BAB I
PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer merupakan sistem yang terdiri dari *hardware*, *software* dan perangkat jaringan yang mempunyai tujuan sebagai media komunikasi dengan bertukar data dan informasi. Banyaknya kalangan atas dan bawah yang menggunakan jaringan komputer untuk fasilitas pribadi maupun instasi perusahaan. Pemanfaatan jaringan komputer sebagai media komunikasi dapat menggunakan *Internet of Things* (IoT). *Internet of Things* dapat membantu untuk kegiatan aktivitas manusia, karena IoT sangat berpengaruh dalam tingkatan teknologi sekarang ini. Hal ini IoT merupakan suatu konsep yang memiliki kemampuan untuk berkomunikasi menggunakan jaringan tanpa harus adanya interaksi dari manusia atau ke perangkat komputer. Salah satu perangkat yang dapat digunakan untuk penerapan IoT adalah mini komputer Raspberry Pi 4.

Penggunaan mini komputer Raspberry Pi 4 sangatlah membantu dalam melakukan pekerjaan karena perangkat ini biasa digunakan sebagai pusat akses dan penghubung. Raspberry Pi 4 dengan keluaran *series* terbaru mempunyai kecepatan dan peningkatan dari model sebelumnya seperti desktop yang lebih lengkap, hemat energi dan hemat biaya mesin. Raspberry Pi 4 dapat dijadikan sebagai desktop komputer, otak robot, rumah pintar ataupun web server dengan perkembangan sekarang ini. Raspberry Pi 4 membutuhkan tingkat keamanan jaringan dalam mengatasi adanya serangan. Serangan yang masuk ke Raspberry Pi 4 dapat membuat performa CPU mengalami peningkatan sehingga tidak dapat bekerja maksimal. Penelitian dengan *software* SNORT dan BRO IDS pada Raspberry Pi sebagai IDS untuk menganalisa performa Raspberry Pi, saat pengujian dengan intensitas serangan yang tinggi mengalami kendala pada BRO IDS sehingga terjadinya *crash* terhadap Raspberry Pi dan hasil pada CPU *load* maupun *Memory Utilization* rata-rata diatas 50%, SNORT hanya membutuhkan sedikit *resource* daripada BRO IDS [Yohanes Priyo A, 2018]. Salah satu cara untuk mengamankan serangan yang masuk ke Raspberry Pi 4 yaitu dengan melakukan penerapan

Intrusion Prevention System pada Raspberry Pi 4.

Intrusion Prevention System (IPS) adalah suatu metode untuk mengantisipasi tindakan serangan yang memanfaatkan sistem pada *firewall*, sistem ini mempuyai kelebihan dalam mendeteksi dan melakukan pencegahan ketika terjadi serangan. Penggunaan IPS dapat diimplementasikan menggunakan *software* Suricata yang merupakan perangkat lunak *open source*. Suricata banyak digunakan berbagai kalangan *non-profit*, Suricata berupa IDS, IPS dan mesin *monitoring engine* keamanan jaringan dengan kinerja tinggi. Suricata sebagai mesin yang dapat mendeteksi dan memblock serangan pada jaringan.

Tujuan dari penelitian ini untuk mengimplementasikan *Intrusion Prevention System* menggunakan Suricata pada Raspberry Pi 4 sebagai salah satu alternatif dalam keamanan jaringan komputer. Berdasarkan permasalahan diatas Penulis melakukan penelitian dengan judul **"IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* SURICATA PADA RASPBERRY PI 4"**.

1.2 Rumusan Masalah

Berdasarkan dari latar belakang yang telah di jelaskan, Penulis mengutip rumusan masalah sebagai berikut:

1. Bagaimana implementasi dan pengujian Suricata sebagai *Intrusion Prevention System* dalam keamanan jaringan komputer pada Raspberry Pi 4?
2. Bagaimana hasil pengukuran *performance* Raspberry Pi 4 ketika dijadikan sebagai *Intrusion Prevention System*?

1.3 Batasan Masalah

Agar tugas akhir dapat fokus pada topik pembahasan maka dibuat pembatasan masalah sebagai berikut:

1. Sistem yang dibangun menggunakan sistem operasi Ubuntu yang hanya dijalankan untuk melakukan keamanan jaringan komputer.
2. *Software* menggunakan Kali Linux dan untuk melakukan serangan

menggunakan beberapa *tools* yaitu Zenmap, Nikto, WPScan, Red Hawk, WPHunter dan WAScan.

3. *Software* yang digunakan untuk mendeteksi dan memblock serangan yaitu Suricata.
4. Penulis hanya mengimplementasikan *Intrusion Prevention System* pada Raspberry Pi 4.
5. Sistem yang dibangun *Host-Based Intrusion Prevention System* dan tidak menggunakan *Network-Based Intrusion Prevention System*.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Membangun *Host-Based Intrusion Prevention System* pada Raspberry Pi 4 untuk keamanan jaringan komputer.
2. Mengukur *performance* Raspberry Pi 4 ketika dijadikan sebagai *Intrusion Prevention System*.

1.5 Manfaat Penelitan

Adapun manfaat yang diperoleh dari penelitian ini diharapkan:

Manfaat dari penelitian ini dapat membangun *Host-Based Intrusion Prevention System* menggunakan Raspberry Pi 4 sebagai alternatif sistem keamanan jaringan komputer.

1.6 Sistematika Penulisan

Untuk memudahkan dalam penulisan dan pembahasan, sistematika penulisan. Berikut dibawah ini merupakan susunan dari tugas akhir:

BAB I: PENDAHULUAN

Meliputi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian dan sistematika penulisan.

BAB II: TINJAUAN PUSTAKA DAN DASAR TEORI

Meliputi landasan teori pendukung sebagai acuan penulisan dari berbagai sumber yang telah diterbitkan.

BAB III: METODOLOGI PENELITIAN

Meliputi skematik perencanaan penelitian, tahapan jalannya penelitian, studi literatur, indentifikasi dan perumusan masalah, analisa kebutuhan Suricata pada Raspberry Pi 4, alat dan bahan penelitian, perancangan Suricata, install Suricata dan Iptables, konfigurasi Suricata, implementasi dan tahapan pengujian sistem Suricata, pengukuran *performance* Raspberry Pi 4 dan laporan penelitian.

BAB IV: ANALISIS DAN PEMBAHASAN

Meliputi tentang hasil pengujian yang diperoleh dari pembahasan penelitian terhadap masalah-masalah yang dialami selama penelitian dan implementasikan hasil pengujian sistem.

BAB V: PENUTUP

Meliputi tentang keseluruhan mengenai kesimpulan dan saran penyusun berdasarkan hasil pembahasan.

DAFTAR PUSTAKA

Memuat daftar sumber literatur dan teori pendukung sebagai referensi untuk pembahasan.

LAMPIRAN

Memuat hasil lampiran-lampiran atau data yang diperoleh dari penelitian.