KIBANA SEARCHES

This document provides some example Kibana searches if you'd like to use it for the lab exercises but don't have any prior experience with the tool. Make sure to also watch my crash course video for an overview of how to navigate Kibana and perform aggregations.

Standard Search
field:value

Compound Search
field:value AND field:value
field:value OR field:value
field:(value1, value2, value3) – This is an OR
field1:value1 AND field2:value2 AND NOT field3:value3

Wildcard Searches
field:val* -- Matches any value starting with val
field:*ue – Matches any value ending with eu
field:v*e – Matches any value starting with v and ending with e

CIDR Notation Search
srcip:"192.168.1.0/24"

Comparison Searches
srcport:<80 – Less than 80
srcport:>80 – Greater than 80
srcport NOT 80 – Any port value other than 80

Range Search
srcport:(0 TO 1024)

Exists Search
exists:username – Matches logs where the username field exists