BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam perkembangan teknologi yang sangat cepat ini mampu mempermudah banyak kebutuhan. Seperti informasi yang didapat sekarang sangat cepat dan proses berbagi informasi semakin mudah. Sehingga teknologi menjadi kebutuhan yang sangat penting bagi manusia. Untuk melakukan semua itu maka diperlukan sebuah penghubung yaitu *Server* dan administrator *Server* yang selalu memperhatikan lalu lintas keluar masuk didalam *Server* tersebut. Jika tidak dilakukan upaya pengamanan terhadap *Server*, maka akan banyak celah bagi penyerang untuk menyusup dan mencuri informasi yang terdapat didalamnya. Seorang penyusup akan melakukan serangkaian percobaan untuk mecari kelemahan *Server*, Salah satunya dengan melakukan *Port Scanning* dengan sebuah *tool* .

Port Scanning merupakan suatu kegiatan atau aktifitas untuk mencari dan melihat serta meneliti *Port* pada suatu Komputer atau *Server*. *Port Scanning* adalah langkah pertama seorang penyarang untuk mencari informasi beberapa *port* yang digunakan dalam sebuah *Server* [1]. Dengan mengetahui informasi *port* yang dapat terbuka, maka penyerang akan memanfaatkannya untuk melakukan eksploitasi dari *port* tersebut sehingga terdapat celah bagi penyerang untuk melakukan *hacking* terhadap *Server*.

Untuk melakukan pengamanan terhadap celah yang terdapat pada *Server* tersebut, maka dibutuhkan upaya salah satunya menggunakan IDS. IDS merupakan kombinasi perangkat lunak atau perangkat keras yang dapat

melakukan deteksi penyusupan pada sebuah jaringan. IDS dapat mendeteksi adanya upaya yang menyangkut kerahasiaan, keaslian, dan ketersediaan data pada sebuah jaringan komputer [2]. IDS tersebut akan dibuat dengan aplikasi *Snort*. *Snort* merupakan aplikasi atau perangkat lunak berbasis *opensource* yang memiliki keunggulan untuk mengetahui adanya indikasi penyusupan pada jaringan berbasis TCP/IP secara *real time*. *Snort* akan melakukan *logging* terhadap paket-paket yang telah terdeteksi sebagai ancaman intrusi berdasarkan *rule* yang telah dibuat [3].

Pada penelitian yang dilakukan oleh Anif, Sindung, dan Huri (2015), menerapkan IDS dengan metode Deteksi *Port Scanning* pada jaringan komputer di Politeknik Negeri Semarang. Dari penerapan yang dilakukan, didapatkan hasil bahwa menggunakan IDS menggunakan *portsentry* cukup efektif dalam menangkal serangan *port scanning* (misalnya menggunakan *ipscan, nmap, LANspy, Nessus* dan *superscan*) yang merupakan langkah awal dari serangan ke sistem jaringan [8].

Pada penelitian yang dilakukan oleh Mentang, dkk (2015), merancang IDS untuk keamanan jaringan nirkabel dengan memanfaatkan BASE (*Basic Anakysis and Security Engine*). Sistem IDS dalam mendeteksi serangan yang terjadi adalah dengan melakukan *scanning* terhadap sejumlah *source* dan lalu lintas yang terjadi didalam jaringan.[5].

Dari beberapa penelitian yang sudah dipaparkan sebelumnya, dapat disimpulkaan bahwa IDS digunakan untuk mendeteksi beberapa serangan pada *Server* dan jaringan *wireless*. Peneliti akan melakukan analisis efektifitas waktu deteksi serangan pada *Virtual Private Server* (VPS) menggunakan IDS berbasis

Snort untuk mendeteksi serangan *Port Scanning*. Dengan sistem ini diharapkan dapat mempermudah dan membantu administrator dalam melakukan *monitoring* keamanan *server*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, maka perlu dirumuskan suatu masalah yang akan diselesaikan pada penelitian ini yaitu:

1. Bagaimana mekanisme yang tepat untuk mendeteksi serangan *Port Scanning* pada VPS menggunakan IDS yang dibuat dengan *Snort* ?
2. Bagaimana mengimplementasikan IDS berbasis Snort pada VPS untuk mendeteksi serangan *Port Scannning* ?
3. Bagaimana cara menganalisa terdeteksinya serangan *Port Scanning* pada IDS ?

1.3 Batasan Masalah

Untuk menjaga fokus penelitian yang akan dilakukan, adapun batasan-batasan dalam pembuatan sistem, yaitu:

a. IDS dibuat dengan aplikasi *Snort*.
b. IDS digunakan untuk mendeteksi serangan *Port Scanning*.
c. Menggunakan *VPS* (*Virtual Private Server*) dengan OS *Ubuntu 16.04*
d. Menggunakan metode pengembangan yaitu NDLC (*Network Development Life Cycle*) namun hanya sampai perancangan.
e. Pengujian serangan *Port Scanning* menngunakan *tool Nmap* pada *Linux Debian 7.11* dan *Zenmap* pada *Windows 8.1*
f. *Linux Debian 7.11* dijalankan dengan *Oracle VM VirtualBox*.

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud Penelitian

Maksud dari penelitian ini adalah sebagai berikut:

1. Merancang sistem yang dapat digunakan untuk mendeteksi serangan *Port Scanning* pada VPS menggunakan IDS yang dibuat dengan *Snort*.
2. Untuk memenuhi persyaratan dalam mencapai Gelar Sarjana pada Program Studi Informatika.

1.4.2 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui performa IDS Snort yang dipasang pada VPS dalam mendeteksi serangan Port Scanning.
2. Melakukan pendeteksian terhadap serangan *Port Scanning*.

1.5 Manfaat Penelitian

Dari penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1.5.1 Pengguna

a. Mengetahui adanya serangan *Port Scanning* yang ditujukan pada VPS.
b. Meningkatkan kualitas keamanan data.

1.5.2 Peneliti

a. Meningkatkan pemahaman pengetahuan, pengalaman dalam menganalisa dan merancang sisitem yang efektif dan efisien.
b. Meningkatkan pemahaman dan pengetahuan dalam jaringan komputer khususnya pada keamanan jaringan.

c. Mengetahui tahapan-tahapan yang harus dilakukan dalam melakukan penelitian dan metode apa saja yang digunakan.

1.5.3 UNIVERSITAS AMIKOM Yogyakarta

Menjadi arsip dan referensi untuk mahasiswa angakatan selanjutnya dalam menyusun tugas akhir, materi perkuliahan, tugas akhir dan skripsi atau penelitian.

1.6 Metode Penelitian

Metode penelitian yang digunakan oleh penulis dalam melakukan pengumpulan data dan pengembangan sistem antara lain:

1.6.1 Metode Pengumpulan Data

Metode ini dilakukan supaya mendapatkan data yang akurat dan relevan tentang penelitian yang akan dilakukan, maka dari itu diperlukan metode untuk mencapai tujuan penelitian, berikut metode penelitian yang digunakan:

1.6.1.1 Studi Literatur

Metode pengumpulan data dan referensi didapatkan dari berbagai media keputusan, buku, jurnal penelitian terdahulu, artikel, dan informasi dari internet yang berkaitan dengan judul penelitian.

1.6.2 Metodologi Pengembangan Sistem

Metode yang digunakan dalam pengembangan jaringan mengacu pada NDLC (*Network Development Life Cycle*) yang terdiri dari beberapa proses diantaranya :

1. Analisis (*Analysis*)

   Tahapan ini dilakukan analisa kebutuhan dan analisa permasalahan yang muncul. Analisis kebutuhan *hardware* dan *software*.

2. Perancangan (*Design*)

   Tahap ini akan membuat suatu rancangan sistem yang dapat mendeteksi adanya intrusi. Melakukan desain topologi jaringan interkoneksi yang akan dibangun.

3. Simulasi Prototipe (*Simulation Prototype*)

   Membuat dalam bentuk simulasi dengan bantuan *tools* khusus di bidang *network*. Hal ini dikmaksudkan untuk mengetahui kelemahan dan kekurangan jaringan yang akan dibangun.

4. Implementasi (Implementation)

   Pada tahapan ini penulis akan menerapkan semua yang telah direncanakan dan didesain sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil atau gagalnya sistem yang akan dibangun.

5. Pengawasan (*Monitoring*)

   Setelah implementasi tahapan monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal pada tahapan analisis, maka perlu dilakukan kegiatan *monitoring*.

6. Manajemen (*Management*)

Pada level manajemen, salah satu yang menjadi perhatian khusus adalah masalah kebijakan. Kebijakan perlu dibuat untuk membuat sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *reliability* tejaga.

1.7 Sistematika Penulisan

Pada bagian ini dituliskan urut-urutan dan sistematika penulisan yang dilakukan.

BAB I PENDAHULUAN

Bab ini merupakan bab yang membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan masalah, manfaat penelitian, metode penelitian dan sistematika penulisan yang diangkat menjadi penulisan laporan Skripsi.

BAB II LANDASAN TEORI

Bab ini membahas tentan dasar-dasar teori berdasarkan permasalahan yang digunakan sebagai landasan dalam penelitian mengenai *Intrusion Detection System* dan perancangan sistem.

BAB III METODE PENELITIAN

Bab ini memuat uraian tentang gambaran umum sistem, perancangan sistem, analisis kebutuhan sistem yang mencakup perangkat lunak yang digunakan dalam penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini memuat dokumentasi hasil pengujian dan pembahasan mengenai kinerja sistem mulai dari tahap instalasi, konfigurasi dan hasil yang didapatkan terhadap sistem yang telah dibuat.

BAB V PENUTUP

Bab ini memuat uraian kesimpulan dari seluruh rangkaian perancangan hingga pengujian sistem terhadap penelitian yang dilaksanakan dan saran untuk pertimbangan sistem keamanan selanjutnya.