BAB I

PENDAHULUAN

1.1 Latar Belakang

pada era perkembangan teknologi yang semakin cepat dengan berbagai macam fungsi dan kemudahan yang ditawarkan, sehingga menuntut untuk meningkatnya kualitas keamanan pada suatu teknologi tersebut, bocornya informasi ke pihak yang tidak berkepentingan dapat menimbulkan kerugian bagi pemilik informasi, sebagai contoh, banyak informasi dalam sebuah instansi atau perusahaan yang hanya diperbolehkan diketahui oleh orang-orang tertentu di dalam instansi atau perusahaan tersebut, seperti informasi tentang produk yang sedang dalam development, algoritma-algoritma atau teknik-teknik yang digunakan untuk menghasilkan produk tersebut, bahkan tentang detail bentuk pemasaran maupun hal-hal penting lainnya. (Fadlin Arsin, Ymin, & Surimi, 2017)

Informasi yang penting perlu dijaga dan dilindungi, karena banyak cara yang bisa dilakukan oleh *hacker* untuk mencuri suatu informasi, karena semakin terbukanya dalam pengetahuan *hacking* dan *cracking*, sehingga banyak kelompok atau perorangan yang tidak bertanggungjawab mencoba untuk mencuri suatu informasi atau menghabiskan *resources* pada server sehingga membuat server tidak bisa bekerja dengan baik.

Ada banyak jenis serangan yang dapat terjadi pada server beberapa diantaranya yaitu serangan *brute force* dan *Distributed Denial of Service (DDoS)*, cara kerja serangan *brute force* ini adalah dengan mencari *password cracking* yang valid, serangan *brute force* akan menempatkan atau mencari semua kemungkinan

password yang sudah disediakan dengan masukan karakter dan panjang password tertentu hal ini mencoba untuk mengkombinasi password (Pratita, 2016), sedangkan serangan *Distributed Denial of Service (DDoS) DDoS* (Distributed Denial Of Services), serangan ini digunakan oleh sekumpulan komputer zombie yang berarti komputer ini sudah disusupi oleh sebuah aplikasi yang berjalan secara background untuk mengirimkan sejumlah data paket ke sebuah server, serangan ini bersifat terkordinasi dan mampu dilakukan secara bersamaan tanpa diketahui oleh pemilik komputer zombie tersebut. (Airlangga & Mualo, 2015)

Dilaporkan pada akhir tahun 2014, serangan *DDoS* adalah suatu teknik serangan yang paling populer dan sering digunakan oleh seorang *hacker* (ArborNetworks, 2014). Dengan demikian, *DDoS* merupakan suatu ancaman utama pada dunia maya dan menjadi masalah utama keamanan cyber. *DDoS* disebut sebagai senjata pilihan oleh para hacker karena telah terbukti menjadi ancaman menakutkan bagi pengguna organisasi dan infrastruktur di internet, di sisi lain serangan jaringan merupakan risiko untuk integritas, kerahasiaan dan ketersediaan sumber daya yang disediakan oleh organisasi (Zhao, Lo, D. C.-T., & Qian, 2015).

Untuk mengatasi masalah keamanan jaringan ada beberapa pendekatan yang dapat dilakukan, seperti menggunakan sistem *IDS* (*intrusion Detection System*), *IPS* (*Intrusion Prevention System*) dan *IDPS* (*Intrusion Detection and Prevention System*), *IDPS* sendiri merupakan perkembangan dari *IDS* yang dipadukan dengan *firewall* pada hal ini menggunakan ip *tables* (Hendri Alamsyah, Riska, & Abdussalam Al Akbar, 2018).

IDPS mampu mendeteksi penyusup atau paket-paket berbahaya dalam jaringan dan memberikan laporan berupa *log* tentang aktivitas dan kondisi jaringan

sekaligus melakukan *drop packet* terhadap upaya penyusupan dan dapat digunakan untuk membantu *administrator* dalam memantau dan menganalisa paket berbahaya yang terdapat dalam sebuah jaringan (Muh. Sadam Husain S.S, LM, Fid Aksara, & Natalis Ransi, 2018).

Pada studi kasus dalam penelitian ini mengambil topologi yang telah diterapkan pada Yayasan Pondok Pesantren Al-Fattah, dimana dalam yayasan tersebut terdapat delapan lembaga didalamnya antara lain Mi Salafiyah, MTS Salafiyah, MA Salafiyah, SMP Simanjaya, SMA 1 Simanjaya, SMA Unggulan BPPT Al-Fattah, Sekolah Tinggi Ilmu Tarbiah Al-Fattah, dan Universitas Billfath, dalam penelitian ini berfokus dalam pembuatan sistem keamanan jaringan pada empat server yaitu server SMP Simanjaya, server SMA Unggulan BPPT Al-Fattah, server SMA 1 Simanjaya, dan server MA Salafiyah, pada ke-empat server tersebut belum terdapat sistem keamanan jaringan, sehingga ada ketakutan sewaktu-waktu terjadi serangan yang mengakibatkan server bermasalah, selain itu ada ketakutan serangan yang sama berulang-ulang terjadi pada server yang berbeda karena tidak adanya sistem keamanan jaringan *multiple* server yang digunakan, sehingga ketika terjadi suatu serangan pada salah satu server, server lain tidak dapat melakukan tindakan pencegahan. Oleh karena itu dibutuhkan suatu sistem keamanan jaringan yang dapat berjalan pada *multiple* server serta dapat dilakukan monitoring pada ke-empat server sekaligus, sehingga akan memudahkan seorang administrator dalam memonitoring semua server dari ancaman serangan.

Berdasarkan hal tersebut maka dalam penelitian ini akan berfokus pada pembuatan sistem keamanan jaringan dengan menerapkan metode *intrusion detection and prevention system (IDPS)* pada *multiple* server yang mana sistem

tersebut dapat melakukan deteksi dan pencegahan serangan dengan melakukan pemblokiran terhadap alamat ip yang dicurigai sebagai penyerang, serta akan dibuat *website* yang dapat digunakan untuk *monitoring* pada server, sehingga akan memudahkan seorang administrator untuk melakukan monitoring pada ke-empat server tersebut..

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan sebelumnya maka didapat rumusan masalah sebagai berikut :

1. Bagaimana cara membuat sistem keamanan jaringan dengan menerapkan metode *IDPS* pada multiple server?
2. Bagaimana perancangan dan pembuatan *website* yang digunakan sebagai *monitoring*?

1.3 Batasan Masalah

Adapun yang menjadi batasan-batasan dalam penelitian ini adalah sebagai berikut :

1. Sistem operasi pada server menggunakan *ubuntu Server 16.04.3*
2. Sistem operasi penyerang menggunakan *ubuntu 20.04 LTS*
3. *Monitoring* pada sistem yang dibuat berbasis *website*
4. Tahap implementasi menggunakan empat komputer sebagai server yang topologinya disesuaikan dengan studi kasus
5. Port yang digunakan dalam penelitian adalah *ssh*.
6. Tahap testing dilakukan dengan dua serangan yaitu serangan *brute force* dan *Distributed Denial of Service (DDoS)*

1.4 Tujuan Penelitian

Adapun Tujuan dari penelitian yang dilakukan oleh penulis dengan judul "Pembuatan sistem keamanan jaringan dengan menerapkan metode *IDPS* pada *multiple server* " antara lain :

1. Membuat sistem keamanan jaringan yang dapat berjalan pada *multiple* server.
2. Membuat *website* yang digunakan sebagai *monitoring* pada sistem keamanan jaringan yang dibuat.

1.5 Manfaat Penelitian

Ada pun manfaat dari pembuatan sistem keamanan jaringan dengan menerapkan metode *IDPS* pada *multiple* server sebagai berikut :

1. Bagi penulis adalah sebagai sarana untuk mengimplementasikan pengetahuan yang telah didapatkan dalam mata kuliah "Keamanan Jaringan" dan "Pemrograman Jaringan" selama perkuliahan berlangsung, dan dapat memahami bagaimana cara menerapkan sistem keamanan jaringan pada *multiple* server.
2. Bagi mahasiswa maupun pembaca sebagai sarana untuk penelitian lebih lanjut tentang keamanan jaringan khususnya pembuatan dan perancangan sistem keamanan jaringan.