POC Task 4

Task 4: File Watcher Script

1. Executive Summary

This PoC demonstrates a file monitoring solution that detects new .txt files in a specified directory and logs events with timestamps. The implementation includes script creation, systemd service configuration, and automated startup.

2. Objectives

- Monitor directory for new .txt files
- Log creation events with timestamps
- Implement as persistent system service
- Operate under restricted user permissions

3. Implementation

3.1 Script Creation

```
┌──(llamafart㉿jaivanti)-[~]
└─$ sudo -u studentuser tee /home/studentuser/projectX/scripts/watch_dir.sh << 'EOF'
#!/bin/bash

# Configuration
WATCH_DIR="/home/studentuser/projectX/logs"
LOG_FILE="/home/studentuser/projectX/log_monitor.txt"
FILE_PATTERN="*.txt"

# Create files if they don't exist
mkdir -p "$WATCH_DIR"
touch "$LOG_FILE"
chown studentuser:studentuser "$LOG_FILE"

# Initial file list
mapfile -t existing_files < <(find "$WATCH_DIR" -name "$FILE_PATTERN" -type f 2>/dev/null)

# Log function
log_event() {
    echo "[$(date '+%Y-%m-%d %H:%M:%S')] $1" >> "$LOG_FILE"
}

log_event "Starting directory monitor on $WATCH_DIR"

# Monitoring loop
while true; do
    # Check for new files
    mapfile -t current_files < <(find "$WATCH_DIR" -name "$FILE_PATTERN" -type f -newermt "-5 seconds" 2>/dev/null)

    for file in "${current_files[@]}"; do
        if [[ ! " ${existing_files[@]} " =~ " ${file} " ]]; then
            log_event "New file detected: ${file##*/}"
            existing_files+=("$file")
        fi
    done

    sleep 5
done
```

3.2 Permission Configuration

```
┌──(llamafart㉿jaivanti)-[~]
└─$ sudo chown studentuser:studentuser /home/studentuser/projectX/scripts/watch_dir.sh

┌──(llamafart㉿jaivanti)-[~]
└─$ sudo chmod +x /home/studentuser/projectX/scripts/watch_dir.sh
```

3.3 Systemd Service Setup

```
┌──(llamafart㉿jaivanti)-[~]
└─$ sudo tee /etc/systemd/system/watch_dir.service << 'EOF'
[Unit]
Description=Directory Watcher Service
After=network.target

[Service]
User=studentuser
ExecStart=/home/studentuser/projectX/scripts/watch_dir.sh
Restart=always
RestartSec=5s

[Install]
WantedBy=multi-user.target
EOF
[Unit]
Description=Directory Watcher Service
After=network.target

[Service]
User=studentuser
ExecStart=/home/studentuser/projectX/scripts/watch_dir.sh
Restart=always
RestartSec=5s

[Install]
WantedBy=multi-user.target
```

3.4. Service Activation

```
┌──(llamafart㉿jaivanti)-[~]
└─$ sudo systemctl daemon-reload

┌──(llamafart㉿jaivanti)-[~]
└─$ sudo systemctl enable watch_dir.service
Created symlink '/etc/systemd/system/multi-user.target.wants/watch_dir.service' → '/etc/systemd/system/watch_dir.service'.

┌──(llamafart㉿jaivanti)-[~]
└─$ sudo systemctl start watch_dir.service
```

3.5. Testing & Verification

```
┌──(llamafart㉿jaivanti)-[~]
└─$ sudo -u studentuser touch /home/studentuser/projectX/logs/test_file.txt

┌──(llamafart㉿jaivanti)-[~]
└─$ sudo -u studentuser cat /home/studentuser/projectX/log_monitor.txt
[2025-07-29 07:51:32] Starting directory monitor on /home/studentuser/projectX/logs
[2025-07-29 07:52:32] New file detected: test_file.txt
```

4. Conclusion

This PoC successfully implemented a file monitoring solution that detects new `.txt` files in `/home/studentuser/projectx/logs` and logs events with timestamps to `log_monitor.txt`. The script was configured as a persistent `systemd` service, ensuring continuous operation under restricted user permissions.