**BAB II**

**TINJAUAN PUSTAKA**

* 1. **Jaringan Komputer**

Menurut Sukmaaji dan Rianto (2008), jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan satu dengan lainnya menggunakan *protocol* komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, aplikasi, dan perangkat keras secara bersama-sama. Dua unit komputer dikatakan terkoneksi apabila keduanya bisa saling bertukar data/informasi, berbagi resource yang dimiliki, seperti file, printer, media penyimpanan (hardisk, floppy disk, cd-rom, flash disk, dll). Data yang berupa teks, audio maupun video bergerak melalui media kabel atau tanpa kabel sehingga memungkinkan pengguna komputer dalam jaringan komputer dapat saling bertukar file/data, mencetak pada printer yang sama dan menggunakan hardware/ software yang terhubung dalam jaringan secara bersama-sama. Tiap komputer, printer atau periperal yang terhubung dalam jaringan disebut dengan node. Sebuah jaringan komputer sekurang-kurangnya terdiri dari dua unit komputer atau lebih, dapat berjumlah puluhan komputer, ribuan, atau bahkan jutaan node yang saling terhubung satu sama lain.

Menurut Techi Wire House (2012), definisi jaringan komputer adalah kumpulan dua atau lebih komputer yang terhubung. Ketika komputer ini bergabung dalam jaringan maka orang dapat berbagi file dan *peripheral* seperti modem, printer, tape drive cadangan, atau CD-ROM drive. Secara luas jaringan komputer bisa terhubung ke beberapa lokasi yang terhubung dengan mengunakan layanan internet, sehingga jaringan komputer dapat mengirim e-mail, berbagai link ke internet global, atau melakukan konferensi video secara real time dengan penggunaan jarak jauh lainnya.

**Gambar2.1**Jaringan Komputer

Berdasarkan skala atau area, jaringan computer dapat dibagi menjadi 4 (empat) jenis yaitu :

1. LAN *(Local Area Network),* adalah suatu jaringan yang terbatas pada daerah yang relative kecil. LAN biasanya terbatas pada daerah geografi tertentu seperti laboratorium, sekolah, kantor atau gedung.
2. MAN *(Metropolitan Area Network),*  adalah suatu jaringan yang meliputi area geografi yang luas, seperti suatu kota atau provinsi. Dengan interkoneksi jaringan dalam area geografi yang luas, informasi dapat disebarkan secara mudah melalui jaringan. Dengan MAN suatu computer dikantor cabang dapat berhubungan dengan server computer yang ada pada kantor pusat melalui jaringan telepon, kabel koaksial atau komunikasi tanpa kabel sekalipun.
3. WAN *(Wide Area Network),* adalah jaringan computer yang meliputi area geografi yang lebih luas dari MAN, yang meliputi suatu Negara atau dunia. Umumnya jaringan ditempatkan pada banyak lokasi yang berbeda. WAN juga merupakan bagian dari banyak LAN yang secara geografi terpisah.
4. *Internet,* adalah interkoneksi jaringan-jaringan computer yang ada di dunia. Sehingga cakupannya sudah mencapai satu planet, bahkan tidak menutup kemungkinan mencakup antar planet. Koneksi antar jaringan computer dapat dilakukan berkat dukungan *protocol* yang khas, yaitu *internet protocol* (IP).
   1. **Arsitektur jaringan**

Sistem operasi jaringan sangat menentukan bentuk arsitektur jaringan yang dibangun. Ada 3 (tiga) macam arsitektur jaringan, yaitu *Peer to Peer*, *File Server*, dan *Client Server*.

1. *Peer to Peer,*adalah Model Jaringan ini tidak memiliki server khusus. Masing-masing komputer membiarkan resources yang ada padanya untuk dapat digunakan oleh komputer lain. Komputer-komputer tersebut diorganisasikan ke dalam sebuah Workgroup.(http://www.ub.ac.id, akses 2012).Bentuk konektivitas *Peer to Peer*, setiap terminal memiliki peran dan derajat yang sama. Jaringan lokal dengan konektivitas *Peer to Peer* ini dibentuk dengan cara menghubungkan setiap terminal secara langsung sehingga masing-masing terminal dapat berbagi data, aplikasi dan peripheral lainnya. Semua terminal dapat bertindak sebagai *workstation* atau server.
2. Server, Pada jaringan client/server, server khusus digunakan untuk pemprosesan, penyimpanan dan manajemen data. Server bertugas menerima request dari client, mengolahnya, dan mengirimkan kembali hasilnya ke client.Untuk itu, server membutuhkan komputer khusus dengan spesifikasi hardware yang jauh lebih baik dan bertenaga dibandingkan hardware untuk client karena komputer harus mampu melayani :
3. Request secara simultan dalam jumlah besar
4. Aktivitas manajemen jaringan
5. Menjamin keamanan pada resource jaringan
6. *Client* Server sesuai dengan namanya, Client-Server berarti adanya pembagian kerja pengolahan data antara client dan server . Saat ini, sebagian besar jaringan menggunakan model client/server.  Secara singkat, jaringan client/server adalah jaringan dimana komputer client bertugas melakukan permintaan data dan server bertugas melayani permintaan tersebut (http://www.ub.ac.id, akses 2012).
   1. **Model TCP (*Transmission Control Protocol*)**

TCP (*Transmission Control Protocol)* merupakan*protocol* yangsecara spesifikdirancanguntukmenyediakanaliran*byte endtoend* yang diandalkaninternetwork yang bisa diandalkan .Layanan TCP diperolehdenganmembiarkanpengirim dan penerimamembuat*endpoint* yang disebutdengan socket. Setiap socket memilikinomor (alamat) socket yang terdiri atas alamat IP hos dan nomorlokal 16 bit bagi host tersebut. (Kristanto, 2003 : 145-146).

Panggilan Socket dapatdilihat pada tabelsebagaiberikut :

**Tabel 2.1**Panggilan Socket

|  |  |
| --- | --- |
| **Primitive** | **Arti** |
| SOCKET | Membentuksuatu end point komunikasi |
| BIND | Memasang alamat lokal pada socket |
| LISTEN | Mengumumkan kesediaan menerima koneksi |
| ACCEPT | Memblok pemanggil sampai usaha koneksi tiba |
| CONNECT | Aktif mencoba membuat koneksi |
| SEND | Mengirimkan data melalui koneksi |
| RECEIVE | Menerima melalui koneksi |
| CLOSE | Melepaskan koneksi |

* 1. **Model UDP (*User Data Protocol*)**

*Protocoltransportconnectionless*yaitu UDP (*User Data Protocol)*menyediakan cara bagiaplikasiuntukmengirimkandatagram IP yang dikemaskemudianmengirimkandatagraminitanpamelakukanpembentukankoneksi. (Kristanto, 2003 : 151).

Segment UDP terdiridariheader 8 *byte* yang diikutioleh data. Duabuahport yang mempunyaifungsi sama seperti yang dikerjakan pada TCP yaitumengidentifikasikan*endpoint*komputersumber dan komputertujuan. Field length UDP meliputiheader 8 *byte* dan data.

**Gambar 2.2** Header UDP

* 1. **ICMP (*Internet Control MessageProtocol*)**

*Internet Message Control Protocol* (ICMP) adalah*protocol* yang bertugasmengirimkan pesan-pesan kesalahan dan kondisilain yang memerlukanperhatiankhusus. Pesan ataupaket ICMP dikirimjikaterjadi masalah pada layer IP dan layerdiatasnya (TCP/UDP). ICMP adalahbagiandarikeluarga*protocol* internet dan didefinisikan di dalam RFC 792. (Sukmaaji, 2004 : 53-54).

**Tabel 2.2**Jenis ICMP

|  |  |  |
| --- | --- | --- |
| **Kategori** | **Tipe** | **Pesan/Message** |
| Pesan Error Reporting | 3 | *DestinationUnreachable* |
| 4 | *SourceQuench* |
| 11 | *Time Exeeded* |
| 12 | *ParameterProblem* |
| 5 | *Redirection* |
| Pesan Query | 8 atau 0 | *Echo RequestorCopy* |
| 13 atau 14 | *Timestamprequest and Reply* |
| 17 atau 18 | *Address mask request and reply* |
| 10 atau 9 | *Router solicitation danadvertisement* |

* 1. **Keamanan Jaringan**

Sistem Keamanan jaringan adalah proses untuk melindungi sistem dalam jaringan dengan mencegah dan mendeteksi penggunaan yang tidak berhak dalam jaringan danperlindungan data selama transmisi dilakukan,untuk menjamin keaslian data yang ditransmisikan, danmemelihara kerahasiaan, integritas, dan ketersediaan data.Satu hal yang perlu diingat bahwa tidak ada jaringan yang anti sadap atau tidak ada jaringan komputer yang benar-benar aman. Sifat dari jaringan adalah melakukan komunikasi. Setiap komunikasi dapat jatuh ke tangan orang lain dan disalahgunakan. Sistem keamanan membantu mengamankan jaringan tanpa menghalangi penggunaannya dan menempatkan antisipasi ketika jaringan berhasil ditembus. Selain itu, pastikan bahwa user dalam jaringan memiliki pengetahuan yang cukup mengenai keamanan dan pastikan bahwa mereka menerima dan memahami rencana keamanan yang Anda buat. Jika mereka tidak memahami hal tersebut, maka mereka akan menciptakan lubang (*hole*) keamanan pada jaringan Anda.

Ada dua elemen utama pembentuk keamanan jaringan :

1. Tembok pengamanan ( *firewall* ), baik secara fisik maupun maya, yang ditaruh diantara piranti dan layanan jaringan yang digunakan dan orang-orang yang akan berbuat jahat.
2. Rencana pengamanan ( *security management* ), yang akan diimplementasikan bersama dengan user lainnya, untuk menjaga agar sistem tidak bisa ditembus dari luar.

**Gambar 2.3***Firewall security*

* 1. ***Intrusion Detektion System* (IDS)**

*Intrusion Detektion System* (IDS) merupakan penghambat atas semua serangan yang akan mengganggu sebuah jaringan. IDS memberikan peringatan kepada administrator server saat terjadi aktivitas tertentu yang tidak di inginkan administrator sebagai penanggung jawab sebua sistem. Selain memberikan peringatan IDS juga mampu melacak jenis aktivitas yang merugikan sebuah sistem. Suatu IDS akan melakukan pengamatan (monitoring) terhadap paket-paket yang melewati dan berusaha menemukan apakah paket berisi aktivitas-aktivitas mencurigakan sekaligus melakukan tindak lanjut pencegahan. Pada dasarna terdapat dua macam IDS, yaitu *Host-Based* dan *network-Based*

1. IDS *Host-Base*, bekerja pada host yang akan dilindungi. IDS semacam ini dapat melakukan berbagai macam tugas untuk mendeteksi serangan-serangan yang dilakukan pada host tersebut. keungulan *Host-Base* adalah pada tugas-tugas yang berhubungan keamanan file, misalnya ada tidaknya file yang telah diubah atau ada tidaknya usaha untuk mendapatkan akses ke file-file sensitif.
2. IDS *Network-Base,* biasanya suatu mesin yang khusus dipergunakan untuk monitoring terhadap seluru sekmen dari jaringan. IDS *Network-Base* akan mengumpulkan paket-paket data yang terdapat dan kemudian menganalisanya serta menentukan paket-paket tersebut berupa suatu paket yang normal atau suatu serangan atau suatu aktivitas yang mencurigakan yang bisa berpotensi terjadinya data *flooding.* (Ariyus : 2005).
   1. **Snort**

Menurut Ariyus (2005:20), Snort merupakan suatu program yang berfungsi untuk memeriksa data-data yang masuk dan melaporkan ke administrator apabilah ada gerak-gerik yang mencurigakan. Snort bekerja dengan peinsip program *sniffer* yaitu mengawasi paket-paket yang melewati jaringan. Snort merupakan suatu IDS (*intrusion detektion system)* akan memperhatikan sekmen jaringan tempat dia berada. Secara sederhana sebua IDS akan mendeteksi semua serangn yang bisa melalui jaringan komputer (*internet* maupun *intranet*) ke jaringan atau komputer yang kita miliki.

Bagi penguna yang memasang Snort pada mesin yang seringkali diserang, ada baiknya memasang ACID (*analisis consoler for intrusion databases*) yang merupakan bagian dari AIR-CERT *project.* ACID menggunakan PHPlot, sebuah *library* untuk membuat sebuah grafik yang baik di PHP, dan ADODB, sebuah *libreryabstrraksi* untuk menggabungkan PHP ke berbagai *database* seperti *MySQL dan Postgre SQL*.

Mengoprasikan Snort secara umum. Snort dapat dioprasikan dalam tiga mode yaitu :

1. *Sniffer mode*, untuk melihat paket yang lewat di jaringan.
2. *Facket loger mode,* untuk mencatat semu paket yang lewat di jaringan untuk dianalisa di kemudian hari.
3. *Intrusion detection mode,* pada *mode* ini Snort berfungsi mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk mengunakan *mode* IDS ini, diperlukan setup dari berbagai aturan (*rules*) yang akan membedakan sebuah paket normal dengan paket yang membawa serangan.

Secara garis besar sistem yang akan dibangun sepertipadagambar 2.4 berikut.

**Gambar 2.4** Cara kerja sistem monitoring

Dari gambar di atas dapat dijelaskan input dari program adalah data jaringan yang masuk kemudian akan di proses melalui aplikasi monitoring WEB BASE dengan mengunakan sensor SNORT apakah data yang ada tersebut melakukan *flooding* atau tidak. Jika data yang datang adalah *flooding* atau serangan dari komputer luar maka sistem akan mencari apakah data merupakan permintaan user atau tidak. Jika data datangnya dari luar yang tidak diinginkan maka secara langsung memberikan informasi kepada admin, kemudian admin bisa mengambil keputusan dengan cara memblok IP dan PORT darimana data itu berasal dan jika data berasal dari user maka data akan ditujukan kepada tujuanya.

* 1. ***Network Monitoring* ( Sistem Pemantau Jaringan )**

Menurut Ariyus (2006: 9) Adalah alat yang digunakan untuk mengetahui adanya lubang keamanan, biasanya digunakan dengan mengunakan *protocol* SNMP ( *Simple network Management* ).

Contoh-contoh program network monitoring antara lain :

1. *Etherboy (Windows), Etherman (UNIK)*
2. *HP Openview (Windows)*
3. *Packetboy (Windows),Packetman (UNIK)*
4. *SNMP Collector (Windows)*
5. *Webboy (Windows)*
6. *Base (linux)*
   1. **Sistem Pemblokiran IP**

Pemblokiran IP tersebut disesuaikan dengan operating system yang ada di server, apakah Linux, Windows 2000, ataukah FreeBSD

* + 1. **WINDOWS 2000**

Di dalam windows 2000 server telah dilengkapi dengan cara untuk mengatur IP baik itu mengeblok IP maupun melewatkan suatu IP. Program tersebut adalah IPSECPOL. Utility ini hampir sama kegunaannya pada iptables dan ipchains dalam program LINUX. Hanya saja untuk utility ini hanya bekerja pada windows 2000 server.

Pengaturan IPSECPOL padatampilan windows dapatdijumpaipada"IP Security Policies on Local Machine" yang berada pada "Computer Configuration Security Settings" di MMC (Microsoft Management Console).

Yang pada defaultnya terdapat 3 ketentuan yang telah ditetapkan :

1. Client (Respond Only), digunakan oleh client untuk memberikan respon kepada windows 2000 server pada saat ada permintaan menggunakan servis yang ada didalamnya.
2. Secure Server (Require Security), ketentuan ini digunakan pada windows 2000 server dan windows 2000 *host* yang menghasilkan*network-based services* untuk meyakinkan bahwa tidak ada *non-authentication* dan *non-encryption traffic* yang di abaikan.
3. Server (Request Security), ketentuan ini hampir sama dengan ketentuan yang ada pada *Secure Server*, yang menjadi perbedaan adalah pada ketentuan ini terdapat ketentuan untuk mengadakan hubungan enkripsi pada tingkat lebih tinggi di user.
   * 1. **FreeBSD**

FreeBSD jugamempunyaiaplikasiuntukpengaturan routing yang fungsinyamiripdengan IPTABLES padalinuxataupun IPSECPOL pada windows, hanyasajapadasistem FreeBSD untukpengaturannyamenggunakanperintah IPFW.

* + 1. **Linux**

Untuksistempemblokirandenganmenggunakan operating system inidenganmenggunakanaplikasi yang sudahtersediayaitudenganmenggunakan IPTABLES atau IPCHAINS tergantungversi yang digunakan.Padaaplikasiinitersediaberbagaifungsitentang routing baik forwarding, accepting ataupunbloking.

* 1. **Data *Flooding***

Menurut Nasution ( 2006 : 23 )*Traffic* data yang ada dalam suatu jaringan akan mengalami turun naik selama pemakaiannya. Pada jam-jam sibuk *traffic* suatu data akan sangat padat, sehingga traffic data tersebut akan terganggu. Baik data yang akan dikirim maupun data yang akan datang akan mengalami antrian data yang mengakibatkan kelambatan dalam pengiriman dan penerimaan data.

Tetapi adakalanya data-data yang berada dalam *traffic* merupakan data yang tidak perlu. Data-data tersebut memang sengaja di dikirim oleh seseorang untuk merusak jaringan data yang ada. Pengiriman data tersebut dapat mengakibatkan lambatnya jalur *traffic* yang ada dalam jaringan, dan juga bisa mengakibatkan kerugian lain yang cukup berarti, misalnya kerusakan alat ataupun kerusakan program karena adanya *intruder* yang masuk ke dalam jaringan. Pengiriman data yang berlebihan baik dari besar paket maupun jumlah paket kedalam suatu jaringan dan umumnya merupakan data yang tidak berguna biasa disebut *Flood*.

Macam-macam*Floodattack* :

1. *Ping of death,*Pengiriman paket *echo request* ICMP (*Internet Control Message Protocol*) ke dalam suatu jaringan secara berlebihan. Pengiriman paket ini dapat mengakibatkan sistem *crash, hang* ataupun *reboot*
2. *Smurf Attack,*Hampir sama dengan *Ping of death* tetapi untuk *smurf attack* paket ICMP tidak dikirim secara langsung ke korban, melainkan melalui perantara. Pada awalnya dikirim sebuah paket ICMP *echo request* ke sebuah host lain, paket ini bertujuan agar host tersebut mengirimkan paket ICMP PING secara terus menerus ke korban terakhirnya.
3. *Syn Flooding,* Dalam proses pengiriman data yang melalui TCP, proses data yangterjadi bias dilihatsepertigambar 2.5 brikut.

**Gambar2.5** Proses data TCP

Hubungan TCP dimulaidenganmengirimkanpaket SYN-TCP ke host yang dituju, pengirimanpaket SYN adalahmerupakanpembukauntukmembukajalurkoneksiantaradua*host*melalui*protocol* TCP. Apabila hubungan tersebut disetujui host tujuan akan mengirimkan paket SYN-ACK sebagai tanda bahwa jalur sudah terbentuk. Dan bagian terakhir adalah pengiriman paket ACK dari *host* awal ke host tujuan sebagai konfirmasi.

Sedangkan flood SYN terjadi bila suatu host hanya mengirimkan paket SYN TCP saja secara kontinyu tanpa mengirimkan paket ACK sebagai konfirmasinya. Hal ini akan menyebabkan host tujuan akan terus menunggu paket tersebut dengan menyimpannya kedalam *backlog*. Meskipun besar paket kecil, tetapi apabila pengiriman SYN tersebut terus menerus akan memperbesar *backlog*. Hal yang terjadi apabila backlog sudah besar akan mengakibatkan host tujuan akan otomatis menolak semua paket SYN yang datang, sehingga host tersebut tidak bisa dikoneksi oleh host-host yang lain.

1. *UDP flood,* Pengiriman data UDP secaraberlebihankedalamsuatujaringan, pengiriman UDP *flood*iniakanmembentuksuatujalurhubungandengansuatuservis UDP dari*host*tujuan. *Flood* UDP ini akan mengirimkan karakter-karakter yang akan mengetes jaringan korban. Sehingga terjadi aliran data yang tidak perlu dalam jaringan korban tersebut.

Menurut Pratama, (2010 dalam Ashadi Soki A 2012 : 7) *Traffic* data yang ada dalam suatu jaringan akan mengalami turun naik selama pemakaiannya. Baik data yang akan dikirim maupun data yang akan datang akan mengalami antrian data yang mengakibatkan kelambatan dalam pengiriman dan penerimaan data. Pengiriman data tersebut dapat mengakibatkan lambatnya jalur *traffic* yang ada dalam jaringan, dan juga bisa mengakibatkan kerugian lain yang cukup berarti. Pengiriman data yang berlebihan baik dari besar paket maupun jumlah paket kedalam suatu jaringan dan umumnya merupakan data yang tidak berguna biasa disebut *flood*.

Menurut Utomo, (2011), Data *flooding* merupakan suatu kejadian di dalam jaringan dimana dalam jaringan tersebut terjadi suatu transfer data dalam jumlah yang besar sehingga mengganggu kinerja komputer yang terhubung di dalam jaringan tersebut, hal ini kemungkinan bisa disebabkan adanya serangan dari luar yang biasa disebut dengan DOS/DDOS (*Denial of Service/Distributed Denial of Services*) yaitu serangan pada jaringan komputer yang berusaha untuk menghabiskan sumber daya sebuah peralatan komputer, sehingga jaringan komputer menjadi terganggu

Menurut Thomas (2005), sedangkan teori lain menyatakan serangan *SYN flood* adalah serangan yang terjadi saat sebuah jaringan dipenuhi paket-paket SYN yang menginisiasi koneksi-koneksi yang tidak lengkap dan jaringan ini tidak dapat memproses koneksi yang sah.

* 1. **Penelitian Sebelumnya**

Penelitian sebelumnyadiambilsebagaisalah-saturefrensiatauacuan yang menunjang proses penelitianini. Adapunbeberapapenelitiansebelumnya yang dijadikansbagairefrensiadalahsbagaibrikut :

* + 1. Penelitian yang dilakolehAshadiSokiAgusaputra.,S.Kom yang berjudulImplementasi Sistem PencegahanData *Flooding*Pada Jaringan Komputer. Berdasarkan hasil penelitian yang telah dilakukan, ashadi soki menyimpulkan sebagai berikut :

1. Sistem yang dibangun dapat mendeteksi adanya peningkatan jumlah aliran data yang menyebabkan flooding dan menurunkan kinerja jaringan.
2. Sistem dapat mengklasifikasikan dan memisahkan jenis aliran data yang masuk, apakah data tersebut menyebabkan flooding atau tidak.
3. Sistem dapat melakukan *blocking data* apabila terjadi flooding.
4. Dengan adanya aplikasi ini maka keamanan jaringan lebih terjamin dan kinerja jaringan lebih optimal.
   * 1. Penelitian yang dilakukanolehyang berjudulrancang bangun sistem pencegahan data *flooding* pada jaringan komputerberdasarkan hasil penelitian yang telah dilakukan, johan anggi pratama menyimpulkan sebagai berikut :
5. Sistem dapat mengambil data dari *Ethernet card*, sehingga semua data bisa dilihat apakah data itu merupakan data yang dibutuhkan atau tidak.
6. Sistem mampu mendeteksi apakah data yang masuk merupakan data *flood* atau tidak. Sistem mampu memblokir alamat IP dan *port* dari asal paket yang melakukan *flooding*. Sistem mampu mengatasi sendiri dengan melakukan pengambilan keputusan data masuk apakah *flood* atau tidak.
7. Jumlah koneksi terhadap sistem berbanding terbalik terhadap kinerja dari sistem.