BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi terutama pada bidang *intranet* dan *internet* semakin berkembang pesat, pertukaran data tidak lagi menjadi sebuah permasalahan, melainkan keamanannya yang menjadi faktor penting sebagai bentuk upaya perlindungan aset data/informasi yang ada di dalam jaringan. Ada begitu banyak jenis serangan yang kerap terjadi di internet, salah satunya adalah *Denial of Service* atau disingkat menjadi *DoS*. *DoS* merupakan serangan yang ditujukan untuk mematikan paksa suatu mesin ataupun sistem dan membuatnya tidak dapat diakses oleh penggunanya membanjiri lalu lintas data atau mengirim informasi yang dapat memicu kegagalan dalam sistem atau jaringan [1].

Menurut hasil laporan dari *Kaspersky Lab* pada kuartal ke-tiga tahun 2021, jenis serangan *DoS* yang sering terjadi adalah serangan *SYN* Flood, metode ini digunakan dalam 51,63% serangan. Diikuti oleh *UDP Flood* sebesar 38%, *TCP Flood* berada di urutan ketiga yaitu 8,33%, *HTTP Attack* 1,02%, dan *GRE* di posisi terakhir yaitu 1,01% [2]. *SYN Flood* itu sendiri merupakan variasi serangan *DoS* yang memanfaatkan mekanisme *three-way-handshake* pada protokol *TCP* [3]. Serangan *DoS* jenis ini cukup berbahaya apabila tidak terdeteksi dengan cepat karena dapat meruntuhkan akses layanan ke sistem, namun ada beberapa cara yang dapat dilakukan untuk mengetahui serangan *TCP SYN Flood* tersebut yaitu dengan menggunakan perangkat lunak yang berfungsi untuk menganalisa lalu lintas pada jaringan secara manual, atau dengan menggunakan *Intrusion Detection System (IDS)*.

IDS merupakan perangkat keras atau lunak yang digunakan untuk memantau aktivitas sistem atau jaringan, *IDS* diprogram untuk me-*monitoring* dan mendeteksi adanya aktivitas mencurigakan pada suatu sistem atau jaringan secara berkala [4]. Ada banyak program *IDS* yang telah dikembangkan hingga kini, *Suricata* adalah salah satu contoh *IDS* yang bersifat *open source* dan dikembangkan oleh *Open*

Information Security Foundation (OISF) [5]. Namun karena pertumbuhan sistem jaringan yang sangat kompleks, praktisi keamanan kemudian mengembangkan suatu platform yang disebut sebagai *Network Security Monitoring* (NSM) untuk mengatur segala kebutuhan *monitoring* keamanan jaringan dalam satu sistem. *NSM* sendiri terdiri dari berbagai program komponen, salah satunya *IDS* [6].

Karena *Suricata* dikembangkan secara *open-source*, hal ini membuat beberapa pihak menggunakan *Suricata* sebagai *IDS* untuk platform *NSM* yang mereka kembangkan, seperti *SELKS* oleh *Stamus Networks* dan *Security Onion* oleh *Security Onion Solution*. Akan tetapi sebuah platform *NSM* tersebut tentu memiliki kelebihan dan kekurangan dalam mengimplementasikan *IDS* di sistemnya, dengan adanya kelebihan dan kekurangannya tersebut, peneliti akan melakukan penelitian yang berjudul ***"Analisis Perbandingan Performa Intrusion Detection System Suricata pada SELKS dan Security Onion Terhadap Serangan SYN Flood"***. Pada penelitian ini, *IDS Suricata* pada *NSM SELKS* dan *Security Onion* akan digunakan untuk mendeteksi serangan *TCP SYN Flood* serta mengukur akurasi deteksi dan penggunaan sumber daya sistem untuk membandingkan performa *IDS Suricata* di kedua platform tersebut.

1.2 Rumusan masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas, diperoleh rumusan masalah yaitu:

1. Bagaimana performa IDS Suricata pada SELKS dan Security Onion dalam mendeteksi DoS SYN Flood?
2. Bagaimana tingkat akurasi deteksi IDS Suricata pada SELKS dan Security Onion terhadap serangan SYN Flood?
3. Bagaimana penggunaan sumber daya sistem IDS Suricata pada SELKS dan Security Onion ketika terjadi serangan SYN Flood?

1.3 Tujuan Penelitian

Tujuan yang ingin diraih penulis berdasarkan rumusan masalah yang diuraikan di atas adalah untuk mengetahui analisis perbandingan performa *intrusion detection system Suricata* pada *SELKS* dan *Security Onion* terhadap serangan *SYN Flood* untuk mempermudah administrator jaringan memilih platform sistem keamanan jaringan yang sesuai dengan kebutuhannya.

1.4 Batasan Masalah

Untuk mempersempit pembahasan pada skripsi ini, maka dibuat batasan-batasan sebagai berikut:

1. Pengujian dilakukan dengan menggunakan sistem operasi Windows 10 Pro 64bit dan sistem operasi Kali Linux 2022.1.
2. *SELKS* dan *Security Onion* diimplementasi berupa mesin virtual menggunakan VirtualBox versi 7.0.4 dengan spesifikasi komputer berikut:
   - Intel Core i3-10100F
   - RAM 2x8GB 2666Mhz
   - GPU Nvidia GTX 1050Ti 4GB
   - HDD Seagate 500GB
3. Menggunakan *custom rule Suricata* dari penulis.
4. Parameter pengujian yang diukur yaitu akurasi deteksi dan sumber daya penggunaan sistem dari CPU dan Memori.

1.5 Manfaat Penelitian

Pada penelitian ini diharapkan dapat memberikan manfaat sebagai berikut :

1. Dapat memahami cara kerja *IDS Suricata* pada *SELKS* dan *Security Onion*.
2. Mengetahui platform mana yang menjalankan *IDS Suricata* lebih optimal.
3. Dapat menjadi bahan evaluasi dan pertimbangan untuk menentukan pemilihan *NSM* berbasis *IDS Suricata* dalam implementasi keamanan jaringan.