ExtraHop Request Analyzer

Sponsor: ExtraHop
Mentor: Eric Ball
Team: Naboo
Karl Finnsson, Brenden Larson, Natasha Li, Matt Sturtevant, Joseph White

Project Problem
When network traffic comes to a halt, one of the first things IT administrators are likely to look at is the round trip times for requests. Digging into the cause of high round trip times is a time consuming task. They must look for requests that have long round trip times and events such as retransmission timeouts, inefficient routing, or spikes in the number of requests.

ExtraHop Platform
The ExtraHop Platform can be broken up into two entities:

- The ExtraHop Operation Intelligence Appliance sits on the user’s network and collects real-time data metrics on L2 - L7 of the OSI model which can be viewed on the appliance web page.
- The PyHop API is a Python library provided by ExtraHop to access data metrics stored on the appliance.

Project Goals
ExtraHop Defined Goals
- Utilize the ExtraHop box metrics using the PyHop API
- Explore real-world applications for network data metrics
- Learn new skills and concepts

Team Defined Goals
- Gain experience with web development
- Learn networking concepts

Glossary
Traceroute: An application that determines each router that must be traversed to reach a specified IP address.
RTO: Retransmission Timeout
RTT: Round Trip Time

Analysis
- Retransmission timeouts indicate congestion
- Traceroutes may show inefficient routing
- Average RTT may show trends in traffic
- Scatter plot of RTTs may indicate outliers
- Breakdown of protocols can explain network traffic

ExtraHop Request Analyzer
The ExtraHop Request Analyzer (ERA) utilizes data metrics obtained from the ExtraHop Operation Intelligence Appliance about requests. Features of ERA include:
- Filtering requests shown based on round trip time
- Pinpointing where requests originated on the network and the paths they take
- Displaying the path a specified request took on a map
- Real-time graphs analyzing protocol percentage, average round trip time and round trip time over all requests

Impact
Our application automatically detects requests with high round trip times and begins performing operations to determine the bottleneck. ERA automates tasks that would normally be performed manually, helping IT quickly detect the cause of problems on their network.

Future Work
- Utilize more metrics
- Provide more filtering options for users
- Store request information for longer periods of time
- Network activity trend recognition

Acknowledgements
A big thank you to:
- Sakire Arslan Ay
- Eric Ball
- Bhushan Khanal
- Vasily Bunakov
- AI Guyer
- John Yates
- Carl Yates
- ExtraHop