

TUGAS PROTEKSI DAN TEKNIK KEAMANAN SISTEM INFORMASI

IKI-83408T

**TELECOMUNICATION AND NETWORK SECURITY
STUDI KASUS PADA
KLINIK PASUTRI BAHAGIA**

OLEH KELOMPOK : 123

ANGGOTA :

M. TAAT BARYANTO (7204000527)

HERALD SETIADI (7204000489)

MUHAMMAD RHEZA (7204000551)

MAGISTER TEKNOLOGI INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS INDONESIA

JAKARTA

2005

Abstraksi

Kerahasiaan data dari para pasien klinik Pasangan Suami Istri Bahagia (Pasutri Bahagia) menjadi syarat utama dari kelangsungan hidup dari usaha konsultasi pada klinik ini. Hal ini dikarenakan pada umumnya konsultasi dilakukan secara sangat privacy karena menyangkut masalah masalah yang sangat pribadi.

Untuk mendukung terselenggaranya usaha tersebut diperlukan beberapa perangkat pendukung yang diperlukan. Perangkat tersebut meliputi perangkat pendukung dari proses pra konsultasi sampai pasca konsultasi.

Proses pra konsultasi dilakukan oleh calon pasien dalam usaha mencari informasi yang dibutuhkan untuk menentukan konsultasi yang tepat bagi pasien. Pada umumnya pasien merasa malu untuk berhubungan dengan klinik ini karena takut diketahui oleh orang yang mengenalnya bahwa dia memiliki masalah dengan hal yang pribadi misalnya keharmonisan rumah tangga. Data data dari hasil pemeriksaan dan konsultasi pasien tersebut juga harus tersimpan dengan aman. Walaupun demikian data tersebut juga harus dapat dengan mudah diakses oleh orang yang berhak misalnya dokter atau pasien itu sendiri.

Dalam tugas ini akan dibahas tentang apa saja yang perlu diperhatikan untuk dapat menjamin data data pasien tersebut dapat dijamin keamanannya dan dapat dengan mudah untuk diakses oleh orang orang yang berhak.

Daftar Isi

Abstraksi	1
Daftar Isi	2
Daftar Gambar	3
BAB I Pendahuluan	4
I.1 Jaringan Komputer	4
I.1.1 Jenis-Jenis jaringan	5
I.1.2 Protokol Jaringan	6
I.1.3 Perangkat keras yang diperlukan	8
I.1.4 Topologi/Bentuk Jaringan	14
BAB II Confidentiality	16
II.1 VPN	17
II.1.1 Prinsip kerja Virtual Private Network (VPN)	17
II.1.2 Dukungan Sistem Operasi	19
II.1.3 Alasan Penggunaan VPN	20
II.1.4 Skenario-skenario VPN	20
II.2 Protokol Keamanan Jaringan VPN	22
II.2.1 Tunneling Protocols	22
II.2.2 Encryption Protocols	23
II.3 VPN Security Process	23
II.4 Masalah Performance VPN	24
BAB III Integrity	25
III.1 Tentang Firewall	25
III.1.1 Karakteristik sebuah firewall	26
III.1.2 Teknik yang digunakan oleh sebuah firewall	27
III.1.3 Tipe-Tipe Firewall	27
III.1.4 Konfigurasi Firewall	29
BAB IV Availability	31
IV.1 Intrusion & Detection	31
IV.2 Denial of Service (DoS)	44
IV.2.1 Motif penyerang melakukan Denial of Service	45
IV.2.2 Denial of Service, serangan yang menghabiskan resource	46
IV.2.3 Teknik Melakukan Denial of Service	47
BAB V Daftar Pustaka	49

Daftar Gambar

Gambar 1 VPN Schema connection	17
Gambar 2 Tunneling	18
Gambar 3 VPN Setting for Windows	19
Gambar 4 VPN Arsitecture 1	20
Gambar 5 VPN Arsitektur 2	21
Gambar 6 VPN Arsitektur Security	21
Gambar 7 VPN connection	22

BAB I Pendahuluan

Jaringan komputer bukanlah sesuatu yang baru saat ini. Hampir di setiap perusahaan terdapat jaringan komputer untuk memperlancar arus informasi di dalam perusahaan tersebut. Internet yang mulai populer saat ini adalah suatu jaringan komputer raksasa yang merupakan jaringan komputer yang terhubung dan dapat saling berinteraksi. Hal ini dapat terjadi karena adanya perkembangan teknologi jaringan yang sangat pesat, sehingga dalam beberapa tahun saja jumlah pengguna jaringan komputer yang bergabung dalam Internet berlipat ganda.

Dalam kasus ini, Klinik Pasutri tidak mungkin lagi dapat menghindari dari penggunaan teknologi jaringan komputer. Karena diperlukan media komunikasi antar cabang cabang klinik dan antara klinik dengan pasien di rumah. Klinik Pasutri haruslah mempersiapkan dahulu infrastruktur jaringan lokalnya. Yang perlu diperhatikan adalah lingkup area komunikasi yang akan berhubungan, topologi jaringan, jenis protokol jaringan yang dipakai, serta mempersiapkan Hardware Network yang berkesesuaian dengan topologi dan jenis protokol yang digunakan. Pemilihan jenis hardware disesuaikan dengan keadaan keuangan, kesiapan SDM, dukungan dari Vendor.

1.1 Jaringan Komputer

Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung. Informasi dan data bergerak melalui kabel-kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama sama menggunakan hardware/software yang terhubung dengan jaringan. Tiap komputer, printer atau periferal yang terhubung dengan jaringan disebut node. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan node. Sebuah jaringan biasanya terdiri dari 2 atau lebih komputer yang saling berhubungan diantara satu dengan yang lain, dan saling berbagi sumber daya misalnya CDROM, Printer, pertukaran file, atau memungkinkan untuk saling berkomunikasi secara elektronik. Komputer yang terhubung tersebut, dimungkinkan berhubungan dengan media kabel, saluran telepon, gelombang radio, satelit, atau sinar infra merah.

I.1.1 Jenis-Jenis jaringan

Untuk mendukung terlaksananya jasa konsultasi, klinik ini menggunakan berbagai jenis jaringan komputer

Ada 3 macam jenis Jaringan/Network yaitu :

a Local Area Network (LAN) /Jaringan Area Lokal

Local area network ini pada umumnya digunakan untuk komunikasi data dalam lingkungan satu kantor klinik

Sebuah LAN, adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran di sebuah gedung, atau sebuah sekolah, dan biasanya tidak jauh dari sekitar 1 km persegi. Beberapa model konfigurasi LAN, satu komputer biasanya dijadikan sebuah *file server*. Yang mana digunakan untuk menyimpan perangkat lunak (*software*) yang mengatur aktifitas jaringan, ataupun sebagai perangkat lunak yang dapat digunakan oleh komputer-komputer yang terhubung ke dalam network. Komputer-komputer yang terhubung ke dalam jaringan (*network*) itu biasanya disebut dengan *workstation*. Biasanya kemampuan *workstation* lebih di bawah dari *file server* dan mempunyai aplikasi lain di dalam harddisknya selain aplikasi untuk jaringan. Kebanyakan LAN menggunakan media kabel untuk menghubungkan antara satu komputer dengan komputer lainnya.

b Metropolitan Area Network (MAN) / Jaringan area Metropolitan

Metropolitan area network ini pada umumnya digunakan untuk komunikasi data dalam lingkungan satu wilayah operasional untuk komunikasi antar klinik

Sebuah MAN, biasanya meliputi area yang lebih besar dari LAN, misalnya antar wilayah dalam satu propinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu : jaringan Bank dimana beberapa kantor cabang sebuah Bank di dalam sebuah kota besar dihubungkan antara satu dengan lainnya. Misalnya Bank BNI yang ada di seluruh wilayah Ujung Pandang atau Surabaya.

c Wide Area Network (WAN) / Jaringan area Skala Besar

Karena klinik Pasutri Bahagia ini hanya beroperasi dalam satu kota maka konsep jaringan jenis ini belum diimplementasikan, ada rencana implementasi apabila ada pengembangan wilayah layanan.

Wide Area Networks (WAN) adalah jaringan yang lingkupnya biasanya sudah menggunakan sarana Satelit ataupun kabel bawah laut sebagai contoh keseluruhan jaringan BANK BNI yang ada di Indonesia ataupun yang ada di Negara-negara lain. Menggunakan sarana WAN, Sebuah Bank yang ada di Bandung bisa menghubungi kantor cabangnya yang ada di Hongkong, hanya dalam beberapa menit. Biasanya WAN agak rumit dan sangat kompleks, menggunakan banyak sarana untuk menghubungkan antara LAN dan WAN ke dalam Komunikasi Global seperti Internet. Tapi bagaimanapun juga antara LAN, MAN dan WAN tidak banyak berbeda dalam beberapa hal, hanya lingkup areanya saja yang berbeda satu diantara yang lainnya.

1.1.2 Protokol Jaringan

Beberapa protokol digunakan untuk komunikasi data karena terdapat beberapa jenis jaringan computer pada klinik Pasutri Bahagia. Protokol yang digunakan tersebut memang sudah sangat populer dipasaran sehingga mudah untuk implementasi pada klinik ini

Protokol adalah aturan-aturan main yang mengatur komunikasi diantara beberapa komputer di dalam sebuah jaringan, aturan itu termasuk di dalamnya petunjuk yang berlaku bagi cara-cara atau metode mengakses sebuah jaringan, topologi fisik, tipe-tipe kabel dan kecepatan transfer data.

Protokol-Protokol yang dikenal adalah sebagai berikut :

- a Ethernet
- b Local Talk
- c Token Ring
- d FDDI
- e ATM

a Ethernet

Protocol Ethernet sejauh ini adalah yang paling banyak digunakan, Ethernet menggunakan metode akses yang disebut CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*). Sistem ini menjelaskan bahwa setiap komputer memperhatikan ke dalam kabel dari network sebelum mengirimkan sesuatu ke dalamnya. Jika dalam jaringan tidak ada aktifitas atau bersih komputer akan mentransmisikan data, jika ada transmisi lain di dalam kabel, komputer akan menunggu dan akan mencoba kembali transmisi jika jaringan telah bersih. kadangkala dua buah komputer melakukan transmisi pada saat yang sama, ketika hal ini terjadi, masing-masing komputer akan mundur dan akan menunggu kesempatan secara acak untuk mentransmisikan data kembali. metode ini dikenal dengan koalisi, dan tidak akan berpengaruh pada kecepatan transmisi dari network. Protokol Ethernet dapat digunakan untuk pada model jaringan Garis lurus, Bintang, atau Pohon. Data dapat ditransmisikan melewati kabel twisted pair, koaksial, ataupun kabel fiber optic pada kecepatan 10 Mbps.

b LocalTalk

LocalTalk adalah sebuah protokol network yang di kembangkan oleh Apple Computer, Inc. untuk mesin-mesin komputer Macintosh . Metode yang digunakan oleh LocalTalk adalah CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Hampir sama dengan CSMA/CD.. Adapter LocalTalk dan cable twisted pair khusus dapat digunakan untuk menghubungkan beberapa komputer melewati port serial. Sistem Operasi Macintosh memungkinkan koneksi secara jaringan peer-to-peer tanpa membutuhkan tambahan aplikasi khusus Protokol LocalTalk dapat digunakan untuk model jaringan Garis Lurus , Bintang , ataupun model Pohon dengan menggunakan kabel twisted pair . Kekurangan yang paling mencolok yaitu kecepatan transmisinya. Kecepatan transmisinya hanya 230 Kbps.

c Token Ring

Protokol Token di kembangkan oleh IBM pada pertengahan tahun 1980. Metode Aksesnya melalui lewatnya sebuah token dalam sebuah lingkaran seperti Cincin Dalam lingkaran token, komputer-komputer dihubungkan satu dengan yang lainnya seperti sebuah cincin. Sebuah Sinyal token bergerak berputar dalam sebuah lingkaran (cincin) dalam sebuah jaringan dan bergerak dari sebuahkomputer-menuju ke

komputer berikutnya, jika pada persinggahan di salah satu komputer ternyata ada data yang ingin ditransmisikan, token akan mengangkutnya ke tempat dimana data itu ingin ditujukan, token bergerak terus untuk saling mengkoneksikan diantara masing-masing komputer.

Protokol Token Ring membutuhkan model jaringan Bintang dengan menggunakan kabel twisted pair atau kabel fiber optic . Dan dapat melakukan kecepatan transmisi 4 Mbps atau 16 Mbps. Sejalan dengan perkembangan Ethernet, penggunaan Token Ring makin berkurang sampai sekarang.

d FDDI

Fiber Distributed Data Interface (FDDI) adalah sebuah Protokol jaringan yang menghubungkan antara dua atau lebih jaringan bahkan pada jarak yang jauh Metode aksesnyayang digunakan oleh FDDI adalah model token . FDDI menggunakan dua buah topologi ring secara fisik. Proses transmisi biasanya menggunakan satu buah ring, namun jika ada masalah ditemukan akan secara otomatis menggunakan ring yang kedua. Sebuah keuntungan dari FDDI adalah kecepatan dengan menggunakan fiber optic cable pada kecepatan 100 Mbps.

e ATM

ATM adalah singkatan dari *Asynchronous Transfer Mode* (ATM) yaitu sebuah protokol jaringan yang mentransmisikan pada kecepatan 155 Mbps atau lebih . ATM mentarnsmisikan data kedalam satu paket dimana pada protokol yang lain mentransfer pada besar-kecilnya paket. ATM mendukung variasi media seperti video, CD-audio, dan gambar. ATM bekerja pada model topologi Bintang dengan menggunakan Kabel fiber optic ataupun kabel twisted pair . ATM pada umumnya digunakan untuk menghubungkan dua atau lebih LAN . dia juga banyak dipakai oleh *Internet Service Providers* (ISP) untuk meningkatkan kecepatan akses Internet untuk klien mereka.

1.1.3 Perangkat keras yang diperlukan

Dalam sebuah jaringan pada Klinik Pasutri Bahagia ini terdapat beberapa peralatan yang digunakan baik sebagai pengguna jaringan maupun penghubung antar jaringan

Perangkat keras yang dibutuhkan untuk membangun sebuah jaringan komputer yaitu : Komputer, Card Network, Hub, dan segala sesuatu yang berhubungan dengan koneksi

jaringan seperti: Printer, CDROM, Scanner, Bridges, Router dan lainnya yang dibutuhkan untuk process transformasi data didalam jaringan

- a File Servers
- b Workstations
- c Network Interface Cards
- d Concentrators/Hubs
- e Repeaters
- f Bridges
- g Routers

a File Servers

Sebuah file server merupakan jantungnya kebanyakan Jaringan, merupakan komputer yang sangat cepat, mempunyai memori yang besar, harddisk yang memiliki kapasitas besar, dengan kartu jaringan yang cepat. Sistem operasi jaringan tersimpan disini, juga termasuk didalamnya beberapa aplikasi dan data

yang dibutuhkan untuk jaringan. Sebuah file server bertugas mengontrol komunikasi dan informasi diantara node/komponen dalam suatu jaringan. Sebagai contoh mengelola pengiriman file database atau pengolah kata dari workstation atau salah satu node, ke node yang lain, atau menerima email pada saat yang bersamaan dengan tugas yang lain terlihat bahwa tugas file server sangat kompleks, dia juga harus menyimpan informasi dan membaginya secara cepat. Sehingga minimal sebuah file server mempunyai beberapa karakter seperti tersebut di bawah ini :

- Processor minimal 166 megahertz atau processor yang lebih cepat lagi
- (Pentium Pro, Pentium II, PowerPC).
- Sebuah Harddisk yang cepat dan berkapasitas besar atau kurang lebih 10
- GB
- Sebuah RAID (Redundant Array of Inexpensive Disks).
- Sebuah tape untuk back up data (contohnya . DAT, JAZ, Zip, atau CDRW)
- Mempunyai banyak port network
- Kartu jaringan yang cepat dan Reliabilitas
- Kurang lebih 32 MB memori

b Workstations

Keseluruhan komputer yang terhubung ke file server dalam jaringan disebut sebagai workstation. Sebuah workstation minimal mempunyai ; Kartu jaringan, Aplikasi jaringan (software jaringan), kabel untuk menghubungkan ke jaringan, biasanya sebuah workstation tidak begitu membutuhkan Floppy karena data yang ingin di simpan bisa dan dapat diletakkan di file server. Hampir semua jenis komputer dapat digunakan sebagai komputer workstation.

c Network Interface Cards (NIC) atau Kartu Jaringan

Kartu Jaringan (NIC) merupakan perangkat yang menyediakan media untuk menghubungkan antara komputer, kebanyakan kartu jaringan adalah kartu internal, yaitu kartu jaringan yang di pasang pada slot ekspansi di dalam komputer. Beberapa komputer seperti komputer MAC, menggunakan sebuah kotak khusus yang ditancapkan ke port serial atau SCSI port komputernya. Pada komputer notebook ada slot untuk kartu jaringan yang biasa disebut PCMCIA slot. Kartu jaringan yang banyak terpakai saat ini adalah : kartu jaringan Ethernet, LocalTalk konektor, dan kartu jaringan Token Ring. Yang saat ini populer digunakan adalah Ethernet, lalu diikuti oleh Token Ring, dan LocalTalk,

d Ethernet Card / Kartu Jaringan Ethernet

Kartu jaringan Ethernet biasanya dibeli terpisah dengan komputer, kecuali seperti komputer Macintosh yang sudah mengikutkan kartu jaringan ethernet didalamnya. kartu Jaringan ethernet umumnya telah menyediakan port koneksi untuk kabel Koaksial ataupun kabel twisted pair, jika didesain untuk kabel koaksial konektorya adalah BNC, dan apabila didesain untuk kabel twisted pair maka akan punya konektor RJ-45. Beberapa kartu jaringan ethernet kadang juga punya konektor AUI. Semua itu di koneksikan dengan koaksial, twisted pair, ataupun dengan kabel fiber optik.

e LocalTalk Connectors/Konektor LocalTalk

LocalTalk adalah kartu jaringan buat komputer macintosh, ini menggunakan sebuah kotak adapter khusus dan kabel yang terpasang ke Port untuk printer. Kekurangan dari LocalTalk dibandingkan Ethernet adalah kecepatan laju transfer datanya, Ethernet Jaringan komputer bukanlah sesuatu yang baru saat ini. Hampir di setiap perusahaan

terdapat jaringan komputer untuk memperlancar arus informasi di dalam peradahaan tersebut. Internet yang mulai populer saat ini adalah suatu jaringan komputer raksasa yang merupakan jaringan jaringan komputer yang terhubung dan dapat saling berinteraksi. Hal ini dapat terjadi karena adanya perkembangan teknologi jaringan yang sangat pesat, sehingga dalam beberapa tahun saja jumlah pengguna jaringan komputer yang tergabung dalam Internet berlipat ganda. asanya dapat sampai 10 Mbps, sedangkan LocalTalk hanya dapat beroperasi pada kecepatan 230 Kbps atau setara dengan

0.23 Mps

f Token Ring Cards

Kartu jaringan Token Ring terlihat hampir sama dengan Kartu jaringan Ethernet. Satu perbedaannya adalah tipe konektor di belakang KArtu jaringannya, Token Ring umumnya mempunyai tipe konektor 9 Pin DIN yang menyambung Kartu jaringan ke Kabel Network.

g Hub/Konsentrator

Sebuah Konsentrator/Hub adalah sebuah perangkat yang menyatukan kabel-kabel network dari tiap-tiap workstation, server atau perangkat lain. Dalam topologi Bintang, kabel twisted pair datang dari sebuah workstation masuk kedalam hub. Hub mempunyai banyak slot concentrator yang mana dapat dipasang menurut nomor port dari card yang dituju. Ciri-ciri yang dimiliki Konsentrator adalah :

- Biasanya terdiri dari 8, 12, atau 24 port RJ-45
- Digunakan pada topologi Bintang/Star
- Biasanya di jual dengan aplikasi khusus yaitu aplikasi yang mengatur manajemen port tersebut.
- Biasanya disebut hub
- Biasanya di pasang pada rak khusus, yang didalamnya ada Bridges, router

h Repeaters

Contoh yang paling mudah adalah pada sebuah LAN menggunakan topologi Bintang dengan menggunakan kabel unshielded twisted pair. Dimana diketahui

panjang maksimal untuk sebuah kabel unshileded twisted pair adalah 100 meter,

maka untuk menguatkan sinyal dari kabel tersebut dipasanglah sebuah repeater

© 2005 Kelompok 123 IKI-83408T MTI UI. Silahkan menggandakan bahan ajar ini, selama tetap mencantumkan nota hak cipta ini

pada jaringan tersebut.

i Bridges / Jembatan

Adalah sebuah perangkat yang membagi satu buah jaringan kedalam dua buah jaringan, ini digunakan untuk mendapatkan jaringan yang efisien, dimana kadang pertumbuhan network sangat cepat makanya di perlukan jembatan untuk itu. Kebanyakan Bridges dapat mengetahui masing-masing alamat dari tiap-tiap segmen komputer pada jaringan sebelumnya dan juga pada jaringan yang lain di sebelumnya pula. Diibaratkan bahwa Bridges ini seperti polisi lalu lintas yang mengatur di persimpangan jalan pada saat jam-jam sibuk. Dia mengatur agar informasi di antara kedua sisi network tetap jalan dengan baik dan teratur. Bridges juga dapat di gunakan untuk mengkoneksi diantara network yang menggunakan tipe kabel yang berbeda ataupun topologi yang berbeda pula.,.

j Routers

Sebuah Router mengartikan informaari dari satu jaringan ke jaringan yang lain, dia hampir sama dengan Bridge namun agak pintar sedikit, router akan mencari jalur yang terbaik untuk mengirimkan sebuah pesan yang berdasarkan atas alamat tujuan dan alamat asal. Sementara Bridges dapat mengetahui alamat masing-masing komputer di masing-masing sisi jaringan, router mengetahui alamat komputerr, bridges dan router lainnya. router dapat mengetahui keseluruhan jaringan melihat sisi mana yang paling sibuk dan dia bisa menarik data dari sisi yang sibuk tersebut sampai sisi tersebut bersih. Jika sebuah perusahaan mempunyai LAN dan menginginkan terkoneksi ke Internet, mereka harus membeli router. Ini berarti sebuah router dapat menterjemahkan informasi diantara LAN anda dan Internet. ini juga berarti mencarikan alternatif jalur yang terbaik untuk mengirimkan data melewati internet. Ini berarti Router itu :

- Mengatur jalur sinyal secara efisien
- Mengatur Pesan diantara dua buah protocol
- Mengatur Pesan diantara topologi jaringan linear Bus dan Bintang(star)
- Mengatur Pesan diantara melewati Kabel Fiber optic, kabel koaksialm atau kabel twisted pair

1.1.4 Topologi/Bentuk Jaringan

Pada Klinik Pasutri Bahagia ini masing masing jaringan dapat memiliki topologi yang berbeda tergantung dari kebutuhan dan kemudahan implementasinya

Topologi suatu jaringan didasarkan pada cara penghubung sejumlah node atau sentral dalam membentuk suatu sistem jaringan. Topologi jaringan yang umum dipakai adalah : Mesh, Bintang (Star), Bus, Tree, dan Cincin (Ring).

a Topologi Jaringan Mesh

Topologi jaringan ini menerapkan hubungan antar sentral secara penuh. Jumlah saluran harus disediakan untuk membentuk jaringan Mesh adalah jumlah sentral dikurangi 1 ($n-1$, n = jumlah sentral). Tingkat kerumitan jaringan sebanding dengan meningkatnya jumlah sentral yang terpasang. Dengan demikian disamping kurang ekonomis juga relatif mahal dalam pengoperasiannya.

b Topologi Jaringan Bintang (Star)

Dalam topologi jaringan bintang, salah satu sentral dibuat sebagai sentral pusat. Bila dibandingkan dengan sistem mesh, sistem ini mempunyai tingkat kerumitan jaringan yang lebih sederhana sehingga sistem menjadi lebih ekonomis, tetapi beban yang dipikul sentral pusat cukup berat. Dengan demikian kemungkinan tingkat kerusakan atau gangguan dari sentral ini lebih besar.

c Topologi Jaringan Bus

Pada topologi ini semua sentral dihubungkan secara langsung pada medium transmisi dengan konfigurasi yang disebut Bus. Transmisi sinyal dari suatu sentral tidak dialirkan secara bersamaan dalam dua arah. Hal ini berbeda sekali dengan yang terjadi pada topologi jaringan mesh atau bintang, yang pada kedua sistem tersebut dapat dilakukan komunikasi atau interkoneksi antar sentral secara bersamaan. topologi jaringan bus tidak umum digunakan untuk interkoneksi antar sentral, tetapi biasanya digunakan pada sistem jaringan komputer.

d Topologi Jaringan Pohon (Tree)

Topologi jaringan ini disebut juga sebagai topologi jaringan bertingkat. Topologi ini biasanya digunakan untuk interkoneksi antar sentral dengan hirarki yang berbeda.

Untuk hirarki yang lebih rendah digambarkan pada lokasi yang rendah dan semakin keatas mempunyai hirarki semakin tinggi. Topologi jaringan jenis ini cocok digunakan pada sistem jaringan komputer .

e Topologi Jaringan Cincin (Ring)

Untuk membentuk jaringan cincin, setiap sentral harus dihubungkan seri satu dengan yang lain dan hubungan ini akan membentuk loop tertutup. Dalam sistem ini setiap sentral harus dirancang agar dapat berinteraksi dengan sentral yang berdekatan maupun berjauhan. Dengan demikian kemampuan melakukan switching ke berbagai arah sentral. Keuntungan dari topologi jaringan ini antara lain : tingkat kerumitan jaringan rendah (sederhana), juga bila ada gangguan atau kerusakan pada suatu sentral maka aliran trafik dapat dilewatkan pada arah lain dalam sistem. Yang paling banyak digunakan dalam jaringan komputer adalah jaringan bertipe bus dan pohon (tree), hal ini karena alasan kerumitan, kemudahan instalasi dan pemeliharaan serta harga yang harus dibayar. Tapi hanya jaringan bertipe pohon (tree) saja yang diakui keandalannya karena putusnya salah satu kabel pada client, tidak akan mempengaruhi hubungan client yang lain.

BAB II Confidentiality

Dalam kasus ini, kerahasiaan data pelanggan menjadi satu hal yang sangat diutamakan karena menyangkut nama bank seseorang. Untuk itu klinik membangun teknologi VPN antara cabang-cabangnya.

Inti utama aspek *privacy* atau *confidentiality* adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Privacy* lebih kearah data-data yang sifatnya privat sedangkan *confidentiality* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah servis) dan hanyadiperbolehkan untuk keperluan tertentu tersebut. Contoh hal yang berhubungan dengan *privacy* adalah e-mail seorang pemakai (*user*) tidak boleh dibaca oleh administrator. Contoh *confidential information* adalah data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) erupakan data-data yang ingin diproteksi penggunaan dan penyebarannya. Contoh lain dari *confidentiality* adalah daftar pelanggan dari sebuah *Internet Service Provider* (ISP). Untuk mendapatkan kartu kredit, biasanya ditanyakan data-data pribadi. Jika seseorang mengetahui data-data pribadi anda, termasuk nama ibu anda, maka orang tersebut dapat melaporkan melalui telepon (dengan berpura-pura sebagai anda) bahwa kartu kreditnya hilang dan mohon penggunaannya diblokir. Institusi (bank) yang mengeluarkan kartu kredit akan percaya bahwa orang tersbeut adalah sah dan akan menutup kartu kredit anda. Masih banyak lagi kekacauan yang dapat ditimbulkan bila data data pribadi ini digunakan oleh orang yang tidak berhak. Dalam bidang kesehatan (*health care*) masalah *privacy* merupakan topik yang sangat serius di Amerika Serikat. *Health Insurance Portability and Accountability Act* (HIPPA), dikatakan akan mulai digunakan di tahun 2002, mengatakan bahwa rumah sakit, perusahaan asuransi, dan institusi lain yang berhubungan dengan kesehatan harus menjamin keamanan dan *privacy* dari data-data pasien. Data-data yang dikirim harus sesuai dengan format standar dan mekanisme pengamanan yang cukup baik. Partner bisnis dari institusi yang bersangkutan juga harus menjamin hal tersebut. Suatu hal yang cukup sulit dipenuhi. Pelanggaran akan *act* ini dapat didenda US\$ 250.000 atau 10 tahun di penjara. Serangan terhadap aspek *privacy* misalnya adalah usaha untuk melakukan penyadapan (dengan program *sniffer*). Usaha-usaha yang dapat dilakukan untuk

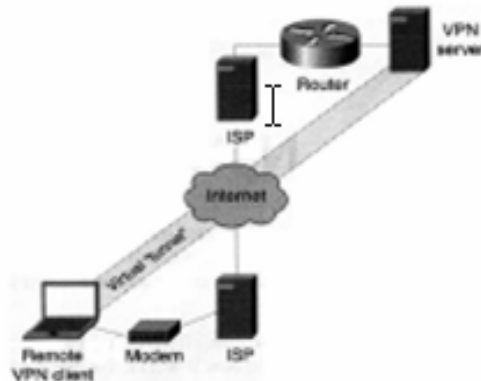
meningkatkan *privacy* dan *confidentiality* adalah dengan menggunakan teknologi kriptografi (dengan enkripsi dan dekripsi). Ada beberapa masalah lain yang berhubungan dengan *confidentiality*. Apabila kita menduga seorang pemakai (sebut saja X) dari sebuah ISP (Z), maka dapatkah kita meminta ISP (Z) untuk membuka data-data tentang pemakai X tersebut? Di luar negeri, ISP Z akan menolak permintaan tersebut meskipun bukti-bukti bisa ditunjukkan bahwa pemakai X tersebut melakukan kejahatan. Biasanya ISP Z tersebut meminta kita untuk menunjukkan surat dari pihak penegak hukum (*subpoena*). Masalah *privacy* atau *confidentiality* ini sering digunakan sebagai pelindung oleh orang yang jahat/nakal. Informasi mengenai *privacy* yang lebih rinci dapat diperoleh dari situs Electronic Privacy Information Center (EPIC) dan Electronic Frontier Foundation (EFF).

II.1 VPN

Untuk menjamin komunikasi antara pasien dengan klinik maupun antar klinik maka disediakan fasilitas protocol keamanan jaringan. Dalam hal ini digunakan infratraktur network yang telah ada yaitu jaringan LAN dan line telpon.

II.1.1 Prinsip kerja Virtual Private Network (VPN)

Virtual Networking: menciptakan ‘tunnel’ dalam jaringan yang tidak harus *direct*. Sebuah ‘terowongan’ diciptakan melalui public network seperti Internet. Jadi seolaholah ada hubungan *point-to-point* dengan data yang dienkapsulasi. Private Networking: Data yang dikirimkan terenkripsi, sehingga tetap rahasia meskipun melalui public network.



Gambar 1 VPN Schema connection

Cara Kerja :

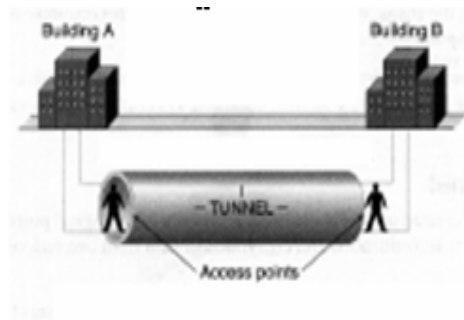
VPN bisa bekerja dengan cara:

- dial-up
- bagian dari router-to-router

Digging the Tunnel

Tunnel dalam VPN sebenarnya hanya logical point-to-point connection dengan autentikasi dan enkripsi. Analoginya adalah kalau sebuah organisasi/perusahaan punya kantor di 2 gedung yang berbeda. Nah, untuk orang/informasi bergerak dari satu kantor ke kantor lainnya, bisa melalui:

- kaki lima atau jalan umum
- menggali lubang di bawah tanah (analog dengan VPN).



Gambar 2 Tunneling

Proses Enkapsulasi

Paket lama dibungkus dalam paket baru. Alamat ujung tujuan terowongan (*tunnel endpoints*) diletakkan di destination address paket baru, yang disebut dengan *encapsulation header*. Tujuan akhir tetap ada pada header paket lama yang dibungkus (encapsulated). Saat sampai di endpoint, kapsul dibuka, dan paket lama dikirimkan ke tujuan akhirnya. Enkapsulasi dapat dilakukan pada lapisan jaringan yang berbeda.

Layer 2 Tunneling

VPN paling sering menggunakan lapisan data link, misalnya:

- Point-to-Point Tunneling Protocol (PPTP) dari Microsoft.

- Contoh yang lain adalah Layer 2 Forwarding (L2F) dari Cisco yang bisa bekerja pada jaringan ATM dan Frame Relay. L2F didukung oleh Internetwork Operating System yang didukung oleh router-router Cisco.
- Yang terbaru adalah Layer 2 Tunneling Protocol (L2TP) yang mengkombinasikan elemen dari PPTP dan L2F.

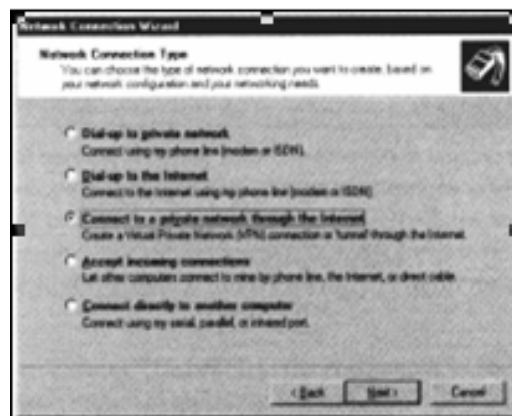
Layer 3 Tunneling

Tunneling dapat dibuat pula pada lapisan IP. Jadi paket IP dibungkus dalam IP Security (IPSec) dengan menggunakan pula IKE (Internet Key Exchange). IPSec bisa dipergunakan dengan beberapa cara:

- transport mode: IPSec melakukan enkripsi, tetapi tunnel dibuat oleh L2TP. Perhatikan bahwa L2TP bisa juga mengenkapsulasi IPX (Internetwork Packet Exchange) dan jenis paket-paket layer 3 lainnya.
- tunneling mode: IPSec melakukan enkripsi dan tunneling-nya. Ini mungkin harus dilakukan jika router/gateway tidak mendukung L2TP atau PPTP.

II.1.2 Dukungan Sistem Operasi

- Windows 9x, Windows NT: PPTP
- Windows 2000: L2TP, PPTP
- Linux: IPSec & SSH (Secure Shell)

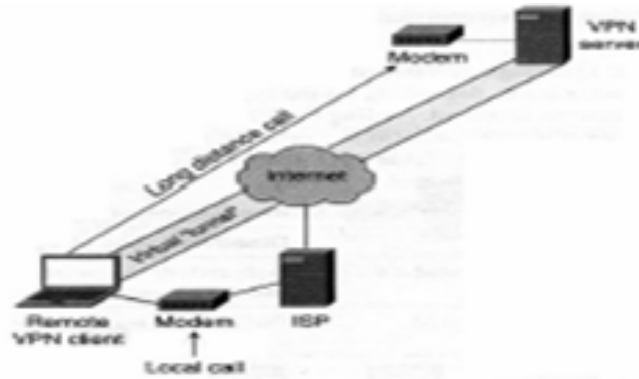


Gambar 3 VPN Setting for Windows

II.1.3 Alasan Penggunaan VPN

II.1.3.1 VPN vs Dial-up Networking:

Misalnya seorang pegawai yang *mobile* bertugas antarkota. Bisa saja pakai dial-up service, tetapi kalau dial-up antar kota, bisa mahal sekali. Oleh karena itu menggunakan ISP lokal + VPN, untuk mengakses LAN perusahaan.



Gambar 4 VPN Arsitektur 1

Selain itu VPN juga akan mereduksi jumlah telephone line & modem bank yang perlu disediakan perusahaan. Perusahaan cukup menyediakan 1 koneksi saja ke Internet. Hal ini akan mereduksi cost dari perusahaan.

II.1.3.2 Keuntungan VPN terhadap *dial-up access*:

1. Menghemat biaya interlokal
2. Membutuhkan lebih sedikit saluran telepon di perusahaan
3. Membutuhkan hardware yang lebih sedikit (seperti modem bank)

II.1.3.3 Kerugian VPN

1. Kedua endpoints dari VPN, koneksinya harus reliable. Sebagai contoh, kalau ISP di sisi client (sang telecommuter employee) tidak bisa diakses/di-dial, maka tentu VPN tidak bisa juga! Lain halnya kalau bisa dial-up service ke kantor.
2. Performance VPN bisa lebih lambat daripada dial-up service yang biasa tanpa VPN. Hal ini disebabkan karena ada proses tunneling dan enkripsi/dekripsi.

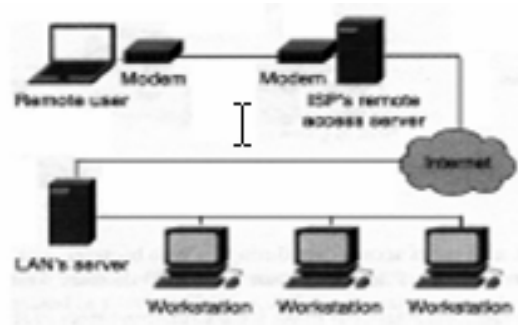
II.1.4 Skenario-skenario VPN

II.1.4.1 Remote Access VPN

Home user atau mobile user men-dial ke ISP

Setelah ada koneksi Internet, client menghubungkan diri ke remote access server yang telah dikonfigurasi dengan VPN.

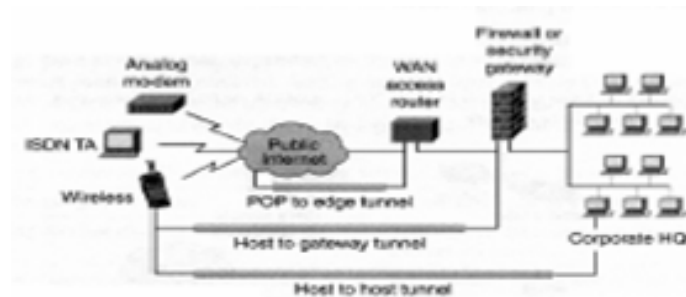
User diotentikasi, dan akses kemudian diizinkan.



Gambar 5 VPN Arsitektur 2

II.1.4.2 Virtual Private Extranets

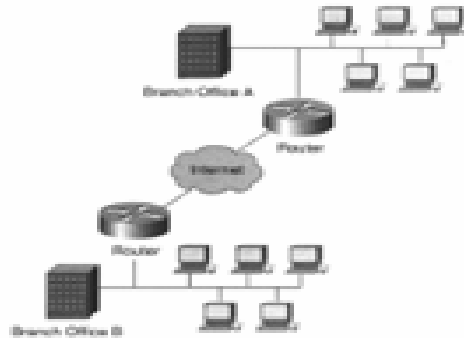
1. Untuk menghubungkan diri partner, supplier atau customer, seperti dalam B2B ecommerce.
2. Hal yang penting adalah melindungi LAN (intranet) dari akses yang mungkin merugikan dari luar. Oleh karena itu harus dilindungi oleh firewall. Koneksi client ke intranet dengan VPN di perimeter network. Karena biasanya yang diakses adalah web server, maka web server juga ada di perimeter network.



Gambar 6 VPN Arsitektur Security

II.1.4.3 VPN Connections Between Branch Offices

Disebut juga *gateway-to-gateway* atau *router-to-router configuration*. Routersnya harus disetup sebagai VPN server dan client. Software seperti *vpnd* (VPNdaemon) bisa dipergunakan untuk menghubungkan LAN dengan Linux atau FreeBSD.



Gambar 7 VPN connection gateway to gateway

II.2 Protokol Keamanan Jaringan VPN

II.2.1 Tunneling Protocols

a PPTP

Dikembangkan oleh Microsoft dari PPP yang dipergunakan untuk remote access.

Caranya:

PPTP mengenkapsulasi frame yang bisa berisi IP, IPX atau NetBEUI dalam sebuah header Generic Routing Encapsulation (GRE). Tetapi PPTP membungkus GRE dalam paket IP. Jadi PPTP membutuhkan IP untuk membuat tunnel-nya, tetapi isinya bisa apa saja.

Data aslinya dienkripsi dengan MPPE.

PPTP-linux adalah client software. Sedangkan yang server adalah PoPToP untuk Linux, Solaris dan FreeBSD.

b L2F

Dibuat Cisco tahun 1996. Bisa menggunakan ATM dan Frame Relay, dan tidak membutuhkan IP. L2F juga bisa menyediakan otentikasi untuk tunnel endpoints.

c L2TP

Dikembangkan oleh Microsoft dan Cisco. Bisa mengenkapsulasi data dalam IP, ATM, Frame Relay dan X.25.

Keunggulan L2TP dibandingkan PPTP:

- multiple tunnels between endpoints, sehingga bisa ada beberapa saluran yang memiliki perbedaan Quality of Service (QoS).
- mendukung kompresi
- bisa melakukan *tunnel authentication*
- bisa bekerja pada jaringan non-IP seperti ATM dan Frame Relay.

d IPsec

Dalam *tunneling mode*, IP Sec bisa dipergunakan untuk mengenkapsulasi paket. IP Sec juga bisa dipergunakan untuk enkripsi dalam protokol tunneling lainnya. IPsec menggunakan 2 protokol

- Authentication Header (AH): memungkinkan verifikasi identitas pengirim. AH juga memungkinkan pemeriksaan integritas dari pesan/informasi.
- Encapsulating Security Payload (ESP): memungkinkan enkripsi informasi sehingga tetap rahasia. IP original dibungkus, dan outer IP header biasanya berisi gateway tujuan. Tetapi ESP tidak menjamin integrity dari outer IP header, oleh karena itu dipergunakan berbarengan dengan AH.

e SSH dan SSH2

Dikembangkan untuk membuat versi yang lebih aman dari rsh, rlogin dan rcp pada UNIX. SSH menggunakan enkripsi dengan public key seperti RSA. SSH bekerja pada *session layer* kalau merujuk pada *OSI reference model*, sehingga disebut *circuit-level VPN*. SSH membutuhkan login account.

f CIPE

Adalah driver kernel Linux untuk membuat secure tunnel antara 2 IP subnet. Data dienkripsi pada lapisan *network layer* (OSI) sehingga di sebut low-level encryption. Oleh karena itu CIPE tidak memerlukan perubahan besar pada layerlayer di atasnya (termasuk aplikasi).

II.2.2 Encryption Protocols

- a MPPE
- b IPsec encryption: DES atau 3DES
- c VPNd: Blowfish
- d SSH: public key encryption

II.3 VPN Security Process

a Authentication

Proses mengidentifikasi komputer *dan* manusia/user yang memulai VPN connection.

Metode otentikasi dapat dilakukan dengan protokol:

- Extensible Authentication Protocol (EAP)
- Challenge Handshake Authentication (CHAP)

- MS-CHAP
- Password Authentication Protocol (PAP)
- Shiva-PAP

b Authorization

Menentukan apa yang boleh dan yang tidak boleh diakses seorang user.

c Enkripsi

II.4 Masalah Performance VPN

Yang paling jadi masalah adalah performa Internet sendiri. Misalnya kadang-kadang bisa terjadi ISP tidak bisa disconnect, atau sedang ada heavy traffic di Internet (karena ada berita besar misalnya). Kemudian adalah masalah kecepatan, dimana circuit-level VPN lebih lambat ketimbang network-level VPN.

BAB III Integrity

Untuk menjamin ketepatan pemberian saran atau pengobatan maka data record konsultasi atau pengobatan dari pasien harus dapat dijamin integritasnya. Pemberian pengobatan lanjutan dengan melihat data yang tidak lengkap dapat berakibat sangat fatal bagi pasien. Untuk diperlukan pengetahuan mengenai serangan-serangan terhadap infrastruktur jaringan, dan juga tindakan preventif dalam melindungi jaringan dengan mengetahui proses penyerangan.

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, *trojan horse*, atau pemakai lain yang mengubah informasi tanpa izin merupakan contoh masalah yang harus dihadapi. Sebuah e-mail dapat saja “ditangkap” (*intercept*) di tengah jalan, diubah isinya (*altered, tampered, modified*), kemudian diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjaga. Penggunaan *enkripsi* dan *digital signature*, misalnya, dapat mengatasi masalah ini. Salah satu contoh kasus trojan horse adalah distribusi paket program *TCP Wrapper* (yaitu program populer yang dapat digunakan untuk mengatur dan membatasi akses TCP/IP) yang dimodifikasi oleh orang yang tidak bertanggung jawab. Jika anda memasang program yang berisi trojan horse tersebut, maka ketika anda merakit (*compile*) program tersebut, dia akan mengirimkan eMail kepada orang tertentu yang kemudian memperbolehkan dia masuk ke sistem anda. Informasi ini berasal dari CERT Advisory, “*CA-99-01 Trojan-TCP-Wrappers*” yang didistribusikan 21 Januari 1999. Contoh serangan lain adalah yang disebut “*man in the middle attack*” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

III.1 Tentang Firewall

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkungannya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN) anda. konfigurasi sederhananya: **pc** (jaringan local) .==. **firewall** .==. **internet** (jaringan lain) Firewall untuk komputer, pertama kali dilakukan dengan menggunakan prinsip “non-routing” pada sebuah Unix host yang menggunakan 2 buah network interface card, network

© 2005 Kelompok 123 IKI-83408T MTI UI. Silahkan menggandakan bahan ajar ini, selama tetap 25
mencantumkan nota hak cipta ini

interface card yang pertama di hubungkan ke internet (jaringan lain) sedangkan yang lainnya di hubungkan ke pc (jaringan lokal)(dengan catatan tidak terjadi “route” antara kedua network interface card di pc ini). Untuk dapat terkoneksi dengan Internet(jaringan lain) maka harus memasuki server firewall (bisa secara remote, atau langsung), kemudian menggunakan resource yang ada pada komputer ini untuk berhubungan dengan Internet(jaringan lain),

apabila perlu untuk menyimpan file/data maka dapat menaruhnya sementara di pc firewall anda, kemudian mengkopikannya ke pc(jaringan lokal). Sehingga internet(jaringan luar) tidak dapat berhubungan langsung dengan pc(jaringan lokal) . Dikarenakan masih terlalu banyak kekurangan dari metoda ini, sehingga dikembangkan berbagai bentuk, konfigurasi dan jenis firewall dengan berbagai policy(aturan) didalamnya. Firewall secara umum di peruntukkan untuk melayani :

1. Mesin/Komputer

Setiap mesin/komputer yang terhubung langsung ke jaringan luar atau internet dan menginginkan semua yang terdapat pada komputernya terlindungi.

2. Jaringan

Jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang di miliki oleh perusahaan, organisasi dsb.

III.1.1 Karakteristik sebuah firewall

- Seluruh hubungan/kegiatan dari dalam ke luar , harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi baik secara fisik semua akses terhadap jaringan Lokal, kecuali melewati firewall. Banyak sekali bentuk jaringan yang memungkinkan agar konfigurasi ini terwujud.
- Hanya Kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan hubungan, hal ini dapat dilakukan dengan mengatur policy pada konfigurasi keamanan lokal. Banyak sekali jenis firewall yang dapat dipilih sekaligus berbagai jenis policy yang ditawarkan.
- Firewall itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan system yang relatif aman.

III.1.2 Teknik yang digunakan oleh sebuah firewall

- Service control (kendali terhadap layanan) Berdasarkan tipe-tipe layanan yang digunakan di Internet dan boleh diakses baik untuk kedalam ataupun keluar firewall. Biasanya firewall akan mengecek no IP Address dan juga nomor port yang di gunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi software untuk proxy yang akan menerima dan menterjemahkan setiap permintaan akan suatu layanan sebelum mengijinkannya. Bahkan bisa jadi software pada server itu sendiri , seperti layanan untuk web ataupun untuk mail.
- Direction Control (kendali terhadap arah) Berdasarkan arah dari berbagai permintaan (request) terhadap layanan yang akan dikenali dan diijinkan melewati firewall.
- User control (kendali terhadap pengguna) Berdasarkan pengguna/user untuk dapat menjalankan suatu layanan, artinya ada user yang dapat dan ada yang tidak dapat menjalankan suatu servis,hal ini di karenakan user tersebut tidak di iijinkan untuk melewati firewall. Biasanya digunakan untuk membatasi user dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.
- Behavior Control (kendali terhadap perlakuan) Berdasarkan seberapa banyak layanan itu telah digunakan. Misal, firewall dapat memfilter email untuk menanggulangi/mencegah spam.

III.1.3 Tipe-Tipe Firewall

a Packet Filtering Router

Packet Filtering diaplikasikan dengan cara mengatur semua packet IP baik yang menuju, melewati atau akan dituju oleh packet tersebut. Pada tipe ini packet tersebut akan diatur apakah akan di terima dan diteruskan atau di tolak. Penyaringan packet ini di konfigurasi untuk menyaring packet yang akan di transfer secara dua arah (baik dari dan ke jaringan lokal). Aturan penyaringan didasarkan pada header IP dan transport header, termasuk juga alamat awal(IP) dan alamat tujuan (IP), protokol transport yang di gunakan(UDP,TCP), serta nomor port yang digunakan. Kelebihan dari tipe ini adalah mudah untuk di implementasikan, transparan untuk pemakai,

relatif lebih cepat. Adapun kelemahannya adalah cukup rumitnya untuk menyetting paket yang akan difilter secara tepat, serta lemah dalam hal autentikasi. Adapun serangan yang dapat terjadi pada firewall dengan tipe ini adalah :

- IP address spoofing : Intruder (penyusup) dari luar dapat melakukan ini dengan cara menyertakan/menggunakan ip address jaringan lokal yang telah diijinkan untuk melalui firewall.
- Source routing attacks : Tipe ini tidak menganalisa informasi routing sumber IP, sehingga memungkinkan untuk membypass firewall.
- Tiny Fragment attacks : Intruder membagi IP kedalam bagian-bagian (fragment) yang lebih kecil dan memaksa terbaginya informasi mengenai TCP header. Serangan jenis ini di design untuk menipu aturan penyaringan yang bergantung kepada informasi dari TCP header.
- Penyerang berharap hanya bagian (fragment) pertama saja yang akan di periksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat di tanggulangi dengan cara menolak semua packet dengan protokol TCP dan memiliki Offset = 1 pada IP fragment (bagian IP)

b Application-Level Gateway

Application-level Gateway yang biasa juga di kenal sebagai proxy server yang berfungsi untuk memperkuat/menyalurkan arus aplikasi. Tipe ini akan mengatur semua hubungan yang menggunakan layer aplikasi ,baik itu FTP, HTTP, GOPHER dll. Cara kerjanya adalah apabila ada pengguna yang menggunakan salah satu aplikasi semisal FTP untuk mngakses secara remote, maka gateway akan meminta user memasukkan alamat remote host yang akan di akses.Saat pengguna mengirimkan user ID serta informasi lainnya yang sesuai maka gateway akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada remote host, dan menyalurkan data diantara kedua titik. apabila data tersebut tidak sesuai maka firewall tidak akan meneruskan data tersebut atau menolaknya. Lebih jauh lagi, pada type ini Firewall dapat di konfigurasi untuk hanya mendukung beberapa aplikasi saja dan menolak aplikasi lainnya untuk melewati firewall. Kelebihannya adalah relatif lebih aman daripada tipe packet filtering router lebih mudah untuk memeriksa (audit) dan mendata (log) semua aliran data yang masuk pada level aplikasi. Kekurangannya adalah pemrosesan tambahan yang berlebih pada setiap hubungan. yang akan

mengakibatkan terdapat dua buah sambungan koneksi antara pemakai dan gateway, dimana gateway akan memeriksa dan meneruskan semua arus dari dua arah.

c Circuit-level Gateway

Tipe ketiga ini dapat merupakan sistem yang berdiri sendiri, atau juga dapat merupakan fungsi khusus yang terbentuk dari tipe application-level gateway. Tipe ini tidak mengizinkan koneksi TCP end to end (langsung). Cara kerjanya: Gateway akan mengatur kedua hubungan TCP tersebut, 1 antara dirinya (gw) dengan TCP pada pengguna lokal (inner host) serta 1 lagi antara dirinya (gw) dengan TCP pengguna luar (outside host). Saat dua buah hubungan terlaksana, gateway akan menyalurkan TCP segment dari satu hubungan ke lainnya tanpa memeriksa isinya. Fungsi pengamanannya terletak pada penentuan hubungan mana

III.1.4 Konfigurasi Firewall

a Screened Host Firewall system (single-homed bastion)

Pada konfigurasi ini, fungsi firewall akan dilakukan oleh packet filtering router dan bastion host*. Router ini dikonfigurasi sedemikian sehingga untuk semua arus data dari Internet, hanya paket IP yang menuju bastion host yang diizinkan. Sedangkan untuk arus data (traffic) dari jaringan internal, hanya paket IP dari bastion host yang diizinkan untuk keluar.

Konfigurasi ini mendukung fleksibilitas dalam akses internet secara langsung, sebagai contoh apabila terdapat web server pada jaringan ini maka dapat di konfigurasi agar web server dapat diakses langsung dari internet.

Bastion Host melakukan fungsi autentikasi dan fungsi sebagai proxy. Konfigurasi ini memberikan tingkat keamanan yang lebih baik daripada packet-filtering router atau application-level gateway secara terpisah.

b Screened Host Firewall system (Dual-homed bastion)

Pada konfigurasi ini, secara fisik akan terdapat patahan/celah dalam jaringan. Kelebihannya adalah dengan adanya dua jalur yang memisahkan secara fisik maka akan lebih meningkatkan keamanan dibanding konfigurasi pertama, adapun untuk server-server yang memerlukan direct akses (akses langsung) maka dapat di letakkan ditempat/segment yang langsung berhubungan dengan internet. Hal ini dapat dilakukan dengan cara menggunakan 2 buah NIC (network interface Card) pada bastion Host. Bastion host packet filtering router

Server

c Screened subnet firewall

Ini merupakan konfigurasi yang paling tinggi tingkat keamanannya. kenapa? karena pada konfigurasi ini di gunakan 2 buah packet filtering router, 1 diantara internet dan bastion host, sedangkan 1 lagi diantara bastian host dan jaringan local konfigurasi ini membentuk subnet yang terisolasi.

Adapun kelebihanannya adalah :

- Terdapat 3 lapisan/tingkat pertahanan terhadap penyususp/intruder .
- Router luar hanya melayani hubungan antara internet dan bastion host sehingga jaringan lokal menjadi tak terlihat (invisible)
- Jaringan lokal tidak dapat mengkonstuksi routing langsung ke internet, atau dengan kata lain ,
- Internet menjadi Invinsible (bukan berarti tidak bisa melakukan koneksi internet).

BAB IV Availability

Kecepatan dan ketersediaan layanan sangat tergantung oleh ketersediaan data. Oleh karena itu Klinik Pasutri Bahagia tidak hanya berfokus bagaimana data dapat disimpan dengan aman tetapi juga harus dapat dijamin kecepatan aksesnya

Aspek availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi. Contoh hambatan adalah serangan yang sering disebut dengan “*denial of service attack*” (DoS attack), dimana server dikirim permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *down, hang, crash*. Contoh lain adalah adanya *mailbomb*, dimana seorang pemakai dikirim e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya (apalagi jika akses dilakukan melalui saluran telepon). Bayangkan apabila anda dikirim 5000 email dan anda harus mengambil (download) email tersebut melalui telepon dari rumah.

IV.1 Intrusion & Detection

Seringkali ketika kita menemukan kerawanan ataupun missconfiguration pada system sendiri, kita akan menganggap hal itu adalah hal yang kecil, karena kita menanggapinya bukan sebagai lubang keamanan. Tools maupun teknik yang digunakan cracker kebanyakan adalah variasi dari serangan yang mereka lakukan sebelumnya. Sebagai Administrator baik system maupun jaringan ataupun end user, Anda haruslah banyak belajar dari pengalaman penyerangan yang terjadi sebelumnya (walaupun serangan tersebut terjadi pada orang lain) untuk menghindari serangan yang akan terjadi berikutnya. Mengetahui jenis serangan sangat penting untuk menjaga stabilitas system, sehingga anda tidak perlu repot untuk menginstall system baru agar lebih aman, anda hanya perlu mempatch atau bahkan sedikit mengkonfigurasi system anda Mungkin bagi beberapa orang tulisan ini merupakan tulisan yang sangat mendasar, tapi tidak ada salahnya jika anda sebagai seorang Profesional untuk mereview sesuatu yang dasar dari waktu ke waktu.. Artikel ini bukan ditujukan untuk menyerang tetapi sebaliknya yaitu untuk bertahan, karena

menurut hemat saya untuk bertahan anda harus tahu cara menyerang. Dalam artikel ini terdapat serangan yang sering dilakukan oleh cracker dan disetiap serangan mempunyai metode-metode tersendiri, contohnya saja dalam melakukan IP spoofing yang mempunyai banyak metode diantaranya *man in the middle attack*.

a IP Spoofing

IP Spoofing juga dikenal sebagai *Source Address Spoofing*, yaitu pemalsuan alamat IP attacker sehingga sasaran menganggap alamat IP attacker adalah alamat IP dari host di dalam network bukan dari luar network. Misalkan attacker mempunyai IP address type A 66.25.xx.xx ketika attacker melakukan serangan jenis ini maka Network yang diserang akan menganggap IP attacker adalah bagian dari Networknya misal 192.xx.xx.xx yaitu IP type C. IP Spoofing terjadi ketika seorang attacker ‘mengakali’ packet routing untuk mengubah arah dari data atau transmisi ke tujuan yang berbeda. Packet untuk routing biasanya di transmisikan secara transparan dan jelas sehingga membuat attacker dengan mudah untuk memodifikasi asal data ataupun tujuan dari data. Teknik ini bukan hanya dipakai oleh attacker tetapi juga dipakai oleh para security profesional untuk men tracing identitas dari para attacker. Protokol yang menangani komunikasi antar komputer kebanyakan berhasil di spoof. ICMP (Internet Control Message Protocol) adalah salah satunya(vulnerable) karena protokol ini dilewati oleh informasi dan pesan-pesan kesalahan diantara dua node dalam network. Internet Group Message Protocol(IGMP) dapat dieksploitasi dengan menggunakan serangan tipe ini karena IGMP melaporkan kondisi kesalahan pada level user datagram, selain itu juga protokol ini mengandung Informasi routing dan Informasi Network. (UDP) User Datagram Protocol juga dapat ‘diminta’ untuk menampilkan identitas host sasaran. Solusi untuk mencegah IP spoofing adalah dengan cara mengamankan packet-packet yang ditransmisikan dan memasang *screening policies*. Enkripsi Point-to-point juga dapat mencegah user yang tidak mempunyai hak untuk membaca data/packet. Autentikasi dapat juga digunakan untuk menyaring source yang legal dan bukan source yang sudah di spoof oleh attacker. Dalam pencegahan yang lain, Administrator dapat menggunakan signature untuk paket-paket yang berkomunikasi dalam networknya sehingga meyakinkan bahwa paket tersebut tidak diubah dalam perjalanan. Anti Spoofing rules(peraturan anti spoof) yang pada dasarnya memberitahukan server untuk menolak packet yang datangnya dari luar yang terlihat datangnya dari dalam, umumnya hal ini akan mematahkan setiap serangan spoofing.

b FTP Attack

Salah satu serangan yang dilakukan terhadap File Transfer Protocol adalah serangan buffer overflow yang diakibatkan oleh *malformed command*. tujuan menyerang FTP server ini rata-rata adalah untuk mendapatkan command shell ataupun untuk melakukan Denial Of Service. Serangan Denial Of Service akhirnya dapat menyebabkan seorang user atau attacker untuk mengambil resource didalam network tanpa adanya autorisasi, sedangkan command shell dapat membuat seorang attacker mendapatkan akses ke sistem server dan file-file data yang akhirnya seorang attacker bisa membuat anonymous root-acces yang mempunyai hak penuh terhadap system bahkan network yang diserang. Tidak pernah atau jarang mengupdate versi server dan mempatchnya adalah kesalahan yang sering dilakukan oleh seorang admin dan inilah yang membuat server FTP menjadi rawan untuk dimasuki. Sebagai contoh adalah FTP server yang populer di keluarga UNIX yaitu WU-FTPD yang selalu diupgrade dua kali dalam sehari untuk memperbaiki kondisi yang mengizinkan terjadinya bufferoverflow Mengexploitasi FTP juga berguna untuk mengetahui password yang terdapat dalam sistem, FTP Bounce attack (menggunakan server ftp orang lain untuk melakukan serangan), dan mengetahui atau mensniff informasi yang berada dalam sistem

c Unix Finger Exploits

Pada masa awal internet, Unix OS finger utility digunakan secara efficient untuk men sharing informasi diantara pengguna. Karena permintaan informasi terhadap informasi finger ini tidak menyalahkan peraturan, kebanyakan system Administrator meninggalkan utility ini (finger) dengan keamanan yang sangat minim, bahkan tanpa kemanan sama sekali. Bagi seorang attacker utility ini sangat berharga untuk melakukan informasi tentang footprinting, termasuk nama login dan informasi contact. Utility ini juga menyediakan keterangan yang sangat baik tentang aktivitas user didalam sistem, berapa lama user berada dalam sistem dan seberapa jauh user merawat sistem. Informasi yang dihasilkan dari finger ini dapat meminimalisasi usaha cracker dalam menembus sebuah sistem. Keterangan pribadi tentang user yang dimunculkan oleh finger daemon ini sudah cukup bagi seorang atacker untuk melakukan social engineering dengan menggunakan social skillnya untuk memanfaatkan user agar ‘memberitahu’ password dan kode akses terhadap system.

d Flooding & Broadcasting

Seorang attacker bisa menguarangi kecepatan network dan host-host yang berada di dalamnya secara significant dengan cara terus melakukan request/permintaan terhadap suatu informasi dari sever yang bisa menangani serangan classic Denial Of Service(Dos), mengirim request ke satu port secara berlebihan dinamakan flooding, kadang hal ini juga disebut spraying. Ketika permintaan flood ini dikirim ke semua station yang berada dalam network serangan ini dinamakn broadcasting. Tujuan dari kedua serangan ini adalah sama yaitu membuat network resource yang menyediakan informasi menjadi lemah dan akhirnya menyerah. Serangan dengan cara Flooding bergantung kepada dua faktor yaitu: ukuran dan/atau volume (size and/or volume). Seorang attacker dapat menyebabkan Denial Of Service dengan cara melempar file berkapasitas besar atau volume yang besar dari paket yang kecil kepada sebuah system. Dalam keadaan seperti itu network server akan menghadapi kemacetan: terlalu banyak informasi yang diminta dan tidak cukup power untuk mendorong data agar berjalan. Pada dasarnya paket yang besar membutuhkan kapasitas proses yang besar pula, tetapi secara tidak normal paket yang kecil dan sama dalam volume yang besar akan menghabiskan resource secara percuma, dan mengakibatkan kemacetan. Attacker sering kali menggunakan serangan flooding ini untuk mendapatkan akses ke system yang digunakan untuk menyerang network lainnya dalam satu serangan yang dinamakan Distributed Denial Of Service(DDOS). Serangan ini seringkali dipanggil *smurf* jika dikirim melalui ICMP dan disebut *fraggles* ketika serangan ini dijalankan melewati UDP. Suatu node (dijadikan tools) yang menguatkan broadcast traffic sering disebut sebagai *Smurf Amplifiers*, tools ini sangat efektif untuk menjalankan serangan flooding. Dengan melakukan spoofing terhadap network sasaran, seorang attacker dapat mengirim sebuah request ke smurf amplifier, Network yang di amplifying(dikuatkan) akan mengirim respon kesetiap host di dalam network itu sendiri, yang berarti satu request yang dilakukan oleh attacker akan menghasilkan pekerjaan yang sama dan berulang-ulang pada network sasaran, hasil dari serangan ini adalah sebuah denial of service yang tidak meninggalkan jejak. Serangan ini dapat diantisipasi dengan cara menolak broadcast yang diarahkan pada router. TCP-level Flooding (kebanyakan SYN ATTACK) telah digunakan pada bulan february tahun 2000 untuk menyerang Yahoo!, eBay dll yang menggunakan serangan DDOS(Distributed Denial Of Service). Network yang tidak menggunakan firewall untuk pengecekan paket-paket TCP biasanya bisa diserang dengan cara ini. Beberapa

© 2005 Kelompok 123 IKI-83408T MTI UI. Silahkan menggandakan bahan ajar ini, selama tetap mencantumkan nota hak cipta ini 34

fungsi penyaringan pada firewall (Firewall Filtering Function) biasanya akan mampu untuk menahan satu serangan flooding dari sebuah alamat IP, tetapi serangan yang dilakukan melalui DDoS akan sulit di cegah karena serangan ini seperti kita ketahui datangnya dari berbagai alamat IP secara berkala. Sebenarnya salah satu cara untuk menghentikan serangan DDoS adalah dengan cara mengembalikan paket ke alamat asalnya atau juga dengan cara mematikan network(biasanya dilakukan oleh system yang sudah terkena serangan sangat parah).

e Fragmented Packet Attacks

Data-data internet yang di transmisikan melalui TCP/IP bisa dibagi lagi ke dalam paket- paket yang hanya mengandung paket pertama yang isinya berupa informasi bagian utama(kepala) dari TCP. Beberapa firewall akan mengizinkan untuk memroses bagian dari paket-paket yang tidak mengandung informasi alamat asal pada paket pertamanya, hal ini akan mengakibatkan beberapa type system menjadi crash. Contohnya, server NT akan menjadi crash jika paket-paket yang dipecah(fragmented packet) cukup untuk menulis ulang informasi paket pertama dari suatu protokol. Paket yang dipecah juga dapat mengakibatkan suasana seperti serangan flooding. Karena paket yang dipecah akan tetap disimpan hingga akhirnya di bentuk kembali ke dalam data yang utuh, server akan menyimpan paket yang dipecah tadi dalam memori kernel. Dan akhirnya server akan menjadi crash jika terlalu banyak paket-paket yang telah dipecah dan disimpan dalam memory tanpa disatukan kembali. Melalui cara enumerasi tentang topographi network sasaran, seorang attacker bisa mempunyai banyak pilihan untuk meng- crash packet baik dengan cara menguji isi firewall, load balancers atau content based routers. Dengan tidak memakai system pertahanan ini, network sasaran jauh lebih rawan untuk kerusakan dan pembobolan. Karena paket yang dipecah(fragmented packet) tidak dicatat dalam file log sebelum disatukan kembali menjadi data yang utuh, packet yang dipecah ini memberikan jalan bagi hacker untuk masuk ke network tanpa di deteksi. Telah banyak Intrusion Detection System (IDS) dan saringan firewall(firewall filters) yang memperbaiki masalah ini, tapi masih banyak juga system yang masih dapat ditembus dengan cara ini.

f E-mail Exploits

Peng-exploitasi e-mail terjadi dalam lima bentuk yaitu: mail floods, manipulasi perintah (command manipulation), serangan tingkat transportasi(transport level attack), memasukkan berbagai macam kode (malicious code inserting) dan social engineering(memfaatkan sosialisasi secara fisik). Penyerangan email bisa membuat

system menjadi crash, membuka dan menulis ulang bahkan mengeksekusi file-file aplikasi atau juga membuat akses ke fungsi fungsi perintah (command function). Serangan mail flood (flood =air bah) terjadi ketika banyak sekali e-mail yang dikirimkan oleh attacker kepada sasaran yang mengakibatkan transfer agent kewalahan menanganinya, mengakibatkan komunikasi antar program lain menjadi tidak stabil dan dapat membuat system menjadi crash. Melakukan flooding merupakan cara yang sangat kasar namun efektif, maksudnya untuk membuat suatu mail server menjadi down. Salah satu jalan yang menarik dalam melakukan serangan mail-flooding adalah dengan mengeksploitasi fungsi auto-responder (auto-responder function) yang terdapat dalam kebanyakan aplikasi email, ketika seorang attacker menemukan auto-responder yang sedang aktif dalam dua system yang berbeda, sang attacker bisa saja mengarahkan yang satu ke yang lainnya, karena kedua-duanya di set untuk merespond secara otomatis untuk setiap pesan, maka kedua-duanya akan terus mengenerate lebih banyak e-mail secara loop(bolak-balik) dan akhirnya kedua-duanya akan kelelahan dan down. Serangan memanipulasi perintah (command manipulation attack) dapat mengakibatkan sebuah system menjadi crash dengan cara menggulingkan mail transfer agent dengan sebuah buffer overflow yang diakibatkan oleh perintah (fungsi) yang cacat (contoh: EXPN atau VRFY). Perbedaan tara mail flood dan command manipulation: command manipulation meng-exploit kekuasaan milik *sendmail* yaitu memperbolehkan attacker untuk mengakses system tanpa informasi otorisasi(menjadi network admin tanpa diketahui) dan membuat modifikasi pada penjalanan program lainnya. Mengaktifkan command yang cacat seperti diatas juga dapat mengakibatkan seorang attacker mendapat akses untuk memodifikasi file, menulis ulang, dan tentunya saja membuat trojan horses pada mail server. Penyerangan tingkat transport (transport level attack) dilakukan dengan cara mengeksploit protokol perutean/pemetaan e-mail diseluruh internet: Simple Mail Transport Protocol (SMTP). Seorang attacker dapat mengakibatkan kondisi kesalahan sementara (temporary error) di target system dengan cara mengoverload lebih banyak data pada SMTP buffer sehingga SMTP buffer tidak bisa menanganinya, kejadian ini dapat mengakibatkan seorang attacker terlempar dari sendmail program dan masuk kedalam shell dengan kekuasaan administrasi bahkan dapat mengambil alih root. Beberapa serangan eksploitasi juga sering terjadi pada POP dan IMAP.

Pada saat kerawanan SMTP sulit untuk di eksploitasi, attacker mungkin saja berpindah ke serangan transport level jika ia tidak berhasil menyerang dengan cara command

manipulation ataupun mail-flood. Serangan ini lebih digunakan untuk membuat gangguan daripada untuk menjebol suatu system. Seorang attacker biasanya akan menggunakan serangan jenis untuk mem flood Exchange Server dan memotong lalu lintas e-mail (traffic e-mail). Serangan ini juga dapat digunakan untuk membuat reputasi suatu organisasi menjadi buruk dengan mengirimkan spam atau offensive e-mail ke organisasi lainnya dengan sumber dan alamat dari organisasi tersebut. Mail relaying, proses memalsukan asal/source email dengan cara meroutekannya ke arah mesin yang akan dibohongi, adalah type lain dari serangan transport-level. Teknik ini sangat berguna untuk membuat broadcasting spam secara anonymous. Berbagai macam isi(content) yang sering dikirim lewat e-mail dengan teknik ini biasanya adalah content-content yang merusak. Beberapa Virus dan Worms akan disertakan dalam e-mail sebagai file attachment yang sah, seperti variant Melissa yang nampak sebagai Ms Word Macro atau loveletter worm yang menginfeksi system dan mengemailkan dirinya sendiri ke users yang berada dalam address booknya outlook. Kebanyakan antivirus scanner akan menangkap attachment seperti ini, tetapi virus dan worm baru serta variannya masih tetap berbahaya. Serangan yang terakhir yang dilakukan oleh seorang attacker selain serangan diatas adalah dengan cara melakukan social engineering, kadang sang attacker mengirim e-mail dengan source memakai alamat admin agar users mengirimkan passwordnya untuk mengupgrade system.

g DNS and BIND Vulnerabilities

Berita baru-baru ini tentang kerawanan (vulnerabilities) tentang aplikasi Berkeley Internet Name Domain (BIND) dalam berbagai versi mengilustrasikan kerapuhan dari Domain Name System (DNS), yaitu krisis yang diarahkan pada operasi dasar dari Internet (basic internet operation). Kesalahan pada BIND sebenarnya bukanlah sesuatu yang baru. Semenjak permulaanya, standar BIND merupakan target yang paling favorite untuk diserang oleh komunitas cracker karena beberapa kerawannya. Empat kerawanan terhadap buffer overflow yang terjadi pada bulan Januari lalu hanya beberapa bagian dari kerawanan untuk dieksploitasi oleh para cracker agar mendapat akses terhadap system dan melakukan perintah dengan hak penuh (command execution privilege). Kerawanan pada BIND merupakan masalah yang sangat serius karena lebih dari 80 persen DNS yang berada di Jagat Internet dibangun menggunakan BIND. Tanpa adanya DNS dalam lingkungan Internet

Modern, mungkin transmisi e-mail akan sulit, navigasi ke situs-situs web terasa rumit dan mungkin tidak ada hal mudah lainnya yang menyangkut internet. Kerawanan BIND bukan hanya terletak pada DNS. System penerjemah alamat (number-address translator) merupakan subject dari kebanyakan exploit, termasuk untuk melakukan penyerangan di tingkat informasi, penyerangan Denial Of Service, pengambil alihan kekuasaan dengan hijacking. Penyerangan di tingkat Informasi bertujuan untuk membuat server menjawab sesuatu yang lain dari jawaban yang benar. Salah satu cara untuk melakukan serangan jenis ini adalah melalui *cache poisoning*, yang mana akan mengelabui remote name server agar menyimpan jawaban dari third-party domain dengan cara menyediakan berbagai macam informasi kepada domain server yang mempunyai otorisasi.

Semua pengimplementasian serangan terhadap DNS akan mempunyai kemungkinan besar untuk berhasil dilakukan jika jawaban dari suatu pertanyaan yang spesifik bisa dibohongi (spoof). DOS atau membuat Server tidak dapat beroperasi, bisa dilakukan dengan cara membuat DNS menyerang dirinya sendiri atau juga dengan cara mengirimkan traffic-flooding yang berlebihan dari luar, contohnya menggunakan "Smurf" ICMP flood. Jika suatu organisasi atau perusahaan memasang *authoritative name server* dalam satu segment yang terletak dibelakang satu link atau dibelakang satu physical area, maka hal ini akan menyebabkan suatu kemungkinan untuk dilakukannya serangan Denial Of Service. Cracker akan mencoba untuk menyerang system melalui DNS dengan cara buffer overflow, yaitu salah satu exploit yang sangat berpotensi pada kerawanan BIND. Gangguan exploit terjadi karena adanya kelemahan dalam pengkodean/pemrograman BIND yang mengizinkan seorang attacker untuk memanfaatkan code-code yang dapat dieksekusi untuk masuk kedalam system. Beberapa system operasi telah menyediakan patch untuk stack agar tidak dapat dieksekusi, sebagaimana juga yang dilakukan compiler (menyediakan patch) yang melindungi stack dari overflow. Mekanisme perlindungan ini stidaknya membuat cracker akan sulit menggunakan exploit. Telah jelas bahwa mengupdate system secara berkala dan menggunakan patch adalah salah satu yang harus dilakukan untuk membangun security yang efektif, jika vendor dari DNS anda tidak menyediakan patch secara berkala, anda lebih baik mengganti software DNS anda yang menyediakan patch secara berkala, tentunya untuk menjaga keamanan system. Pada system Unix , BIND harus dijalankan sebagai root untuk mengatur port yang lebih rendah (kodekode mesin). Jika software DNS dapat dibodohi untuk menjalankan

© 2005 Kelompok 123 IKI-83408T MTI UI. Silahkan menggandakan bahan ajar ini, selama tetap mencantumkan nota hak cipta ini

code-code berbahaya, atau membuka file-file milik root, user local mungkin saja bisa menaikkan kekuasaannya sendiri didalam mesin. Organisasi atau perusahaan yang mengubah authoritative server juga harus waspada bahwa mengganti server mereka dalam waktu yang bersamaan akan mengakibatkan domain mereka di hijack melalui cache poisoning. Mengubah server seharusnya dilakukan sebagai proses transisi. Untuk mencegah domain hijacking sebaiknya network admin terlebih dahulu menambahkan server barunya kedalam network infrastucture sebelum mengganti server yang lama.

h Password Attacks

Password merupakan sesuatu yang umum jika kita bicara tentang keamanan. Kadang seorang user tidak peduli dengan nomor pin yang mereka miliki, seperti bertransaksi online di warnet, bahkan bertransaksi online dirumah pun sangat berbahaya jika tidak dilengkapi dengan software security seperti SSL dan PGP. Password adalah salah satu prosedur keamanan yang sangat sulit untuk diserang, seorang attacker mungkin saja mempunyai banyak tools (secara teknik maupun dalam kehidupan sosial) hanya untuk membuka sesuatu yang dilindungi oleh password. Ketika seorang attacker berhasil mendapatkan password yang dimiliki oleh seorang user, maka ia akan mempunyai kekuasaan yang sama dengan user tersebut. Melatih karyawan/user agar tetap waspada dalam menjaga passwordnya dari social engineering setidaknya dapat meminimalisir risiko, selain berjaga-jaga dari praktek social engineering organisasi pun harus mewaspadai hal ini dengan cara teknis. Kebanyakan serangan yang dilakukan terhadap password adalah menebak (guessing), brute force, cracking dan sniffing. Penebakan(guessing) password bisa dilakukan dengan cara memasukan password satu persatu secara manual ataupun dengan bantuan script yang telah diprogram. Kebanyakan user menggunakan hal-hal yang umum untuk password mereka diantaranya tanggal lahir, dan biasanya user tidak mengkhawatirkan tentang aturan yang berlaku pada perusahaan untuk menggunakan kombinasi alphanumeric dan minimal 7 karakter. Jika saja user memakai tanggal lahirnya sebagai password maka hal penyerangan akan sangat mudah dilakukan, karena cracker tidak membutuhkan waktu yang lama hanya untuk menjebol 6 digit angka tanggal lahir. Beberapa user atau bahkan administrator dapat membuat pekerjaan cracker menjadi mudah andai saja mereka lupa untuk merubah password default dari sebuah software. Sebenarnya, password guessing merupakan sesuatu yang sangat tidak efektif, dan dapat menghabiskan waktu. Network admin bisa dengan mudah mendetect serangan jika

seorang attacker mencoba login dengan menebak password berkali-kali. Brute-force merupakan serangan yang menggunakan logika yang sama dengan password guessing tetapi serangan brute-force lebih cepat dan lebih powerful. Dalam tipe serangan ini seorang attacker menggunakan script (biasanya program cracking gratis) yang akan mencoba password-password umum(biasanya terdapat dalam dictionary). Tujuan dari serangan jenis ini adalah untuk mempercepat penemuan password sebelum network admin menyadari adanya serangan. Walaupun serangan Brute-force lebih efisien daripada password guessing, kedua teknik tersebut pada dasarnya sama. Attacker umumnya lebih sulit untuk berhasil dengan kedua metoda tersebut. Lebih jauh lagi, kedua teknik tersebut sangat mudah di lawan dengan memanfaatkan features *blacklisting*, yang akan mengunci sebuah account user jika seseorang(attacker) berkali-kali memasukkan password secara tidak tepat. Contohnya, default blacklist dalam system unix adalah tiga kali (kesempatan memasukkan password).

Kelemahan dari perlindungan blacklist adalah bahwa feature blacklist ini dapat igunkan untuk menyerang system oleh attacker. Sebagai contoh, jika seorang attacker dapat mengidentifikasi siapa login name untuk network admin, sang attacker bisa saja menngunakan login name itu dan memasukkan password yang salah berulang kali dan akhirnya mengunci account admin .. Ketika sang admin sedang berusaha untuk mendapatkan aksesnya kembali, seorang attacker masih bisa untuk berhubungan dengan system. Password cracking adalah metoda untuk melawan perlindungan password yang dienkripsi yang berada di dalam system. Dengan anggapan bahwa atacker telah masuk kedalam system, ia bisa saja mengubah kekuasaannya didalam system dengan cara meng crack password file menggunakan metode *brute-force dictionary attack* (mencocokkan kata-kata yang berada dalam kamus dengan kata-kata yang dienkripsi dalam file password). Keberhasilan menggunakan cara ini bergantung pada kecepatan prosesor dan

program yang dimiliki oleh attacker. Cara yang terbaik untuk menghindari serangan jenis ini adalah dengan memonitor kewenangan akses pada file.

Dengan cara mengintip lalulintas pada port telnet(23) ataupun HTTPD (80), seorang attacker dapat mendapatkan password yang digunakan untuk internet dan koneksi secara remote melalui proses yang dinamakan password sniffing. Cara inilah yang paling mudah dilakukan karena kedua koneksi tersebut tidak menggunakan enkripsi, kecuali koneksi yang menggunakan SSL (secure socket layer) pada HTTPD(biasanya

ada tanda gembok terkunci dibawah browser, yang menandakan transaksi aman) atau juga menggunakan SSH (Secure SHell) untuk koneksi ke mesin lain secara remote.

i Proxy Server Attacks

Salah satu fungsi Proxy server adalah untuk mempercepat waktu response dengan cara menyatukan proses dari beberapa host dalam suatu trusted network. Dalam kebanyakan kasus, tiap host mempunyai kekuasaan untuk membaca dan menulis (read/write) yang berarti apa yang bisa saya lakukan dalam sistem saya akan bisa juga saya lakukan dalam system anda dan sebaliknya. Jika firewal yang berada dalam trusted network tidak dikonfigurasi secara optimal, khususnya untuk memblok akses dari luar, apalagi jika autentikasi dan enkripsi tidak digunakan, seorang attacker bisa menyerang proxy server dan mendapatkan akses yang sama dengan anggota trusted network lainnya. Jika attacker sudah masuk ke sistem ia tentunya bisa melakukan apa saja dan ia bisa melakukan DDOS(distributed denial of service) secara anonymous untuk menyerang network lain.Router yang tidak dikonfigurasi secara optimal juga akan berfungsi sebagai proxy server dan akan mengakibatkan kerawanan yang sama dengan proxy server.

j Remote Command Processing Attacks

Trusted Relationship antara dua atau lebih host menyediakan fasilitas pertukaran informasi dan *resource sharing*. Sama halnya dengan proxy server, trusted relationship memberikan kepada semua anggota network kekuasaan akses yang sama di satu dan lain system (dalam network). Attacker akan menyerang server yang merupakan anggota dari trusted system. Sama seperti kerawanan pada proxy server, ketika akses diterima, seorang attacker akan mempunyai kemampuan mengeksekusi perintah dan mengakses data yang tersedia bagi user lainnya.

k Remote File System Attack

Protocol-protokol untuk transportasi data –tulang punggung dari internet— adalah tingkat TCP (TCPLLevel) yang mempunyai kemampuan dengan mekanisme untuk baca/tulis (read/write) Antara network dan host. Attacker bisa dengan mudah mendapatkan jejak informasi dari mekanisme ini untuk mendapatkan akses ke direktori file. Tergantung pada OS (operating system) yang digunakan, attacker bisa meng extract informasi tentang network, sharing privileges, nama dan lokasi dari user dan groups, dan spesifikasi dari aplikasi atau banner (nama dan versi software).

System yang dikonfigurasi atau diamankan secara minimal akan dengan mudah membeberkan informasi ini bahkan melalui firewall sekalipun. Pada system UNIX,
© 2005 Kelompok 123 IKI-83408T MTI UI. Silahkan menggandakan bahan ajar ini, selama tetap 41
mencantumkan nota hak cipta ini

informasi ini dibawa oleh NFS (Network File System) di port 2049. system Windows menyediakan data ini pada SMB (server messaging block) dan Netbios pada port 135 - 139(NT) dan port 445 pada win2k. Network administrator bisa meminimalisasi resiko yang akan terjadi dengan menggunakan Protokol-protokol tersebut dengan memberikan sedikit peraturan. Network dengan system windows, harusnya memblokir akses ke port 139 dan 445 dari luar network, jika dimungkinkan. Dalam system unix port 2049 seharusnya diblok, sharing file dibatasi dan permintaan file melalui *showmount*(perintah dalam unix) seharusnya dicatat dalam log.

l Selective Program Insertions

Selective Program Insertions adalah serangan yang dilakukan ketika attacker menaruh program-program

penghancur, seperti virus, worm dan trojan (mungkin istilah ini sudah anda kenal dengan baik .) pada system sasaran. Program-program penghancur ini sering juga disebut malware. Program-program ini mempunyai kemampuan untuk merusak system, pemusnahan file, pencurian password sampai dengan membuka backdoor. Biasanya antivirus yang dijual dipasaran akan dapat mendeteksi dan membersihkan program-program seperti ini, tetapi jika ada virus baru (anggap saja variant melissa) virus scanner belum tentu dapat menghadapi script-script baru. Beberapa network administrator melakukan pertahanan terhadap malware dengan teknologi alternatif seperti *behaviour blockers*, yang memberhentikan kode-kode yang dicurigai berdasarkan contoh kelakuan malware, bukan berdasarkan signature. Beberapa aplikasi lainnya akan mengkarantina virus dan code-code yang dicurigai didalam daerah yang dilindungi, biasanya disebut *sandboxes*.

m Port Scanning

Melalui port scanning seorang attacker bisa melihat fungsi dan cara bertahan sebuah system dari berbagai macam port. Seorang atacker bisa mendapatkan akses kedalam sistem melalui port yang tidak dilindungi. Sebaia contoh, scanning bisa digunakan untuk menentukan dimana default SNMP string di buka untuk publik, yang artinya informasi bisa di extract untuk digunakan dalam *remote command attack*.

n TCP/IP Sequence Stealing, Passive Port Listening and Packet Interception

TCP/IP Sequence Stealing, Passive Port Listening dan Packet Interception berjalan untuk mengumpulkan informasi yang sensitif untuk mengkases network. Tidak seperti serangan aktif maupun brute-force, serangan yang menggunakan metoda ini

mempunyai lebih banyak kualitas *stealth-like*. TCP/IP Sequence Stealing adalah pemetaan dari urutan nomor-nomor (angka), yang bisa membuat packet milik attacker terlihat legal. Ketika suatu system meminta sesi terhadap mesin lain, kedua system tersebut saling bertukar nomor-nomor sinkronisasi TCP. Jika tidak dilakukan secara acak, Attacker bisa mengenali algoritma yang digunakan untuk meng-generate nomor-nomor ini. Urutan nomor yang telah dicuri bisa digunakan attacker untuk menyamar menjadi salah satu dari system tadi, dan akhirnya memperbolehkannya untuk melewati firewall. Hal ini sebenarnya efektif jika digunakan bersama IP Spoofing. Melalui passive port listening, seorang attacker dapat memonitor dan mencatat (log) semua pesan dan file yang dikirim ke semua port yang dapat diakses pada target system untuk menemukan titik kerawanan.

Packet Interception adalah bagian (tepatnya pelapis) dari active listener program yang berada pada port di system sasaran yang berfungsi untuk menerima ataupun mengembalikan semua tipe pesan (data) spesifik yang dikirim. Pesan tersebut bisa dikembalikan ke unauthorized system, dibaca dan akhirnya dikembalikan lagi baik tanpa perubahan atau juga dengan perubahan kepada attacker, atau bahkan tidak dikembalikan.

Dalam beberapa versi atau juga menurut konfigurasi dari user SSHD(secured shell daemon), otentikasi bisa dilakukan dengan cara menggunakan public key (milik mesin tentunya). Jika seorang attacker mempelajari public key yang digunakan, ia bisa menciptakan atau memasukan paket-paket palsu. System sasaran akan menganggap pengirim paket palsu tersebut mempunyai hak akses.

o HTTPD Attacks

Kerawanan yang terdapat dalam HTTPD ataupun webserver ada lima macam: buffer overflows, httpd bypasses, cross scripting, web code vulnerabilities, dan URL floods. HTTPD Buffer Overflow bisa terjadi karena attacker menambahkan errors pada port yang digunakan untuk web traffic dengan cara memasukan banyak carackter dan string untuk menemukan tempat overflow yang sesuai. Ketika tempat untuk overflow ditemukan, seorang attacker akan memasukkan string yang akan menjadi perintah yang dapat dieksekusi. Bufer-overflow dapat memberikan attacker akses ke command prompt. Beberapa feature dari HTTPD bisa digunakan untuk meciptakan HTTPD byapass, memberi akses ke server menggunakan fungsi logging. Dengan cara ini, sebuah halaman web bisa diakses dan diganti tanpa dicatat oleh web server. Cara ini sering digunakan oleh para cracker, hacktivist dan cyber vandals untuk mendeface

website. Sedangkan kerawanan pada script-script web bisa terjadi pada semua bahasa pemrograman web dan semua ekstensi aplikasi. Termasuk VB, Visual C++, ASP, TCL, Perl, PHP, XML, CGI dan Coldfusion. Pada dasarnya, attacker akan mengeksploitasi kelemahan dari sebuah aplikasi, seperti CGI script yang tidak memeriksa input atau kerawanan pada IIS RDS pada showcode.asp yang mengizinkan menjalankan perintah secara remote (remote command priviledges). Melalui cross scripting dan cross-site scripting seorang attacker bisa mengeksploitasi pertukaran cookies antara browser dan webserver. Fasilitas ini dapat mengaktifkan script untuk merubah tampilan web dll. Script ini bisa menjalankan malware, membaca informasi penting dan meng expose data sensitive seperti nomor credit card dan password.

Pada akhirnya attacker dapat menjalankan denial of service dengan URL flood, yang dilakukan dengan cara mengulang dan terus mengulang permintaan terhadap port 80 httpd yang melalui batas TTL (time to live). Beberapa user ataupun manager mungkin benci mendengar serangan-serangan tersebut. Tapi pada kenyataanya memang tidak ada yang benar-benar fix untuk mengamankan network ataupun website. Keamanan adalah suatu proses, bukan produk. Jika anda memasang firewall, IDSes(instrusion detectionsystem), routers dan honeypots (system untuk jebakan) mungkin dapat menyediakan lapisan-lapisan untuk bertahan, tetapi sekali lagi peralatan paling canggih di dunia tidak akan menolong suatu organisasi sampai organisasi tersebut mempunyai proses untuk mengupgrade system, memakai patch, mengecek security pada system sendiri dan metode lain. Telah banyak perusahaan yang memakai IDSes tetapi tidak memonitor file log, mereka menginstall firewall, tetapi tidak mengupgradenya. Jalan terbaik untuk melindungi website maupun network dari serangan adalah mendekati keamanan sebagaimana tantangan yang sedang terjadi terhadap keamanan itu sendiri, terus berusaha, selalu ingat basicnya dan jangan lupa untuk berdoa...:)

IV.2 Denial of Service (DoS)

Denial of Service adalah aktifitas menghambat kerja sebuah layanan (servis) atau mematikan-nya, sehingga user yang berhak/berkepentingan tidak dapat menggunakan layanan tersebut. Dampak akhir dari aktifitas ini menjurus kepada terhambatnya aktifitas korban yang dapat berakibat sangat fatal (dalam kasus tertentu). Pada dasarnya Denial of Service merupakan serangan yang sulit diatasi, hal ini disebabkan oleh resiko layanan publik dimana admin akan berada pada kondisi yang

membbingungkan antara layanan dan kenyamanan terhadap keamanan. Seperti yang kita tahu, keyamanan berbanding terbalik dengan keamanan. Maka resiko yang mungkin timbul selalu mengikuti hukum ini.

Beberapa aktifitas DoS adalah:

1. Aktifitas 'flooding' terhadap suatu server.
2. Memutuskan koneksi antara 2 mesin.
3. Mencegah korban untuk dapat menggunakan layanan.
4. Merusak sistem agar korban tidak dapat menggunakan layanan.

IV.2.1 Motif penyerang melakukan Denial of Service

Menurut Hans Husman (t95hhu@student.tdb.uu.se), ada beberapa motif cracker dalam melakukan Denial of Service yaitu:

- Status Sub-Kultural.
- Untuk mendapatkan akses.
- Balas dendam.
- Alasan politik.
- Alasan ekonomi.
- Tujuan kejahatan/keisengan.

Status subkultural dalam dunia hacker, adalah sebuah unjuk gigi atau lebih tepat kita sebut sebagai pencarian jati diri. Adalah sebuah aktifitas umum dikalangan hacker-hacker muda untuk menunjukkan kemampuannya dan Denial of Service merupakan aktifitas hacker diawal karirnya. Alasan politik dan ekonomi untuk saat sekarang juga merupakan alasan yang paling relevan. Kita bisa melihat dalam 'perang cyber' (cyber war), serangan DoS bahkan dilakukan secara terdistribusi atau lebih dikenal dengan istilah 'distribute Denial of Service'. Beberapa kasus serangan virus semacam 'code-red' melakukan serangan DoS bahkan secara otomatis dengan memanfaatkan komputer yang terinfeksi, komputer ini disebut 'zombie' dalam jargon.

Lebih relevan lagi, keisengan merupakan motif yang paling sering dijumpai. Bukanlah hal sulit untuk mendapatkan program-program DoS, seperti nestea, teardrop, land, boink, jolt dan vadim. Program-program DoS dapat melakukan serangan Denial of Service dengan sangat tepat, dan yang terpenting sangat mudah untuk melakukannya. Cracker cukup mengetikkan satu baris perintah pada Linux Shell yang berupa `./nama_program argv argc ...`

IV.2.2 Denial of Service, serangan yang menghabiskan resource

Pada dasarnya, untuk melumpuhkan sebuah layanan dibutuhkan pemakaian resource yang besar, sehingga komputer/mesin yang diserang kehabisan resource dan menjadi hang. Beberapa jenis resource yang dihabiskan diantaranya:

- a Swap Space
- b Bandwidth
- c Kernel Tables
- d RAM
- e Disk
- f Caches
- g INETD

a Swap Space

Hampir semua sistem menggunakan ratusan MBs spasi swap untuk melayani permintaan client. Spasi swap juga digunakan untuk mem-'forked' child process. Bagaimanapun spasi swap selalu berubah dan digunakan dengan sangat berat. Beberapa serangan Denial of Service mencoba untuk memenuhi (mengisi) spasi swap ini.

b Bandwidth

Beberapa serangan Denial of Service menghabiskan bandwidth.

c Kernel Tables

Serangan pada kernel tables, bisa berakibat sangat buruk pada sistem. Alokasi memori kepada kernel juga merupakan target serangan yang sensitif. Kernel memiliki kernelmap limit, jika sistem mencapai posisi ini, maka sistem tidak bisa lagi mengalokasikan memory untuk kernel dan sistem harus di re-boot.

d RAM

Serangan Denial of Service banyak menghabiskan RAM sehingga sistem mau-tidak mau harus di re-boot.

e Disk

Serangan klasik banyak dilakukan dengan memenuhi Disk.

f Caches

g INETD

Sekali saja INETD crash, semua service (layanan) yang melalui INETD tidak akan bekerja.

IV.2.3 Teknik Melakukan Denial of Service

Melakukan DoS sebenarnya bukanlah hal yang sulit dilakukan. Berhubung DoS merupakan dampak buruk terhadap sebuah layanan publik, cara paling ampuh untuk menghentikannya adalah menutup layanan tersebut. Namun tentu saja hal ini tidak mengasikkan dan juga tidak begitu menarik. Kita akan bahas tipe-tipe serangan DoS.

1. SYN-Flooding

SYN-Flooding merupakan network Denial ofService yang memanfaatkan 'loophole' pada saat koneksi TCP/IP terbentuk. Kernel Linux terbaru (2.0.30 dan yang lebih baru) telah mempunyai option konfigurasi untuk mencegah Denial of Service dengan mencegahmenolak cracker untuk mengakses sistem.

2. Pentium 'FOOF' Bug

Merupakan serangan Denial of Service terhadap prosessor Pentium yang menyebabkan sistem menjadi reboot. Hal ini tidak bergantung terhadap jenis sistem operasi yang digunakan tetapi lebih spesifik lagi terhadap prosessor yang digunakan yaitu pentium. Ping Flooding Ping Flooding adalah brute force Denial of Service sederhana. Jika serangan dilakukan oleh penyerang dengan bandwidth yang lebih baik dari korban, maka mesin korban tidak dapat mengirimkan paket data ke dalam jaringan (network). Hal ini terjadi karena mesin korban di banjiri (flood) oleh peket-paket ICMP. Varian dari serangan ini disebut "smurfing" (<http://www.quadrunner.com/~chuegen/smurf.txt>).

3. Serangan menggunakan exploits.

Beberapa hal yang harus dipahami sebelum melakukan serangan ini adalah:

1. Serangan membutuhkan Shell Linux (Unix/Comp)
2. Mendapatkan exploits di: <http://packetstormsecurity.nl> (gunakan fungsi search agar lebih mudah)
3. Menggunakan/membutuhkan GCC (Gnu C Compiler) diantaranya:
 - a KOD (Kiss of Death)

Merupakan tool Denial of Service yang dapat dugunakan untuk menyerang Ms.Windows pada port 139 (port netbios-ssn). Fungsi utama dari tool ini adalah membuat hang/blue screen of death pada komputer korban.

Cara penggunaan:

Dapatkan file kod.c

Compile dengan Gcc: `$ gcc -o kod kod.c`

Gunakan: \$ kod [ip_korban] -p [port] -t [hits]

Kelemahan dari tool ini adalah tidak semua serangan berhasil, bergantung kepada jenis sistem operasi dan konfigurasi server target (misalnya: blocking)

b BONG/BOINK

Bong adalah dasar dari teardrop (teardrop.c). Boink merupakan Improve dari bonk.c yang dapat membuat crash mesin MS. Windows 9x dan NT

c Jolt

Jolt sangat ampuh sekali untuk membekukan Windows 9x dan NT. Cara kerja Jolt yaitu mengirimkan serangkaian series of spoofed dan fragmented ICMP Packet yang tinggi sekali kepada korban.

d NesTea

Tool ini dapat membekukan Linux dengan Versi kernel 2.0. kebawah dan Windows versi awal. Versi improve dari NesTea dikenal dengan NesTea2

e NewTear

Merupakan varian dari teardrop (teardrop.c) namun berbeda dengan bonk (bonk.c)

f Syndrop

Merupakan 'serangan gabungan' dari TearDrop dan TCP SYN Flooding.

Target serangan adalah Linux dan Windows

g TearDrop

TearDrop mengirimkan paket Fragmented IP ke komputer (Windows) yang terhubung ke jaringan (network). Serangan ini memanfaatkan overlapping ip fragment, bg yang terdapat pada Windowx 9x dan NT. Dampak yang timbul dari serangan ini adalah Blue Screen of Death

BAB V Daftar Pustaka

1. Krutz, Ronal L and Vines, Russel. 2003. The CISSP Prep Guide - Gold Edition. Indianapolis. Wiley Publishing
2. Thomas, Tom. 2005. Network Security - First Step (Indonesian Edition). Yogyakarta. ANDI Yogyakarta
3. Husman, Hans. 2000. Introduction to Denial of Service. t95hhu@student.tdb.uu.se
4. Aji, R. Kresno, Hartanto, Agus, iswanto, Deny dan Chandra, Tomi. 2000. Kejahatan Internet, Trik Aplikasi dan Tip Penanggulangannya. Jakarta. Elexmedia Komputindo.
5. Reza, Muhammad. 2003. 15 Serangan Hacker. Artikel Populer Ilmu Komputer. <http://www.ilmukomputer.com>
6. <http://www.ai3.itb.ac.id/Tutorial/LAN.html>
7. <http://www.w3.org/TR/REC-html40>