# Snort IDS Lab – Executive Project Summary

This project implemented and tested Snort as an Intrusion Detection System (IDS) in a controlled lab environment. The goal was to detect reconnaissance activity such as ICMP pings, TCP SYN scans, and optional HTTP brute force attacks.

## ■■ Lab Environment

- **Snort Sensor**: Ubuntu Linux VM
- **Victim Host**: Windows 10 VM
- **Attacker Host**: Kali Linux VM
- **Internal Network (LAN10)** with static IPs

## ■ Custom Rules

Two detection rules were created:
- ICMP Ping Detection
- TCP SYN Scan Detection

## ■ Key Findings

- ■ Snort detected ICMP ping sweeps
- ■ Snort detected TCP SYN scans
- ■■ HTTP brute force attempted, requires extended rules

## ■ Results Summary

Snort successfully identified early-stage reconnaissance activity. This demonstrates its role in network defense and monitoring, providing defenders with visibility into potential threats.

## ■ Next Steps

- Expand ruleset for HTTP brute force
- Integrate Snort alerts with SIEM (Splunk/ELK)
- Automate lab setup using Ansible or scripts

## ■ Closing Notes

This lab reinforced my skills in IDS fundamentals, Snort rule writing, and packet analysis. Snort caught attacks in real-time, showcasing its value in early reconnaissance detection.

■ Branded for the journey: **#CyberBabeLoading #ThreatDetection #SnortIDS #BlueTeam**