#!/bin/bash

if [ $UID -ne 1000 ]

then

echo "Please run this script as sysadmin."

exit

fi

output=$HOME/research3/sys\_info.txt

ip=$(sudo ip addr | grep inet | tail -2 | head -1)

execs=$(sudo find /home -type f -perm 777 )

files=('/etc/passwd' '/etc/shadow')

if [ ! -d $HOME/research3 ]

then

mkdir $HOME/research3

sudo chown sysadmin:sysadmin $HOME/research3

fi

if [ -f $output ]

then

rm $output

fi

#Name the script

echo "A Quick System Audit Script" > $output

#Display Date

date >> $output

echo "" >> $output

#Display Machine Info

echo "Machine Type Info:" >> $output

echo $MACHTYPE >> $output

echo -e "Uname info: $(uname -a) \n" >> $output

echo -e "IP Info:" >> $output

echo -e " $ip \n" >> $output

echo -e "Hostname: $(hostname -s) \n" >> $output

echo "DNS Servers: " >> $output

cat /etc/resolv.conf >> $output

echo -e "\nExecute File: \n" >> $output

echo $execs >> $output

echo -e "\nMemory Info:" >> $output

free >> $output

echo -e "\nCPU Info:" >> $output

lscpu | grep CPU >> $output

echo -e "\nDisk Usage:" >> $output

df -H | head -2 >> $output

echo -e "\nWho is logged in: \n $(who -a) \n" >> $output

echo -e "\nSUID Files:" >> $output

echo -e "\nTop 10 Processes" >> $output

ps aux -m | awk {'print $1, $2, $3, $4, $11'} | head >> $output

echo -e "\n DEMO: $ip" >> $output

echo -e "\nThe permissions for sensitive /etc files: \n"

for file in ${files[@]};

do

ls -l $file >> $output

done