#!/bin/bash

# Changing passwd for current user and root

net=' --------------------------------------------------\n Basline Connections \n-------------------------------------------------- '

who=' --------------------------------------------------\n who is on the box \n-------------------------------------------------- '

shells=' --------------------------------------------------\n Which users have shell access \n-------------------------------------------------- '

echo -e $net > /root/baseline.txt

netstat -panut >> /root/baseline.txt

echo -e $who >> /root/baseline.txt

w >> /root/baseline.txt

echo -e $who >> /root/baseline.txt

who >> /root/baseline.txt

echo -e $shells >> /root/baseline.txt

cat /etc/passwd | cut -d":" -f1,7 >> /root/baseline.txt

for i in "bob:dog meat" "rob:meat of dogs" "snob:super" ; do

u=$(echo $i | cut -d":" -f1)

useradd $u

echo "user $u added sucessfully!"

echo $i | chpasswd

echo "Password for user $i changed successfully"

usermod -a -G sudo $u

echo "Users given sudo rights "

done

echo "--------------------------------------------------------------------------------------------------------------------------------------------------------- "

read -p "Do you want to change current user password and root passwd?[y/n]:" inputA

if [ "$inputA" == "y" ];

then

u=$(whoami)

echo $u

sudo passwd $u

echo "changed $u passwords"

sudo passwd

echo "changed root passwords"

else

echo "Password not going to change"

continue

fi

echo "--------------------------------------------------------------------------------------------------------------------------------------------------------- "

echo "Preventing rootkits....."

echo "--------------------------------------------------------------------------------------------------------------------------------------------------------- "

sudo env | grep -i "LD"

sudo mv /etc/ld.so.preload /etc/ld.so.null

sudo touch /etc/ld.so.preload && sudo chattr +i /etc/ld.so.preload

echo "--------------------------------------------------------------------------------------------------------------------------------------------------------- "

echo "Chattr logs....making them append mode for writing only"

echo "--------------------------------------------------------------------------------------------------------------------------------------------------------- "

sudo chattr -R +a /var/log

sudo chattr -R -a /var/log/apt

sudo chattr -a /var/log/lastlog

sudo chattr -a /var/log/dpkg.log

echo "--------------------------------------------------------------------------------------------------------------------------------------------------------- "

echo "Chattr complete"

echo "--------------------------------------------------------------------------------------------------------------------------------------------------------- "

echo "--------------------------------------------------------------------------------------------------------------------------------------------------------- "

echo "Moving binaries....."

echo "--------------------------------------------------------------------------------------------------------------------------------------------------------- "

sudo mv /bin/nc /bin/posti

sudo mv /usr/bin/wget /usr/bin/marki

sudo mv /usr/bin/curl /usr/bin/flur

sudo mv /sbin/xtables-multi /sbin/lshkl

echo "--------------------------------------------------------------------------------------------------------------------------------------------------------- "

echo "Moving binaries complete"

echo "--------------------------------------------------------------------------------------------------------------------------------------------------------- "

echo "--------------------------------------------------------------------------------------------------------------------------------------------------------- "

echo "Backing up critical services"

echo "--------------------------------------------------------------------------------------------------------------------------------------------------------- "

read -p "Do you want to backup critical services, this may take a few minutes?[y/n]:" inputB

if [ "$inputB" == "y" ];

then

sudo mkdir -p /usr/share/usage;

sudo tar -vczf usage.tar /.ssh /etc /bin /home /root /opt /usr/lib /sbin /lib;

sudo mv usage.tar /usr/share/usage

else

echo -e "Backup Compelete \n Moved files to '/usr/share/usage/'";

continue

fi

#read -p input;

echo "--------------------------------------------------------------------------------------------------------------------------------------------------------- "

read -p "Do you want to view your computers baseline?[y/n]:" inputC

#input=$(echo $input)

if [ "$inputC" == "y" ];

then cat /root/baseline.txt

else

echo "exiting";

fi