

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 disconnected"
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 eds0
***** 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      0B          0B          0B
***** DISK USAGE *****
```

<continued in next page>

```

***** DISK USAGE *****
Disk usage :
Filesystem      Size  Used Avail Use% Mounted on
udev            3.6G   0  3.6G   0% /dev
tmpfs           743M  2.0M  741M   1% /run
/dev/sda2       916G  30G  840G   4% /
tmpfs           3.7G  46M  3.6G   2% /dev/shm
tmpfs           5.0M  4.0K  5.0M   1% /run/lock
tmpfs           3.7G   0  3.7G   0% /sys/fs/cgroup
/dev/loop1      818M  818M   0 100% /snap/android-studio/99
/dev/loop0      926M  926M   0 100% /snap/android-studio/100
/dev/loop2      282M  282M   0 100% /snap/atom/273
/dev/loop3      283M  283M   0 100% /snap/atom/275
/dev/loop4       33M   33M   0 100% /snap/chromium-ffmpeg/17
/dev/loop6      100M  100M   0 100% /snap/core/10859
/dev/loop5       99M   99M   0 100% /snap/core/10823
/dev/loop7       56M   56M   0 100% /snap/core18/1944
/dev/loop8       56M   56M   0 100% /snap/core18/1988
/dev/loop10     163M  163M   0 100% /snap/gnome-3-28-1804/145
/dev/loop11     256M  256M   0 100% /snap/gnome-3-34-1804/36
/dev/loop9       62M   62M   0 100% /snap/core20/904
/dev/loop12     219M  219M   0 100% /snap/gnome-3-34-1804/66
/dev/loop13      65M   65M   0 100% /snap/gtk-common-themes/1514
/dev/loop17      50M   50M   0 100% /snap/snap-store/467
/dev/loop20      32M   32M   0 100% /snap/snapd/11036
/dev/loop19      33M   33M   0 100% /snap/snapd/11107
/dev/loop18      52M   52M   0 100% /snap/snap-store/518
/dev/loop16      63M   63M   0 100% /snap/gtk-common-themes/1506
/dev/loop15     125M  125M   0 100% /snap/vscode/93
/dev/loop14     149M  149M   0 100% /snap/opera/113
/dev/sda1       511M  7.9M  504M   2% /boot/efi
tmpfs           743M  44K  743M   1% /run/user/1000
***** LOAD AVERAGE *****
Load Average :  2.19,1.09,0.53
***** SYSTEM UPTIME *****
Uptime (in Hours:Minutes) :  3:28
kailash@18mis1074:~/Linux/Week5$

```

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.