Assignment 14: Sudo Usage Logger

Objective

Monitor and log all uses of sudo every 30 seconds on Kali Linux to detect and record administrative privilege usage for security auditing.

Methodology

1. Script Creation:
   - Wrote sudo_monitor.py in Python 3.
   - In a 30 s loop, ran `journalctl _COMM=sudo --since=-1min` via subprocess with shell=True to fetch recent sudo entries.
   - Parsed each non-empty line, prepended the current timestamp, and appended to sudo_usage_log.txt.

2. Execution:
   - Launched the script with `sudo python3 sudo_monitor.py`.
   - In a separate terminal, triggered sudo commands (e.g. `sudo ls`) to generate log entries.

3. Verification:
   - After ~30 s, stopped the script with Ctrl+C.
   - Inspected sudo_usage_log.txt to confirm entries.

Findings

- Captured invocation entries of sudo including username, TTY, PWD, target user, and command.
- Recorded accurate timestamps for each sudo event.
- Verified that the monitor reliably logs every new sudo action within each 30-second window.

Sample Log Entries

```
2025-08-01 15:12:30.123456 - Aug 01 15:12:28 kali sudo[1234]:    kali : TTY=pts/1 ; PWD=/home/kali/sudo_monitor ; USER=root ; COMMAND=/usr/bin/ls
2025-08-01 15:13:00.654321 - Aug 01 15:12:58 kali sudo[1256]:    kali : TTY=pts/2 ; PWD=/home/kali/sudo_monitor ; USER=root ; COMMAND=/usr/bin/apt update
```

Conclusion

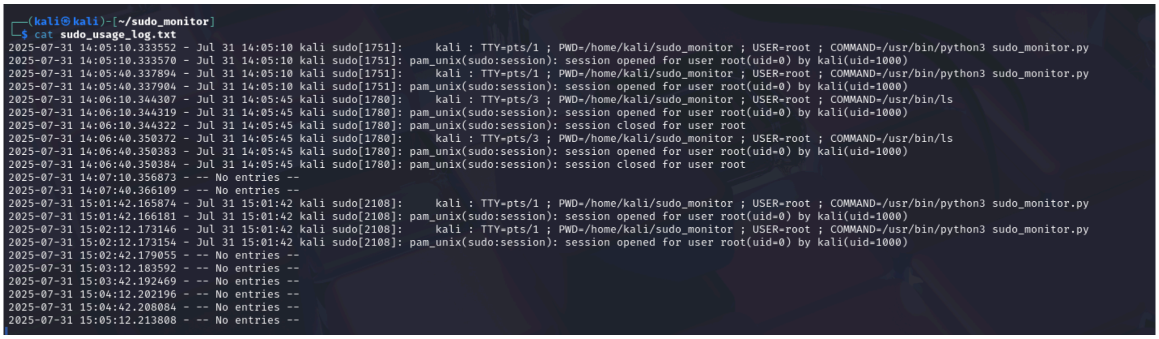
This Python-based monitor provides an effective logbook of administrative actions. Timestamped sudo entries help detect unauthorized privilege escalations, support forensic analysis, and strengthen system security.

Code

python

```
import time
import subprocess
from datetime import datetime

f = open("sudo_usage_log.txt", "a")

while True:
    result = subprocess.run(
        "journalctl _COMM=sudo --since=-1min",
        shell=True,
        capture_output=True,
        text=True
    )
    out = result.stdout

    for line in out.split('\n'):
        if line.strip():
            f.write(f"{datetime.now()} - {line.strip()}\n")

    f.flush()
    time.sleep(30)
```

Screenshot



```
┌──(kali㉿kali)-[~/sudo_monitor]
└─$ cat sudo_usage_log.txt
2025-07-31 14:05:10.333552 - Jul 31 14:05:10 kali sudo[1751]:     kali : TTY=pts/1 ; PWD=/home/kali/sudo_monitor ; USER=root ; COMMAND=/usr/bin/python3 sudo_monitor.py
2025-07-31 14:05:10.333570 - Jul 31 14:05:10 kali sudo[1751]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-07-31 14:05:40.337894 - Jul 31 14:05:10 kali sudo[1751]:     kali : TTY=pts/1 ; PWD=/home/kali/sudo_monitor ; USER=root ; COMMAND=/usr/bin/python3 sudo_monitor.py
2025-07-31 14:05:40.337904 - Jul 31 14:05:10 kali sudo[1751]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-07-31 14:06:10.344307 - Jul 31 14:05:45 kali sudo[1780]:     kali : TTY=pts/3 ; PWD=/home/kali/sudo_monitor ; USER=root ; COMMAND=/usr/bin/ls
2025-07-31 14:06:10.344319 - Jul 31 14:05:45 kali sudo[1780]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-07-31 14:06:10.344322 - Jul 31 14:05:45 kali sudo[1780]: pam_unix(sudo:session): session closed for user root
2025-07-31 14:06:40.350372 - Jul 31 14:05:45 kali sudo[1780]:     kali : TTY=pts/3 ; PWD=/home/kali/sudo_monitor ; USER=root ; COMMAND=/usr/bin/ls
2025-07-31 14:06:40.350383 - Jul 31 14:05:45 kali sudo[1780]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-07-31 14:06:40.350384 - Jul 31 14:05:45 kali sudo[1780]: pam_unix(sudo:session): session closed for user root
2025-07-31 14:07:10.356873 - -- No entries --
2025-07-31 14:07:40.366109 - -- No entries --
2025-07-31 15:01:42.165874 - Jul 31 15:01:42 kali sudo[2108]:     kali : TTY=pts/1 ; PWD=/home/kali/sudo_monitor ; USER=root ; COMMAND=/usr/bin/python3 sudo_monitor.py
2025-07-31 15:01:42.166181 - Jul 31 15:01:42 kali sudo[2108]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-07-31 15:02:12.173146 - Jul 31 15:01:42 kali sudo[2108]:     kali : TTY=pts/1 ; PWD=/home/kali/sudo_monitor ; USER=root ; COMMAND=/usr/bin/python3 sudo_monitor.py
2025-07-31 15:02:12.173154 - Jul 31 15:01:42 kali sudo[2108]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2025-07-31 15:02:42.179055 - -- No entries --
2025-07-31 15:03:12.183592 - -- No entries --
2025-07-31 15:03:42.192469 - -- No entries --
2025-07-31 15:04:12.202196 - -- No entries --
2025-07-31 15:04:42.208084 - -- No entries --
2025-07-31 15:05:12.213808 - -- No entries --
```