Report

Name: مهاب محمد عبد الفتاح

ID: 2205147

Log File Analyzed: apache_logs
Total Requests Processed: 10,000

Executive Summary

This analyzes web server traffic patterns, identifies anomalies, and provides actionable recommendations. Key findings include:

- **99.5% GET requests**, suggesting minimal form/API interaction
- **2.2% failure rate**, primarily from missing resources (404 errors)
- **Suspicious activity** from IP 66.249.73.135 (482 requests)
- **Peak failure periods** on May 18-19 and early morning hours

---

Traffic Overview

1. Request Distribution

Request Type	Count	Percentage
GET	9,952	99.52%
POST	5	0.05%

Observation:
The near-absence of POST requests may indicate malfunctioning forms or APIs requiring investigation.

Visitor Analysis

2. Unique Visitors

- **1,753 unique IP addresses** accessed the server
- **Top 3 most active IPs:**
    1. 66.249.73.135 (482 requests)
    2. 46.105.14.53 (364 requests)
    3. 130.237.218.86 (357 requests)

Security Note:
The top IP accounts for 4.8% of total traffic. While this could be a search engine crawler, verification is recommended to rule out malicious scraping.

Error Analysis

3. Failure Statistics

- **Total failed requests:** 220 (2.2%)
- **Error type breakdown:**
    - Page not found (404): 213 cases
    - Server errors (500): 3 cases
    - Access denied (403): 2 cases

4. Failure Patterns

- **Worst days:** May 18-19 (66 failures each)
- **Peak failure times:** 5:00 AM - 9:00 AM

Recommendation:
Implement enhanced monitoring during early morning hours when errors spike, particularly for missing page resources.

Traffic Patterns

5. Hourly Trends

- **Peak traffic period:** 10:00 AM - 8:00 PM (~450-500 requests/hour)
- **Quiet period:** 11:00 PM - 4:00 AM (~350 requests/hour)

6. Daily Averages

- Average daily requests: 2,500
- Highest traffic days correlated with increased failure rates

Optimization Opportunity:
Consider scheduling maintenance during low-traffic overnight hours to minimize user impact.

Security Observations

1. **Abnormal GET Request Volume**
   - One IP generated 482 identical requests
   - Typical user behavior shows more varied request patterns
2. **POST Request Anomalies**
   - Only 5 POST requests logged
   - Single IP (78.173.140.106) responsible for 60% of POST activity

Action Items:

- Verify legitimacy of high-volume IPs
- Investigate POST request scarcity (potential form submission issues)

Recommendations

Performance Improvements

- **Address missing resources** causing 404 errors
- **Optimize server capacity** for peak hours (10AM-8PM)
- **Investigate server errors** (500 status codes)

Security Enhancements

- **Implement rate limiting** for IPs exceeding 300 requests
- **Monitor early morning traffic** for suspicious patterns
- **Review POST request handling** to ensure proper functionality

Monitoring Suggestions

- Track 404 errors by requested resource
- Set alerts for sudden traffic spikes
- Log detailed information for POST requests

Conclusion

The web server demonstrates generally healthy traffic patterns with a 91% success rate. Primary areas requiring attention include:

1. **Resource management** for missing pages (404 errors)
2. **Security verification** of high-volume IPs
3. **Form/API functionality** due to abnormally low POST requests

Proactive monitoring during peak failure periods (early mornings, May 18-19) will help maintain service quality. Further investigation into the 500 server errors should be prioritized as these indicate critical system issues.

Final Assessment: The server shows good stability but would benefit from targeted optimizations and security hardening.