Adversary Emulation Techniques

Purpose: Emulation validates detections by reproducing adversary TTPs in a controlled environment (MITRE Caldera, Atomic Red Team).

Example Scenario: Emulate T1566 (phishing) followed by T1210 (exploitation of remote service) to validate email filters and Wazuh detection rules.

Emulation Steps: 1) Define objectives & scope. 2) Select TTPs & mapping. 3) Execute on isolated lab. 4) Capture telemetry & refine detections.