code_alpha-task2-setting-of-network-intrusion-detection-system

Network Intrusion Detection System (NIDS) using Snort, implemented on Ubuntu with Kali Linux attack simulations. Detects real-time threats like port scans and exploits through customized rules. Validated in a virtual lab environment, demonstrating effective traffic monitoring and alerting. Provides a foundation for network security hardening

📌 Objectives

Deploy Snort on Ubuntu as a NIDS to monitor a designated network.

Simulate reconnaissance attacks from Kali Linux using:

Nmap (port scanning, OS fingerprinting)

Evaluate Snort's detection accuracy by analyzing generated alerts.

Document rules and configurations for reproducibility.

Part I: Lab Environment Setup

1. Virtual Infrastructure Attacker Machine: Kali Linux (Offensive Security Tools)

Monitored Machine: Ubuntu 22.04 LTS (Running Snort IDS)

Network: Host-only/NAT configuration to isolate lab traffic

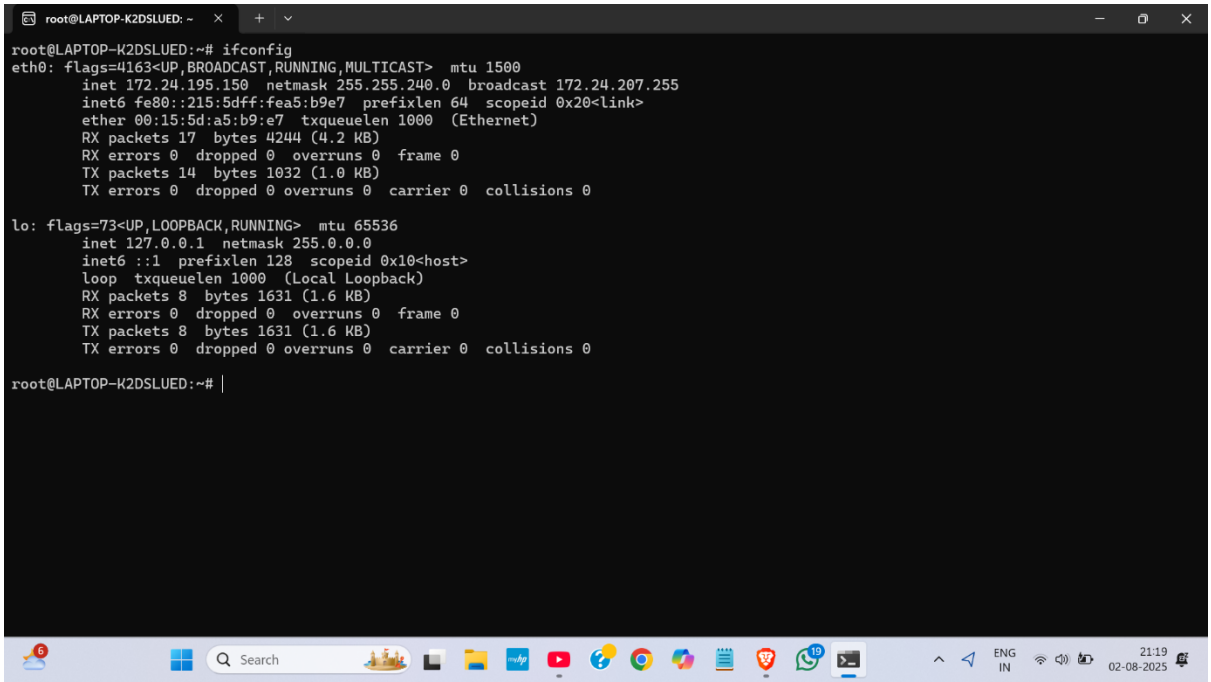

Figure 1.1: IP address and Network Interface Card for Ubuntu

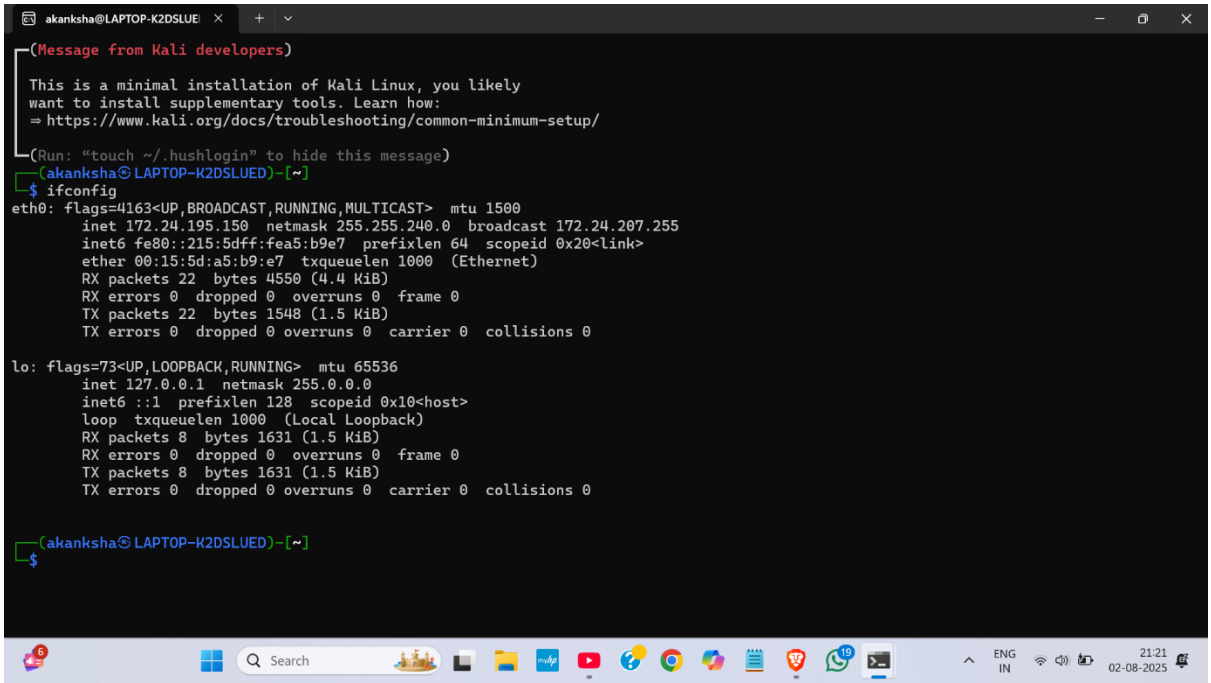

Figure 1.2: Verifying attacking machine IP address

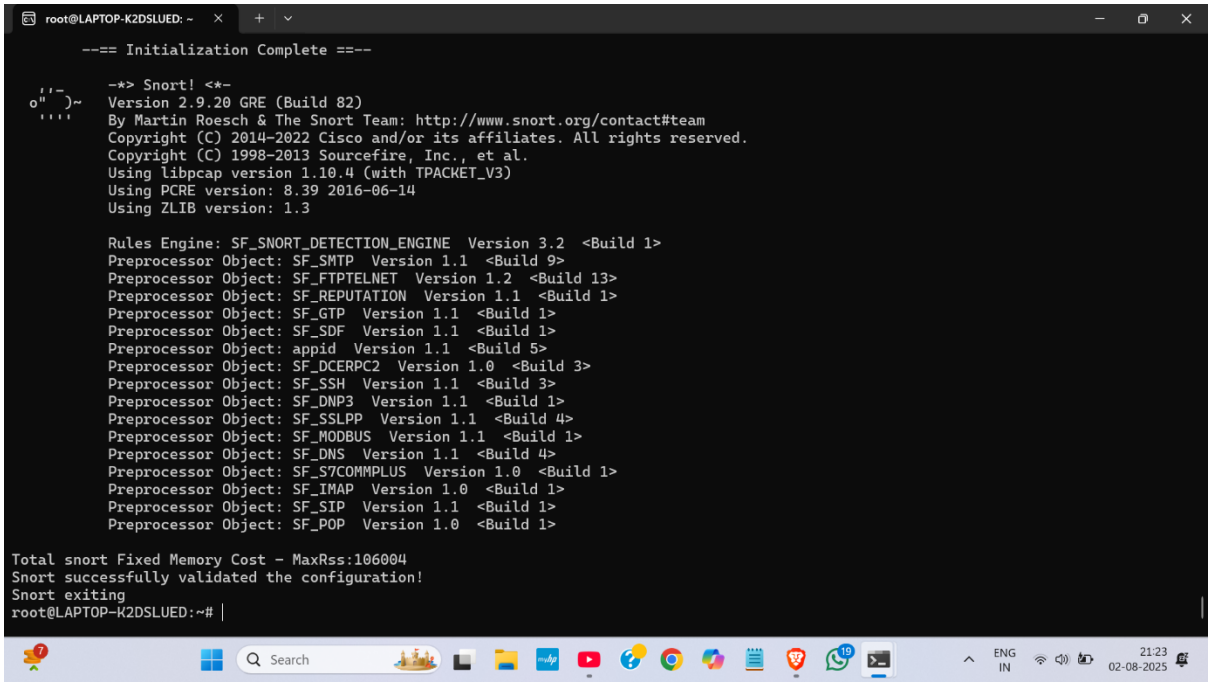

Figure 1.3: Snort successfully validated the configuration

Part II: Attack Simulation & Detection Analysis

Simulated Attacks from Kali
Linux

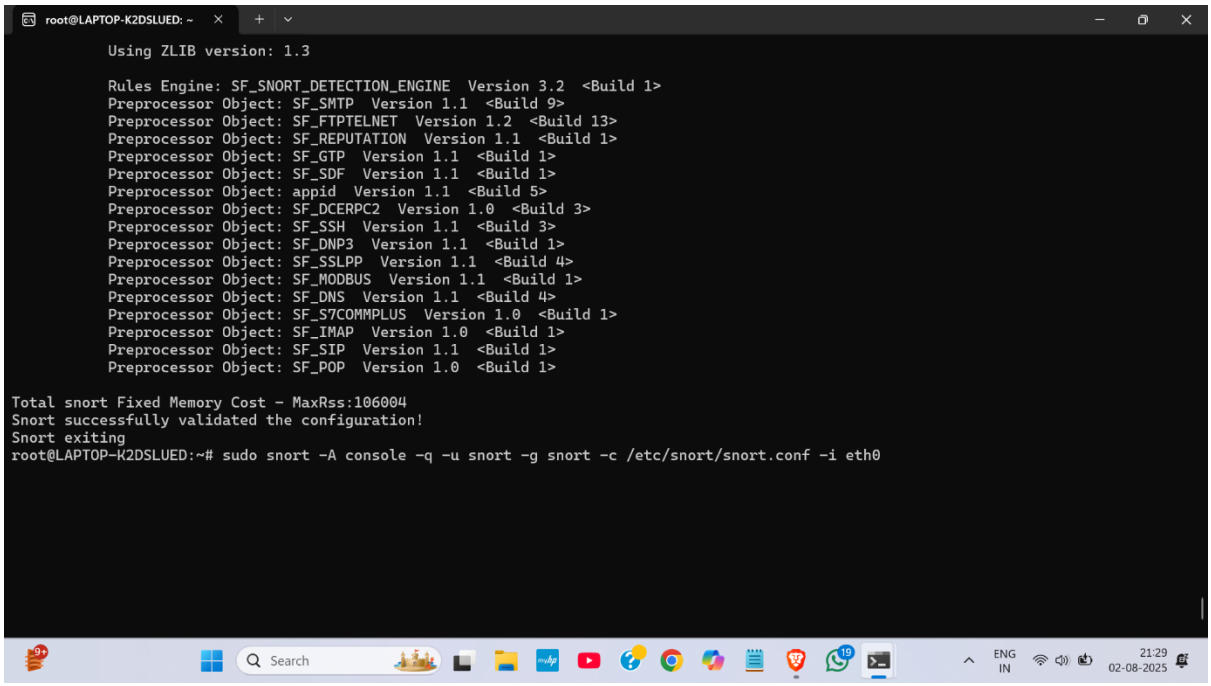

Figure 2.1: Monitoring enabled

Kali Linux initiated an Nmap scan against an Ubuntu machine to test Snort's reconnaissance detection. The scan probed for open ports,

services, and OS fingerprints, generating detectable network traffic. Snort (if properly configured) should log alerts for scan patterns (e.g., SYN floods, service probes). This simulation validates Snort's ability to detect basic Nmap scans as part of intrusion detection.

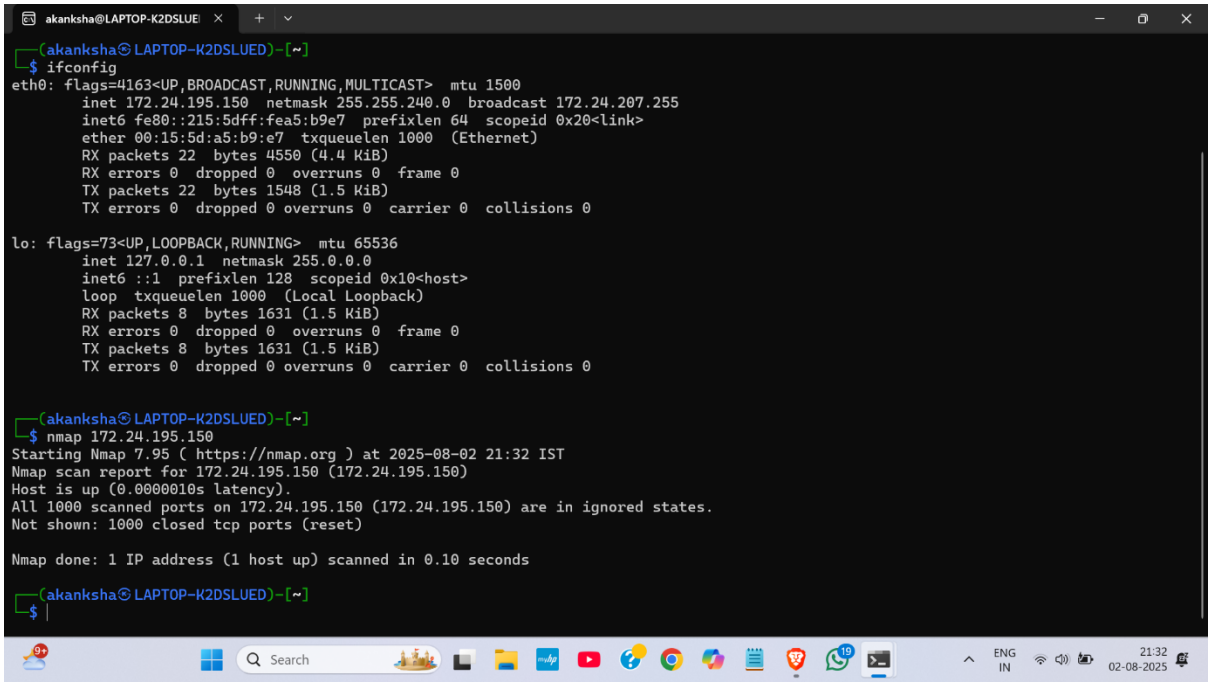

Figure 2.2: Nmap scan Snort successfully detected the scan and generated alerts.

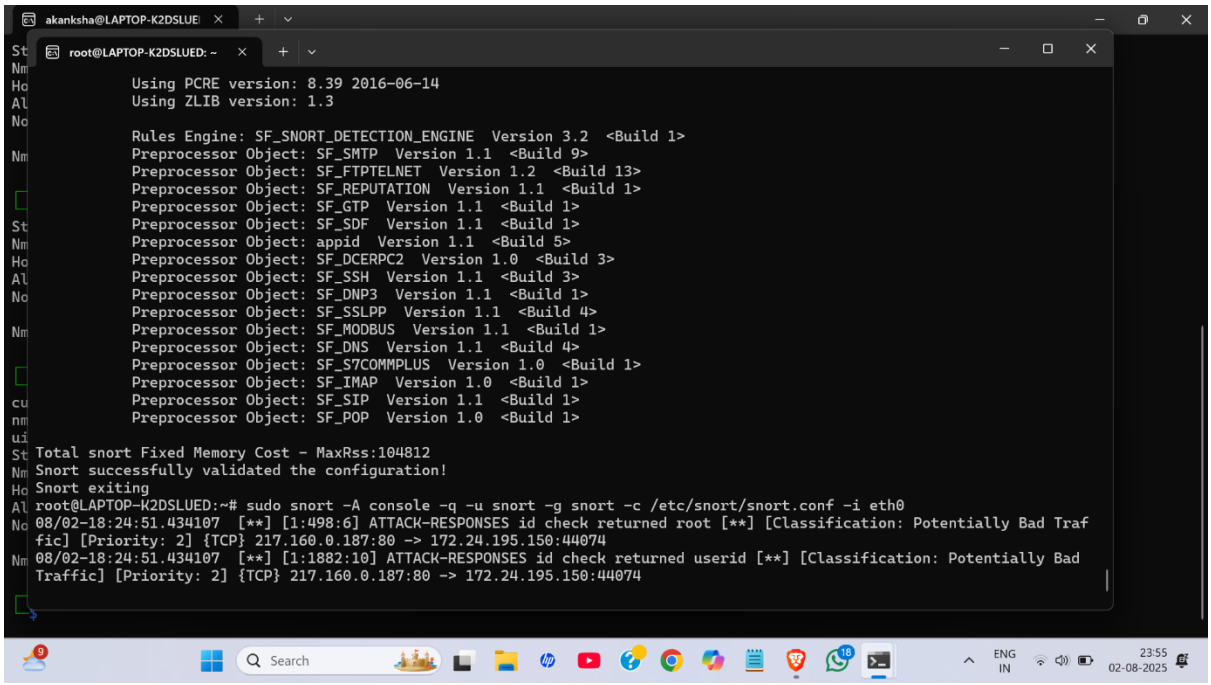

Figure 2.3: Snort detecting the Nmap scan Legion is another tool for information gathering. This tool was employed to simulate more advanced reconnaissance and network mapping attacks. Using Legion, the IP address of the Ubuntu machine was scoped, and detailed scans were performed.

The attack targeted different services running on the Ubuntu machine, attempting to map open ports and exploit known vulnerabilities.

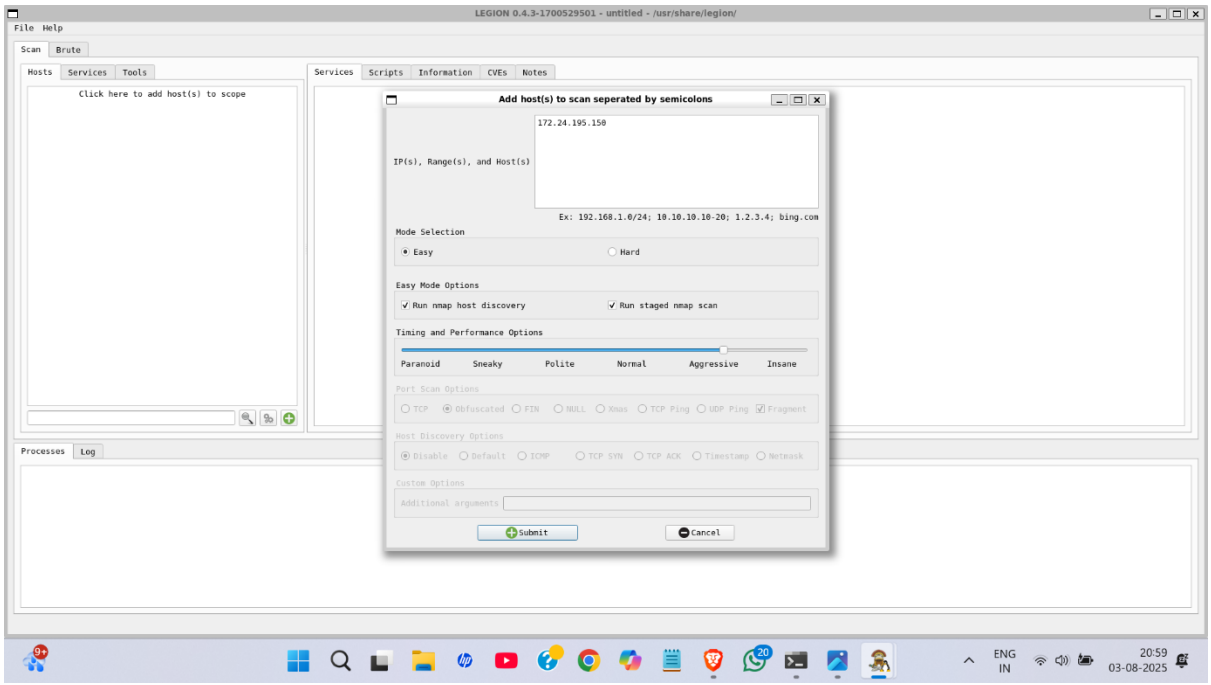

Figure 2.4: adding Ubuntu machine IP address to scope Snort was again successful in detecting these malicious activities and issued real-time
alerts

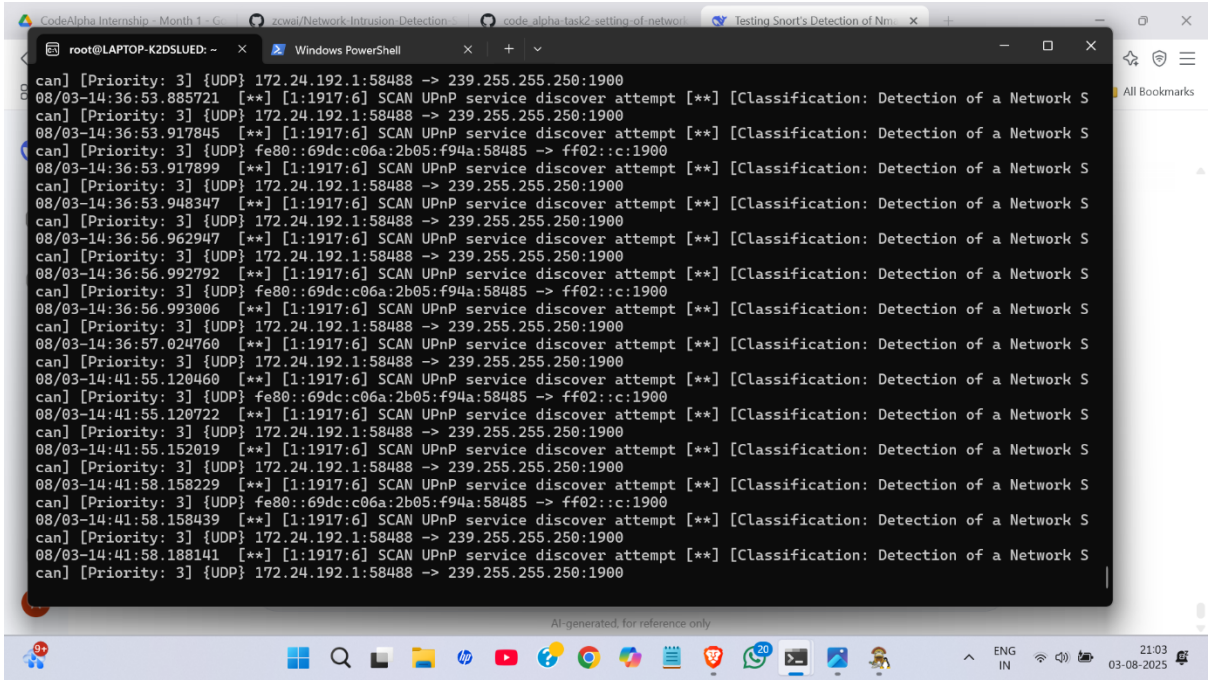

Figure 2.5: Snort detecting Legion scanning attack