Sudo Usage Logging

Name:Prajin S(2462348)

OBJECTIVE:

The objective of this document is to define and implement a method for tracking and logging all usage of the sudo command on a system.

STEP-BY-STEP COMMAND:

STEP 1: Save the python script

```
nano sudo_monitor.py
```

STEP 2: Make it executable

```
chmod +x sudo_monitor.py
```

STEP 3: Run the script with root privileges (to access /var/log/auth.log):

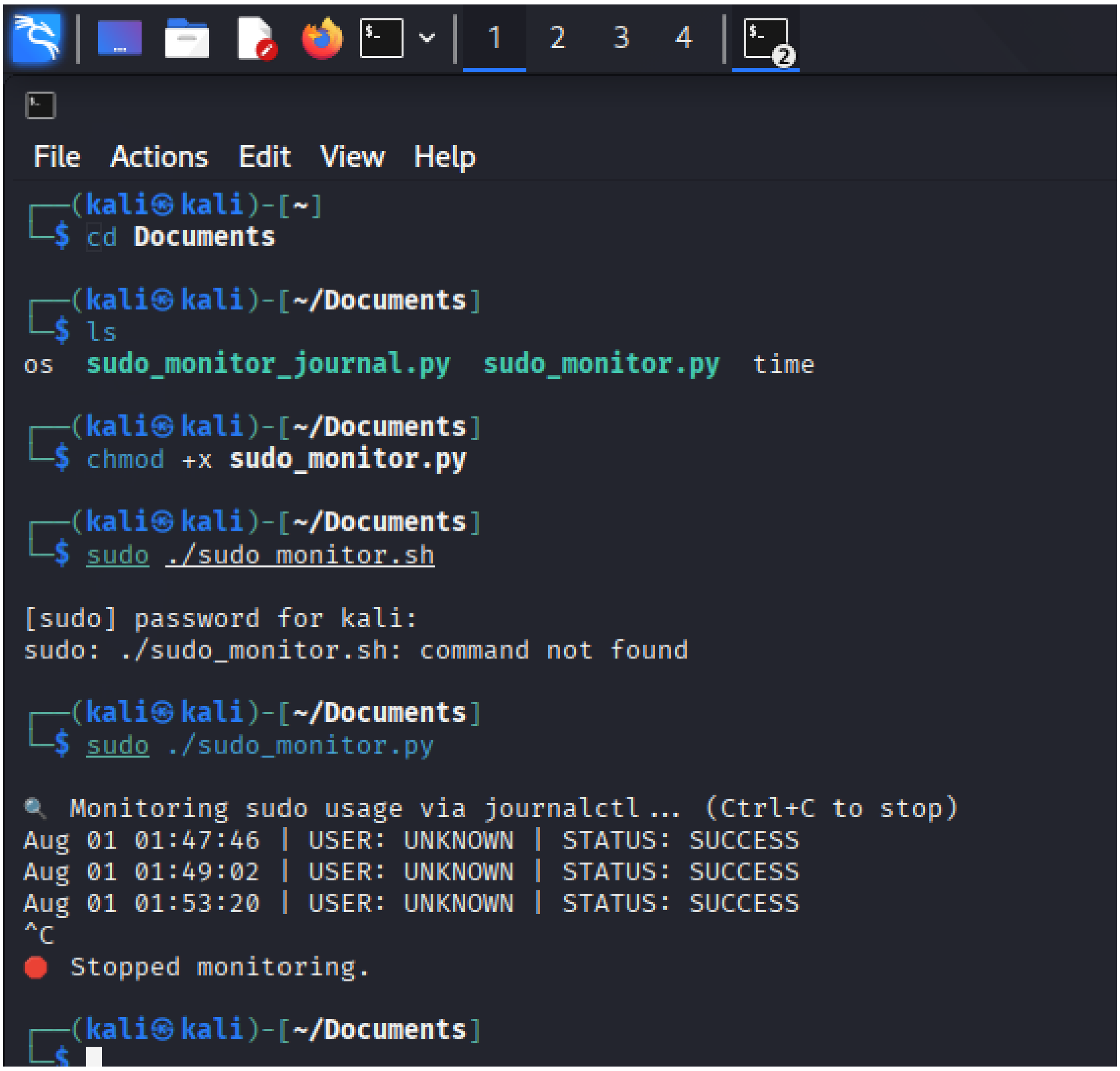
```
sudo ./sudo_monitor.py
```

PYTHON CODE:

```
#!/bin/bash


LOG_FILE="/var/log/auth.log"
OUTPUT_LOG="/var/log/sudo_monitor.log"
LAST_LINE=0


echo "Monitoring sudo usage... Press Ctrl+C to stop."


while true; do
  TOTAL_LINES=$(wc -l < "$LOG_FILE")
  NEW_LINES=$(tail -n $(($TOTAL_LINES - $LAST_LINE)) "$LOG_FILE")
  LAST_LINE=$TOTAL_LINES


  echo "$NEW_LINES" | grep 'sudo' | grep 'COMMAND=' | while read -r line; do
    USER=$(echo "$line" | awk '{for (i=1;i<=NF;i++) if ($i=="sudo:") print $(i+1)}')
    TIME=$(echo "$line" | awk '{print $1, $2, $3}')
    RESULT="SUCCESS"
    echo "$line" | grep -iq "authentication failure" && RESULT="FAILED"
    echo "$(date) - USER: $USER - $RESULT - $line" >> "$OUTPUT_LOG"
    echo "$(date) - USER: $USER - $RESULT"
  done
```

```
    sleep 30
done
```

RESULT:



```
┌──(kali㉿kali)-[~]
└─$ cd Documents

┌──(kali㉿kali)-[~/Documents]
└─$ ls
os  sudo_monitor_journal.py  sudo_monitor.py  time

┌──(kali㉿kali)-[~/Documents]
└─$ chmod +x sudo_monitor.py

┌──(kali㉿kali)-[~/Documents]
└─$ sudo ./sudo_monitor.sh

[sudo] password for kali:
sudo: ./sudo_monitor.sh: command not found

┌──(kali㉿kali)-[~/Documents]
└─$ sudo ./sudo_monitor.py

🔍 Monitoring sudo usage via journalctl... (Ctrl+C to stop)
Aug 01 01:47:46 | USER: UNKNOWN | STATUS: SUCCESS
Aug 01 01:49:02 | USER: UNKNOWN | STATUS: SUCCESS
Aug 01 01:53:20 | USER: UNKNOWN | STATUS: SUCCESS
^C
🔴 Stopped monitoring.

┌──(kali㉿kali)-[~/Documents]
└─$
```

CONCLUSION:

Logging and monitoring sudo usage is a critical component of system security and operational transparency.