Lab 4: Hands On

Hurricane Labs

- Using Splunk environment, explore the linux:netfilter source type
  - These are the firewall logs we onboarded earlier
- Search for your (public) IP address and review the fields available
- Experiment with the time range picker
  - Search for logs from a 15 minute window earlier today
- Practice with logical operators and by using different search terms
- Stop a running job, and share the results with a classmate
- Export raw search results
- View your search history/activity