ANALISIS IMPLEMENTASI INTRUSION DETECTION SISTEM SNORT DALAM MENDETEKSI SERANGAN BRUTE FORCE SSH

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi *S1 Informatika*

disusun oleh

AHMAD RIZALDI

24.21.1588

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

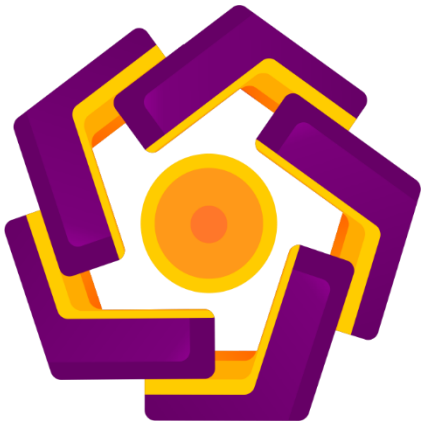
ANALISIS IMPLEMENTASI INTRUSION DETECTION SISTEM SNORT DALAM MENDETEKSI SERANGAN BRUTE FORCE SSH

HALAMAN JUDUL

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi *S1 Informatika*



disusun oleh

AHMAD RIZALDI

24.21.1588

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS IMPLEMENTASI INTRUSION DETECTION SISTEM SNORT DALAM MENDETEKSI SERANGAN BRUTE FORCE SSH

yang disusun dan diajukan oleh

Ahmad Rizaldi

24.21.1588

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 19 Desember 2025

Dosen Pembimbing,

Pramudhita Ferdiansyah, S.Kom., M.Kom.
NIK. 190302409

ii

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS IMPLEMENTASI INTRUSION DETECTION SISTEM SNORT DALAM MENDETEKSI SERANGAN BRUTE FORCE SSH

yang disusun dan diajukan oleh

Ahmad Rizaldi

24.21.1588

Telah dipertahankan di depan Dewan Penguji
pada tanggal 19 Desember 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Ahlihi Masruro, S.Kom., M.Kom. **NIK. 190302148**	
Bambang Pilu Hartato, S.Kom., M.Eng **NIK. 190302707**	
Pramudhita Ferdiansyah, S.Kom., M.Kom. **NIK. 190302409**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 19 Desember 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ahmad Rizaldi
NIM : 24.21.1588

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS IMPLEMENTASI INTRUSION DETECTION SISTEM SNORT DALAM MENDETEKSI SERANGAN BRUTE FORCE SSH

Dosen Pembimbing : Pramudhita Ferdiansyah, M.Kom

Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.

1. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
2. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
3. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
4. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 19 Desember 2025

Yang Menyatakan,

Ahmad Rizaldi

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga Skripsi yang berjudul "Analisis Implementasi Intrusion Detection Sistem Snort Dalam Mendeteksi Serangan *Brute Force SSH*" dapat di selesaikan tepat waktu. Dalam penyelesaian skripsi ini, Penulis banyak mendapat motivasi dan bantuan berupa masukan-masukan yang sangat membantu dalam penyelesaian skripsi ini, oleh karena itu penulis mengucapkan banyak terima kasih atas segala dukunganya. Ucapan terima kasih yang terhingga juga penulis sampaikan kepada :

1. Bapak Prof. Dr. M. Suyanto, M.M Selaku Rektor Universitas AMIKOM yang telah memberikan kesempatan kepada penulis untuk menempuh dan menyelesaikan pendidikan di Universitas ini.

2. Bapak Pramudhita Ferdiansyah, M.Kom selaku Dosen Pembimbing yang telah berkenan dan meluangkan waktu memberikan bimbingan kepada penulis sampai dengan selesainya penyusunan skripsi ini.

3. Kedua orang tua penulis yang telah melahirkan, membesarkan, membimbing dan memberi dukungan, kesempatan serta membiayai penulis sampai dengan selesai dalam menempuh pendidikan di Universitas ini

4. Ucapan terima kasih juga penulis sampaikan kepada rekan-rekan seangkatan yang telah memberikan masukan dan saran dalam penyelesaian skripsi ini.

Yogyakarta, 15 Desember 2025

Ahmad Rizaldi

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Keamanan jaringan komputer merupakan hal yang sangat penting diperhatikan mengingat di era digital sekarang tekno*log*i makin berkembang dan ancaman pun makin banyak, serangan *cyber* yang sering terjadi sangat merugikan bagi pihak-pihak instansi bahkan masyarakat pun ikut terkena dampaknya. Salah satu ancaman yang sering terjadi adalah serangan *Brute Force* pada layanan *Secure Shell* (*SSH*). Penelitian ini bertujuan untuk menganalisis Implementasi *Intrusion Detection System* (IDS) berbasis Snort dalam mendeteksi serangan *Brute Force* pada protokol *SSH*. Metode penelitian yang digunakan adalah pendekatan eksperimental dengan melakukan konfigurasi pada Snort yang terinstal pada sistem operasi Ubuntu sebagai pendeteksi serangan intrusi. Serangan *Brute Force SSH* dilakukan menggunakan Hydra. Data hasil serangan dianalisis berdasarkan *log* yang dihasilkan oleh Snort. Hasil penelitian menunjukkan bahwa Snort mampu mendeteksi seluruh skenario serangan *Brute Force* yang di lakukan secara konsisten. Berdasarkan enam kali percobaan serangan, Snort berhasil menghasilkan *alert* sesuai dengan *custom rules* yang dibuat, dengan waktu deteksi berada pada rentang 1 hingga 3 detik. Variasi waktu deteksi dipengaruhi oleh kompleksitas password yang digunakan, di mana password dengan tingkat kompleksitas lebih tinggi menyebabkan *threshold rules* Snort terpenuhi dalam waktu yang lebih lama. Berdasarkan hasil tersebut, dapat disimpulkan bahwa sistem *Intrusion Detection System* berbasis Snort memiliki efektivitas yang baik dalam mendeteksi serangan *Brute Force* pada protokol *SSH* secara cepat, konsisten, dan andal, sehingga dapat digunakan sebagai salah satu solusi dalam meningkatkan keamanan jaringan.

Kata kunci: Keamanan jaringan, *Intrusion Detection System*, Snort, *SSH*, *Brute Force Attack*.

ABSTRACT

Computer network security is a very important thing to pay attention to considering that in today's digital era, technology is increasingly developing and threats are increasing. Frequent cyber attacks are very detrimental to agencies and even the public are affected. One of the frequent threats is Brute Force attacks on Secure Shell (SSH) services. This study aims to analyze the implementation of a Snort-based Intrusion Detection System (IDS) in detecting Brute Force attacks on the SSH protocol. The research method used is an experimental approach by configuring Snort installed on the Ubuntu operating system as an intrusion attack detector. SSH Brute Force attacks were carried out using Hydra. Attack data were analyzed based on logs generated by Snort. The results showed that Snort was able to detect all Brute Force attack scenarios that were carried out consistently. Based on six attack attempts, Snort successfully generated alerts according to the custom rules created, with detection times ranging from 1 to 3 seconds. Variations in detection time were influenced by the complexity of the password used, where passwords with a higher level of complexity caused the Snort threshold rules to be met in a longer time. Based on these results, it can be concluded that the Snort-based Intrusion Detection System is highly effective in detecting brute force attacks on the SSH protocol quickly, consistently, and reliably, making it a viable solution for improving network security.

Keywords : Network security, Intrusion Detection System, Snort, SSH, Brute Force Attack.