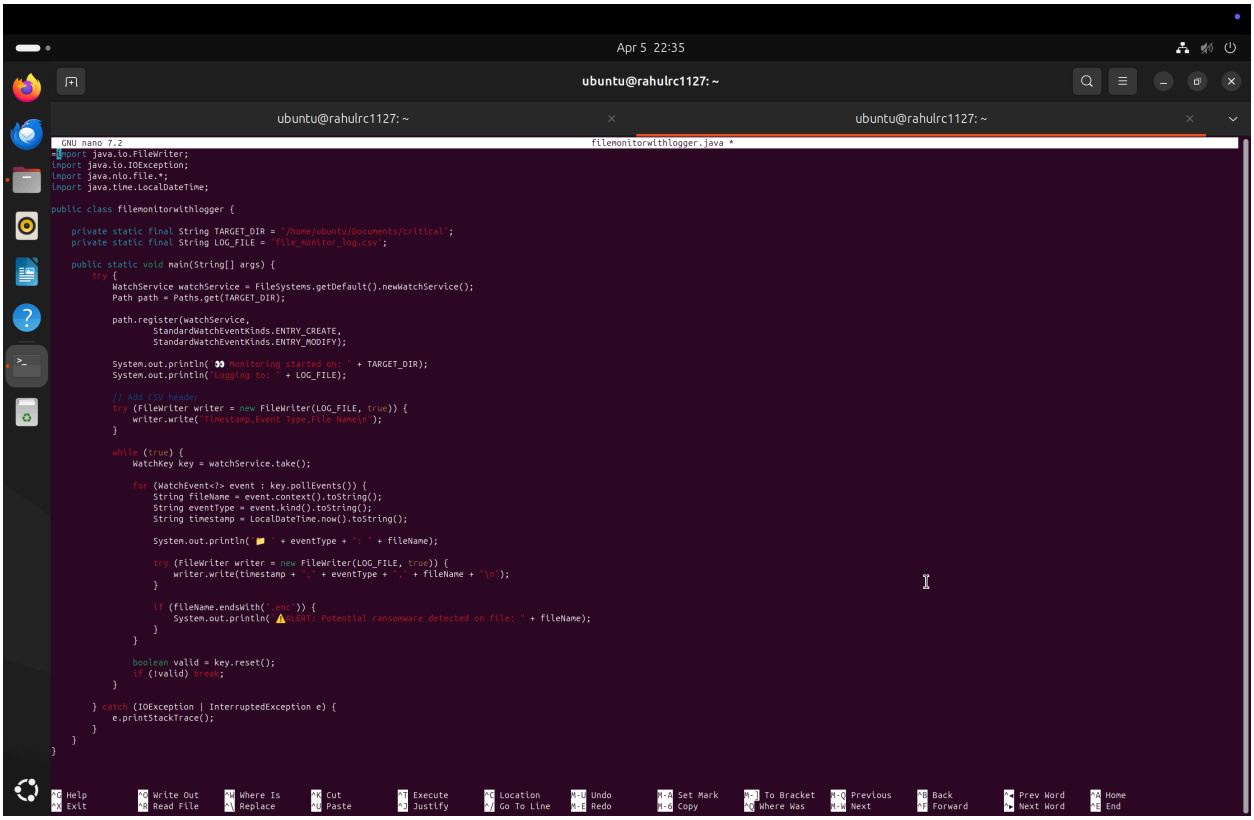
Group 12

Step 4: Monitoring

We'll use:

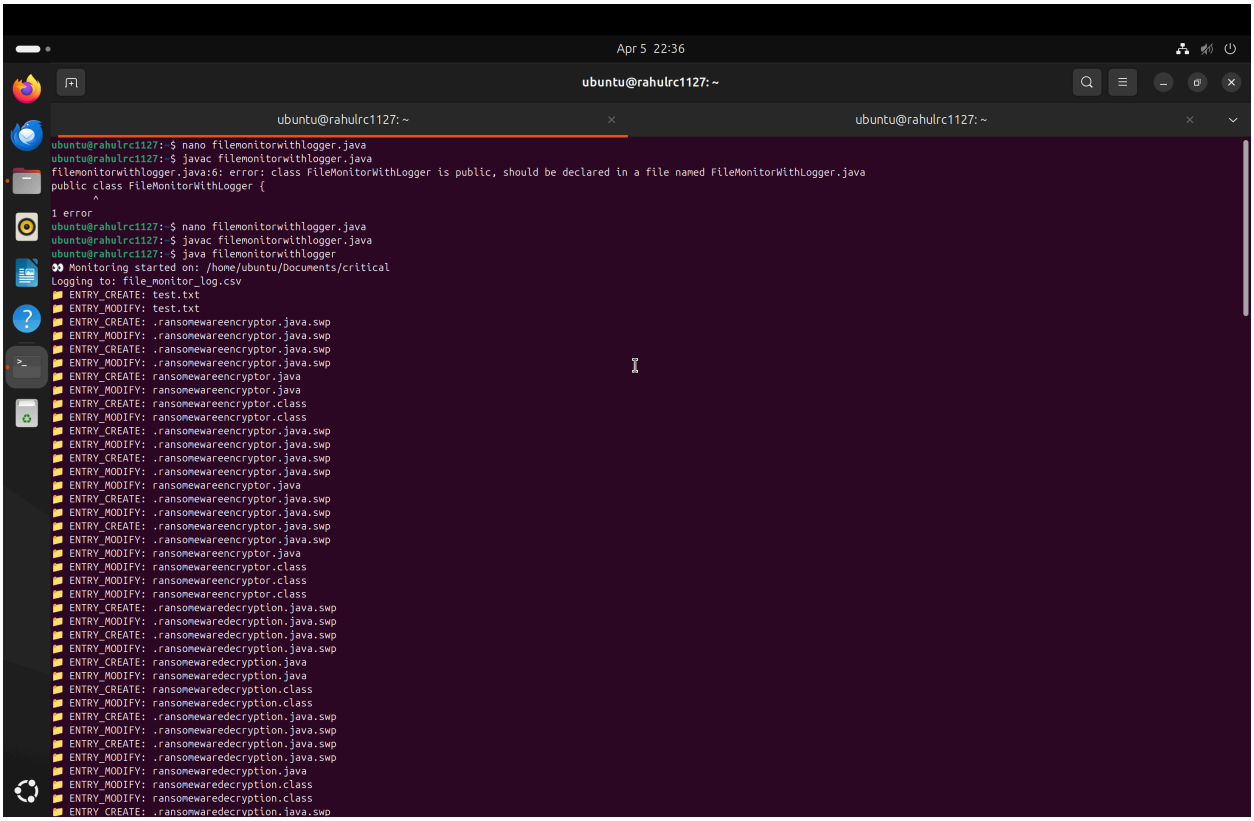
- **Java**
- **WatchService API** to monitor files in real-time
- **CSV file logging** (easy to implement and counts as structured)

The creation of filemonitorwithlogger.java



Group 12

This is the output for monitoring started in critical folder.



The third step required designers to create FileMonitorLogger.java which served as a Java-based file monitoring system for detecting ransomware activities operating on the victim's system.

The monitor implements Java's WatchService API to track live changes which occur in the /home/ubuntu/Documents/critical sensitive directory. The program records three elements of file system changes — creation, modification, and removal — to file_monitor_log.csv as a structured log file.

The active monitoring component of the system checks for the creation of .enc files because this action indicates ransomware has encrypted files.

The system detects these events through its API it will create console warning alerts. The component actively behaves like a HIDS system while it also supports automation capabilities to launch a decryptor post-payment and to isolate the system.

Real-time ransomware detection operates similarly to OSSEC among other tools according to their detection methods.