**Log\_analysis.sh**

**#!bin/bash**

**sed s/INCORRECT\_PASSWORD/ACCESS\_DENIED/ LogA.txt > access\_denied.txt**

**awk '{print $4, $6}' access\_denied.txt > filtered\_logs.txt**

**sys\_info.sh**

**#!/bin/bash**

**#Check if script was run as root. Exit if true.**

**if [ $UID -eq 0 ]; then**

**echo "Please do not run this script as root."**

**exit**

**fi**

**# Define Variables**

**output=$HOME/research/sys\_info.txt**

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

**execs=$(sudo find /home -type f -perm 777 2>/dev/null)**

**# Check for research directory. Create it if needed.**

**if [ ! -d $HOME/research ]; then**

**mkdir $HOME/research**

**fi**

**# Check for output file. Clear it if needed.**

**if [ -f $output ]; then**

**rm $output**

**fi**

**echo "A Quick System Audit Script" >>$output**

**date >>$output**

**echo "" >>$output**

**echo "Machine Type Info:" >>$output**

**echo -e "$MACHTYPE \n" >>$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 "\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 "\nexec Files:" >>$output**

**echo $execs >>$output**

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

**ps aux --sort -%mem | awk {'print $1, $2, $3, $4, $11'} | head >>$output**

**sys\_info\_2.sh**

**#!/bin/bash**

**#Check if script was run as root. Exit if false.**

**if [ $UID -ne 0 ]; then**

**echo "Please run this script as root."**

**exit**

**fi**

**# Define Variables**

**output=$HOME/research/sys\_info.txt**

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

**execs=$(sudo find /home -type f -perm 777 2>/dev/null)**

**cpu=$(lscpu | grep CPU)**

**disk=$(df -H | head -2)**

**# Define Lists to use later**

**commands=(**

**'date'**

**'uname -a'**

**'hostname -s'**

**)**

**files=(**

**'/etc/passwd'**

**'/etc/shadow'**

**)**

**#Check for research directory. Create it if needed.**

**if [ ! -d $HOME/research ]; then**

**mkdir $HOME/research**

**fi**

**# Check for output file. Clear it if needed.**

**if [ -f $output ]; then**

**>$output**

**fi**

**##################################################**

**#Start Script**

**echo "A Quick System Audit Script" >>$output**

**echo "" >>$output**

**for x in {0..2}; do**

**results=$(${commands[$x]})**

**echo "Results of "${commands[$x]}" command:" >>$output**

**echo $results >>$output**

**echo "" >>$output**

**done**

**# Display Machine type**

**echo "Machine Type Info:" >>$output**

**echo -e "$MACHTYPE \n" >>$output**

**# Display IP Address info**

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

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

**# Display Memory usage**

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

**free >>$output**

**#Display CPU usage**

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

**lscpu | grep CPU >>$output**

**# Display Disk usage**

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

**df -H | head -2 >>$output**

**#Display who is logged in**

**echo -e "\nCurrent user login information: \n $(who -a) \n" >>$output**

**# Display DNS Info**

**echo "DNS Servers: " >>$output**

**cat /etc/resolv.conf >>$output**

**# List exec files**

**echo -e "\nexec Files:" >>$output**

**for exec in $execs; do**

**echo $exec >>$output**

**done**

**# List top 10 processes**

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

**ps aux --sort -%mem | awk {'print $1, $2, $3, $4, $11'} | head >>$output**

**# Check the permissions on files**

**echo -e "\nThe permissions for sensitive /etc files: \n" >>$output**

**for file in ${files[@]}; do**

**ls -l $file >>$output**

**done**

**for\_loops.sh**

**#!/bin/bash**

**# Create Variables**

**nums=$(echo {0..9})**

**states=('Nebraska' 'California' 'Texas' 'Hawaii' 'Washington')**

**ls\_out=$(ls)**

**execs=$(find /home -type f -perm 777 2>/dev/null)**

**# Create For Loops**

**# Create a loop that prints only 3, 5 and 7**

**for num in ${nums[@]}; do**

**if [ $num = 3 ] || [ $num = 5 ] || [ $num = 7 ]; then**

**echo $num**

**fi**

**done**

**# Create a loop that looks for 'Hawaii'**

**for state in ${states[@]}; do**

**if [ $state == 'Hawaii' ]; then**

**echo "Hawaii is the best!"**

**else**

**echo "I'm not a fan of Hawaii."**

**fi**

**done**

**# Create a `for` loop that prints out each item in your variable that holds the output of the `ls` command.**

**for x in ${ls\_out[@]}; do**

**echo $x**

**done**

**# Bonus**

**# Create a for loop to print out execs on one line for each entry**

**for exec in ${execs[@]}; do**

**echo $exec**

**done**

**System.sh**

**#!/bin/bash**

**# INSTRUCTIONS: Edit the following placeholder command and output filepaths**

**# For example: cpu\_usage\_tool > ~/backups/cpuuse/cpu\_usage.txt**

**# The cpu\_usage\_tool is the command and ~/backups/cpuuse/cpu\_usage.txt is the filepath**

**# In the above example, the `cpu\_usage\_tool` command will output CPU usage information into a `cpu\_usage.txt` file.**

**# Do not forget to use the -h option for free memory, disk usage, and free disk space**

**# Free memory output to a free\_mem.txt file**

**free > ~/backups/freemem/free\_mem.txt**

**# Disk usage output to a disk\_usage.txt file**

**du > ~/backups/diskuse/disk\_usage.tx**

**# List open files to a open\_list.txt file**

**lsof > ~/backups/openlist/open\_list.txt**

**# Free disk space to a free\_disk.txt file**

**df > ~/backups/freedisk/free\_disk.txt**