Magos Lab – Week 08: Mini Red/Blue Exercise

# 🎯 Objectives

Explore basic offensive and defensive techniques in a contained red vs blue scenario.

# 📋 Lab Tasks

* ☐ Red Team: Use `hydra` or `medusa` to brute-force SSH or HTTP login.
* ☐ Blue Team: Use Wazuh/Splunk to detect the brute-force attack.
* ☐ Document timestamp, IP, and account targeted.

# 💡 Challenge Task

☐ Generate a custom alert and email it to the Blue Team inbox.

# 🧠 Reflection

What surprised you most about how easily credentials can be brute-forced?