TASK : 4 FILE WATCHER SCRIPT

Directory Watcher – PoC

This PoC demonstrates monitoring a directory for new `.txt` files using `inotifywait`. When a new `.txt` file is created, the script logs the filename along with a timestamp.

Instructions

We wrote a script **`watch_dir.sh`** that:

- Watches the directory `/home/studentuser/projectX/logs`
- Detects when a **new `.txt` file** is created
- Logs the event with a **timestamp** into `log_monitor.txt`

Script: `watch_dir.sh`

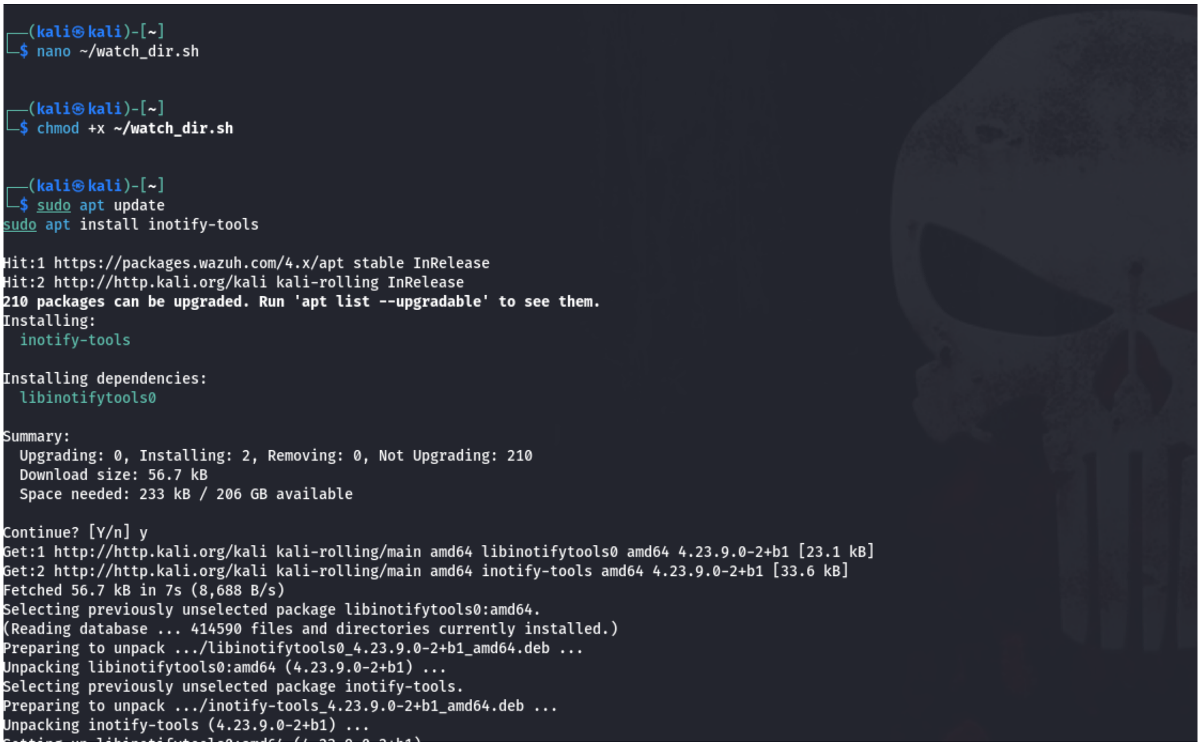
```
#!/bin/bash

WATCH_DIR="/home/studentuser/projectX/logs"
LOG_FILE="/home/studentuser/projectX/log_monitor.txt"

echo "Watching directory: $WATCH_DIR"

inotifywait -m -e create --format '%f' "$WATCH_DIR" | while read FILENAME
do
    if [[ "$FILENAME" == *.txt ]]; then
        TIMESTAMP=$(date '+%Y-%m-%d %H:%M:%S')
        echo "[$TIMESTAMP] New .txt file detected: $FILENAME" >> "$LOG_FILE"
    fi
done
```

Setup & Run

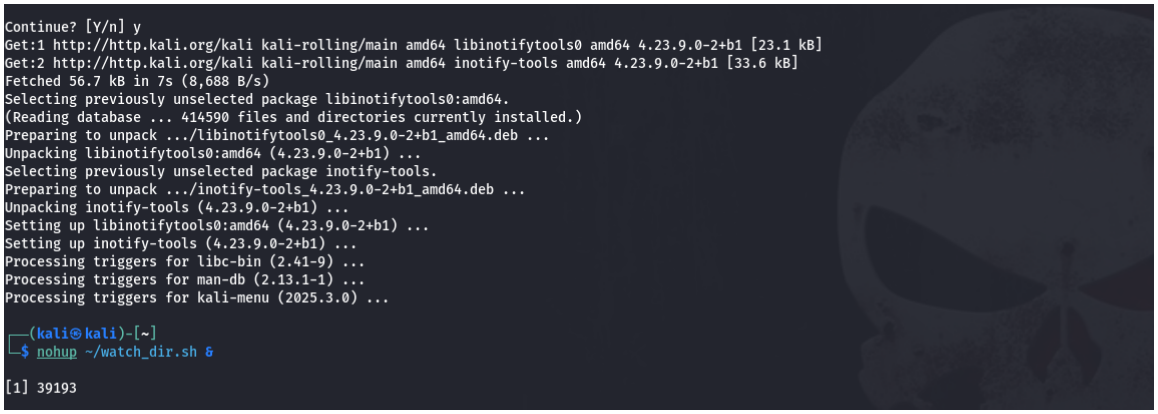
```
chmod +x watch_dir.sh
sudo ./watch_dir.sh &
```

- The script runs in the background (`&`) and outputs:

  ```
  Watching directory: /home/studentuser/projectX/logs
  Setting up watches.
  Watches established.
  ```



```
┌──(kali㉿kali)-[~]
└─$ nano ~/watch_dir.sh


┌──(kali㉿kali)-[~]
└─$ chmod +x ~/watch_dir.sh


┌──(kali㉿kali)-[~]
└─$ sudo apt update
sudo apt install inotify-tools

Hit:1 https://packages.wazuh.com/4.x/apt stable InRelease
Hit:2 http://http.kali.org/kali kali-rolling InRelease
210 packages can be upgraded. Run 'apt list --upgradable' to see them.
Installing:
  inotify-tools

Installing dependencies:
  libinotifytools0

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 210
  Download size: 56.7 kB
  Space needed: 233 kB / 206 GB available

Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libinotifytools0 amd64 4.23.9.0-2+b1 [23.1 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 inotify-tools amd64 4.23.9.0-2+b1 [33.6 kB]
Fetched 56.7 kB in 7s (8,688 B/s)
Selecting previously unselected package libinotifytools0:amd64.
(Reading database ... 414590 files and directories currently installed.)
Preparing to unpack .../libinotifytools0_4.23.9.0-2+b1_amd64.deb ...
Unpacking libinotifytools0:amd64 (4.23.9.0-2+b1) ...
Selecting previously unselected package inotify-tools.
Preparing to unpack .../inotify-tools_4.23.9.0-2+b1_amd64.deb ...
Unpacking inotify-tools (4.23.9.0-2+b1) ...
```



```
Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libinotifytools0 amd64 4.23.9.0-2+b1 [23.1 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 inotify-tools amd64 4.23.9.0-2+b1 [33.6 kB]
Fetched 56.7 kB in 7s (8,688 B/s)
Selecting previously unselected package libinotifytools0:amd64.
(Reading database ... 414590 files and directories currently installed.)
Preparing to unpack .../libinotifytools0_4.23.9.0-2+b1_amd64.deb ...
Unpacking libinotifytools0:amd64 (4.23.9.0-2+b1) ...
Selecting previously unselected package inotify-tools.
Preparing to unpack .../inotify-tools_4.23.9.0-2+b1_amd64.deb ...
Unpacking inotify-tools (4.23.9.0-2+b1) ...
Setting up libinotifytools0:amd64 (4.23.9.0-2+b1) ...
Setting up inotify-tools (4.23.9.0-2+b1) ...
Processing triggers for libc-bin (2.41-9) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.0) ...

┌──(kali㉿kali)-[~]
└─$ nohup ~/watch_dir.sh &

[1] 39193
```