PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE

ACADEMIC YEAR: 2023-24

DEPARTMENT OF COMPUTER ENGINEERING DEPARTMENT

CLASS: B.E. **SEMESTER: I**
SUBJECT: LP-IV

ASSIGNMENT NO.	A5
TITLE	Write a program for Log Capturing and Event Correlation
PROBLEM STATEMENT /DEFINITION	Write a C++/Java program for Log Capturing and Event Correlation
OBJECTIVE	1. Understand Trojans and Backdoors 2. Understand Computer Forensics Investigation Process
OUTCOME	Students will be able to - 1. Learn Hard Disks and File Systems 2. Learn forensics Investigation Using AccessData FTK 3. Learn forensics Investigation Using EnCase 4. Learn log Capturing and Event Correlation
S/W PACKAGES AND HARDWARE APPARATUS USED	1. 64 bit open source LINUX 2. Eclipse- 64 bit.
REFERENCES	1. https://ilabs.eccouncil.org/log-capturing-event-correlation-2/
STEPS	Refer to theory, algorithm, test input, test output
INSTRUCTIONS FOR WRITING JOURNAL	1. Date 2. Assignment no. 3. Problem definition 4. Learning objective 5. Learning Outcome 6. Concepts related Theory 7. Algorithm 8. Test cases 9. Conclusion/Analysis

Prerequisites:

Concepts related Theory:

- **Introduction:**

System administrators have utilized log analysis for decades to monitor and automate their environments. As com-pute environments grow, and the scope and volume of the logs increase, it becomes more difficult to get timely, use-ful data and appropriate triggers for enabling automation using traditional tools like Swatch.

Event correlation is a technique for making sense of a large number of events and pinpointing the few events that are really important in that mass of infor-mation.

The goal of integrated management is to integrate the management of net- works (data, telephone and multimedia), systems (hosts and applications) and IT services in a coherent manner. The scope of this discipline notably includes network management, systems management and Service-Level Management.

Events and event correlator Event correlation usually takes place inside one or several management platforms (also known as Network Management Stations or Network Management Systems). It is implemented by a piece of software known as the event correlator. This tool is automatically fed with events orig- inating from managed elements, monitoring tools, the Trouble Ticket System, etc.

The event correlator plays a key role in the integration of management, for only there do network, system and service events come together.

Event filtering Event filtering consists in discarding events that are deemed to be irrelevant by the event correlator. For instance, a number of bottom-of- the-range devices are difficult to configure and occasionally send events of no interest to the management platform (e.g., printer P needs A4 paper in tray 1). Another example is the filtering of informational or debugging events by an event correlator that is only interested in availability and faults.

Event aggregation Event aggregation (also known as event de-duplication) consists in merging duplicates of the same event. Such duplicates may be caused by network instability (e.g., the same event is sent twice by the event source because the first instance was not acknowledged sufficiently quickly, but both instances eventually reach the event destination). Another example is temporal aggregation, when the same event is sent over and over again by the event source until the problem is solved.

Event masking[edit] Event masking (also known as topological masking in network management) consists in ignoring events pertaining to systems that are downstream of a failed system. For example, servers that are downstream of a crashed router will fail availability polling.

ALGORITHM

```
1. Start.
2. Display log menu and
If user enters choice 4
If user enters choice 5
If user enters choice 6
If user enters choice 4
If user enters choice 5
If user enters choice 6
ask for choice.
go to step 3.
go to step 4.
go to step 5.
go to step 6.
go to step 7.
go to step 8.
3. Display Boot log.
4. Display Mysql log.
5. Display Kern log.
6. Display Mail log.
7. Display all log files.
8. Stop.
```

Conclusion: successfully studied Log Capturing and Event Correlation.

Review Questions:

1) How to investigating System Log Data Using XpoLog Center Suite Tool?
2) justify Viewing Event Logs Using Kiwi Syslog Server Tool.