Network Security Lab – Intrusion Detection with Snort

Title: “Configuring and Testing a Snort-based Intrusion Detection System”

Description:

In this laboratory exercise, you will configure and test a network intrusion detection system (IDS) using Snort. The objective is to detect and analyze network attacks through packet inspection and rule-based pattern matching.

You are required to install Snort on a Linux virtual machine, configure rule files to detect suspicious activities such as port scanning, brute-force SSH attempts, and DNS tunneling.

Run packet capture sessions using Wireshark or tcpdump and simulate basic attack scenarios using Nmap and Hydra.

Document your findings, including system configuration steps, rule syntax explanations, packet analysis screenshots, and alert logs generated by Snort.

Your report should conclude with a reflection on IDS limitations, potential false positives, and future improvements such as integrating Snort with Security Information and Event Management (SIEM) systems.