BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Jaringan komputer saat ini mengalami perkembangan yang sangat pesat, terlepas dari kemajuan teknologi informasi yang memberikan kemudahan pengguna dalam mendapatkan Informasi selalu tersedia saat dibutuhkan melalui jaringan internet. Dibalik kemudahan pengaksesan informasi yang disediakan oleh internet terdapat bahaya besar yang mengintai, yaitu berbagai macam serangan yang berusaha mencari celah dari sistem keamanan jaringan komputer yang digunakan. Serangan-serangan itu dapat mengakibatkan kerusakan data dan bahkan kerusakan pada *hardware* [1].

Berdasarkan data yang dihimpun Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN), mencatat 88.414.296 serangan siber telah terjadi sejak 1 Januari hingga 12 April 2020. Pada bulan Januari terpantau 25.224.811 serangan dan kemudian pada bulan Februari terekam 29.188.645 serangan lalu kemudian pada bulan Maret terjadi 26.423.989 serangan dan sampai dengan 12 April 2020 telah tercatat 7.576.851 serangan [2].

Serangan DoS memanfaatkan kelemahan sistem pada keterbatasan sumber daya, baik *Bandwidth*, kemampuan menyimpan memori, *server* dan kelemahan lainnya. Kebanyakan DoS menyerang bisnis kecil hingga menengah yang tidak memiliki sumber daya yang besar seperti penjual yang memulai untuk berjualan online dengan membuat *website*. Dalam serangan DoS penyerang menggunakan satu komputer dan satu koneksi internet saja ketika meluncurkan serangan. Pada dasarnya tujuan penyerang hanya untuk membuat sistem lumpuh, tapi tidak jarang juga ada yang kemudian meminta biaya tebusan untuk menghentikan serangan [3].

Dalam penanggulangannya ada 2 jenis penanggulangan intrusi yang bisa digunakan oleh seorang Sistem Administrator, yaitu *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS). Aplikasi yang digunakan untuk melakukan pengawasan terhadap paket dalam jaringan (*signature based*), memonitoring keadaan trafik pada jaringan (*anomaly based*), dan pendeteksi dan pemberi peringatan (*passive IDS*). Padahal hasil monitoring IDS ini sangat penting sekali bagi Sistem Administrator dalam mengambil keputusan untuk meningkatkan langkah keamanan jaringan [4].

IDS (*Intrusion Detection System*) merupakan sebuah sistem yang dapat melakukan fungsi pendeteksian aktivitas yang *abnormal* terhadap suatu layanan *server*. IDS merupakan *service* tambahan pada *Firewall* sistem jaringan yang dapat mendeteksi aktivitas yang tidak biasa sekaligus memberikan respon berupa pencatatan dan notifikasi peringatan terhadap sisem atau administrator jaringan [5].

Dari penjabaran latar belakang tersebut di atas, peneliti mengajukan penelitian yang berjudul "**Analisis Dan Implementasi Sistem Keamanan Jaringan Dengan Metode *Signature-based* Menggunakan Suricata Pada Mikrotik RB951G-2HND**".

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, akan timbul berbagai macam permasalahan, diantara lain :

1. Bagaimana cara mengimplementasikan *suricata* sebagai *tools Intrusion Detection System* dalam mendeteksi serangan pada *server website* usaha online.
2. Bagaimana menganalisis kehandalan *suricata* sebagai perangkat IDS dan menguji seberapa besar pengaruh penggunaan *suricata* dan metode *signature-based* untuk mendeteksi adanya serangan dan ancaman dalam jaringan komputer.

1.3 Batasan Masalah

Beberapa batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut.

1. Penelitian dilakukan pada jaringan komputer.
2. Memasang dan mengkonfigurasi *suricata* sebagai *tools Intrusion Detection System* dan *tools* lainnya pada komputer *server*.
3. Melakukan pengujian terhadap jaringan komputer.
4. Melakukan analisis terhadap kehandalan *suricata* pada komputer.
5. Menggunakan *IP-Address* versi 4 dalam pengimplementasiannya.
6. Serangan yang akan digunakan dalam pengujian ditentukan dan terbatas.

1.4 Maksud Penelitian

Maksud dari penelitian ini adalah menganalisis dan mengimplementasikan sistem keamanan jaringan dengan *Intrusion Detection*

System (IDS) berbasis *signature-based* yang memeriksa setiap lalu lintas jaringan terhadap pola serangan yang telah dikonfigurasikan dan ditentukan sebelumnya.

1.5 Tujuan Penelitian

Tujuan yang akan dicapai dalam penelitian ini adalah:

1. Untuk mendeteksi serangan seperti *Port Scanning, Denial of Service* (*DoS*).
2. Untuk mengetahui sebuah sistem *Intrusion detection system* (IDS) *suricata* dapat mendeteksi adanya serangan dan penyalahgunaan jaringan.
3. Untuk mengetahui penganalisaan *log* yang dihasilkan sebagai peringatan kepada *administrator*.
4. Untuk mengetahui *signature-based* dapat mengurangi ancaman yang muncul secara bersamaan menggunakan *suricata*.

1.6 Manfaat Penelitian

Hasil penelitian ini diharapkan bermanfaat untuk dapat memahami penggunaan IDS dengan *suricata* dalam mendeteksi sebuah ancaman pada jaringan komputer. Manfaat lain penelitian ini juga sebagai pendeteksian awal saat mengetahui jalur mana saja yang digunakan penyusup agar nantinya dapat dilakukan pemblokiran sehingga tidak dimanfaatkan kembali. Penelitian ini dapat diterapkan pada jaringan dengan skala sedang.

1.7 Metode Penelitian

Pada pembuatan skripsi ini, penulis menggambarkan beberapa metode penelitian. Adapun metode-metode penelitian yang digunakan adalah sebagai berikut :

1.7.1 Studi Literatur

Mengumpulkan dan mempelajari data, informasi dan teori-teori mengenai *IDS, Suricata* dan *Signature-based* yang bersumber pada berbagai jurnal, publikasi, artikel, *e-book,* dan *video* literature yang diperoleh dari perpustakaan maupun internet.

1.7.2 Metode Analisis

Metode analisis yang digunakan dalam penelitian ini adalah metode pengembangan sistem model *Security Policy Development Life Cycle* (SPDLC) [6]. Metode ini dipilih karena metode *security policy development life cycle* sejalan dengan penelitian ini yang fokus membahas mengenai keamanan jaringan. Analisis pada aspek lainnya juga dilakukan seperti analisis fungsional dan non-fungsional, analisis kebutuhan sistem (spesifikasi sistem) yang diperlukan dalam menunjang proses penelitian ini. Adapun tahapan dalam metode Analisis SPDLC adalah sebagai berikut.

1. Identifikasi : Pada tahap ini penulis melakukan identifikasi masalah yang dijadikan dasar dalam pencarian jurnal, publikasi ilmiah, buku-buku penunjang penelitian serta media *online open document* dari vendor pembuatan sistem IDS yang digunakan dalam penelitian.
2. Analisis : Penulis melakukan analisis pada masalah yang telah dibuat dan menentukan apa saja yang dibutuhkan pada masalah seperti menentukan *software* dan *hardware* yang sesuai dan berkaitan dengan masalah.
3. Desain : Penulis membuat suatu gambar rancangan

topologi sistem keamanan yang akan dibangun, dan menjelaskan skenario sistem jaringan yang akan dipakai.

4. Implementasi : Setelah semua skenario telah dirancang dan diatur, berikutnya dilakukan implementasi dengan menginstall dan mengkonfigurasi semua aplikasi yang akan digunakan dan siap untuk diuji cobakan.
5. Audit : Pada tahap ini sistem yang telah diimplementasikan akan melakukan proses pemeriksaan dan pengujian secara sistematis untuk memastikan bahwa sistem keamanan yang diterapkan sudah sesuai dengan tujuan awal.
6. Evaluasi : Tahap ini akan memberikan penilaian secara menyeluruh terhadap sistem baru yang diterapkan.

1.8 Sistematika Penulisan

Secara umum sistematika penulisan yang digunakan dalam skripsi ini memuat uraian-uraian dalam setiap bab, yaitu :

BAB I **PENDAHULUAN**

Bab ini berisi tentang latar belakang permasalahan, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, metode penelitian dan sistematika penulisan. Bab ini merupakan bagian pengantar dari penelitian yang akan dibahas pada skripsi ini.

BAB II **LANDASAN TEORI**

Bab ini berisikan tinjauan pustaka dan teori-teori pendukung yang berkaitan dengan skripsi untuk

menunjang dalam proses penelitian ini. Teori yang akan diangkat yaitu mengenai performa *suricata* pada mikrotik dalam mendeteksi serangan *DoS* dan *Port Scanning* terhadap *server*.

BAB III **ANALISIS DAN PERANCANGAN**

Bab ini menjelaskan mengenai analisa kebutuhan sistem, metode yang digunakan, perancangan topologi, perancangan perangkat lunak dan proses instalasi dan konfigurasi semua aplikasi baik itu pada pc *intruder* maupun pc *server*.

BAB IV **HASIL DAN PEMBAHASAN**

Bab ini akan menjelaskan mengenai proses pengujian dengan skenario yang telah dibuat. Lalu dilakukan analisis hasil pengujian yang akan menjadi acuan untuk menentukan perfoma *IDS Suricata* pada mikrotik dalam mendeteksi serangan *DoS dan Port Scanning* terhadap *server*.

BAB V **PENUTUP**

Bab ini berisi kesimpulan yang didapat dari penelitian yang dibuat dan saran kepada pembaca guna pengembangan lebih lanjut.

DAFTAR PUSTAKA Pada bagian ini akan dipaparkan tentang sumber-sumber dan literatur yang digunakan dalam pembuatan laporan tugas akhir.