Dreadnought Lab – Week 07: SIEM Detection Engineering I

# 🎯 Objectives

Parse logs using ELK or Wazuh and write custom detection rules based on simulated attacks.

# 📋 Lab Tasks

* ☐ Use Sysmon to generate logs for process creation and file writes.
* ☐ Ingest logs into Wazuh/Splunk/ELK.
* ☐ Write a rule to detect suspicious PowerShell activity or brute-force attempts.

# 💡 Challenge Task

☐ Map your detection to a MITRE ATT&CK technique.

# 🧠 Reflection

How do logs expose attacker behavior beyond signature-based detection?