BAB II

TINJAUAN PUSTAKA

II.1. Definisi Jaringan Komputer

Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan. Informasi dan data bergerak melalui kabel-kabel atau tanpa 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. Setiap komputer, printer atau *periferal* yang terhubung dengan jaringan disebut *node*. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan *node*.

II.1.1 Jenis Jaringan Komputer

Secara umum jaringan komputer dibagi atas lima jenis, yaitu:

1. Local Area Network (LAN)

   Local Area Network (LAN), merupakan jaringan milik pribadi di dalam ssebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumberdaya (misalnya printer) dan saling bertukar informasi.

2. Metropolitan Area Network (MAN)

   Metropolitan Area Network (MAN), pada dasarnya merupakan versi LAN

yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.

3. Wide Area Network (WAN)

   Wide Area Network (WAN), jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai.

4. Internet

   Sebenarnya terdapat banyak jaringan didunia ini, seringkali menggunakan perangkat keras dan perangkat lunak yang berbeda-beda. Orang yang terhubung ke jaringan sering berharap untuk bisa berkomunikasi dengan orang lain yang terhubung ke jaringan lainnya. Keinginan seperti ini memerlukan hubungan antar jaringan yang seringkali tidak kampatibel dan berbeda. Biasanya untuk melakukan hal ini diperlukan sebuah mesin yang disebut *gateway* guna melakukan hubungan dan melaksanakan terjemahan yang diperlukan, baik perangkat keras maupun perangkat lunaknya. Kumpulan jaringan yang terinterkoneksi inilah yang disebut dengan internet.

5. Jaringan Tanpa Kabel (*Nirkable*)

   Jaringan tanpa kabel merupakan suatu solusi terhadap komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel. Misalnya orang yang

ingin mendapat informasi atau melakukan komunikasi walaupun sedang berada diatas mobil atau pesawat terbang, maka mutlak jaringan tanpa kabel diperlukan karena koneksi kabel tidaklah mungkin dibuat di dalam mobil atau pesawat. Saat ini jaringan tanpa kabel sudah marak digunakan dengan memanfaatkan jasa satelit dan mampu memberikan kecepatan akses yang lebih cepat dibandingkan dengan jaringan yang menggunakan kabel.

II.1.2 Network Monitoring

Network Monitoring atau Sistem Pemantau Jaringan adalah aplikasi program yang dipergunakan untuk mengetahui ada tidaknya celah keamanan dalam suatu sistem. Network Monitoring biasanya dilakukan dengan menggunakan SNMP *(Simple Network Management Protocol).* Hal-hal yang bakal dimonitoring dalam network tentunya akan sangat kompoleks, dan sistem monitoring yang baik seharusnya menyediakan history dan log yang memungkinkan kita membuat laporan, statistik dan graph dari masing-masing object yang dimonitoring sehingga sistem yang digunakan memberikan kontribusi penuh dalam pendeteksian secara dini terhadap kemungkinan masalah-masalah yang timbul.

II.2. Komponen – Komponen Dari Sistem Jaringan

Sistem jaringan komputer merupakan kumpulan hardware dan software yang sesuai (compatible) yang disusun untuk mengkomunikasikan berbagai macam informasi dari satu lokasi ke lokasi yang lain Fungsi dari sistem

telekomunikasi adalah untuk mengirim dan menerima data dari satu lokasi ke lokasi yang lain Protocol adalah sekumpulan aturan dan prosedur yang mengatur transmisi data antara dua terminal dalam satu sistem jaringan.

Jaringan Komputer tersusun dari beberapa elemen dasar yang meliputi komponen hardware dan software, yaitu :

1. Komponen *Hardware*

   Personal Komputer (PC) , Network Interface Card (NIC), Kabel dan topologi jaringan.

2. Komponen *Software*

   Sistem Operasi Jaringan, Network Adapter Driver, Protokol Jaringan.

II.3. Jenis Serangan Pada Sebuah Jaringan

Berikut ini akan dijelaskan beberapa jenis serangan yang dapat dilancarkan oleh pihak-pihak tertentu terhadap sebuah jaringan komputer :

1. Dos/Ddos

   Denial of Services dan *Distributed Denial of Services* adalah sebuah metode serangan yang bertujuan untuk menghabiskan sumber daya sebuah peralatan jaringan komputer sehingga layanan jaringan komputer menjadi terganggu. Salah satu bentuk serangan ini adalah '*Syn Flood Attack*' yang mengandalkan kelemahan dalam sistem *there way handshake* adalah proses awal dalam melakukan koneksi dengan protocol TCP. Proses ini di mulai dengan pihak klien mengirimkan paket dengan tanda SYN. Lalu kemudian pihak server

akan menjawab dengan mengirimkan paket dengan tanda SYN dan ACK. Terakhir pihak klien akan mengrimkan paket ACK.

Jenis serangan ini bertujuan untuk menghentikan layanan yang diberikan oleh server tersebut sehingga terjadi gangguan terhadap layanan atau jaringan komputer tersebut. Tipe serangan semacam ini disebut sebagai Denial of Service (DoS) attack. LAND attack dikategorikan sebagai serangan SYN (SYN attack) karena menggunakan packet SYN (synchronization) pada waktu melakukan 3-way handshake untuk membentuk suatu hubungan berbasis TCP/IP. Dalam 3-way handshake untuk membentuk hubungan TCP/IP antara client dengan server.

2. Packet Sniffing

Packet Sniffing adalah sebuah metode serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi, baik itu media kabel maupun radio. Setelah paket-paket yang lewat itu didapatkan, paket-paket tersebut kemudian disusun ulang sehingga data yang dikirimkan oleh sebuah pihak dapat dicuri oleh pihak yang tidak berwenang.

Hal ini dapat dilakukan karena pada dasarnya semua koneksi *ethernet* adalah koneksi yang bersifat *broadcast*, di mana semua *host* dalam sebuah kelompok jaringan akan menerima paket yang dikirimkan oleh sebuah *host*. Pada keadaan normal, hanya *host* yang menjadi tujuan paket yang akan memproses paket tersebut sedangkan *host* yang lainnya akan mengacuhkan paket-paket tersebut. Namun pada keadaan tertentu, sebuah *host* bisa merubah konfigurasi

sehingga *host* tersebut akan memproses semua paket yang dikirimkan oleh *host* lainnya.

3. DNS Forgery (Manipulasi Folder Dan File)

Salah satu cara yang dapat dilakukan oleh seseorang untuk mencuri data-data penting orang lain adalah dengan cara melakukan penipuan. Salah satu bentuk penipuan yang bisa dilakukan adalah penipuan data-data DNS. DNS adalah sebuah sistem yang akan menterjemahkan nama sebuah situs atau *host* menjadi alamat IP situs atau *host* tersebut. Cara kerja DNS cukup sederhana, yaitu sebuah *host* mengirimkan paket (biasanya dengan tipe UDP) yang pada *header* paket tersebut berisikan alamat *host* pengirim, alamat DNS *resolver*, pertanyaan yang diinginkan serta sebuah nomor identitas. DNS *resolver* akan mengirimkan paket jawaban yang sesuai ke pengirim. Pada paket jawaban tersebut terdapat nomor identitas, yang dapat dicocokkan oleh pengirim dengan nomor identitas yang dikirimnya. Oleh karena cara kerja yang sederhana dan tidak adanya metode otentikasi dalam sistem komunikasi dengan paket UDP, maka sangat memungkinkan seseorang untuk berpura-pura menjadi DNS *resolver* dan mengirimkan paket jawaban palsu dengan nomor identitas yang sesuai ke penanya sebelum paket jawaban dari DNS *resolver* resmi diterima oleh penanya. Dengan cara ini, seorang penyerang dapat dengan mudah mengarahkan seorang pengguna untuk melakukan akses ke sebuah layanan palsu tanpa diketahui pengguna tersebut. Sebagai contoh, seorang penyerang dapat mengarahkan seorang

pengguna *Internet Banking* untuk melakukan akses ke situs *Internet Banking* palsu yang dibuatnya untuk mendapatkan data-data pribadi dan kartu kredit pengguna tersebut. Untuk dapat melakukan gangguan dengan memalsukan data DNS, seseorang membutuhkan

informasi-informasi di bawah ini :

a. Nomor identitas pertanyaan (16 *bit*)

b. Port tujuan pertanyaan

c. Alamat IP DNS *resolver*

d. Informasi yang ditanyakan

e. Waktu pertanyaan.

4. DNS Cache Poisoning

Bentuk lain serangan dengan menggunkan DNS adalah *DNS Cache Poisoning*. Serangan ini memanfaatkan cache dari setiap server DNS yang merupakan tempat penyimpanan sementara data-data domain yang bukan tanggung jawab *server DNS* tersebut. Sebagai contoh, sebuah organisasi X memiliki *server DNS* (ns.x.org) yang menyimpan data mengenai domain x.org. Setiap komputer pada organisasi X akan bertanya pada server (ns.x.org) setiap kali akan melakukan akses internet. Setiap kali server ns.x.org menerima pertanyaan diluar domainx.orgserver tersebut akan bertanya pada pihak otoritas domain. Setelah mendapatkan jawaban yang dibutuhkan, jawaban tersebut akan disimpan dalam *cache*, sehingga jika ada pertanyaan yang sama, server ns.x.org dapat langsung memberikan jawaban yang benar. Dengan tahapan – tahapan tertentu, seorang

penyerang dapat mengirimkan data – data palsu mengenai sebuah domain yang kemudian akan disimpan di *cache* sebuah server DNS, sehingga apabila server tersebut menerima pertanyaan mengenai domain tersebut, server akan memberikan jawaban yang salah. Patut dicatat, bahwa dalam serangan ini, data asli server DNS tidak mengalami perubahan sedikitpun. Perubahan hanya terjadi pada *cache* server DNS tersebut.

II.4. Pengertian Serangan Pada Komputer

Definisinya serangan komputer adalah kejahatan yang berkaitan dengan komputer. Hal ini berhubungan dengan computer abuse (penyalah gunaan komputer), computer crime (kejahatan komputer) dan computer relater crime (kejahatan yang berhubungan dengan komputer). Computer abuse merupakan tindakan sengaja dengan melibatkan komputer dimana satu pelaku kejahatan atau lebih dapat memperoleh keuntungan atau korban (satu atau lebih) dapat menderita kerugian. Computer crime merupakan tindakan melanggar hukum di mana pengetahuan tentang komputer sangat penting agar pelaksanaannya berjalan dengan baik. Computer related crime adalah kejahatan yang berkaitan dengan komputer tidak terbatas pada kejahatan bisnis, kerah putih atau ekonomi. Kejahatan itu mencakup kejahatan yang menghancurkan komputer atau isinya atau membahayakan kehidupan dan kesejahteraan manusia karena semua tergantung apakah komputer dapat bekerja dengan benar atau tidak. Kejahatan komputer itu dapat dikatagorikan sebagai “White Collar Crime” yang dalam beroperasinya lebih banyak menggunakan pikiran/otak. Kejahatan ini sangat sulit

untuk diberantas, dikarenakan banyak faktor, diantaranya yaitu: Penanganan yang kurang serius, Pada umumnya kejahatan komputer dilakukan oleh orang-orang yang teramat fanatik terhadap komputer.

II.5. Cara Kerja DNS Frogery (Manipulasi Folder Dan File)

Dalam trik DNS Frogery adalah, Yaitu Melakukan penipuan data data DNS karena cara kerja DNS adalah sederhana yaitu sebuah host mengirimkan paket (biasanya tipe UDP) yang pada *header* paket tersebut berisikan alamat host penanya, alamat DNS *resolver*, pertanyaan yang diinginkan dan sebuah nomor id, DNS akan mengirimkan jawaban sesuai dengan pertanyaan.karena sistem yang begitu sederhana seorang penyerang dapat berpura pura menjadi DNS Dengan cara ini , maka seorang penyerang dapat mengarahkan seorang korban ke sebuah layanan palsu tanpa diketahui oleh pengguna tersebut. pertnayaan yang sangat karakteristik adalah

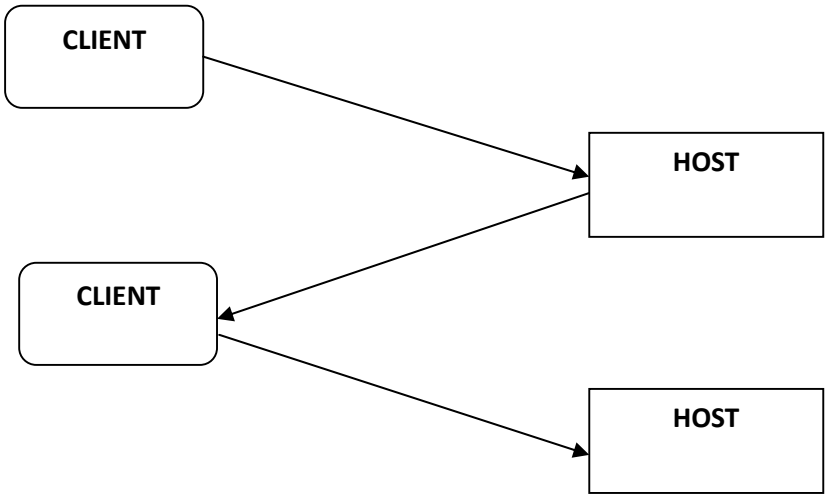
1.Nomor ID pertanyaan.

2. Port tujuan pertanyaan

3. Alamat IP DNS resolver

4. Informasi yang di tanyakan

5. Waktu Pertanyaan



Gambar II.1. Ilustrasi Cara Kerja DNS Frogery
Sumber : Web Hacking Serangan Dan Pertahanan, 2006

1. Pertama, *client* mengirimkan sebuah paket SYN ke server/host untuk membentuk hubungan TCP/IP antara client dan host.
2. Kedua, host menjawab dengan mengirimkan sebuah paket SYN/ACK (Synchronization/Acknowledgement) kembali ke client.
3. Akhirnya, client menjawab dengan mengirimkan sebuah paket ACK (Acknowledgement) kembali ke host. Dengan demikian, hubungan TCP/IP antara client dan host terbentuk dan transfer data bisa dimulai Dalam sebuah DNS Frogery, komputer penyerang yang bertindak sebagai client mengirim sebuah paket SYN yang telah direkayasa atau dispoof ke suatu server yang hendak diserang. Paket SYN yang telah direkayasa atau dispoof ini berisikan alamat asal (*source address*) dan nomer port asal (source *port* number) yang sama persis dengan alamat tujuan (destination address) dan nomer port tujuan (destination port number). Dengan demikian, pada

waktu host mengirimkan paket SYN/ACK kembali ke client, maka terjadi suatu infinite loop karena host sebetulnya mengirimkan paket SYN/ACK tersebut ke dirinya sendiri.

II.6. Konsep UML (*Unified Modelling Language*)

Menurut Munawar (2005 : 17) *Unified Modelling Language (UML)* adalah salah satu alat bantu yang sangat handal di dunia pengembangan sistem yang berorientasi obyek. Hal ini disebabkan karena UML menyediakan bahasa pemodelan visual yang memungkinkan bagi pengembangan sistem untuk membuat cetak biru atas visi mereka dalam bentuk yang baku, mudah dimengerti serta dilengkapi dengan mekanisme yang efektif untuk berbagi *(sharing)* dan mengkomunikasikan rancangan mereka dengan yang lain.

UML adalah hasil kerja dari konsorsium berbagai organisasi yang berhasil dijadikan sebagai standar baku dalam OOAD (*Object Oriented Analysis* dan *Design*). UML tidak hanya domain dalam penotasian dilingkungan OO tetapi juga populer di luar lingkungan OO. Ada tiga karakter penting yang melekat di UML yaitu sketsa, cetak biru dan bahasa *pemrograman*. Sebagai sebuah sketsa UML bisa berfungsi sebagai sebuah cetak biru karena sangat lengkap dan detil. Dengan cetak biru ini maka akan bisa diketahui informasi detil tentang coding program (*Forward engineering*) atau bahkan membaca program dan mengimplementasikannya kembali ke dalam diagram (*reverse engineering*). *Reverse engineering* sangat berguna pada situasi dimana kode program yang tidak terdokkumentasi asli hilang atau bahkan belum perna dibuat sama sekali. Sebagai

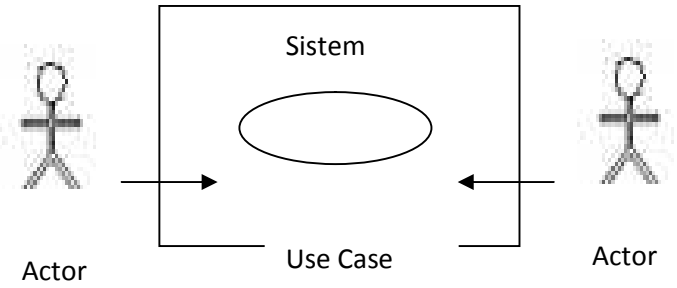
bahasa pemrograman, UML dapat diterjemahkan diagram yang ada di UML menjadi kode program siap untuk dijalankan.

UML dibangun atas model 4+1 *view*. Model ini didasarkan pada fakta bahhwa struktur sebuah sistem dideskripsikan dalam *view* dimana salah satu diantaranya *use case view*. *use case view* ini memegang peran khusus untuk mengintegrasikan *content* ke *view* yang lain

II.6.1. Diagram – Diagram Pada Metode UML

1. *Use Case Diagram*

   Use case adalah alat bantu terbaik guna menstimulasikan pengguna potensial untuk mengatakan tentang suatu sistem dari sudut pandangnya. Tidak selalu mudah bagi pengguna untuk menyatakan bagaimana mereka bermaksud menggunakan sebuah sistem. Ide dasarnya adalah bagaimana melibatkan penggunaan sistem di fase – fase awal analisis dan perancangan sistem. Diagram *use case* menunjukkan 3 aspek dari sistem yaitu *actor*, *use case* dan sistem / sub sistem *boundary*. *Actor* mewakili peran orang, sistem yang lain atau alat ketika berkomunikasi dengan *use case*. Gambar II.1 mengilustrasikan *actor*, *use case* dan *boundary*.

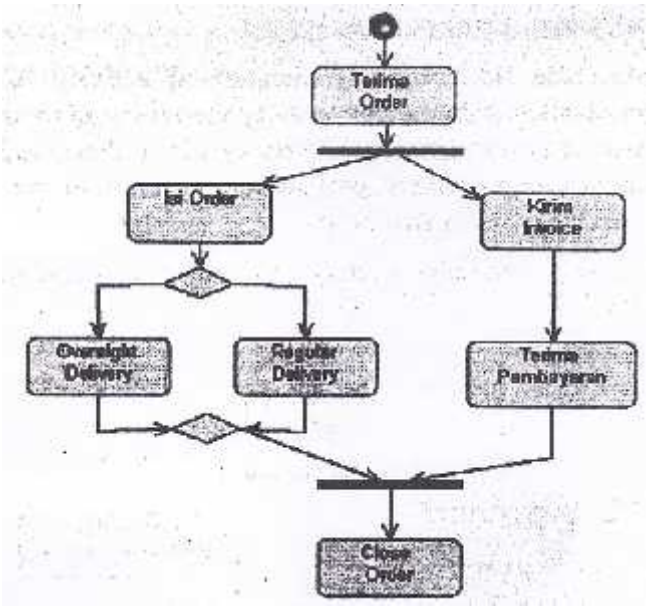


Gambar II.2 ***Use Case Model***

(Sumber : Munawar 2005 : 64)

2. *Activity Diagram*

Activity diagram adalah teknik untuk mendeskripsikan logika prosedural, proses bisnis dan aliran kerja dalam banyak kasus. *Activity diagram* mempunyai peran seperti halnya *flowchart*, akan tetapi perbedaannya dengan *flowchart* adalah *activity diagram* ias mendukung perilaku paralel sedangkan *flowchart* tidak bisa. Berikut gambar dari sederhana dari *Activity diagram.*



Gambar II.3 Contoh *Activity Diagram* Sederhana

(Sumber : Munawar 2005 : 111)

3. *Class Diagram*

Menurut Prabowo Pudjo Widodo dan Herlawati (2011 : 10) *Class diagram* bersifat statis. Diagram ini memperlihatkan himpunan kelas-kelas, antamuka-antarmuka, kolaborasi-kolaborasi, serta relasi-relasi. Diagram ini umum dijumpai pada pemodelan sistem berorientasi objek. Meskipun bersifat statis, sering pula diagram kelas memuat kelas-kelas aktif.

4. *Sequence Diagram*

Sequence Diagram digunakan untuk menggambarkan prilaku pada sebuah skenario. Diagram ini menunjukan sejumlah contoh obyek dan pesan yang diletakan diantara obyek – obyek ini di dalam *use case.*

Komponen utama *sequence diagram* terdiri atas obyek yang dituliskan dengan kotak segiempat bernama. *Message* diwakili oleh garis dengan tanda panah dan waktu yang ditunjukan dengan *progress vertical.*

1. Objek / *participant*

Objek diletakkan di dekat bagian atas diagram dengan urutan dari kiri ke kanan. Mereka diatur dalam urutan guna menyederhanakan diagram. Setiap *participant* dihubungkan garis titik-titik yang disebut *lifeline.* Sepanjang *lifeline* ada kotak yang disebut *activation*. *Activation* mewakili sebuah eksekusi operasi dari *participant*. Panjang kotak ini berbanding lurus dengan durasi *activation*. *Activation* mewakili sebuah eksekusi operasi dari participant. Panjang kotak ini berbanding lurus dengan durasi *activation.* Bentuk *participant* dapat dilihat pada gambar II.4

Gambar II.4 Bentuk *Participant*

Sumber : Pemodelan Visual dengan UML, Munawar, 2005 : 88

2. *Messege*

Sebuah *messege* bergerak dari suatu *participant* ke *participant* yang lain dan dari *lifeline* ke *lifeline* yang lain. Sebuah *participant* bisa mengirim sebuah *message* kepada dirinya sendiri.

Sebuah *message* bisa jadi *simple*, *synchronous* atau *asynchoronous*. *Message* yang *simple* adalah sebuah perpindahan (transfer), contoh dari satu *participant* ke *participant* yang lainnya. Jika suatu *participant* mengirimkan sebuah *message* tersebut akan ditunggu sebelum di proses dengan urusannya. Namun jika *message asynchoronous* yang dikirimkan, maka jawabannya atas *message* tersebut tidak perlu ditunggu. Simbol *message* pada *squnence diagram* dapat dilihat pada gambar II.5

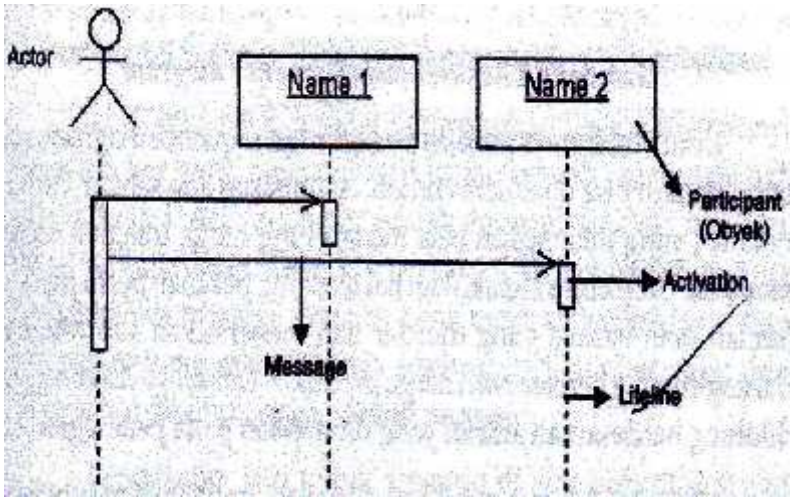
Gambar II.5 Bentuk *Messege*

Sumber : Pemodelan Visual dengan UML, Munawar, 2005 : 88

3. *Time*

Time adalah diagram yang mewakili waktu pada arah vertikal. Waktu dimulai dari atas ke bawah. *Message* yang lebih dekat dari atas akan dijalankan terlebih dahulu dibanding *message* yang lebih dekat kebawah.

Terdapat dua dimensi pada *squence diagram* yaitu dimensi dari kiri ke kanan menunjukkan tata letak participant dan dimensi dari atas ke bawah menunjukkan lintasan waktu. Simbol-simbol yang ada pada *squence diagram* ditunjukkan pada gambar II.6



Gambar II.6 Contoh Bentuk *Time*

Sumber : Pemodelan Visual dengan UML, Munawar, 2005 : 89

II.7. Sistem Deteksi Serangan

Tujuan utama dari keamanan sistem adalah memberikan jalur yang aman antaraentitas yang saling bertukar informasi dan untuk menyediakan perlindungan data. Insiden keamanan jaringan komputer adalah suatu aktivitas yang berkaitan dengan jaringan komputer, dimana aktivitas tersebut memberikan implikasi terhadap keamanan. Secara garis besar insiden dapat diklasifikasikan menjadi :

1. Probe/scan: Usaha-usaha yang tidak lazim untuk memperoleh akses ke dalam suatu sistem, atau untuk menemukan informasi tentang sistem tersebut. Kegiatan probe dalam jumlah besar dengan menggunakan tool secara otomatis biasa disebut *Scan.* Bermacam-macam tool yang dipergunakan

untuk keperluan ini seperti : *network mapper, port mapper network scanner, port scanner, atau vulnerability scanner*. Informasi yang diperoleh misalkan :

a. Topologi dari jaringan target

b. Hosts yang aktif

c. Sistem operasi pada host

d. Software yang berjalan pada server dan versinya.

2. *Account Compromisse* : Penggunaan account sebuah komputer secara ilegal oleh seseorang yang bukan pemilik account, dimana account tersebut tidak mempunyai privelege sebagai administrator sistem.
3. *Root Compromisse* : Mirip *account compromisse* tetapi mempunyai privelege sebagai administrator sistem.
4. *Packet sniffer* : Perangkat lunak/keras yang digunakan untuk memperoleh informasi yang melewati jaringan komputer, biasanya dengan NIC bermode promiscuous.
5. *Denial of service (DOS)* : Membuat sumberdaya jaringan maupun komputer tidak bekerja, sehingga tidak mampu memberikan layanan kepada user. Misalkan saja dengan membanjiri sumber daya komputer, misal CPU,memori,ruang disk, bandwith jaringan. Serangan dapat dilakukan dari satu komputer atau beberapa komputer (*Distributed* DOS).

II.7.1 Pertimbangan Sistem

Mobile *agent* merupakan teknologi yang menjanjikan untuk implementasi tool yang beroperasi pada sumber data yang terdistribusi. Misalkan saja administrator ingin melihat kondisi di setiap host, maka mobile agent yang akan dikirimkan ke setiap host yang akan melakukannya. Di sini IDS dirancang sebagai external sensor, dengan pengumpulan data dari sejumlah host (multi host based), dan sumber data diambil baik secara langsung maupun tidak. Kelebihan yang diinginkan :

a. Respon lebih cepat untuk mendeteksi pemyusupan terdistribusi pada beberapa host.

b. Tetap memberikan laporan meski host mendapat serangan.

II.8. Tujuan Penggunaan IDS

IDS merupakan *software* atau hardware yang melakukan otomatisasi proses monitoring kejadian yang muncul di sistem komputer atau jaringan, menganalisanya untuk menemukan permasalahan keamanan. IDS adalah pemberi sinyal pertama jika seorang penyusup mencoba membobol sistem keamanan komputer kita. Secara umum penyusupan bisa berarti serangan atau ancaman terhadap keamanan dan integritas data, serta tindakan atau percobaan untuk melewati sebuah sistem keamanan yang dilakukan oleh seseorang dari internet maupun dari dalam sistem. IDS tidak dibuat untuk menggantikan fungsi firewall karena kegunaanya berbeda. Sebuah sistem firewall tidak bisa mengetahui apakah

sebuah serangan sedang terjadi atau tidak. IDS mengetahuinya. Dengan meningkatnya jumlah serangan pada jaringan, IDS merupakan sesuatu yang diperlukan pada infrastruktur keamanan di kebanyakan organisasi. Secara singkat, fungsi IDS adalah pemberi peringatan kepada administrator atas serangan yang terjadi pada sistem kita. Alasan mempergunakan IDS :

a. Untuk mencegah resiko timbulnya masalah.
b. Untuk mendeteksi serangan dan pelanggaran keamanan lainnya yang tidak dicegah oleh perangkat keamanan lainnya.
c. Biasanya penyusupan berlangsung dalam tahapan yang bisa diprediksi. Tahapan pertama adalah probing, atau eksploitasi pencarian titik masuk. Pada sistem tanpa IDS, penyusup memiliki kebebasan melakukannya dengan resiko kepergok lebih kecil. IDS yang mendapati *probing*, bisa melakukan blok akses, dan memberitahukan tenaga keamanan yang selanjutnya mengambil tindakan lebih lanjut.
d. Untuk mendeteksi usaha yang berkaitan dengan serangan misal *probing* dan aktivitas *dorknob rattling.*
e. Untuk mendokumentasikan ancaman yang ada ke dalam suatu organisasi. IDS akan mampu menggolongkan ancaman baik dari dalam maupun dari luar organisasi. Sehingga membantu pembuatan keputusan untuk alokasi sumber daya keamanan jaringan.
f. Untuk bertindak sebagai pengendali kualitas pada adminitrasi dan perancangan keamanan, khususnya pada organisasi yang besar dan kompleks. Saat ini IDS

dijalankan dalam waktu tertentu, pola dari pemakaian sistem dan masalah yang ditemui bisa nampak. Sehingga akan membantu pengelolaan keamanan dan memperbaiki kekurangan sebelum menyebabkan insiden.

g. Untuk memberikan informasi yang berguna mengenai penyusupan yang terjadi, peningkatan diagnosa, *recovery*, dan perbaikan dari faktor penyebab. Meski jika IDS tidak melakukan block serangan, tetapi masih bisa mengumpulkan informasi yang relevan mengenai serangan, sehingga membantu penanganan insiden dan *recovery*. Hal itu akan membantu konfigurasi atau kebijakan organisasi. Meskipun vendor dan administrator berusaha meminimalkan vulnerabilitas yang memungkinkan serangan, ada banyak situasi yang tidak memungkinkan hal ini.

II.9. Jaringan Peer To Peer

Peer to Peer adalah adalah suatu teknologi sharing (pemakaian bersama) *resource* dan *service* antara satu komputer dan komputer yang lain. pengertian yang lebih tepat mengenai peer to peer (p2p) adalah sistem terkomputerisasi *Client-Server* dimana suatu komputer berfungsi sebagai client sekaligus sebagai *server*, sehingga memungkinkan komunikasi dan pertukaran resource antara dua komputer secara langsung (real time). Peer adalah pihak pemasok dan konsumen sumber daya Berbeda dengan model client-server di mana server hanya memasok, dan klien mengkonsumsi.

II.10. Pengertian Switch / Hub

Hub adalah peralatan sentral yang berfungsi menghubungkan komputer-komputer atau peralatan-peralatan jaringan lainnya. Hub menerima pesan dari node pengirim dan menjalankannya ke node tujuan. Hub identik dengan topologi star. Hub terdiri dari beberapa port. Port ini digunakan untuk memasang konektor RJ-45 yang sudah dipasangi kabel UTP. Hub adalah peralatan sentral yang berfungsi menghubungkan komputer-komputer atau peralatan-peralatan jaringan lainnya.

Hub menerima pesan dari node pengirim dan menjalankannya ke node tujuan. Hub identik dengan topologi star. Hub terdiri dari beberapa port. Port ini digunakan untuk memasang konektor RJ-45 yang sudah dipasangi kabel UTP. Dilihat dari jumlah portnya, hub terdiri dari hub port 5, 8, 16, 24 dan 32. Salah satu port digunakan untuk hubungan antar-hub (cascading). Port yang digunakan untuk hubungan antar-hub disebut port uplink. karakteristik dan fitur utama hub Hub awalnya mensupport kecepatan ethernet 10 Mbps. Namun dewasa ini banyak hub memiliki kecepatan data 100 Mbps. Beberapa jenis hub mendukung dua kecepatan 10 Mpbs / 100 Mbps atau dikenal dengan dengan dual-speed hubs. Karakteristik Hub:

a. Tergolong peralatan Layer 1 dalam OSI model (Physical layer). Tidak dapat membaca paket-paket data.
b. Tidak dapat mengetahui sumber dan tujuan data.

c. Hanya berperan menerima dan meneruskan data yang masuk ke semua peralatan di jaringan termasuk yang mengirim data.
d. Dapat memperkuat sinyal elektrik data yang masuk sebelum dikirimkan ke tujuan.

Cara kerja HUB Cara kerja alat ini adalah dengan cara mengirimkan sinyal paket data ke seluruh port pada hub sehingga paket data tersebut diterima oleh seluruh computer yang berhubungan dengan hub tersebut kecuali computer yang mengirimkan. Sinyal yang dikirimkan tersebut diulang-ulang walaupun paket data telah diterima oleh komputer tujuan Keuntungan menggunakan HUB Menggunakan hub memungkinkan Anda untuk atap-drop pada percakapan dengan penganalisa protokol jaringan, sering disebut sebagai sniffer Kekurangan menggunakan HUB Karena mereka mengulang semua lalu lintas yang mereka terima pada semua port tiap terhubung terpasang NIC akan memiliki waktu yang lebih sulit mendapatkan dengan lalu lintas ke jaringan.

II.11. Penjelasan Kabel UTP / Unshielded Twisted Pair

Pengertian dan arti definisi Kabel UTP atau kabel unshielded twisted pair adalah kabel yang biasa digunakan untuk membuat jaringan atau network komputer berupa kabel yang didalamnya berisi empat 4 pasang kabel. Kabel Twisted Pair Cable ini ada dua jenis yaitu shielded dan unshielded. Shielded adalah jenis kabel yang memiliki selubung pembungkus sedangkan unshielded tidak mempunyai selubung pembungkus. Untuk koneksinya kabel jenis ini menggunakan konektor RJ-11 atau RJ-45.

Twisted-pair (dikenal juga sebagai 10 BaseT) cocok untuk jaringan kecil, sedang maupun besar yang membutuhkan fleksibilitas dan kapasitas untuk berkembang sesuai dengan pertumbuhan pemakai network.

Pada twisted-pair network, komputer disusun membentuk suatu pola star. Setiap PC memiliki satu kabel twisted-pair yang tersentral pada HUB. Twisted-pair umumnya lebih reliable dibandingkan dengan thin coax karena HUB mempunyai kemampuan data error correction dan meningkatkan kecepatan transmisi. Bahkan dengan HUB ini bisa dirangkai menjadi suatu jaringan yang besar. Kabel UTP kategori satu dan dua tidak digunakan dalam jaringan komputer karena kemampuan transfer datanya sangat rendah.Kabel kategori ini banyak digunakan untuk komunikasi telepon ,atau berfungsi sebagai kabel telepon.

dalam pengkabelan jaringan komputer ada dua macam konfigurasi pengkabelan yaitu:

1. kabel straight

2. kabel cross

kabel stright adalah kabel yang sangat simpel karena untuk konfigurasi nya adalah tetap. kabel ini digunakan untuk jaringan yang melewati hub atau antar komputer tidak terhubung langsung tapi melewati sebuah media. biasanya kabel ini digunakan untuk jaringan lokal dengan hub sebagai perantaranya. Jadi intinya adalah antara pin yang satu dengan ujung yang lain urutan kabel nya sama yaitu : putih orange, orange, putih hijau, biru, biru putih, hijau, putih coklat, coklat.

kabel cross adalah kabel ini berbeda dengan kabel straight biasanya di gunakan untuk jaringan point to point atau hub pc ke pc secara langsung tanpa melewati media lain. dan antara urutan kabel pada ujung satu dengan ujung yang lain berbeda.

II.12. Pemrograman C##

Bahasa Pemrograman C## merupakan bahasa pemrograman tingkat tinggi, itu dikarenakan bahasa c dapat dimengerti dan dipelajari dengan mudah karena kedekatanya dengan bahasa manusia. Tapi banyak orang juga mengatakan bahwa bahasa c adalah *medium level progamming language* karena bahasa c juga dapat digunakan untuk memasukkan program ke mesin. Bahasa C# dirancang oleh Dennis M. Ritchie pada tahun 1972 di AT&T Bell Labs. Bahasa C# dikembangkan dari bahasa BPCL (*Basic Combined Programming Language*) dan bahasa B. Bahasa BPCL di kembangkan oleh Martin Richard pada tahun 1967 sebagai bahasa system operasi dan compiler. Bahasa C# adalah sebuah bahasa pemrograman modern yang bersifat *general-purpose*, berorientasi objek, yang dapat digunakan untuk membuat program di atas *arsitektur Microsoft NET Framework*. Bahasa C# ini memiliki kemiripan dengan bahasa Java, C dan C++. Bahasa pemrograman ini dikembangkan oleh sebuah tim pengembang di *Microsoft* yang dipimpin oleh Anders Hejlsberg, seorang yang telah lama malang melintang di dunia pengembangan bahasa pemrograman karena memang ialah yang membuat Borland Turbo Pascal, Borland Delphi, dan juga *Microsoft J++*.