Dreadnought Lab – Week 11: Purple Team Simulation

# 🎯 Objectives

Simulate a red/blue engagement end-to-end. The red team attacks, and the blue team responds with detections and logs.

# 📋 Lab Tasks

* ☐ Red team performs enumeration, basic attack (e.g., brute-force, reverse shell).
* ☐ Blue team captures logs using Sysmon, ELK, or Wazuh.
* ☐ Correlate timestamps, tools used, and IOC (Indicators of Compromise).

# 💡 Challenge Task

☐ Generate an alert using your SIEM and report on how the blue team responded.

# 🧠 Reflection

What did each team learn from this exercise? What can improve for real-world readiness?