BAB II
TINJAUAN PUSTAKA

2.1 Keamanan Server

Berdasarkan penelitian yang dilakukan (Nazwita & Ramadhani, 2017) menyatakan bahwa:

> 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 menggangu kinerjanya sehingga pelayanan terhadap *client* berfungsi secara maksimal. …. Suatu serangan ke dalam server jaringan komputer dapat terjadi kapan saja. Baik pada saat administrator yang sedang bekerja ataupun tidak. Dengan demikian dibutuhkan sistem keamanan di dalam server itu sendiri yang mampu mendeteksi langsung. …. Keamanan adalah suatu proses, bukan hasil dari sebuah produk. Keamanan bukan merupakan suatu sistem yang terletak pada hardware atau software yang digunkan, seperti *Firewall* atau *Intruder Detection*. Kerena memang keamanan bukanlah hasil dari suatu produk, keamanan lebih kepada proses yang dilewati untuk mendapatkan aman itu sendiri[5].

Berdasarkan kutipan tersebut, keamanan server sangat penting untuk menjaga data yang ada di dalamnya beserta menjaga kinerjanya. Ada beberapa cara untuk menjaga keamanan server, salah satunya melakukan konfigurasi *firewall*.

Menurut penelitian yang dilakukan (Khadafi, S. Nurmuslimah, & Anggakusuma, 2019) menyatakan bahwa:

> *Firewall* adalah sebuah sistem aplikasi di dalam sistem komputer yang berfungsi untuk melindungi komputer yang terkoneksi dalam jaringan komputer dari berbagai macam ancaman atau gangguan dari user yang tidak bertanggung jawab. Penggunan *firewall* merupakan suatu cara untuk memastikan informasi yang bersifat pribadi atau data yang terhubung dengan internet tidak dapat diakses oleh pihak yang tidak bersangkutan. Jika terdapat adanya percobaan akses oleh pihak yang tidak bersangkutan maka akan dilakukan pemblokiran oleh *firewall*.

Berdasarkan kutipan tersebut, *firewall* yang berfungsi melindungi komputer dari berbagai ancaman dapat digunakan sebagai salah satu pilihan untuk menjaga keamanan server. Pada *firewall* dapat dilakukan pengaturan blokir dan terima koneksi yang masuk maupun keluar.

Penelitian yang dilakukan (Purwaningrum, Purwanto, & Darmadi, 2018) menyatakan bahwa:

> Pada dasarnya, semakin banyak *port* yang terbuka pada *firewall* maka semakin tidak aman PC tersebut, terutama pada file dan printer-sharing di bawah Windows sering menemukan dan memanfaatkan titik-titik kelemahan yang ada. …. Apabila kita terkoneksi ke *internet* melalui sebuah router ada baiknya jika mengkonfigurasi router tersebut. Settingan router yang perlu dirubah adalah fungsi *Port Forwarding* yang harus diaktifkan, karena pada kebanyakan router suatu fungsi *Port Forwarding* biasanya telah dimatikan secara *default*. Dengan konfigurasi yang tepat, router akan menolak paket IP dengan pengirim palsu.

Berdasarkan kutipan tersebut *port forwarding* dapat digunakan untuk melindungi atau memberi keamanan pada komputer yang terkoneksi ke *internet* dari ancaman. Pada penelitian ini, komputer yang dilindungi adalah Windows server 2008.

2.2 Windows Server 2008

Server dapat diartikan sebagai perangkat yang menyediakan data yang dibutuhkan *client* dan bertugas melayani permintaan *client*. Salah satu perangkat yang berbasis server adalah Windows Server 2008 yang dirilis oleh Microsoft pada 4 Februari 2008. Windows Server 2008 merupakan pengembangan dari versi sebelumnya yaitu Windows Server 2003 dan Windows Vista. Windows Server 2008 berbasis Web dan teknologi virtualisasi, sehingga memungkinkan untuk meningkatkan kernampuan yang fleksibilitas dan infrastruktur pada komputer server (Gani & Permadi, 2020).

Windows Server 2008 memiliki sistem tools virtualisasi, web *resources*, dan peningkatan sistem keamanan yang tangguh dalam akses data. Tampilnya tools baru Windows Server 2008 adalah IIS 7, Windows Server Manager, dan Windows PowerShell memungkinkan untuk memiliki kendali yang lebih kuat terhadap komputer server serta pada server web dan mendukung prosesor 64 bit dan 32 bit.

Berdasarkan penelitian yang dilakukan (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" yang artinya masih terdapat celah keamanan pada Windows Server 2008 sehingga rentan dibajak. Selain itu keamanan dari Internet Information Service (IIS) yang digunakan sebagai web server kurang terjamin. banyak port yang terbuka secara *default* pada Windows server 2008 diantaranya port 80, 135, 139, 445, dan 5357.

Tabel 2.1 Fungsi *port* pada Windows server 2008

Port	Fungsi
80	Web server *port* default
135	*Location service* (TCP/UDP)
139	NET bios *session service*
445	*File sharing*, rawan worm dan virus
5357	*Web service* untuk windows vista, windows 7, windows server 2008 (unofficial for tcp/udp)

2.3 Ubuntu

Ubuntu merupakan salah satu distro linux debian yang saat ini banyak digunakan. Pada sisi server, ubuntu menjadi salah satu opsi, karena selain mudah digunakan ubuntu juga distro yang stabil, aman, cepat, dan perintahnya cukup mudah terutama bagi pemula. Hal ini dibuktikan dengan beberapa penjual VPS

banyak yang menyediakan distro ini sebagai pilihan OS untuk ditanam dalam server mereka (Idrus, 2021). Linux ubuntu merupakan sistem operasi *open source*. Sumber terbuka atau *open source* adalah sistem pengembangan yang tidak dikoordinasi oleh suatu individu / lembaga pusat, tetapi oleh para pelaku yang bekerja sama dengan memanfaatkan kode sumber (*source code*) yang tersebar dan tersedia bebas (biasanya menggunakan fasilitas komunikasi *Internet*).

Ubuntu memiliki sebuah *tools firewall* yang disebut iptables. Menurut (Jullev A & Susanto, 2017) "IPTables adalah program aplikasi (berbasis linux) yang memungkinkan administrator sistem untuk mengkonfigurasi tabel yang disediakan oleh firewall kernel linux (diimplementasikan sebagai modul Netfilter yang berbeda) dan rantai dan aturan di tempat itu. …. IPTables membutuhkan hak akses yang tinggi untuk beroperasi atau melakukan konfigurasi yang dijalankan oleh "root" pengguna, selain itu gagal". IPTables berfungsi untuk mengatur lalu lintas jaringan dengan mengizinkan atau memblokir koneksi masuk, keluar, atau sekedar melewati server. IPTables pada server dapat digunakan untuk membuat tabel sekumpulan *rules*.

Beberapa tabel yang ada di IPTables adalah tabel filter, Network Address Translation (NAT), dan *mangle*. Tabel filter berfungsi untuk menyaring paket masuk, keluar, atau sekedar lewat. Tabel ini yang digunakan untuk melakukan blokir port yang tidak digunakan yang memiliki aturan *accept, reject, drop,* dan *log*. Selain itu memiliki *chain input, output*, dan *forward*. Tabel NAT berfungsi untuk mengubah alamat asal tujuan paket. Pada tabel NAT memiliki *chain PREROUTING* (dstnat) dan *POSTROUTING* (srcnat), tabel inilah yang nantinya digunakan untuk konfigurasi *port forwarding*. Yang terakhir adalah tabel *mangle*

berfungsi untuk melakukan penghalusan pada proses pengaturan paket. Tabel *mangle* dapat menggunakan semua *chain* yang ada pada iptables.

2.4 Port Forwarding

Port forwarding atau pemetaan *port* adalah nama yang diberikan untuk teknik gabungan. Tujuannya memungkinkan *port* jaringan yang telah ditetapkan (asumsi protokol seperti TCP dan UDP, meskipun proses ini tidak terbatas) pada *host* dalam penyamaran NAT, biasanya jaringan pribadi, berdasarkan nomor *port* di mana ia diterima di *gateway* dari *host* asal. *Port forwarding* memungkinkan pengendalian komputer, misalnya dari *Internet* untuk menghubungkan ke komputer tertentu atau kamera ip dalam jaringan area lokal (LAN). *Port Forwarding* bertugas sebagai penerjemah alamat atau nomor *port* dari sebuah paket ke tujuan baru dan meneruskan paket sesuai dengan tabel *routing* yang telah dibuat (Dry & Munir, 2017).

Port forwarding menyediakan kemampuan untuk mengkonversi koneksi TCP tidak aman ke koneksi SSH aman untuk pengalihan koneksi dari suatu IP ke IP lain sehingga seolah-olah klien menghubungi IP tujuan secara langsung, *port forwarding* melalui SSH akan membentuk sambungan yang aman antara komputer lokal dengan komputer *remote* melalui layanan yang disampaikan (Jusuf, 2015). Selain itu, menurut (Pratama & Puspitasari, 2020) menyatakan bahwa "Fungsi *port forwarding* adalah membuka akses terhadap perangkat pada jaringan lokal untuk dapat diakses melalui jaringan publik". *Port forwarding* merupakan salah satu jenis proxy server yang fungsinya sebagai perantara antara pengguna *internet* dengan server tujuan.

Berdasarkan buku *Linux Server Hack* (Flickenger, 2003) "*Port forwarding is now native to iptables. The nat table uses a feature called Destination NAT in the PREROUTING chain to accomplish this. The following rule can be used to port forward HTTP requests to a system (10.0.0.3) on the internal network*." Kutipan tersebut, jika diartikan secara bebas berarti bahwa *port forwarding* merupakan bagian dari iptables. Untuk melakukan *port forwarding*, tabel nat menggunakan fitur *Destination* NAT dalam *chain* PREROUTING. Diberikan contoh sebuah aturan untuk meneruskan *request* HTTP ke sistem (10.0.0.3) di jaringan internal yang menggunakan perintah sebagai berikut:

```
#Use DNAT to forward http
iptables -t nat -A PREROUTING ! -i $INT_IFACE -p tcp --destination-port 80 -j DNAT -to 10.0.0.3:80
```

Untuk menambah keamanan, setelah dilakukan *port forwarding* dilakukan penambahan konfigurasi *port blocking* untuk memblokir *port-port* yang tidak digunakan. *Port blocking* dapat digunakan untuk mengatur hak akses jaringan pada setiap port LAN (Local Area Network) (Sartomo & Sulistyo, 2022). Konfigurasi *port blocking* berguna untuk menghalangi akses pihak yang dikenal maupun tidak dikenal untuk mencegah terjadinya pencurian data.

2.5 Jaringan Komputer

Menurut (Sumardi & Asri Zaen, 2018) "Jaringan komputer merupakan kumpulan dari beberapa *host* dan konektivitasnya. *Host* bisa berupa komputer (PC), laptop, atau jenis lainnya, sedangkan konektivitas adalah media penghubung yang bisa berupa kabel (*wire*) atau tanpa kabel (*wireless*)". Jaringan komputer ada yang bersifat publik yang artinya dapat diakses oleh semua orang yang memiliki jaringan

internet. Sedangkan jaringan lokal merupakan jaringan yang hanya dapat diakses oleh orang yang berada pada area dengan menggunakan koneksi pada alamat tertentu.

Jenis jaringan terbagi menjadi 3 yaitu: LAN *(Local Area Network)*, MAN *(Metropolitan Area Network)*, dan WAN *(Wide Area Network)*. LAN merupakan jaringan yang areanya yang relatif kecil seperti di perkantoran, sekolah, dan areanya sekitar 1 km persegi. Sedangkan MAN, meliputi area yang lebih besar seperti antar wilayah dalam satu propinsi. Wide Area Networks (WAN) meruapakan jaringan yang lingkupnya sudah menggunakan sarana satelit atau kabel bawah laut.