Assumptions:

- The provided HTTP logs are representative of the enterprise web server's traffic.

- Reconnaissance activities can be identified based on abnormal patterns in the HTTP logs.

- Baseline statistics derived from normal web traffic are accurate representations of legitimate behaviour.

- Thresholds for abnormal behaviour detection are set appropriately to minimize false positives and false negatives.

Steps:

1) Data Pre-processing
    - Download & extract the dataset
    - Parse and pre-process the HTTP logs to obtain relevant information
    - Filter out all irrelevant data
2) Metrics calculation
    - Calculate key metrics that indicate reconnaissance activities
    - Calculate all activities related to abnormal behaviour such as a high number of failed requests, repeated access to restricted areas etc
    - Take time-based metrics into consideration such as the number of requests within a specific time window to detect scanning/probing behaviour
3) Establishing Baseline
    - Analysing a period of web traffic
    - Calculate statistical measures such as mean, standard deviation, percentiles for the metrics obtained
    - Use the statistics above as thresholds for abnormal behaviour detection
4) Identify Suspicious IPs
    - Compare the calculated metrics of each IP address with the baseline thresholds
    - Identify IPs that exceed the threshold and categorize IPs based on the severity of their suspicious behaviour.
5) False Positive Reduction
    - Conduct analysis to reduce false positives
6) Alert Generation
    - Generate alerts and reports listing the shortlisted IPs that exhibit potential reconnaissance activities