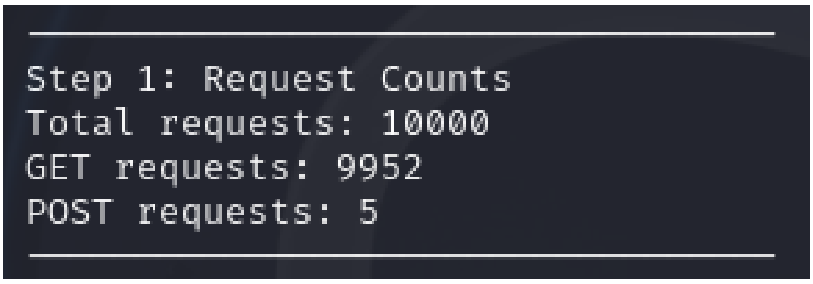
INFORMATION SECURITY

This assignment focuses on analyzing an Apache log file using a Bash script in Kali Linux. The script extracts key metrics such as request counts, unique IPs, failure rates, and request trends by hour. I created and executed the script to summarize traffic behavior, identify issues, and provide improvement suggestions based on the findings.

PREPARED BY :

Mariam Beshr

STEP 1: REQUEST COUNTS



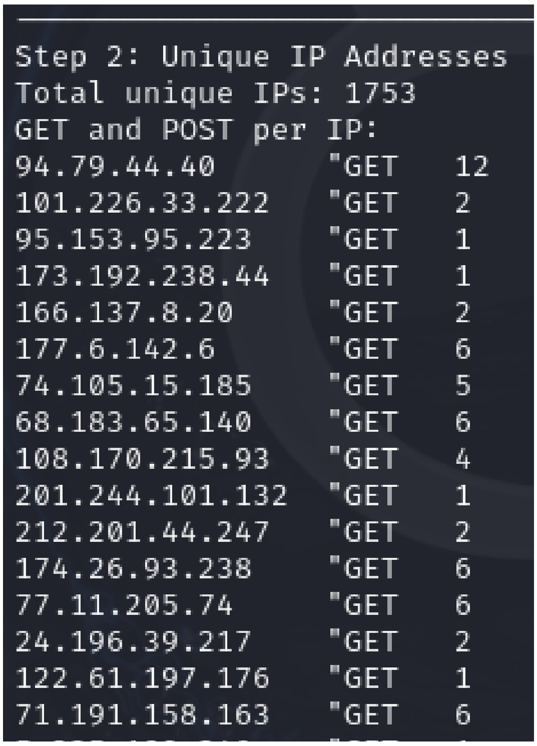
```
Step 1: Request Counts
Total requests: 10000
GET requests: 9952
POST requests: 5
```

- Total Requests: 10,000
- GET Requests: 9,952
- POST Requests: 5
- GET requests make up 99.52% of all traffic, indicating static content access is predominant.

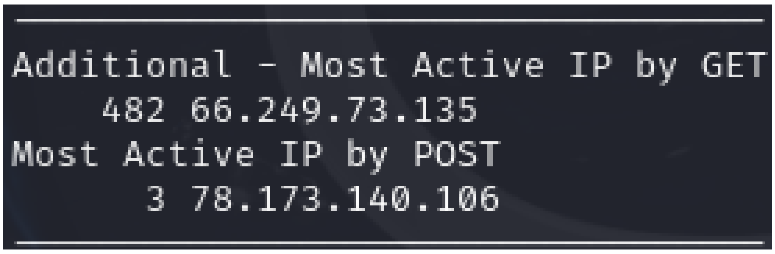
Recommendation:

If the application is expected to handle dynamic interactions, ensure POST operations are being processed and logged correctly.

STEP 2: UNIQUE IP ADDRESSES & ADDITIONAL: MOST ACTIVE IP BY GET/POST



```
Step 2: Unique IP Addresses
Total unique IPs: 1753
GET and POST per IP:
94.79.44.40        "GET   12
101.226.33.222     "GET   2
95.153.95.223      "GET   1
173.192.238.44     "GET   1
166.137.8.20       "GET   2
177.6.142.6        "GET   6
74.105.15.185      "GET   5
68.183.65.140      "GET   6
108.170.215.93     "GET   4
201.244.101.132    "GET   1
212.201.44.247     "GET   2
174.26.93.238      "GET   6
77.11.205.74       "GET   6
24.196.39.217      "GET   2
122.61.197.176     "GET   1
71.191.158.163     "GET   6
```



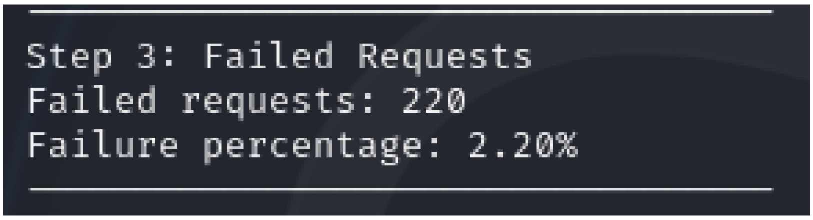
```
Additional - Most Active IP by GET
    482 66.249.73.135
Most Active IP by POST
      3 78.173.140.106
```

- Unique IPs: 1,753
- Most IPs made minimal requests, indicating bot traffic or occasional access.
- Top GET requester: 66.249.73.135 (likely Googlebot)
- Top POST requester: 78.173.140.106 (3 requests)

Recommendation:

Implement rate limiting or CAPTCHA to prevent scraping or abuse from bots. Monitor high-frequency IPs.

STEP 3: FAILED REQUESTS



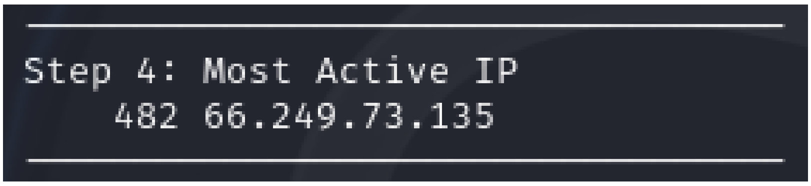
```
Step 3: Failed Requests
Failed requests: 220
Failure percentage: 2.20%
```

- Total Failures: 220
- Failure Rate: 2.20%
- Majority were 404 Not Found errors (213 times)

Recommendation:

Audit your site for broken or outdated links. Implement user-friendly error pages and consider automatic redirects for common 404s.

STEP 4: MOST ACTIVE IP



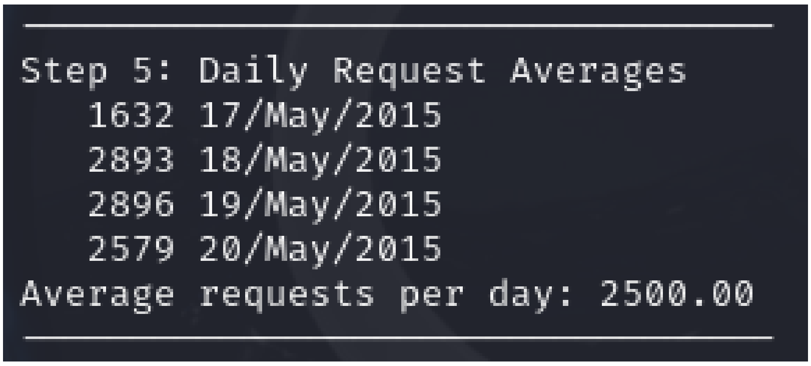
```
Step 4: Most Active IP
    482 66.249.73.135
```

- IP: 66.249.73.135
- Requests: 482 (highest)

Recommendation:

Monitor this IP’s activity closely. If it's a crawler, ensure your robots.txt is properly configured to guide its behavior.

STEP 5: DAILY REQUEST AVERAGES



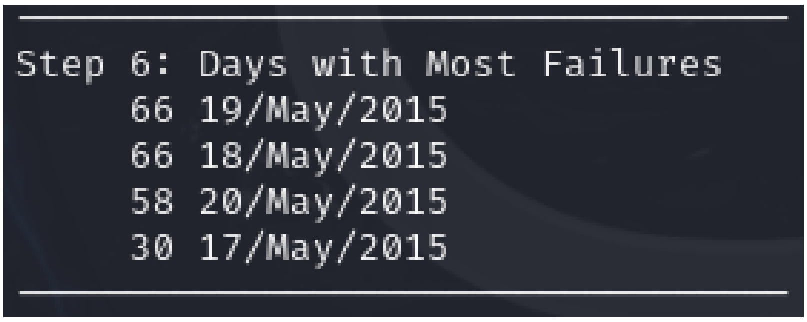
```
Step 5: Daily Request Averages
   1632 17/May/2015
   2893 18/May/2015
   2896 19/May/2015
   2579 20/May/2015
Average requests per day: 2500.00
```

- 4 days of logs analyzed
- Average: 2,500 requests per day
- Peak days: 18 May and 19 May (~2,900 requests each)

Recommendation:

Plan server resource allocation according to peak usage days. Use this data for load testing.

Step 6: Days with Most Failures



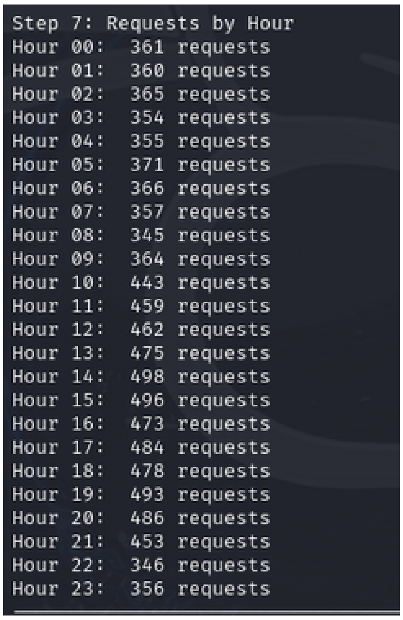
```
Step 6: Days with Most Failures
     66 19/May/2015
     66 18/May/2015
     58 20/May/2015
     30 17/May/2015
```

- 19 May and 18 May: 66 failures each they were also the peak days
- Likely server or deployment issues

Recommendation:

Review error logs and recent code or server changes around these dates.

Step 7: Requests by Hour



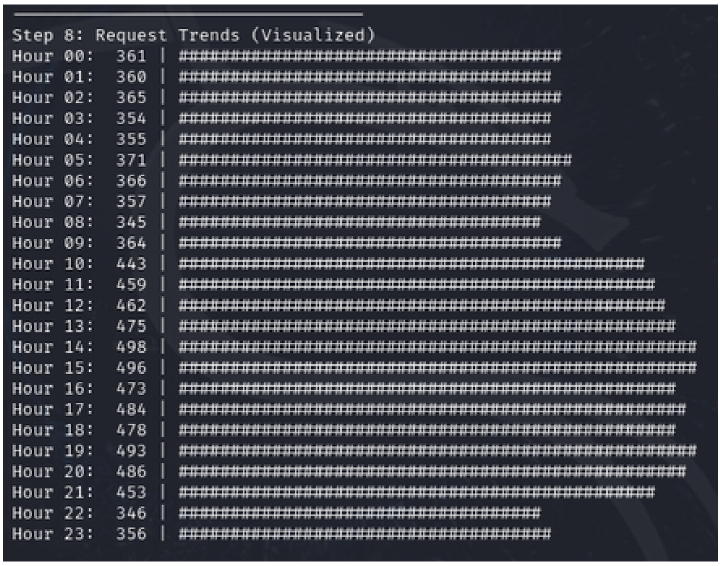
```
Step 7: Requests by Hour
Hour 00:  361 requests
Hour 01:  360 requests
Hour 02:  365 requests
Hour 03:  354 requests
Hour 04:  355 requests
Hour 05:  371 requests
Hour 06:  366 requests
Hour 07:  357 requests
Hour 08:  345 requests
Hour 09:  364 requests
Hour 10:  443 requests
Hour 11:  459 requests
Hour 12:  462 requests
Hour 13:  475 requests
Hour 14:  498 requests
Hour 15:  496 requests
Hour 16:  473 requests
Hour 17:  484 requests
Hour 18:  478 requests
Hour 19:  493 requests
Hour 20:  486 requests
Hour 21:  453 requests
Hour 22:  346 requests
Hour 23:  356 requests
```

- Traffic gradually increases from morning and peaks between 14:00 to 20:00
- Highest at 14:00 with 498 requests

Recommendation:

Optimize server performance during peak periods. Use caching or load balancers if needed.

Step 8: Request Trends (Visualized)



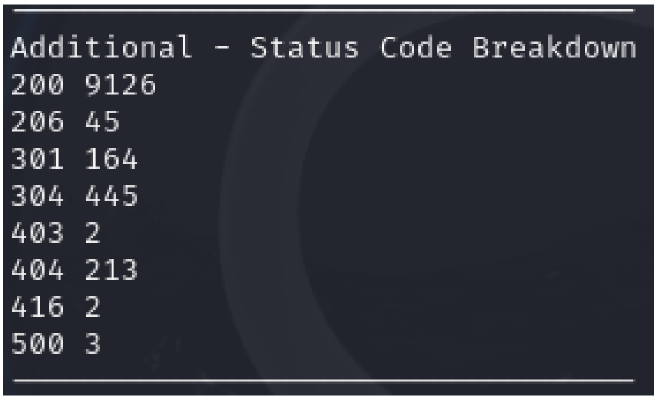
```
Step 8: Request Trends (Visualized)
Hour 00:  361 | #####################################
Hour 01:  360 | ####################################
Hour 02:  365 | #####################################
Hour 03:  354 | ####################################
Hour 04:  355 | ####################################
Hour 05:  371 | ######################################
Hour 06:  366 | #####################################
Hour 07:  357 | ####################################
Hour 08:  345 | ###################################
Hour 09:  364 | #####################################
Hour 10:  443 | #############################################
Hour 11:  459 | ##############################################
Hour 12:  462 | ###############################################
Hour 13:  475 | ################################################
Hour 14:  498 | ##################################################
Hour 15:  496 | ##################################################
Hour 16:  473 | ################################################
Hour 17:  484 | #################################################
Hour 18:  478 | ################################################
Hour 19:  493 | ##################################################
Hour 20:  486 | #################################################
Hour 21:  453 | ##############################################
Hour 22:  346 | ###################################
Hour 23:  356 | ####################################
```

- Consistent and steady usage throughout the day
- No unusual spikes, indicating normal activity

Recommendation:

Use visual trends to forecast usage. If any spikes occur later, investigate for DDoS or viral content.

Additional: Status Code Breakdown



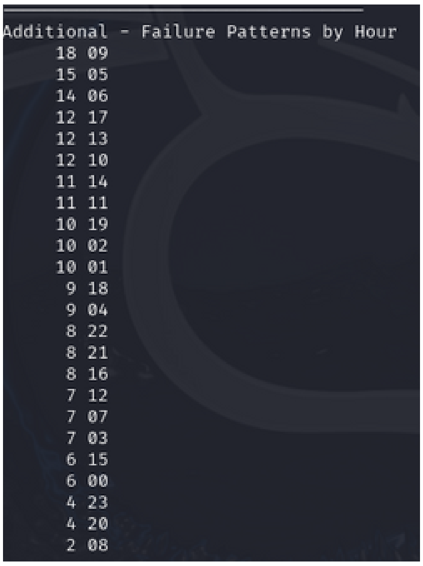
```
Additional - Status Code Breakdown
200 9126
206 45
301 164
304 445
403 2
404 213
416 2
500 3
```

- 200 OK: 9126
- 404 Not Found: 213
- 500 Internal Server Error: 3
- Others: 301, 304, 403, 416

Recommendation:

Urgently fix 500 errors. Consider monitoring tools to notify about recurring 4xx and 5xx statuses.

Additional: Failure Patterns by Hour



```
Additional - Failure Patterns by Hour
     18 09
     15 05
     14 06
     12 17
     12 13
     12 10
     11 14
     11 11
     10 19
     10 02
     10 01
      9 18
      9 04
      8 22
      8 21
      8 16
      7 12
      7 07
      7 03
      6 15
      6 00
      4 23
      4 20
      2 08
```

- Most failures occurred between 09:00 and 14:00, aligning with peak load.

Recommendation:

Reinforce infrastructure or backend handling during this time. Automate alerting for failure surges.

General Summary

The system is stable, but some improvements are needed in error handling and crawler management.
Resource planning should account for peak hours (14:00–20:00) and high-traffic days (18–19 May).
Security and performance can be enhanced by applying proper monitoring, optimization, and access control.

THE END