Alexandria National University

Faculty of Computers and Data Science Cyber Security Program

NAME :MOHAMED ahmed Aly mobarak

Id:2205249

Log File Analysis

1. Error Reduction Strategy (Current Error Rate: 2.91%)

Top Failing URLs (close to 100% failure rates):

- /sitemap.xml.gz – 586errors
- /admin.php – 239errors
- /comments/feed – 527 errors, with a 97.9% failure rate

HTTP Status Breakdown:

- 404 Not Found: 4,408 (≈ 99.4% of all errors)

- 405 Method Not Allowed: 11

- 500 Internal Server Error: 7 (critical)

High-Failure Time Windows:

- 18/00/2011 – 41.2% failure rate (472 errors)

- 15/00/2012 – 10.9% failure rate (349 errors)

- 14/00/2012 – 8.5% failure rate (281 errors)

Recommendations:

- Resolve Broken Links: Fix /sitemap.xml.gz, /admin.php, and investigate /comments/feed.

- Custom 404 Pages: Redirect to useful content to improve UX and SEO.

- 500 Error Audits: Review application logs for server error patterns.

- Review API Usage: 405 errors may indicate incorrect HTTP methods in use.

2. Critical Traffic Windows

Traffic Highlights:

- Busiest Hour: 22:00–22:59 → 8,977 requests (5.83% of daily traffic)

- Lowest Hour: 02:00–02:59 → 3,815 requests

Failure-Prone Hours:

- 07:00–07:59 → 7.5% error rate (403 failures)

- 14:00–14:59 → 6.67% error rate (578 failures)

- 19:00–19:59 → 6.02% error rate (393 failures)

Recommendations:

- Maintenance Window: Schedule updates from 02:00–03:00.

- Auto-Scaling Setup: Scale resources during 22:00–23:00 peaks.

- Error Pattern Investigation: Analyze background jobs at peak error times.

3. Security & Anomalies

Potential DoS Activity:

- 76.108.110.119 – 9,945 rapid requests

- 95.108.151.244 – 2,187 requests

- 188.40.97.2 – 1,532 requests

Suspicious IPs (targeting /admin.php, etc.):

- 221.224.13.25 – 253 attempts

- 195.238.176.90 – 242 attempts

- 61.221.28.243 – 194 attempts

Security Measures:

- Immediate Blocking: Deny IPs with >1,000 requests/minute.

- Rate Limiting: Limit per IP and tighten for admin paths.

- Long-Term: Use WAF, enable CAPTCHA, and monitor sensitive paths.

4. System Enhancements

Performance:

- Caching: Enable caching for static files.

- CDN: Use CDN for assets with high 404s.

Error Handling:

- Redirect broken links to valid resources (/comments/feed → /feed).

Capacity Planning:

- Horizontal scaling during peaks, optimize DB queries.

Security Hardening:

- Whitelist Access: Restrict /admin.php access.

- Enhanced Logging: Capture payloads for all 4xx/5xx errors.

- Alerts: Notify on 500 errors/day and IPs >500 reqs/minute.

Key Actions & Roadmap

Urgent (Next 24–48 hrs):

- Patch /admin.php and block abusive IPs.

Short-Term (1–2 weeks):

- Fix high-error URLs and deploy WAF.

Long-Term:

- Enable auto-scaling and structured logging.

This analysis highlights the critical role of access log monitoring in understanding system behavior and identifying points of failure or suspicious activity. By examining error rates, traffic

patterns, and security anomalies, we have developed actionable recommendations aimed at enhancing performance, increasing reliability, and strengthening security posture.

Such analysis serves as a foundational step toward building a more resilient and scalable system. It enables data-driven decision-making and prioritization of improvements based on real usage patterns rather than assumptions.

It is highly recommended to continue regular log analysis, maintain proactive security measures, and align infrastructure scaling with evolving user demand.