|  |
| --- |
| #!/bin/bash |
|  |  |
|  | # 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) |
|  |  |
|  | # The Title |
|  | echo -e "\nThe permissions for sensitive /etc files: \n" >> $output |
|  | files=('/etc/passwd' '/etc/shadow') |
|  | for file in ${files[@]} |
|  | do |
|  | ls -l $file >> $output |
|  | done |
|  |  |
|  | #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 |
|  |  |
|  | # 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 |
|  |  |
|  | # 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 current user |
|  | echo -e "\nWho is logged in: \n $(who -a) \n" >>$output |
|  | echo -e "\nexec Files:" >>$output |
|  | echo $execs >>$output |
|  |  |
|  | # Display Top 10 processes |
|  | echo -e "\nTop 10 Processes" >>$output |
|  | ps aux --sort -%mem | awk {'print $1, $2, $3, $4, $11'} | head >>$output |