BAB I

PENDAHULUAN

1.1 Latar Belakang

Diera teknologi jaringan komputer saat ini peningkatan baik dari skalabilitas, keperluan *node* dan teknologi yang digunakan, sangat dibutuhkan pengelolaan jaringan yang baik. Admin jaringan yang bertindak sebagai pengelola jaringan diharuskan memahami pemahaman dasar keamanan. Tujuan utama dari keamanan sistem adalah memberikan jalur komunikasi informasi yang aman antar entitas serta untuk perlindungan data dari pengguna anonim.

Intrusion (Gangguan) merupakan kegiatan yang berusaha menyalahgunakan sistem seperti aktivitas memata-matai, pencurian data hingga merusak sistem. Kesadaran akan pentingnya ancaman dunia siber khususnya keamanan jaringan yang berkaitan dengan komputer server, diperlukan pengamanan khusus terhadap server agar terhindar dari gangguan pihak yang tidak berkepentingan. Suricata dipilih dari banyaknya tool IDS dan IPS dikarenakan *open source*, *free*, dan handal dalam menangani kasus keamanan komputer dan jaringan, sebagai mesin perangkat lunak suricata mampu menangani berbagai macam ancaman terhadap komputer server seperti aktivitas *Scanning*, *DoS*, dan yang paling berbahaya adalah aktivitas eksploitasi komputer server. Suricata akan melakukan pendeteksian dini terhadap segala kemungkinan yang mencurigakan dan juga melakukan tindakan pencegahan apabila hal tersebut dianggap diperlukan.

Oleh karena itu pada skripsi kali ini akan di implementasikan dengan judul Sistem Monitoring dan Pencegahan Dengan Rules Penanganan Spesifik Serangan *Scanning, DoS, Exploit* Pada Komputer Server Menggunakan Suricata.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka dirumuskan masalah yang akan dibahas, antara lain :

1. Bagaimana cara mengimplementasikan suricata ke dalam sebuah jaringan?
2. Bagaimana cara suricata dalam melindungi server dari serangan?
3. Bagaimana cara suricata berinteraksi dengan admin jaringan ketika serangan berupa *Port scaning, DoS,* dan *Exploit -Meterpreter* sedang berlangsung?

1.3 Ruang Lingkup

Agar mencapai sasaran dan tujuan yang diharapkan maka diberikan batasan masalah sebagai berikut :

1. Sistem Suricata yang akan dirancang berbasis linux ubuntu server.
2. Proses pengujian menggunakan *software Intrusion Prevention System* berbasis *open source.*
3. Menggunakan 2 tipe IPS: *Host-based* dan *Network-based.*
4. Menggunakan *IP-Address* versi 4 dalam pengimplementasiannya.

5. Proses pengujian terbatas pada rules emerging tertentu yang diaktifkan.

6. Serangan yang akan diimplementasikan berupa *Scanning*, *DoS* dan *Exploit.*

7. Implementasi dilakukan menggunakan satu buah laptop yang terhubung pada jaringan. IDPS Host dan *Attacker* akan beroperasi dalam *virtual machine* secara bersamaan.

8. Parameter yang digunakan untuk pengujian dalam kegiatan ini adalah serangan yang berhasil terdeteksi, dan tindakan pencegahan yang dilakukan sistem.

9. Tidak membahas fungsional web server.

1.4 Tujuan Penelitian

Tujuan dari analisis ini adalah :

1. Melakukan implementasi suricata pada komputer server.
2. Sebagai refrensi penggunaan Suricata sebagai *Intrusion Detection Prevention System.*
3. Membangun sistem keamanan berbasis pencegahan intrusi/gangguan.

1.5 Manfaat Penelitian

Manfaat dalam penelitian ini adalah memberikan pengetahuan kepada seorang administrator jaringan akan pentingnya keamanan data informasi secara minimal dengan menggunakan sistem IDPS yang telah dibangun menggunakan Suricata.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penyusunan skripsi ini adalah sebagai berikut :

Pada bagian awal adalah halaman judul skripsi meliputi informasi skripsi seperti judul, nama dan NIM mahasiswa, logo institusi, nama institusi, jurusan, program studi dan tahun. Halaman persetujuan unutk pengesahan skripsi oleh ketua jurusan dan dosen pembimbing.

Intisari adalah suatu sinopsis yang menggambarkan isi keseluruhan skripsi yang mencakup masalah utama yang diteliti dan ruang lingkupnya, metode yang digunakan, hasil yang diperoleh dan kesimpulan utama.

Kata pengantar berisi pernyataan penghargaan penulis kepada pihak-pihak yang berjasa dalam penyelesaian penulisan skripsi. Daftar isi berisi urutan halaman penulisan mulai dari halaman judul sampai daftar pustaka. Kemudian daftar gambar dan daftar tabel yang ada dalam skripsi.

Bab 1. Pendahuluan berisi latar belakang, rumusan masalah, ruang lingkup, tujuan, manfaat penelitian dan sistematika penulisan.

Bab 2. Tinjauan Pustaka dan Dasar Teori berisi teori dasar yang mendukung penulisan skripsi, mencakup metode atau teknik yang digunakan, teori tentang permasalahan, uraian singkat perangkat implementasi yang dipakai, dan kerangka penyelesaian masalah.

Bab 3. Metode Penelitian berisi penjelasan tentang definisi kebutuhan dari permasalahan yang dijadikan topik skripsi berikut pemodelannya. Analisis sistem, perancangan sistem dan perancangan antarmuka.

Bab 4. Implementasi dan Pembahasan berisi penjelasan tentang pelaksanaan implementasi berdasarkan pada hasil perancangan. Dan pengujian program aplikasi atau kinerja sistem.

Bab 5. Kesimpulan dan Saran berisi kesimpulan(hasil yang didapat sesuai ruang lingkup batasan masalah) dan saran (terhadap masalah yang belum terselesaikan sebagai pengembang dan perbaikan-perbaikan) tentang kasus skripsi.

Bagian akhir Daftar Pustaka berisi urutan informasi sumber daya seperti buku, situs internet sebagai acuan dan referensi dalam skripsi.