then

fileperm=`ls -ld $file | cut -f1 -d" "`

if [ `echo $fileperm | cut -c5` != "-" ]; then

echo "Group Read set on $file"

fi

if [ `echo $fileperm | cut -c6` != "-" ]; then

echo "Group Write set on $file"

fi

if [ `echo $fileperm | cut -c7` != "-" ]; then

echo "Group Execute set on $file"

fi

if [ `echo $fileperm | cut -c8` != "-" ]; then

echo "Other Read set on $file"

fi

if [ `echo $fileperm | cut -c9` != "-" ]; then

echo "Other Write set on $file"

fi

if [ `echo $fileperm | cut -c10` != "-" ]; then

echo "Other Execute set on $file"

fi

fi

done

fi

done

#ensure no users have .rhosts files

echo -e "\e[36m---------ensure no users have .rhosts files---------\e[0m"

cat /etc/passwd | egrep -v '^(root|halt|sync|shutdown)' | awk -F: '($7 != "/usr/sbin/nologin" && $7 != "/bin/false") {print $1 " " $6 }' | while read user dir;do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist."

else

for file in $dir/.rhosts; do

if [ ! -h "$file" -a -f "$file" ]; then

echo ".rhosts file in $dir"

fi

done

fi

done

#ensure all groups in /etc/passwd exist in /etc/group

echo -e "\e[36m---------ensure all groups in /etc/passwd are in /etc/group---------\e[0m"

for i in $(cut -s -d: -f4 /etc/passwd | sort -u ); do

grep -q -P "^.\*?:[^:]\*:$i:" /etc/group

if [ $? -ne 0 ]; then

echo "Group $i is referenced by /etc/passwd but does not exist in /etc/group"

fi

done

#ensure no duplicate UIDs exist

echo -e "\e[36m---------ensure no duplicate UIDs exist---------\e[0m"

cat /etc/passwd | cut -f3 -d":" | sort -n | uniq -c | while read x ; do

[ -z "${x}" ] && break set -$x

if [ $1 > 1 ]; then

users=`awk -F: '($3 == n) { print $1 }' n=$2 /etc/passwd | xargs`

echo "Duplicate UID ($2): ${users}"

fi

done

#ensure no duplicate GIDs exist

echo -e "\e[36m---------ensure no duplicate GIDs exist---------\e[0m"

cat /etc/group | cut -f3 -d":" | sort -n | uniq -c | while read x ; do [ -z "${x}" ] && break set -$x

if [ $1 > 1 ]; then

groups=`awk -F: '($3 == n) { print $1 }' n=$2 /etc/group | xargs`

echo "Duplicate GID ($2): ${groups}"

fi

done

#ensure no duplicate user names exist

echo -e "\e[36m---------ensure no duplicate user names exist----------\e[0m"

cat /etc/passwd | cut -f1 -d":" | sort -n | uniq -c | while read x ; do [ -z "${x}" ] && break set -$x

if [ $1 > 1 ]; then

uids=`awk -F: '($1 == n) { print $3 }' n=$2 /etc/passwd | xargs`

echo "Duplicate User Name ($2): ${uids}"

fi

done

#ensure no duplicate group names exist

echo -e "\e[36m---------ensure no duplicate group names exist---------\e[0m"

cat /etc/group | cut -f1 -d":" | sort -n | uniq -c | while read x ; do [ -z "${x}" ] && break set -$x

if [ $1 > 1 ]; then

gids=`gawk -F: '($1 == n) { print $3 }' n=$2 /etc/group | xargs`

echo "Duplicate Group Name ($2): ${gids}"

fi

done