

BAB I

PENDAHULUAN

1.1 Latar Belakang

Asrama Mahasiswa Bogani Yogyakarta sudah menggunakan layanan internet fiber optik untuk menunjang kegiatan belajar para mahasiswa dan sebagai sarana untuk mengakses berbagai informasi bagi para mahasiswa. Namun layanan jaringan internet yang mencakup area asrama bogani belum sepenuhnya aman, sehingga masih memiliki berbagai masalah yang menjadi gangguan pada sistem jaringan diantaranya yaitu pada sistem keamanan jaringannya yang masih lemah yang bisa berdampak pada masuknya spam-spam yang dapat merusak sistem jaringan itu sendiri, serta belum memiliki sistem deteksi penyusup, akibatnya penyusup (intruder) dapat melancarkan aksi penyerangan dengan berbagai metode atau *tools-tools* yang dapat dioperasikan untuk menyerang sistem keamanan jaringan.

Serangan bisa diartikan sebagai ancaman yang serius. Contoh serangan yang sering dilakukan seperti *DDoS Attack*, *Port Scanning*, *Sniffing*, *FTP brute force*, *SQL Injection*, *Malware*, *Phishing*, *Exploit*, *spamming*, *HackWeb*, *Hacking* dsb. Dampak yang ditimbulkan pun bisa bermacam-macam tentunya, seperti pencurian data penting, sabotase, spionase, terganggunya kestabilan internet, server mengalami down, sampai merusak sistem itu sendiri. Itulah akibat umum yang dihasilkan dari serangan di jaringan internet. Sama halnya juga dengan virus, serangan yang dihasilkannya pun dapat melumpuhkan suatu sistem.

Kurang optimalnya sistem keamanan jaringan seperti inilah yang membuat pengguna internet merasa kurang aman dalam penggunaannya, oleh karena itu diperlukan solusi untuk menangani permasalahan tersebut. Ada beberapa contoh sistem keamanan jaringan yang bisa menjadi solusi dalam membantu menangani permasalahan yang terjadi pada objek penelitian, diantaranya yaitu dengan menggunakan IDS (*Intrusion Detection System*) snort sebagai salah satu solusi untuk menangani serangan-serangan tersebut. Snort merupakan sebuah aplikasi atau *tool* sekuriti yang berfungsi untuk mendeteksi intrusi-intrusi jaringan (penyusupan, penyerangan, pemindaian, dan beragam bentuk ancaman lainnya), sekaligus juga melakukan pencegahan. Dalam praktiknya, snort sangat andal untuk membentuk *logging* paket-paket dan analisis trafik-trafik secara *real-time* dalam jaringan berbasis TCP/IP.

Snort bukanlah sebatas protokol analisis atau sistem pendeteksi penyusupan IDS (*Intrusion Detection System*), melainkan sedikit gabungan dari keduanya, dan bisa sangat berguna dalam merespon insiden-insiden penyerangan terhadap *host-host* jaringan.

Fitur-fitur snort dapat menjadi penolong administrator-administrator sistem dan jaringan, dimana mampu memperingatkan kita atas *even-even* yang berpeluang bahaya. Hal ini karena snort bisa melakukan *capture* sesi-sesi dasar jaringan dan memberikan fungsi analisis.

Dalam penelitian ini penulis akan membangun sistem monitoring jaringan yang akan mendeteksi serangan-serangan yang masuk pada jaringan yang

terhubung pada komputer *server IDS*, sehingga seluruh paket yang masuk kedalam jaringan tersebut akan dianalisa oleh *snort-engine* apakah sesuai dengan *rules* atau tidak. Apabila sesuai dengan *rules* maka akan dihasilkan peringatan yang disimpan pada *log file* dan *database* yang kemudian dikirimkan kepada administrator berupa informasi penyerangan dalam bentuk *Telegram message*, jika tidak sesuai dengan *rules* maka paket dapat diteruskan masuk kedalam jaringan.

Berdasarkan masalah dan tinjauan diatas, maka penelitian ini mengangkat sebuah judul "*Perancangan dan Implementasi Sistem Monitoring Keamanan Jaringan Menggunakan Snort*". Peneliti memilih *Telegram* dibanding *Whatsapp* atau *SMS Gateway* sebagai media pengiriman notifikasi *alert* karena *Telegram* memungkinkan para pengembang aplikasi untuk menambah *tools* sesuai dengan kebutuhan mereka. Hal ini dimungkinkan karena *Telegram* membuka antarmuka pemrograman aplikasi (*application programming interface/API*). Dan memiliki fitur *Bot* yang bisa melakukan berbagai tugas seperti menjadi pengingat/*reminder*, dapat diintegrasikan dengan perangkat lain, dan juga fitur chat bot atau chat otomatis milik *Telegram* tidak memerlukan bantuan aplikasi tambahan seperti *Whatsapp*. Serta tidak membutuhkan *cost/biaya* dalam pengiriman *message* seperti penggunaan *SMS Gateway*. Dengan demikian, peneliti akan menerapkan sistem monitoring keamanan jaringan berbasis *IDS (Intrusion Detection System)* *snort* yang dikombinasikan dengan *instant messaging Telegram*, diharapkan dapat mengatasi masalah yang dihadapi oleh Asrama Mahasiswa Bogani Yogyakarta.

1.2 Rumusan Masalah

Rumusan Masalah pada penelitian ini adalah :

1. Bagaimana merancang sistem monitoring keamanan jaringan pada Asrama Mahasiswa Bogani Yogyakarta ?
2. Bagaimana cara mengkombinasikan IDS (*Intrusion Detection System*) Snort dengan *instant messaging* Telegram ?

1.3 Batasan Masalah

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

1. Konsep sistem monitoring keamanan jaringan diterapkan pada jaringan wireless milik Asrama Bogani Yogyakarta.
2. Menggunakan aplikasi IDS (*Intrusion Detection System*) Snort pada sistem operasi berbasis Linux Ubuntu 16.04 LTS.
3. Menggunakan aplikasi *instant messaging* Telegram sebagai media notifikasi terhadap serangan yang terjadi pada jaringan.
4. Skenario pengujian adalah *Port Scanning*, *FTP bad login*, *SSH Brute Force*, *DDoS Attack*.
5. Sistem hanya sebatas melakukan pendeteksian serangan, tidak sampai melakukan pencegahan serangan.

1.4 Maksud dan Tujuan Penelitian

Maksud dari penyusunan skripsi ini adalah sebagai solusi untuk meningkatkan keamanan jaringan yang efektif dan efisien di Asrama Mahasiswa Bogani Yogyakarta.

Sedangkan tujuan dari penelitian ini adalah :

1. Membangun sistem monitoring keamanan jaringan menggunakan Snort pada Asrama Mahasiswa Bogani Yogyakarta.
2. Menerapkan IDS (*Intrusion Detection System*) Snort yang dapat mengirimkan notifikasi *alert* terhadap aktivitas serangan pada jaringan melalui aplikasi *instant messaging* Telegram secara *real time*.
3. Dan khusus bagi peneliti, penelitian ini bertujuan untuk memenuhi salah satu persyaratan menempuh Tugas Akhir sebagai ketentuan kelulusan Sarjana Strata 1 (S1) Teknik Informatika pada UNIVERSITAS AMIKOM YOGYAKARTA.

1.5 Manfaat Penelitian

1. Peneliti

Adapun manfaat penelitian ini bagi peneliti :

- a. Meningkatkan pengetahuan dan wawasan mengenai ilmu jaringan komputer.
- b. Memahami tahapan-tahapan yang harus dilakukan dalam melakukan penelitian dan metode-metode yang digunakan sesuai kasus pada objek penelitian.

- c. Mampu mencari, mengetahui, menganalisis dan mendata ke dalam bentuk laporan yang tersusun baik dan sistematis.

2. Akademis

Adapun manfaat penelitian ini bagi Akademis :

- a. Membantu perkembangan ilmu pengetahuan khususnya dalam bidang ilmu jaringan komputer.
- b. Menambah literatur perpustakaan dan bahan pertimbangan yang berhubungan dengan penyusunan karya ilmiah untuk dijadikan bahan acuan.

1.6 Metode Penelitian

Adapun metode penelitian yang digunakan oleh penulis dalam menyelesaikan skripsi ini adalah sebagai berikut :

1.6.1 Metode Pengumpulan Data

Terdapat beberapa metode dalam pengumpulan data, yaitu :

1. Observasi

Pengumpulan data dan informasi dengan meninjau langsung dan mengamati secara langsung kegiatan yang terjadi di lapangan.

2. Interview (Wawancara)

Pengumpulan data dan informasi dengan cara mengadakan tanya jawab dengan pihak terkait.

3. Studi Pustaka dan Literatur

Pengumpulan data dan informasi dengan cara membaca buku-buku referensi yang dapat dijadikan acuan pembahasan dalam masalah ini.

1.6.2 Metode Pengembangan Sistem

Penelitian ini menggunakan metode NDLC (*Network Development Life Cycle*) sebagai acuan dalam membuat penelitian ini. Metode NDLC meliputi :

1. Analysis

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna dan analisa topologi atau jaringan yang sudah ada saat ini.

2. Design

Dari data-data yang didapatkan sebelumnya, tahap design ini akan membuat gambaran rancangan sistem yang akan dibangun.

3. Simulation Prototype

Pada tahap ini, peneliti mencoba melakukan simulasi terhadap jaringan yang akan dibangun. Simulasi ini nantinya sebagai gambaran implementasi dan evaluasi terhadap rancangan jaringan yang diusulkan.

4. Implementation

Ditahapan ini akan diterapkan semua yang telah direncanakan dan didesign sebelumnya.

5. Monitoring

Tahap ini tidak dilakukan, hanya sampai pada tahap implementasi.

6. Management

Manajemen atau pengaturan, salah satu yang menjadi perhatian serius adalah masalah *policy*. Kebijakan perlu dibuat untuk mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *reliability* terjaga.

1.6.3 Metode Analisis PIECES

Untuk menentukan suatu sistem baru itu layak atau tidak, maka diperlukan suatu analisis terhadap kriteria-kriteria yaitu kinerja (*Performance*), informasi (*Information*), ekonomi (*Economic*), kontrol (*Control*), efisiensi (*Efficiency*), dan pelayanan (*Services*) yang lebih dikenal sebagai Analisis PIECES.

1.7 Sistematika Penulisan

Untuk memahami lebih jelas penulisan ini, maka materi-materi yang tertera pada penulisan skripsi ini dikelompokkan menjadi beberapa sub bab dengan sistematika penulisan sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, serta sistematika penulisan.

BAB II : LANDASAN TEORI

Pada bab ini membahas tentang dasar teori-teori yang mendukung pelaksanaan penelitian.

BAB III : ANALISIS DAN PERANCANGAN

Pada bab ini membahas tentang analisis dan rancangan yang akan digunakan untuk implementasi dan pembahasan penelitian.

BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini membahas tentang implementasi serta pembahasan mengenai kinerja sistem mulai dari tahap instalasi, konfigurasi dan hasil yang didapatkan terhadap sistem yang telah dibuat.

BAB V : PENUTUP

Pada bab ini berisi tentang kesimpulan-kesimpulan dari hasil penelitian yang sudah dilakukan oleh penulis dan mengemukakan saran yang diperlukan.

