Dreadnought Lab – Week 08: SIEM & Visual Threat Hunting

# 🎯 Objectives

Build visual dashboards to identify anomalies and possible intrusions in real-time log streams.

# 📋 Lab Tasks

* ☐ Create a dashboard in Kibana or Splunk with visualizations for login events and process tree anomalies.
* ☐ Simulate beaconing behavior (e.g., regular ICMP pings or DNS exfiltration).
* ☐ Use your dashboard to identify patterns of concern.

# 💡 Challenge Task

☐ Detect a stealthy lateral movement attempt using parent-child process analysis.

# 🧠 Reflection

What types of patterns do stealthy attacks try to hide from visual detection?