

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