Rubric: ARIMA for Anomaly Detection in DDOS Attacks

Ben Harris

DS 4002: Prototyping – 4/28/2025

This rubric outlines the expectations for completing the ARIMA-based anomaly detection case study. There are 3 final deliverables:

1. A 1–2 page PDF summarizing EDA results with context, stats, and plots
2. A script (R or Python) that tests stationarity using the ADF test
3. A script (R or Python) implementing an ARIMA model for each server metric

Spec Category	Spec Details
Exploratory Data Analysis	Create a PDF (1-2 pages) with the following: - Description/context for each server metric from the Numenta Anomaly Benchmark repository - Summary statistics (mean, median, standard deviation, etc.) for each variable - Relevant plot for each variable (Hint: plot the values over time)
Assumption Testing	Create a script to conduct an Augmented Dickey Fuller (ADF) test. This will verify that the time series data is stationary, a necessary assumption for ARIMA analysis.

	Your script should satisfy the following: - Format: R or Python - Use a 5% confidence level - Output a chart that indicates if stationarity assumption is met for each of the 3 server metrics - Include highly detailed comments for each step to describe what the code is accomplishing
ARIMA Model	Create a script (or scripts) to create an ARIMA model for anomaly detection. Your script should satisfy the following: - Format: R or Python - Include highly detailed comments for each step to describe what the code is accomplishing You may break up the code into one file for each of the 3 server metrics if desired for simplicity.