CYBER SECURITY INTERNSHIP

Task 12

LOG MONITORING & ANALYSIS

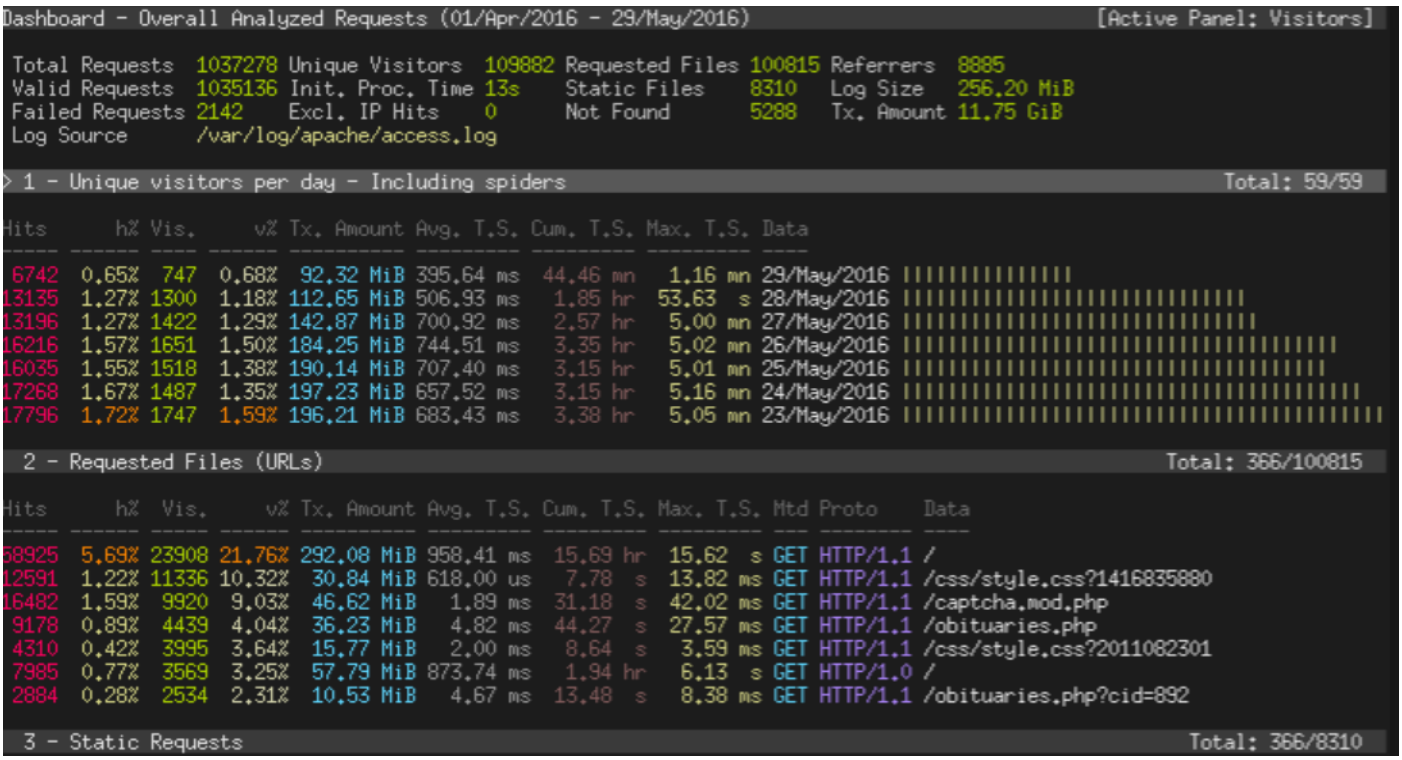
JASHMI KS

Log monitoring is the practice of collecting, aggregating, analyzing and processing network log data.

This information is generated from a variety of sources: network nodes, networking devices, applications, devices and third-party services. It may also contain:

- Security incidents and events information
- User traffic and access data
- Transactional logs
- Information about network and application performance

Information streams from heterogeneous sources are continuously monitored in real-time. The idea behind log monitoring initiatives is to identify anomalous incidents and understand insights from log data patterns. These insights can allow the organization to make proactive decisions on network security and performance by correctly predicting the future state of their networks based on real-time information streams.



Analyze Authentication Logs

Authentication logs provide detailed information about **user access attempts**.
They include data such as:

- Username
- Timestamp
- Source IP address
- Login method
- Success or failure status

By analyzing these logs, security teams can verify **who accessed the system**, **when**, and **from where**, ensuring only authorized users gain access.

Identify Failed Logins

Failed login attempts occur when a user enters **incorrect credentials** or tries to access a system without permission.
These events are important because:

- Repeated failures may indicate **brute-force attacks**
- Attempts using non-existent usernames may signal **reconnaissance activity**
- Sudden spikes in failures suggest **automated attack tools**

Monitoring failed logins helps detect early signs of compromise.

Detect Anomalies

Anomaly detection focuses on identifying abnormal behavior compared to normal system activity.
Examples include:

- Logins at unusual times
- Access from unfamiliar locations or IP addresses
- Sudden increase in data transfer
- Rare or unexpected system errors

Detecting anomalies allows security teams to spot potential threats before damage occurs.

Correlate Events

Event correlation means linking **multiple log entries from different sources** to form a complete picture.
For example:

- Multiple failed logins followed by a successful login
- Login event followed by data access and file changes
- Network traffic logs matching authentication logs

Correlation helps understand **attack patterns, timelines, and root causes**, instead of viewing logs in isolation.

Learn SIEM Basics

SIEM (Security Information and Event Management) systems **collect and centralize logs** from servers, applications, firewalls, and network devices.
Key functions of SIEM include:

- Log collection and storage
- Real-time monitoring
- Event correlation
- Threat detection

- Alert generation

SIEM tools improve visibility and help organizations **detect and respond to security incidents efficiently**.

Alerts

Alerts are automated warnings generated when predefined conditions are met.
They notify administrators about:

- Multiple failed login attempts
- Unauthorized access
- Suspicious traffic patterns
- Policy violations

Well-written alerts reduce response time and ensure **critical threats are not ignored**.