Dreadnought Lab – Week 09: Offensive Scripting & Network Recon

# 🎯 Objectives

Write Python or Bash scripts to perform recon, port scanning, and stealth enumeration for internal network targets.

# 📋 Lab Tasks

* ☐ Write a Python script that scans a subnet for live hosts using ICMP or TCP.
* ☐ Use `socket` or `nmap` in script form to probe open ports and services.
* ☐ Log results to a file and include banners or fingerprints when available.

# 💡 Challenge Task

☐ Add multithreading to your scanner or develop an evasion mechanism (e.g., spoofed user-agent or delay).

# 🧠 Reflection

What makes a scan obvious or stealthy from a defender’s point of view?