Document Generated: 11/24/2026

Learning Style: On Demand

Technology:

Difficulty: Beginner

Course Duration: 1 Hour

Lab - Writing and Testing Suricata Rules with PCAP



Practice writing and testing custom Suricata detection rules against PCAP files containing port scanning activity. You'll validate rule effectiveness offline, then implement and test the rules in a live environment to ensure accurate detection without disrupting normal operations.