LINUX PROGRAMMING
WEEK 5

NAME : S KAILASH
REG. NO : 18MIS1074
SLOT : B1 + TB1
COURSE CODE : SWE4009

==========

1. Write a Script file to monitor the system logs and ensure security

AIM: To write a shell script to automate the monitoring the system logs to ensure security.

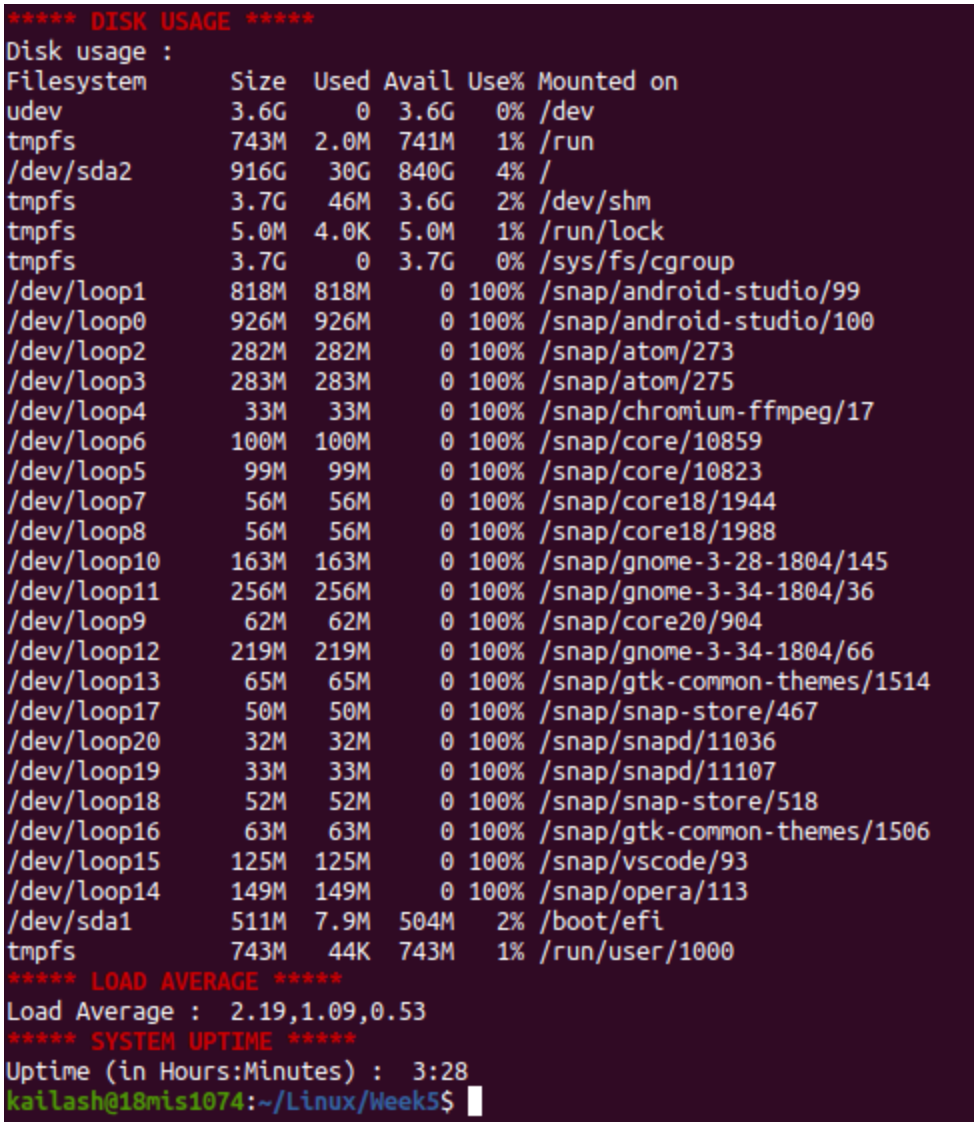
PROCEDURE:

```
kailash@18mis1074:~/Linux/Week5$ cat mon.sh
#!/bin/bash
echo -e "\e[31;1m***** INTERNET STATUS *****\e[0m"
ping -c 1 google.com &> /dev/null && echo -e "Internet connected" || echo -e "Internet discon
nected"
echo -e "\e[31;1m***** OS TYPE AND VERSION *****\e[0m"
echo -e "OS Type : " $(uname -o)
cat /etc/os-release | grep 'NAME\|VERSION' | grep -v 'VERSION_ID'> /tmp/osrelease
echo -n -e "OS Version : " && cat /tmp/osrelease | grep -v "VERSION" | cut -f2 -d\"
echo -e "\e[31;1m***** ARCHITECTURE *****\e[0m"
arch=$(uname -m)
echo "Architecture : " $arch
echo -e "\e[31;1m***** KERNEL RELEASE *****\e[0m"
ker=$(uname -r)
echo "Kernal : " $ker
echo -e "\e[31;1m***** HOSTNAME *****\e[0m"
echo $HOSTNAME
echo -e "\e[31;1m***** INTERNAL IP *****\e[0m"
iip=$(hostname -I)
echo "Internal IP : " $iip
echo -e "\e[31;1m***** EXTERNAL IP *****\e[0m"
eip=$(curl -s ipecho.net/plain;echo)
echo "External IP : " $eip
echo -e "\e[31;1m***** DNS *****\e[0m"
ns=$(cat /etc/resolv.conf | sed '1 d' | awk '{print $2}')
echo "Name servers : " $ns
echo -e "\e[31;1m***** LOGGED IN USERS  *****\e[0m"
who>/tmp/who
echo "Logged in users : " && cat /tmp/who
echo -e "\e[31;1m***** RAM AND SWAP USAGE*****\e[0m"
free -h | grep -v + >/tmp/ramcache
echo "Ram usage : " && cat /tmp/ramcache | grep -v "Swap"
echo "Swap usage : " && cat /tmp/ramcache | grep -v "Mem"
echo -e "\e[31;1m***** DISK USAGE *****\e[0m"
df -h |sort -rn | head -5 | grep 'Filesystem|\/dev/sda*' > /tmp/diskusage
echo -e "Disk usage : " && df -h
echo -e "\e[31;1m***** LOAD AVERAGE *****\e[0m"
la=$(top -n 1 -b | grep "load average: " | awk '{print $10 $11 $12}')
echo "Load Average : " $la
echo -e "\e[31;1m***** SYSTEM UPTIME *****\e[0m"
sup=$(uptime | awk '{print $3 $4}' | cut -f1 -d,)
echo "Uptime (in Hours:Minutes) : " $sup
kailash@18mis1074:~/Linux/Week5$
```

OUTPUT:

```
kailash@18mis1074:~/Linux/Week5$ ./mon.sh
***** INTERNET STATUS *****
Internet connected
***** OS TYPE AND VERSION *****
OS Type :  GNU/Linux
OS Version : Ubuntu
Ubuntu 20.04.2 LTS
UBUNTU_CODENAME=focal
***** ARCHITECTURE *****
Architecture :  x86_64
***** KERNEL RELEASE *****
Kernal :  5.8.0-44-generic
***** HOSTNAME *****
18mis1074
***** INTERNAL IP *****
Internal IP :  192.168.1.10 192.168.122.1
***** EXTERNAL IP *****
External IP :  27.5.137.239
***** DNS *****
Name servers :  DO 127.0.0.53 run 127.0.0.53 edns0
***** LOGGED IN USERS  *****
Logged in users :
kailash  :0           2021-03-16 09:31 (:0)
***** RAM AND SWAP USAGE*****
Ram usage :
              total        used        free      shared  buff/cache   available
Mem:          7.2Gi       1.8Gi       2.4Gi        52Mi       3.0Gi       5.1Gi
Swap usage :
              total        used        free      shared  buff/cache   available
Swap:         2.0Gi          0B       2.0Gi
***** DISK USAGE *****
```

<continued in next page>



RESULT: Thus, the system logs with regards to internet connectivity status, OS kernel, architecture, external and internal IP, DNS, logged in users, ram, swap and disk usage, load average and system uptime are listed. The script can be executed periodically to monitor for security.