BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi berkembang kian pesat setiap harinya dikarenakan teknologi jaringan yang makin hari menunjukkan kecanggihannya. Berbagai ragam data-data mampu diakses dengan cepat. Data-data tersebut baik berupa teks, dokumen, audio maupun video semuanya dapat diunduh atau diunggah dengan cepat. Data-data tersebut dikirim melalui banyak media yang terhubung ke banyak orang antara satu dengan yang lain.

Dengan semakin tingginya tingkat kompleksitas penggunaan jaringan komputer, maka semakin tinggi pula ancaman yang ada. Misalnya saja untuk mengambil alih hak akses komputer lain sebagai *user*, penyerang dapat melakukan kontrol jarak jauh atau *remote* melalui port ssh dari komputer yang akan di-*remote*. Dan apabila hal ini dilakukan oleh para pelaku *cybercrime* tentunya dapat merugikan pihak-pihak tertentu.

Maka dari itu aspek keamanan data di dalam jaringan pun harus ikut diperhatikan dan tidak juga diremehkan. Keamanan pada jaringan merupakan segala aktifitas pengamanan suatu jaringan dengan bertujuan menjaga *privacy*, *integrity*, *availability*, *authentication*, *access control* dan *safety* terhadap suatu

serangan. Keamanan jaringan harus mampu mencegah dan menghentikan berbagai potensi serangan agar tidak memasuki dan menyebar pada sistem jaringan. Serangan atau *Intrusion* dapat diartikan sebagai aktivitas tidak sah atau tidak diinginkan yang mengganggu privasi, integritas dan atau ketersediaan dari informasi yang terdapat di sebuah sistem.

Salah satu *software* yang dapat digunakan untuk memonitoring jaringan adalah Snort. Snort adalah sebuah *software opensource* ringkas yang sangat berguna untuk mengamati aktivitas dalam suatu jaringan komputer. Snort dapat digunakan sebagai suatu NIDS (*Network Intrusion Detection System*) yang ber-skala ringan (*lightweight*), dan *software* ini menggunakan sistem peraturan-peraturan *(rules system*) yang dapat dibuat sesuai kebutuhan untuk melakukan deteksi dan pencatatan (*logging*) terhadap berbagai macam serangan pada jaringan komputer. Selain itu Snort juga memiliki beberapa mode yang dapat digunakan untuk mengamankan suatu jaringan seperti *sniffer mode*, *packet logger mode*, NIDS mode dan *Inline mode*.

Sistem keamanan *firewall* tidaklah cukup untuk meminimalkan terjadinya serangan terhadap suatu jaringan komputer. Banyak serangan yang terjadi pada jaringan komputer dapat diketahui setelah adanya kejadian-kejadian yang aneh pada jaringan. para administrator jaringan tidak bisa mengetahui dengan pasti apa yang sedang terjadi, sehingga dibutuhkan waktu yang cukup lama untuk diatasi.

Kantor dinas kebudayaan dan pariwisata sudah memiliki jaringan komputer yang terpadu. Terdapat komputer di banyak ruangan yang mana satu sama lain terhubung sehingga dapat bertukar data atau informasi. Namun belum adanya mekanisme keamanan guna mencegah terjadi tindakan yang akan membahayakan data-data atau informasi apapun di dalamnya.

Oleh karena itu, untuk mengatasi permasalahan yang ada, perlu dibangun sebuah sistem keamanan jaringan pada kantor dinas kebudayaan dan pariwisata yang dapat digunakan untuk memonitoring aktivitas sebuah *server* secara *realtime* dengan menggunakan Snort dan mengirimkan notifikasi serangan yang terekam pada Snort melalui notifikasi *alert* pada *smartphone*. Sehingga jika terjadi upaya penyerangan , sedapat mungkin dapat diketahui dan diantisipasi selanjutnya.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas didapati suatu rumusan masalah yaitu "Bagaimana membuat atau mengatur Snort agar dapat memonitor dan mendeteksi serangan hingga memberikan notifikasi ke *smartphone* ?".

1.3 Batasan Masalah

Untuk lebih mengarahkan masalah yang ada serta tidak menyimpang dari permasalahan yang akan dilakukan dalam penelitian. Maka, penulis hanya membatasi pada permasalahan berikut ini:

1. Menggunakan hanya *snort (tool)* untuk sebagai NIDS (*Network Intrusion Detection System*).
2. Memonitor 3 tipe penyerangan seperti PING ATTACK, DDOS (*Distributed Denial of Service*) dan PORT SCANNING
3. Memonitor *server* yang dijadikan pusat data bagi aplikasi perkantoran di dinas kebudayaan dan pariwisata.
4. Aplikasi untuk menerima notifikasi di smartphone dibuat secara sederhana saja.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Tujuan yang hendak dicapai dalam penelitian ini adalah sebagai berikut:

a. Merancangan suatu mekanisme pada snort agar dapat memonitoring lalu lintas data
b. Menganalisa catatan untuk mengetahui apa yang benar-benar terjadi dan bagaimana snort menanggulanginya hingga mampu mengirimkan notifikasi ke *smartphone*.

1.4.2 Manfaat Penelitian

Adapun manfaat dalam penelitian ini adalah sebagai berikut:

a. Agar dapat terhindar dari permasalahan yang akan terjadi di masa yang akan datang , terutama masalah privasi data.
b. Menjamin terpenuhinya aspek-aspek dalam keamanan jaringan yaitu, *confidentiality*, *integrity* dan *accountability*.

c. Mempermudah administrator dalam mengelola tindakan yang diperlukan untuk menangani permasalahan dalam keamanan jaringan.

1.5 Metodologi Penelitian

1.5.1 Waktu dan Tempat Penelitian

Tempat dalam melakukan penelitian tugas akhir ini yaitu berlokasi di Kantor dinas kebudayaan dan pariwisata April 2019 sampai dengan Juli 2019.

1.5.2 Alat dan Bahan Penelitian

Adapun alat dan bahan penelitian yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Perangkat Keras (*Hardware)*
   a. *Laptop*
   b. *Printer*
   c. RAM 8 Gb
   d. *Hardisk* 500Gb
   e. Spesifikasi 4 Core AMD
2. Perangkat Lunak (*Software*)
   a. Sistem Operasi *Windows 10*
   b. Snort for Windows ver 2.9.15
   c. PHP 5.6.4 & MySQL 8
   d. Barnyard2
   e. *Firefox Mozilla* digunakan untuk mencari literature dari *internet*

f. *Microsoft Office* sebagai aplikasi pengolahan data untuk penulisan laporan.

g. Android Studio

1.5.3 Metode Penelitian

Metode penelitian merupakan suatu cara yang dapat digunakan untuk mencapai tujuan yang diharapkan melalui suatu penelitian dengan teknik-teknik dan alat-alat tertentu. Adapun metode yang digunakan dalam penelitian ini yaitu metode eksperimen. Menurut Cochran (1957) mengartikan eksperimen sebagai sebuah atau sekumpulan percobaan yang dilakukan melalui perubahan-perubahan terencana terhadap variabel input suatu proses atau sistem sehingga dapat ditelusuri penyebab dan faktor-faktor sehingga membawa perubahan pada output sebagai respon dari eksperimen yang telah dilakukan.

Adapun tujuan dari metode eksperimen menurut Dedi Sutedi (2009: 54) adalah untuk menguji efektifitas dan efisiensi dari suatu pendekatan, metode,teknik, atau media pengajaran dan pembelajaran, sehingga hasilnya bisa diterapkan jika memang baik atau tidak digunakan jika memang tidak baik dalam pengajaran sebenarnya.

1.5.4 Metode Pengumpulan Data

Pengumpulan data merupakan tahap penting dalam penulisan karya ilmiah. Pengumpulan data menurut Sugiyono (2012:137) dapat dilakukan dengan berbagai *setting*, berbagai sumber, dan berbagai cara dalam upaya mengumpulkan data. Adapun teknik atau metode pengumpulan data yang penulis lakukan :

1. Studi kepustakaan (*literature)*

   Data diperoleh melalui studi kepustakaan (*literature)* yaitu dengan mencari bahan dari *internet*, jurnal dan perpustakaan serta buku yang ada dan sesuai dengan objek yang akan diteliti oleh penulis.

2. Pengamatan *(Observasi)*

   Untuk mendapatkan data-data yang jelas tentang penelitian ini dengan cara mengadakan pengamatan langsung pada data hasil dari monitoring pada jaringan guna dianalisis hasilnya.

1.5.5 Metode Pengujian

Metode pengujian menggunakan *Penetration Testing*. Proses pengujian keamanan jaringan melalui beberapa tahap sebagai berikut (Rathore dkk, 2006) :

1. Information Gathering

Pada tahap ini peneliti mencari informasi yang dibutuhkan sebelum melakukan tindakan pengujian. Bagaimana melakukan serangan sederhana melalui perangkat lunak yang tersedia (*tool*) seperti *ping Attack*, DDOS dan *port scanning*.

2. Analisis

Peneliti selanjutnya melakukan analisis bagaimana serangan tersebut bekerja untuk menentukan rule. Peneliti mempelajari akan pentingnya *rule* tersebut bekerja dengan baik jika serangan tersebut dilancarkan dari suatu *host*.

3. Attacking

Pada tahap ini peneliti akan melakukan serangan terhadap *server* yang sudah ditentukan sehingga diperoleh dari *information gathering* dengan menggunakan *tools. Alert* yang dihasilkan snort berdasarkan *rule* tersebut tersimpan oleh barnyard2 ke *database* MySQL.

4. Evaluasi

Pada tahap ini hasil yang didapat dari pengujian kemudian dijadikan bahan evaluasi dan diakhiri dengan mengirimkan notifikasi.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini memberikan penjelasan garis besar penelitian ini secara jelas supaya dapat lebih terlihat berhubungan yang disusun dalam kerangka bab dan sub-bab. Adapun sistematika penulisan dijabarkan di bawah ini sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini membahas tentang latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat, metode penelitian, metode pengumpulan data, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini membahas tentang tinjauan pustaka yang digunakan dalam penelitian antara lain tinjuan umum, visi dan misi Dinas kebudayaan dan pariwisata, landasan teori meliputi definisi *jaringan komputer*, keamanan dan Snort.

BAB III ANALISIS DAN PERANCANGAN

Pada bab ini membahas tentang analisis kebutuhan dan perancangan Snort serta aplikasi sederhana untuk menerima notifikasi.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi hasil dan pembahasan tentang aplikasi penerapan snort sebagai NIDS, hasil penyerangan dan perilaku sistem setelah ditemukan penyerangan.

BAB V KESIMPULAN DAN SARAN

Bab ini menguraikan tentang kesimpulan dari keseluruhan bab-bab dan saran-saran dalam implementasi lebih lanjut.