BAB I
PENDAHULUAN

1.1 Latar belakang

Sistem keamanan komputer, dalam beberapa tahun ini telah menjadi focus utama dalam dunia Jaringan Komputer, hal ini disebabkan tingginya ancaman yang mencurigakan (*Suspicous Threat*) dan serangan dari internet.

Intrusion Detection System (IDS) merupakan sebuah aplikasi perangkat lunak atau perangkat keras yang mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan) apakah termasuk kategori ancaman atau tidak. Jika ternyata ancaman, maka IDS akan memberikan peringatan untuk memberitahu administrator bahwa terdapat ancaman terhadap jaringan. Jika tidak, IDS akan menganggap sebagai packet normal atau bukan ancaman.

IDS umumnya sebuah aplikasi yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan *isnpeksi* terhadap lalu lintas komunikasi data dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan penyusupan (termasuk kategori atau tidak) jika sudah termasuk dalam kategori penyusupan maka IDS akan melakukan alert terhadap proses penyusupan tersebut kemudian admin yang akan menindak lanjuti dari penyusupan tersebut.

Raspberry PI adalah ARM multi guna dan murah perangkat miniatur berbasis prosesor yang dapat digunakan untuk deteksi intrusi di lingkungan jaringan komputer seperti : SOHO (Small Office Home), Lembaga Pendidikan atau di Negara Berkembang. Makalah ini menguraikan hasil dari Perancangan dan Implementasi IDS Snort, Suricata, dan Fail2ban pada Raspberry PI.

Dengan menerapkan IDS dapat mengamankan jaringan dari penyusup tanpa perlu rasa khawatir dan apabila terjadi proses penyusupan maka IDS akan mendeteksinya setelah itu melaporkan kepada administrator jaringan yang nantinya akan diproses lebih lanjut oleh administrator jaringan.

Dari hal tersebut penulis akan merancang system Intrussion Detection System Suricata, Snort, Fail2ban dengan menggunakan Raspberry PI.

1.2 Perumusan Masalah

Masalah yang diangkat dalam Tugas Akhir ini adalah :

1. Bagaimana melakukan rancang bangun IDS Suricata, Snort, Fail2ban pada Raspberry PI?
2. Bagaimana efektivitas dari IDS Suircata, Snort, dan Fail2ban sebagai pendeteksi intrussion pada Raspberry PI ?

1.3 Tujuan dan Manfaat Penelitian

Penyusunan Tugas Akhir ini memiliki tujuan dan manfaat untuk :

1. Memasang dan mengkonfigurasi sistem IDS Suricata, Snort, dan Fail2ban pada Raspberry Pi.
2. Mengetahui kinerja dari masing-masing sistem IDS Suricata, Snort, dan Fail2ban.
3. Memberikan referensi bagi siapapun yang ingin membuat karya tulis ilmiah PERANCANGAN DAN IMPLEMENTASI IDS SURICATA, SNORT, DAN FAIL2BAN PADA RASPBERRY PI.

1.4 Batasan Masalah

Batasan masalah pada Tugas Akhir ini adalah :

1. Perancangan sistem hanya menggunakan single board computer berupa Raspberry PI.

2. Implementasi dilakukan hanya menggunakan jaringan LAN dan Wifi.
3. Proses pengujian serangan/intrusi menggunakan software Ubuntu 20.04.
4. Proses pengujian serangan/intrusi hanya menggunakan 1 server.
5. Proses pengujian dilakukan dengan rules/konfigurasi original dari IDS tersebut.
6. Proses pengujian menggunakan serangan Nmap, BruteForce, dan DDoS.
7. Poses pengujian menggunakan Suricata Versi : 6.0.6, Snort Versi : 2.9.7.0, Fail2ban Versi : 0.11.1-1

1.5 Sistematika Penulisan

Semua kegiatan yang mengandung dengan Sistematika Penulisan sebagai berikut :

BAB I : PENDAHULUAN

Bab ini berisi latar belakang dari penulisan proposal tugas akhir, perumusan masalah, tujuan dan manfaat penulisan, batasan masalah, dan sistematika dari penulisan proposal tugas akhir ini.

BAB II : LANDASAN TEORI

Bab ini berisi mengenai pembahasan teori tentang Implementasi *Intrussion Detection System (IDS)* dengan menggunakan Raspberry Pi.

BAB III : METODE PENELITIAN

Bab ini berisi tahapan yang dilakukan dalam Implementasi Intrusion Detection System (IDS) dengan menggunakan Raspberry Pi. Mulai dari persiapan hardware dan software, mengestimasi waktu pengerjaan.

BAB IV : PERANCANGAN

Bab ini membahas proses perancangan yang akan dilakukan terkait penelitian sesuai dengan alur / tahapan penelitian yang sudah ditentukan pada bab III.

BAB V : PENGUJIAN DAN HASIL

Bab ini membahas hasil dari perancangan dari penelitian yang telah dilakukan oleh penulis.

BAB VI : PENUTUP

Bab ini adalah penutup berupa saran dari penelitian.