Document Generated: 11/24/2026

Learning Style: On Demand

Technology:

Difficulty: Beginner

Course Duration: 1 Hour

Lab - Ruling Snort



Analyze network traffic using tcpdump and configure Snort rules to detect specific types of traffic. You'll learn to create, implement, and verify Snort rules for ICMP and FTP traffic.