ABSTRACT

TITLE	**:**	**AUTOMATED SNORT CONFIGURATION USING ANSIBLE FOR IDPS (INTRUSION DETECTION AND PREVENTION SYSTEM) IMPLEMENTATION AT PT SEMEN PADANG**
STUDENT NAME	**:**	**MHD. ARIF HIDAYAT**
STUDENT NUMBER	**:**	**21101152630071**
STUDY PROGRAM	**:**	**INFORMATIC ENGINEERING**
DEGREE GRANTED	**:**	**STRATA 1 (S1)**
ADVISERS	**:**	**1. Dr. Ir. Sumijan, M.Sc** **2. Romi Wijaya, S.Kom., M.Kom.**

Network security is a critical aspect in supporting organizational operations, especially in facing increasingly complex cyber threats. This study aims to analyze the effectiveness of implementing an Intrusion Detection and Prevention System (IDPS) using Snort and automating its configuration with Ansible to improve efficiency and accuracy of the network security system at PT Semen Padang. The method involves a network simulation using three virtual nodes: an Ansible control node, a Snort IDPS node, and a Kali Linux attacker node. Automation is conducted through Ansible Playbooks developed to configure Snort settings, rule sets, IPTables, and system daemon services. The system was tested against several simulated attacks, including Ping of Death, SYN Flooding, and Nmap Scanning.The results indicate that Ansible effectively automates Snort configuration consistently and efficiently. Snort successfully detected and blocked most of the attacks while generating alerts based on the detected intrusion type. Thus, the implementation of Snort-based IDPS automated with Ansible significantly improves the overall effectiveness of the network security system.

Keyword : IDPS, Snort, Ansible, Network Security, Automation.

ABSTRAK

JUDUL	**:**	**AUTOMASI KONFIGURASI SNORT MENGGUNAKAN ANSIBLE UNTUK SISTEM IDPS (INTRUSION DETECTION PREVENTION SYSTEM) PADA PT. SEMEN PADANG**
NAMA	**:**	**MHD. ARIF HIDAYAT**
NO. BP	**:**	**21101152630071**
PROGRAM STUDI	**:**	**TEKNIK INFORMATIKA**
PENDIDIKAN	**:**	**STRATA 1 (S1)**
PEMBIMBING	**:**	**1. Dr. Ir. Sumijan, M.Sc** **2. Romi Wijaya, S.Kom., M.Kom.**

Keamanan jaringan merupakan aspek krusial dalam mendukung operasional perusahaan, terutama dalam menghadapi ancaman siber yang semakin kompleks. Penelitian ini bertujuan untuk menganalisis efektivitas penerapan Intrusion Detection and Prevention System (IDPS) menggunakan Snort serta mengotomatisasi konfigurasinya dengan Ansible guna meningkatkan efisiensi dan akurasi sistem keamanan jaringan di PT Semen Padang. Metode yang digunakan meliputi simulasi jaringan menggunakan tiga node virtual, yaitu node Ansible sebagai kontrol, node Snort sebagai IDPS, dan node Kali Linux sebagai penyerang. Automasi dilakukan melalui Ansible Playbook yang dikembangkan untuk mengatur konfigurasi Snort, rules, IPTables, hingga pembuatan daemon service. Pengujian dilakukan dengan mensimulasikan berbagai jenis serangan seperti Ping of Death, Syn Flooding, dan Nmap Scanning. Hasil penelitian menunjukkan bahwa Ansible mampu mengotomatisasi konfigurasi Snort secara efisien dan konsisten. Sementara itu, Snort berhasil mendeteksi dan memblokir sebagian besar serangan, serta menghasilkan alert sesuai jenis ancaman yang terjadi. Dengan demikian, penerapan IDPS berbasis Snort yang dikonfigurasi menggunakan Ansible terbukti meningkatkan efektivitas sistem keamanan jaringan.

Kata Kunci : IDPS, Snort, Ansible, Keamanan Jaringan, Automasi.