

BAB I

PENDAHULUAN

1.1 Latar Belakang

Guna menjamin keberlangsungan sebuah aplikasi berbasis *website* dibutuhkan server yang tangguh. Server sebagai sarana vital untuk menyimpan database, aplikasi dan layanan penting sangat diperlukan sisi keamanannya. Baik dari segi infrastruktur sendiri maupun aplikasi pendukungnya. Diharapkan server terhindar dari hal-hal yang mengganggu kinerjanya sehingga pelayanan terhadap client berfungsi secara maksimal (Nazwita & Ramadhani, 2017).

Pemerintahan banyak membuat aplikasi dengan menggunakan server Windows sebagai wadah aplikasinya. Salah satunya adalah aplikasi data pokok pendidikan (dapodik) milik Dinas Pendidikan Kab. Pasuruan yang menggunakan Windows Server 2008. Aplikasi tersebut terhubung dengan aplikasi kementerian pusat melalui ip publik untuk desentralisasi data. Proses ini dilakukan dengan sinkronisasi secara berkala dari aplikasi kementerian pusat ke aplikasi daerah milik Dinas Pendidikan Kab. Pasuruan.

Berdasarkan penelitian yang dilakukan oleh (Nugroho & Kusban, 2015) menyatakan bahwa “Hasil yang telah dicapai dari penelitian tentang eksploitasi system keamanan RPC (*Remote Procedure Call*) pada jaringan Windows Server 2008 diantaranya adalah pengubahan terhadap password administrator, proses reboot, dan pengambilan file yang ada pada direktori Windows Server 2008”. Penelitian tersebut menunjukkan adanya celah keamanan pada Windows Server 2008. Keamanan dari Internet Information Service (IIS) yang digunakan sebagai web server pun kurang terjamin. Banyak port yang secara *default* sudah terbuka

diantaranya port 80, 135, 139, 445, dan 5357. Semakin banyak *port* yang terbuka menyebabkan server lebih rentan dipenetrasi.

Salah satu insiden pernah terjadi pada server milik Dinas Pendidikan Kab. Pasuruan yang dibajak oleh pihak tidak bertanggung jawab. *Hacker* tersebut mengubah konfigurasi koneksi *database* sehingga aplikasi tidak dapat menampilkan data dari *database*. Beberapa kali juga mengubah *script* aplikasi dapodik. Usaha yang pernah dilakukan adalah melakukan pemasangan *firewall* di server tetapi masih dapat ditembus oleh *hacker*.

Salah satu cara mengatasi permasalahan tersebut adalah dengan melakukan migrasi server dari Windows server 2008 ke linux server. Namun migrasi server tidak dapat dilakukan karena aplikasi Kementrian Pusat untuk kebutuhan sinkronisasi data berbasis Windows. Pada penelitian ini diusulkan untuk menyandingkan server Windows dengan server linux guna menambah keamanan. Sebelum mengakses aplikasi yang ada di server Windows 2008 akan ditahan terlebih dahulu oleh keamanan linux. Server linux berperan sebagai router *firewall* dengan menggunakan metode *port forwarding*.

Berdasarkan latar belakang permasalahan tersebut, maka fokus dari penelitian ini adalah mengimplementasikan metode *port forwarding* untuk mengamankan data yang ada di Windows server 2008. Metode *port forwarding* ini akan membatasi akses ke Windows server 2008, sehingga Windows server 2008 hanya dapat dihubungi oleh router. *Request* dari *client* diterima oleh router, kemudian diteruskan ke server Windows 2008, sehingga server Windows 2008 lebih aman karena tidak dapat diakses langsung dari jaringan luar dan untuk

berkomunikasi dengan server Windows 2008 harus melalui perantara router terlebih dahulu.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah yaitu:

- a. Bagaimana mengimplementasikan *port forwarding* untuk mengamankan data pada Windows Server 2008 agar terhindar dari *hacker*?
- b. Bagaimana aplikasi yang ada di Windows server 2008 dapat diakses secara normal pada jaringan luar?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini terdiri dari dua poin, yaitu sebagai berikut:

- a. Menghasilkan konfigurasi *port forwarding* untuk mengamankan Windows Server 2008.
- b. Jaringan luar dapat mengakses aplikasi yang ada di Windows server 2008 dengan normal dan aman.

1.4 Batasan Penelitian

Batasan masalah pada penelitian Implementasi *Port Forwarding* Untuk Keamanan Data Pada Server (Studi Kasus: Dinas Pendidikan Kab. Pasuruan) adalah:

- a. Penelitian dilakukan di Dinas Pendidikan Kab. Pasuruan.
- b. Penelitian dilakukan menggunakan Windows server 2008 yang diinstall IIS.

- c. Konfigurasi *port forwarding* dilakukan menggunakan linux ubuntu sebagai router.
- d. Penelitian dilakukan menggunakan *protoype* dengan hasil akhir jaringan luar dapat mengakses tampilan index yang ada pada server Windows 2008.
- e. Pengujian dilakukan menggunakan nmap untuk melihat port yang terbuka.
- f. Tidak melakukan penertasi terhadap server.

1.5 Kontribusi Penelitian

Kontribusi Implementasi *Port Forwarding* Untuk Keamanan Data Pada Server (Studi Kasus: Dinas Pendidikan Kabupater Pasuruan) adalah:

- a. Memberi keaman pada Windows server 2008.
- b. Menyediakan perantara agar jaringan luar dapat mengakses aplikasi website dapodik yang ada di Windows server 2008.
- c. Menambah pengetahuan *port forwarding* untuk pengamanan server.