ANALISIS PENERAPAN JARINGAN KEAMANAN MENGUNAKAN IDS DAN HONEYPOT

Bayu Setia Candra
Fakultas Ilmu Komputer, Universitas Dian Nuswantoro, Semarang 50131
E-mail : i.blue89@yahoo.co.id

BAB I
PENDAHULUAN

1.1 Latar Belakang

Internet merupakan sebuah jaringan global dan terbuka, dimana setiappengguna dapat saling berkomunikasi dan bertukar informasi. Seiring dengan maraknya penggunaan Internet, banyak perusahaan yang kemudian beralih menggunakan internet sebagai bagian dari jaringan mereka untuk menghemat biaya. akan tetapi permasalahan keamanan masih menjadi faktor utama.

Keamanan jaringan komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya. Sistem keamanan jaringan komputer harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak.

Sistem deteksi penyusup jaringan yang ada saat ini umumnya mampu mendeteksi berbagai jenis serangan tetapi tidak mampu mengambil tindakan lebih lanjut. Selain itu sistem juga tidak memiliki interaktivitas dengan administrator pada saat administrator tidak sedang mengadministrasi sistemnya. Hal ini merupakan suatu hal yang tidak efektif terutama pada saat sistem berada dalam kondisi kritis.

Selain itu sistem pertahanan terhadap aktivitas gangguan saat ini umumnya dilakukan secara manual oleh administrator. hal ini mengakibatkan integritas sistem bergantung pada ketersediaan dan kecepatan administrator dalam merespons gangguan. Apabila terjadi malfungsi, administrator tidak dapat lagi mengakses sistem secara remote sehingga tidak akan dapat melakukan pemulihan sistem dengan cepat.

Oleh karena itu dibutuhkan suatu sistem yang dapat menanggulangi ancaman yang mungkin terjadi secara optimal dalam waktu yang cepat dan secara otomatis sehingga memungkinkan administrator mengakses sistem walaupun terjadi malfungsi jaringan. Hal ini akan mempercepat proses penanggulangan gangguan serta pemulihan sistem atau layanan.

Keamanan komputer atau dalam Bahasa Inggris computer security atau dikenal juga dengan sebutan cybersecurity atau IT security adalah keamanan infromasi yang diaplikasikan kepada komputer dan jaringannya. Computer security atau keamanan komputer bertujuan

membantu user agar dapat mencegah penipuan atau mendeteksi adanya usaha penipuan di sebuah sistem yang berbasis informasi , teknologi yang dikenal dan dikembangkan dengan nama keamanan informasi yang diterapkan pada komputer.

Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadap pencurian , korupsi dan pemalsuan data pada server , atau pemeliharaan dan kebijakan keamanan data .

Sistem keamanan komputer merupakan sebuah upaya yang dilakukan untuk mengamankan kinerja dan proses komputer. Penerapan computer security dalam kehidupan sehari-hari berguna sebagai penjaga sumber daya sistem agar tidak digunakan, modifikasi , interupsi , diganggu oleh orang yang tidak berwenang dan bertangung jawab . Keamanan bisa diindentifikasikan dalam masalah teknis, manajerial, legalitas, dan politis. computer security akan membahas 2 hal penting yaitu Ancaman/Threats dan Kelemahan sistem/vulnerabillity.

Keamanan komputer adalah suatu system yang memberi persyaratan khusus ,pembatasan terhadap komputer yang berbeda untuk Sali terkorelasi / berhubungan . Dilihat dari meluasnya dan perkembangan tehnologi yang pesat , maka berkembanglah juga system pengamanannya.

Penggunaan computer yang terkoneksi dengan jaringan baik intranet maupun internet tidak luput dari yang namanya serangan pada system komputer . Serangan tersebut tentunya sangat merugikan user apabila serangan tersebut mengambil , memodifikasi data penting dan merusak sistem atau melumpuhkan system yang sudah dimasukinya. Hingga saat ini, pendekatan yang dilakukan oleh administrator sistem adalah bagaimana caranya supaya para penyusup (krecker dan hecker) tidak dapat memasuki server dan mengambil atau merubah data.

Namun, ternyata ada cara yang dapat digunakan untuk menanggulangi serangan hacker dengan membangun sistem computer yang memang sengaja dirancang untuk diserang oleh penyusup (krecker dan hacker).

Namun, ternyata ada cara yang dapat digunakan untuk menanggulangi serangan hacker dengan membangun sistem computer yang memang sengaja dirancang untuk diserang oleh penyusup (krecker dan hacker).

Keamanan sistem komputer adalah untuk menjamin sumber daya sistem tidak digunakan / dimodifikasi, diinterupsi dan diganggu oleh orang yang tidak diotorisasi. Pengamanan termasuk masalah teknis, manajerial, legalitas dan politis.

3 macam keamanan sistem, yaitu :

1. Keamanan eksternal / external security berkaitan dengan pengamanan fasilitas komputer dari penyusup dan bencana seperti kebakaran /kebanjiran.

2. Keamanan interface pemakai / user interface security berkaitan dengan indentifikasi pemakai sebelum pemakai diijinkan mengakses program dan data yang disimpan

3. Keamanan internal / internal security berkaitan dengan pengamanan beragam kendali yang dibangun pada perangkat keras dan sistem operasi yang menjamin operasi yang handal dan tak terkorupsi untuk menjaga integritas program dan data.

2 masalah penting keamanan, yaitu :

1. Kehilangan data / data loss

Yang disebabkan karena kesalahan perangkat keras dan perangkat lunak, contohnya ketidak berfungsinya pemroses, disk / tape. yang tidak terbaca, kesalahan komunikasi, kesalahan program / bugs.kesalahan / kelalaian manusia, contohnya kesalahan pemasukkan data, memasang tape / disk yang salah, kehilangan disk / tape.

2. Penyusup / intruder

· Penyusup pasif, yaitu yang membaca data yang tidak terotorisasi
· Penyusup aktif, yaitu mengubah data yang tidak terotorisasi.

Contohnya penyadapan oleh orang dalam, usaha hacker dalam mencari uang, spionase militer / bisnis, lirikan pada saat pengetikan password.

Sasaran keamanan adalah menghindari, mencegah dan mengatasi ancaman terhadap sistem.

3 aspek kebutuhan keamanan sistem komputer, yaitu :

1. Kerahasiaan / secrecy, diantaranya privasi

Keterjaminan bahwa informasi di sistem komputer hanya dapat diakses oleh pihak-pihak yang terotorisasi dan modifikasi tetap menjaga konsistensi dan keutuhan data di sistem

2. Integritas / integrity

Keterjaminan bahwa sumber daya sistem komputer hanya dapat dimodifikasi oleh pihak-pihak yang terotorisasi

3. Ketersediaan / availability

Keterjaminan bahwa sumber daya sistem komputer tersedia bagi pihak-pihak yang diotorisasi saat diperlukan.

Tipe ancaman terhadap keamanan sistem komputer dapat dimodelkan dengan memandang fungsi system komputer sebagai penyedia informasi.

Banyak aspek yang bisa mengancam keamanan sistem jaringan komputer, yaitu ancaman yang bersifat *interruption* dimana informasi dan data dalam system dirusak dan dihapus sehingga jika dibutuhkkan data atau informasi tersebut telah rusak atau hilang. Kemudian ancaman yang bersifat *interception* yaitu informasi yang

ada disadap oleh orang yang tidak berhak mengakses informasi yang terdapat pada sistem ini. Selanjutnya *modifikasi* yaitu ncaman terhadap integritas dari system informasi tersebut. Dan yang terakhir adalah *fabrication* yaitu orang yang tidak berhak berhasil memalsukan suatu informasi yang ada sehingga orang yang menerima informasi tersebut menyangka bahwa informasi tersebut berasal dari yang dikehendaki oleh penerima informasi tersebut.dengan sistem ini diharapkan dapat mengetahui akan sistem keamanan jaringan komputer, khususnya mendeteksi segala sesuatu yang akan mengancamweb server.

Dalam penelitian ini diberikan gambaran bagaimana melakukan pencegahan atas serangan yang akan dilakukan oleh hacker dengan menekankan pada pendeteksian atas serangan yang dilakukan hacker sehingga admin dapat mempelajari serangan tersebut dan mencari solusi untuk mencegahannya.

Karena itu peneliti untuk melakukan observasi, dan melakukan pengumpulan data yang berkaitan dengan pendeteksian terhadap serangan *sql injection* dan *denial of service* . Dan dari beberapa ditemuik,,, terdapat salah satu metode yaitu Honeypot yang melakukan pendeteksian dengan menipu hacker yang akan merusak sistem dengan suatu jaringan palsu, sehingga admin dengan mudah mempelajari trik yang dilakukan hacker tersebut.

Berdasarkanlatarbelakang di atas maka bagaimana cara merancang sistem honeypots guna mengamankan sebuah sistem informasi dari serangan *sql injection* dan *denial of service*. Dalam penulisan penelitian ini, dibatasi masalah pada penerapan aplikasi honeypots dengan simulasi pada sebuah jaringan guna mengenali dan memberikan pengamanan sistem informasi dari dua jenis serangan yaitu *sql injection* dan *denial of service. dengan tujuan* mengamankan sistem informasi dari serangan *sql injection* dan *denial of service*

1.2 Rumusan Masalah

Suatu sistem keamanan jaringan komputer yang dapat mendeteksi gangguan secara otomatis dan melakukan tindakan pengalihan dengan membuat server bayangan dan harus adanya system yang terkordinasi dengan baik , adanya juga pengamanan yang berlapis untuk menjaga agar system server tetap aman.

Mengintegrasikan aplikasi yang terkait dengan sistem keamanan jaringan computer untuk mengalihkan serangan dari data yang sebenarnya supaya data tetap aman.

1.3 Batasan Masalah

Analisa yang. dilakukan pada penerapan system keamanan jaringan mengunakan IDS dan Hanepot .

honeypot sendiri adalah sebuah sumber daya sistem keamanan yang dibuat sebagai tujuan utama penyerang yan

g sebenarnya merupakan sistem yang palsu untuk menjebak penyerang. Sistem honeypot biasanya hanya sebuah sistem yang dihubungkan dengan jaringan produktif, atau sistem yang asli, yang ada dengan tujuan untuk menjebak penyerang.

Intrusion Detection System (disingkat IDS) sendiri adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah sistem atau jaringan.

1.4 Tujuan Penelitian

Dengan adanya penelitian ini diharapkan agar mahasiswa dapat mengetahui bagaimana cara mengamankan jaringan server dengan lebih aman , lebih terjaminya keamanan pada data itu sendiri dari user yang tidak memiliki otoritas terhadap data pada computer server.

1.5 Manfaat Penelitian

Dengan adanya sistem keaman pada jaringan hotspot ini akan mengurasi resiko penyerangan pada system server , dan membantu administrator jaringan untuk mendeteksi dan mengalihkan penyusupan pada suatu system server yang berjalan.

BAB II
LANDASAN TEORI

2.1 Kajian Jurnal

1. “Perancangan Kolaborsi Sistem Deteksi Intruksi Jaringan Tersebar Dengan Honeypot mengunakan Metode elert Correlation “oleh Noven Indra Prasetyo, Supeno janali , Muhamat Husni .

   Permasalahan yang diangkat adalah kejahatan didunia internet yang dikenal dengan cybercrime telah banyak menimbulkan kerugian dan pembobolan data sepanjang tahun. Metode yang digunakan adalah IDS akan dikolaborasikan dengan honeypot,dimana honepot merupakan system yang dibuat menyerupai system aslinya untuk melakukan korelasi alert yang dihasilkan oleh masing-masing sensor(IDS dan Honepot).

   Hasilnya system server terlindungi para penyusup dapat dialihkan ke server palsu dan dan data diserver asli lebih aman.maka kesimpulanya honepot dapat dikolaborasikandengan beberapa system deteksi.

2. “Solusi Network Scurity dari Ancaman SQL Injection dan Danial of service (DOS)”Ir .Sumarno M.M dan Sabto Bisosro
   Permasalahan yang diangkat banyak aspek yang bisa mengancam keamanan sistem jaringan komputer, yaitu ancaman yang bersifat *interception* yaitu informasi yang ada disadap oleh orang

yang tidak berhak mengakses informasi yang terdapat pada sistem ini. Selanjutnya *modifikasi* yaitu ncaman terhadap integritas dari system informasi tersebut. Dan yang terakhir adalah *fabrication* yaitu orang yang tidak berhak berhasil memalsukan suatu informasi yang ada sehingga orang yang menerima informasi tersebut menyangka bahwa informasi tersebut berasal dari yang dikehendaki oleh penerima informasi tersebut.

Metode yang digunakan yaitu yaitu Honeypot yang melakukan pendeteksian dengan menipu hacker yang akan merusak sistem dengan suatu jaringan palsu, penerapan aplikasi honeypots dengan simulasi pada sebuah jaringan guna mengenali dan memberikan pengamanan sistem informasi dari dua jenis serangan yaitu *sql injection* dan *denial of service.*

2.2 TCP/IP

TCP/IP (singkatan dari *Transmission Control Protocol*/*Internet Protocol*) jika diterjemahkan adalah *Protokol Kendali Transmisi/Protokol Internet*, adalah gabungan dari protokol TCP (Transmission Control Protocol) dan IP (Internet Protocol) sebagai sekelompok protokol yang mengatur komunikasi data dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan internet yang akan memastikan pengiriman data sampai ke alamat yang dituju. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (*protocol suite*). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini, karena protokol ini mampu bekerja dan diimplementasikan pada lintas perangkat lunak (software) di berbagai sistem operasi Istilah yang diberikan kepada perangkat lunak ini adalah TCP/IP stack.

Protokol TCP/IP dikembangkan pada akhir dekade 1970-an hingga awal 1980-an sebagai sebuah protokol standar untuk menghubungkan komputer-komputer dan jaringan untuk membentuk sebuah jaringan yang luas (WAN). TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme transport jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (*IP Address*) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya di Internet. Protokol ini juga bersifat *routable* yang berarti protokol ini cocok untuk menghubungkan sistem-sistem berbeda (seperti Microsoft Windows dan keluarga UNIX) untuk membentuk jaringan yang heterogen.

Protokol TCP/IP selalu berevolusi seiring dengan waktu, mengingat semakin banyaknya kebutuhan terhadap jaringan komputer dan Internet. Pengembangan ini dilakukan oleh beberapa badan,

seperti halnya Internet Society (ISOC), Internet Architecture Board (IAB), dan Internet Engineering Task Force (IETF). Macam-macam protokol yang berjalan di atas TCP/IP, skema pengalamatan, dan konsep TCP/IP didefinisikan dalam dokumen yang disebut sebagai Request for Comments (RFC) yang dikeluarkan oleh IETF.

2.2.1Arsitektur

Arsitektur TCP/IP diperbandingkan dengan DARPA Reference Model dan OSI Reference Model

Arsitektur TCP/IP tidaklah berbasis model referensi tujuh lapis OSI, tetapi menggunakan model referensi DARPA. Seperti diperlihatkan dalam diagram, TCP/IP merngimplemenasikan arsitektur berlapis yang terdiri atas empat lapis. Empat lapis ini, dapat dipetakan (meski tidak secara langsung) terhadap model referensi OSI. Empat lapis ini, kadang-kadang disebut sebagai *DARPA Model*, *Internet Model*, atau *DoD Model*, mengingat TCP/IP merupakan protokol yang awalnya dikembangkan dari proyek ARPANET yang dimulai oleh Departemen Pertahanan Amerika Serikat.

Setiap lapisan yang dimiliki oleh kumpulan protokol (protocol suite) TCP/IP diasosiasikan dengan protokolnya masing-masing. Protokol utama dalam protokol TCP/IP adalah sebagai berikut:

- Protokol lapisan aplikasi: bertanggung jawab untuk menyediakan akses kepada aplikasi terhadap layanan jaringan TCP/IP. Protokol ini mencakup protokol *Dynamic Host Configuration Protocol* (DHCP), *Domain Name System* (DNS), Hypertext Transfer Protocol (HTTP), *File Transfer Protocol* (FTP), *Telnet*, *Simple Mail Transfer Protocol* (SMTP), *Simple Network Management Protocol* (SNMP), dan masih banyak protokol lainnya. Dalam beberapa implementasi stack protokol, seperti halnya Microsoft TCP/IP, protokol-protokol lapisan aplikasi berinteraksi dengan menggunakan antarmuka Windows Sockets (Winsock) atau NetBIOS over TCP/IP (NetBT).
- Protokol lapisan antar-*host*: berguna untuk membuat komunikasi menggunakan sesi koneksi yang bersifat *connection-oriented* atau *broadcast* yang bersifat *connectionless*. Protokol dalam lapisan ini adalah Transmission Control Protocol (TCP) dan User Datagram Protocol (UDP).
- Protokol lapisan *internetwork*: bertanggung jawab untuk melakukan pemetaan (*routing*) dan enkapsulasi paket-paket data jaringan menjadi paket-paket IP. Protokol yang bekerja dalam lapisan ini adalah *Internet Protocol* (IP), *Address Resolution Protocol* (ARP), Internet Control Message Protocol (ICMP), dan Internet Group

Management Protocol (IGMP).

- Protokol lapisan antarmuka jaringan: bertanggung jawab untuk meletakkan frame-frame jaringan di atas media jaringan yang digunakan. TCP/IP dapat bekerja dengan banyak teknologi transport, mulai dari teknologi transport dalam LAN (seperti halnya Ethernet dan Token Ring), MAN dan WAN (seperti halnya dial-up modem yang berjalan di atas Public Switched Telephone Network (PSTN), *Integrated Services Digital Network* (ISDN), serta *Asynchronous Transfer Mode* (ATM)).

2.2.2 Pengalamatan

Protokol TCP/IP menggunakan dua buah skema pengalamatan yang dapat digunakan untuk mengidentifikasikan sebuah komputer dalam sebuah jaringan atau jaringan dalam sebuah internetwork, yakni sebagai berikut:

- Pengalamatan IP: yang berupa alamat logis yang terdiri atas 32-bit (empat oktet berukuran 8-bit) yang umumnya ditulis dalam format `www.xxx.yyy.zzz`. Dengan menggunakan *subnet mask* yang diasosiasikan dengannya, sebuah alamat IP pun dapat dibagi menjadi dua bagian, yakni *Network Identifier* (NetID) yang dapat mengidentifikasikan jaringan lokal dalam sebuah *internetwork* dan *Host identifier* (HostID) yang dapat mengidentifikasikan host dalam jaringan tersebut. Sebagai contoh, alamat `205.116.008.044` dapat dibagi dengan menggunakan subnet mask `255.255.255.000` ke dalam *Network ID* `205.116.008.000` dan *Host ID* 44. Alamat IP merupakan kewajiban yang harus ditetapkan untuk sebuah *host*, yang dapat dilakukan secara manual (statis) atau menggunakan *Dynamic Host Configuration Protocol* (DHCP) (dinamis).
- Fully qualified domain name (FQDN): Alamat ini merupakan alamat yang direpresentasikan dalam nama alfanumerik yang diekspresikan dalam bentuk ***<nama_host>.<nama_domain>***, di mana <nama_domain> mengindentifikasikan jaringan di mana sebuah komputer berada, dan <nama_host> mengidentifikasikan sebuah komputer dalam jaringan. Pengalamatan FQDN digunakan oleh skema penamaan domain Domain Name System (DNS). Sebagai contoh, alamat FQDN `id.wikipedia.org` merepresentasikan sebuah

host dengan nama "**id**" yang terdapat di dalam domain jaringan "`wikipedia.org`". Nama domain `wikipedia.org` merupakan *second-level domain* yang terdaftar di dalam *top-level domain* `.org`, yang terdaftar dalam root DNS, yang memiliki nama "**.**" (titik). Penggunaan FQDN lebih bersahabat dan lebih mudah diingat ketimbang dengan menggunakan alamat IP. Akan tetapi, dalam TCP/IP, agar komunikasi dapat berjalan, FQDN harus diterjemahkan terlebih dahulu (proses penerjemahan ini disebut sebagai **resolusi nama**) ke dalam alamat IP dengan menggunakan *server* yang menjalankan DNS, yang disebut dengan *Name Server* atau dengan menggunakan berkas *hosts* (`/etc/hosts` atau `%systemroot%\system32\drivers\etc\hosts`) yang disimpan di dalam mesin yang bersangkutan.

1

2.3 Database (Basis data)

Database atau basis data (bahasa Inggris: *database*), atau sering pula dieja basisdata, adalah kumpulan informasi yang disimpan di dalam komputer secara sistematik sehingga dapat diperiksa menggunakan suatu program komputer untuk memperoleh informasi dari basis data tersebut. Perangkat lunak yang digunakan untuk mengelola dan memanggil kueri (*query*) basis data disebut sistem manajemen basis data (*database management system*, DBMS). Sistem basis data dipelajari dalam ilmu informasi.

Istilah "basis data" berawal dari ilmu komputer. Meskipun kemudian artinya semakin luas, memasukkan hal-hal di luar bidang elektronika, artikel ini mengenai basis data komputer. Catatan yang mirip dengan basis data sebenarnya sudah ada sebelum revolusi industri yaitu dalam bentuk buku besar, kuitansi dan kumpulan data yang berhubungan dengan bisnis.

Konsep dasar dari basis data adalah kumpulan dari catatan-catatan, atau potongan dari pengetahuan. Sebuah basis data memiliki penjelasan terstruktur dari jenis fakta yang tersimpan di dalamnya: penjelasan ini disebut skema. Skema menggambarkan obyek yang diwakili suatu basis data, dan hubungan di antara obyek tersebut. Ada banyak cara untuk mengorganisasi skema, atau memodelkan struktur basis data: ini dikenal sebagai model basis data atau model data. Model yang umum digunakan sekarang adalah model relasional, yang menurut istilah layman mewakili semua informasi dalam bentuk tabel-tabel yang saling berhubungan dimana setiap tabel terdiri dari baris dan kolom (definisi yang sebenarnya menggunakan terminologi matematika). Dalam model ini, hubungan antar tabel diwakili denga menggunakan nilai yang sama antar tabel. Model yang lain seperti model hierarkis dan model jaringan menggunakan cara yang lebih eksplisit untuk mewakili hubungan antar tabel.

Istilah *basis data* mengacu pada koleksi dari data-data yang saling berhubungan, dan perangkat lunaknya seharusnya mengacu sebagai *sistem manajemen basis data* (*database management system/DBMS*). Jika konteksnya sudah jelas, banyak administrator dan programer menggunakan istilah basis data untuk kedua arti tersebut.

1.1

1.2 2.3.1 Lingkungan basis data

1.3

Lingkungan basis data adalah sebuah habitat di mana terdapat basis data untuk bisnis. Dalam lingkungan basis data, pengguna memiliki alat untuk mengakses data. Pengguna melakukan semua tipe pekerjaan dan keperluan mereka bervariasi seperti menggali data (*data mining*), memodifikasi data, atau berusaha membuat data baru. Masih dalam lingkungan basis data, pengguna tertentu tidak diperbolehkan mengakses data, baik secara fisik maupun logis. (Koh, 2005, dalam Janner Simarmata & Imam Paryudi 2006: 33).

1.4 2.3.2Tahapan perancangan basis data

Perancangan basis data merupakan upaya untuk membangun sebuah basis data dalam suatu lingkungan bisnis. Untuk membangun sebuah basis data terdapat tahapan-tahapan yang perlu kita lalui yaitu:

1. Perencanaan basis data
2. Mendefinisikan sistem
3. Analisa dan mengumpulkan kebutuhan
4. Perancangan basis data
5. Perancangan aplikasi
6. Membuat prototipe
7. Implementasi
8. Konversi data
9. Pengujian
10. Pemeliharaan operasional

1.5

1.6 2.3.3 Bahasa pada basis data

Terdapat dua jenis bahasa komputer yang digunakan saat kita ingin membangun dan memanipulasi sebuah basis data, yaitu:

1. Data Definition Language (DDL)
2. Data Manipulation Language (DML)

1.7 2.3.4 Perangkat lunak basis data

Perangkat lunak basis data yang banyak digunakan dalam pemrograman dan merupakan perangkat basis data aras tinggi (*high level*):

- Microsoft SQL Server
- Oracle
- Sybase
- Interbase
- XBase
- Firebird
- MySQL
- PostgreSQL
- Microsoft Access
- dBase III
- Paradox
- FoxPro
- Visual FoxPro

- Arago
- Force
- Recital
- dbFast
- dbXL
- Quicksilver
- Clipper
- FlagShip
- Harbour
- Visual dBase
- Lotus Smart Suite Approach
- db2
- MongoDB

2.4 Jaringan

Menurut Sukamanji dan Rianto (2008:1) Jaringan Komputer adalah sekelompok kumputer otonom yang berhubungan satu dengan yan lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, aplikasi dan perangkat keras secara bersama-sama. Jaringan komputer dibangun untuk membawa informasi secara tepat.

Menurut Vygoriviva (2008:107) Komputer yang memiliki bug DCOM bias membuat orang lain mengakses komputer itu dari jarak jauh. Hal ini terjadi karena DCOM akan mengaktifkan COM dalam komputer untuk berkomusi dengan COM lainnya, seperti menggunakan netbios untuk sharing dalam Windows.

2.5 Firewall

Sistem/mekanisme yang diterapkan terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN) Firewall secara umum di peruntukkan untuk melayani :

i. Mesin/komputer

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

ii. 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.

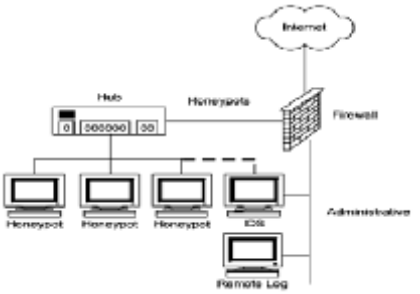
2.6 System Honeypots

Spitzner, Lance (2003*) Honeypot* merupakan salah satu jenis teknologi terbaru di bidang keamanan sistem dan jaringan komputer yang digunakan sebagai pelengkap teknologi keamanansebelumnya. Teknologi keamanan sebelumnya seperti firewall dan IDS *(Intrusion Detection System)* merupakan teknologi konvensional dimana sistem pertahanan di bangun untuk mencegah penyerang menembus masuk ke dalam area yang di lindungi.

Honeypot berbeda dari teknologi pertahanan konvensional sebelumnya dimana sistem pertahanan akan bernilai apabila penyerang telah masuk ke dalam sistem. Sistem honeypot akan melakukan monitoring terhadap aktivitas penyerang dengan menggunakan berbagai macam teknologi sehingga penyerang merasa aktivitas yang dilakukannya telahberhasil dan mengira sedang melakukan interaksi dengan sistem yang sebenarnya.

Honeynet mengimplementasikan Data Control dan Data Capture secara sederhana namun efektif. *Honeynet* yang menjadi gateway adalah firewall layer 3 (tiga). Firewall digunakan untuk memisahkan sistem *Honeynet* menjadi tiga jaringan yaitu Internet, *Honeypots* dan *Administrative.*Setiap paket yang menuju ataupun meninggalkan sistem Honeynet harus melewati firewall.

Firewall tersebut yang juga berfungsi sebagai Data Control akan diset untuk mengatur koneksi inbound dan outbound. Dikarenakan firewall tersebut merupakan bagian dari system Honeynet, maka konfigurasi firewall tersebut sedikit berbeda dengan konfigurasi firewall pada umumnya yaitu mengizinkan setiap koneksi inbound untuk masuk dan mengontrol / membatasi setiap koneksi outbound yang keluar dari sistem.



Gambar 2.1 Implementasi honeypot 3 layer

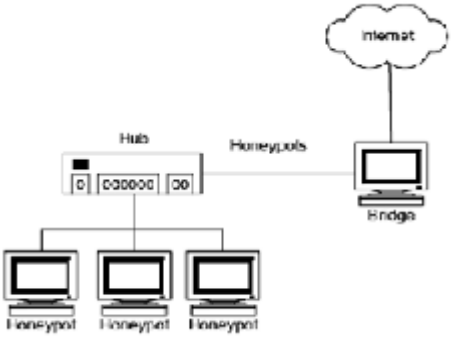
Data Capture yang diterapkan pada Honeynet terdiri dari beberapa layer / bagian. Layer pertama adalah log yang terdapat pada firewall itu sendiri. Firewall log akan mencatat setiap koneksi yang menuju atau meninggalkan Honeynet.layer kedua adalah sistem IDS. Fungsi IDS adalah untuk menangkap setiap aktivitas yang terjadi pada jaringan dan juga karena pada umumnya IDS mempunyai signature database maka IDS dapat memberikan informasi yang lengkap dari suatu koneksi yang terjadi.

Layer ketiga adalah pada honeypot-honeypot itu sendiri. Ini dilakukan dengan cara mengaktifkan system log pada honeypot –honeypot yang digunakan. System log kemudian diset agar tidak hanya melakukan pencatatan secara lokal, tetapi juga secara remote ke sebuah remote log server

Remote log server ini harus didisain lebih aman daripada *honeypot* . *honeypot* yang ada agar data-data yang didapat tidak hilang. Untuk membuat suatu solusi yang lebih mudah untuk diterapkan tetapi lebih susah untuk dideteksi oleh penyerang.

Pada GenII *Honeynet* semua kebutuhan honeynet (Data Control dan Capture) diterapkan hanya pada satu sistem saja (gateway) dan yang menjadi gateway adalah bridge layer 2 (dua).

Keuntungan menggunakan gateway berupa bridge layer 2 (dua) adalah layer 2 bridge tidak mempunyai IP stack sehingga ketika paket melewatinya tidak terjadi routing ataupun pengurangan TTL yang mengakibatkan gateway akan semakin sulit untuk dideteksi.



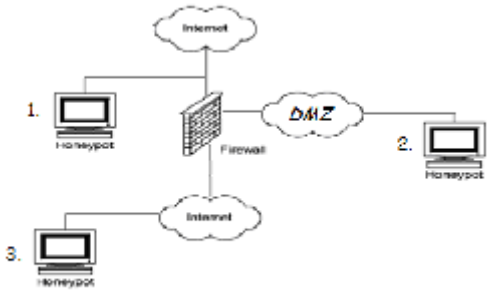
Gambar 2.2 Implementasi honeypot 2 layer

Spitzner (*www.tracking-attacker.com*) *honeypot* merupakan sebuah sistem atau computer yang sengaja .dikorbankan. untuk menjadi target serangan dari attacker. Komputer tersebut melayani setiap serangan yang dilakukan oleh attacker dalam melakukan penetrasi terhadap server tersebut.

Metode ini ditujukan agar administrator dari server yang akan diserang dapat mengetahui trik penetrasi yang dilakukan oleh attacker serta agar dapat melakukan antisipasi dalam melindungi server yang sesungguhnya. Setiap tindakan yang dilakukan oleh penyusup yang mencoba melakukan koneksi ke honeypot tersebut, maka honeypot akan mendeteksidan mencatatnya.

Peran dari honeypot bukanlah menyelesaikan suatu masalah yang akan dihadapi server, akan tetapi memiliki kontribusi dalam hal keseluruhan keamanan. Dan besarnya kontribusi tersebut tergantung dari bagaimana kita menggunakannya.
Intinya, walaupun tidak secara langsung melakukan pencegahan terhadap serangan (firewall) tetapi dapat mengurangi dari intensitas serangan yang akan dilakukan oleh penyusup ke server yang sesungguhnya.

Biasanya honeypot ditempatkan di lokasi –lokasi berikut ;
A. Didepan gateway(dekat dengan jaringan public (internet))
B. Didalam DMZ (Demiliterized Zone)
C . Dibelakang gateway (dekat dengan jaringan public (internet))



Gambar 2.3 Letak Honepot

Setiap lokasi memiliki kelebihan dan kekurangan masing-masing , oleh karma itu dibutuhkan pertimbangan-pertimbangan sebelum lokasi ditentukan .

A. Didepan gateway(dekat dengan jaringan public (internet))
Kelebihan dari penempatan honeypot dilokasi iniadalah honepot akan di angap sama seperti dengan system external sehingga akan mengurangi resiko terhadap jaringan privat ,apabila honeypot berhasil disusupi atau diambil alih oleh penyerang ,kekurangan adalah terafik-trafik tidak sah yang dicatat oleh honeypot tidak akan tercatat dan membangkitkan alert oleh firewall dan IDS sehingga informasi sangan berkurang.

B. Didalam DMZ (Demiliterized Zone)

Pada gateway biasanya terdapat pengamanan sama seperti firewall,di lokasi ini ,kelebihan yang didapat terhadap trafik tidak sah yang menuju honeypot akan melewati firewall akan tercatat di firewall log, dengan demikian ada informasi yang terkumpul ,kekurangan dari letak honepot di lokasi ini adalah system lain yang berada di DMZ harus di amankan dari honeypot , karena bila honepot berhasil disusupi dan di ambil alih maka kemungkinan honeypot tersebut dapat digunakan untuk menyerang system lain yang berada di DMZ bahkan menyerang firewall yang terdapat pada gateway.

C . Dibelakang gateway (dekat dengan jaringan public (internet))

Alasan honeypot ditempatkan dilokasi ini aadalah untuk mengantisipasi penyerang yang berasal dari dalam atau untuk mendeteksi firewall yang tidak terkonfigurasi dengan baik sehinga menyebabkan adanya trafik tidak sah yang
Menuju jaringan prifat. Penempatan honeypot pada lokasi ini akan menambah resiko pada jaringan privat karma bila honeypot berhasil disusupi dan diambil alih maka penyerang akan mendapatkan akses menuju jaringan privat dari honeypot, dengan kata lain honeypot akan dapat digunakan sebagai batu loncatan untuk menyerang jaringan privat.

2.6.1 Klassifikasi Honeypots

berdasarkan level of involvement (tingkat keterlibatan). Level of involvement mengukur derajat interaksi seorang penyerang dengan sistem informasi. Terdiri dari dua jenis yakni low involvement Honeypot dan high involvement Honeypot.

1. Low Involvement Honeypot

Low-Interaction Honeypot merupakan yang paling mudah diinstal dan dipelihara karena desainnya yang sederhana dan fungsionalitas dasar. Normalnya teknologi ini hanya meniru berbagai macam service. Contohnya, honeypot dapat meniru server Unix dengan beberapa service yang berjalan,

seperti Telnet dan FTP. Penyerang dapat melakukan Telnet ke honeypot, mendapatkan identitas system operasi, dan bahkan mendapatkan prompt login. Penyerang dapat melakukan login dengan metode brute force atau

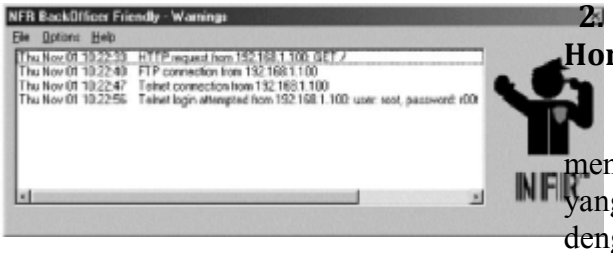
menebak password. Honeypot akan merekam dan mengumpulkan percobaan login yang dilakukan oleh penyerang.

Karena low-interaction honeypot mudah untuk dideploy dan dipelihara karena keterbatasan kemampuan interaksi yang juga mengurangi resiko. Juga karena keterbatasan itu pula, low-interaction honeypot hanya menyimpan data sebagai berikut :

· Tanggal dan waktu serangan

· Sumber alamat IP dan port dari serangan

· Tujuan alamat IP dan port serangan



Gambar 2.4 Informasi yang didapat oleh tools BackOfficer

keterbatasan fitur yang dimiliki oleh low-interaction honeypot, terdapat beberapa kekurangan yang dimiliknya. Yang paling krusial yaitu apabila penyerang merupakan orang asli dan tidak menggunakan tools otomatis seperti trojan atau worm maka penyerang dapat segera menyadari bahwa yang dihadapi olehnya adalah honeypot dan bukan system sebenarnya karena minimnya service yang bisa diakses.

Pada Low Involvement Honeypot tidak ada sistem operasi nyata yang dapat dipakai sebagai tempat operasi penyerang. Ini akan dapat mengurangi resiko secara signifikan karena kompleksitas dari suatu sistem operasi telah ditiadakan. Di sisi lain ini adalah juga suatu kelemahan yang berakibat tidak adanya kemungkinan untuk memperhatikan interaksi penyerang dengan sistem operasi yang bisa jadi sangat menarik. Low Involvement Honeypot adalah seperti sebuah koneksi satu arah. Kita hanya akan dapat mendengarkan tanpa bisa menanyakan pertanyaan sendiri. Pendekatan cara ini sangat pasif.

2. Medium-Interaction Honeypot

Medium-interaction honeypot menyediakan kemampuan interaksi yang lebih bila dibandingkan dengan low-interaction honeypot namun fungsionalitasnya masih dibawah high-interaction honeypot. Contohnya, honeypot dapat dibuat untuk meniru Microsoft IIS web server termasuk fungsionalitas tambahan yang biasa terdapat pada dirinya. IIS web server yang ditiru dapat dirubah sesuai dengan keiginan penyerang. Ketika koneksi HTTP dibuat oleh honeypot, ia akan merespon sebagai IIS web server dan memberikan peluang kepada penyerang.

Dengan kemampuan yang dimiliki oleh medium-interaction honeypot, perlu diperhatikan bahwa medium-interaction honeypot cukup kompleks sehingga diperlukan usaha yang lebih untuk

pemeliharaan dan deploy system sehingga penyerang tidak akan mencurigai system yang diserangnya adalah sebuah honeypot. Walaupun begitu, medium-interaction honeypot menghasilkan informasi yang lebih banyak bila dibandingkan dengan low-level interaction.

3. High Involvement Honeypot

High-Interaction Honeypot adalah teknologi honeyspot yang paling ekstrim. Ia memberikan informasi yang sangat banyak mengenai penyerang tapi memerlukan waktu untuk mendapatkannya. Tujuan dari high-interaction honeyspot adalah memberikan akses system operasi yang nyata kepada penyerang dimana tidak ada batasan yang ditentukan.

```
220-Serv-U FTP-Server v2.5h for WinSock ready...
220--------H-A-C-K T-H-E P-L-A-N-E-T--------
220-W3l_c0m3 T0 JohnA's 0d4y Ef-Tec-Pec 63rv3r.
220-Featuring 100% elite hax0r warez!@$@@
220-Im running win 95 (Release candidate 1),.
220 -------H-A-C-K  T-H-E  P-L-A-N-E-T--------
USER johna2k
331 User name okay, need password.
PASS haxedj00
230 User logged in, proceed.
PORT 172,16,1,106,12,71
200 PORT Command successful.
RETR nc.exe
150 Opening ASCII mode data connection for nc.exe (59392 bytes).
226 Transfer complete.
PORT 172,16,1,106,12,72
200 PORT Command successful.
RETR pdump.exe
150 Opening ASCII mode data connection for pdump.exe
(32768 bytes).
226 Transfer complete.
PORT 172,16,1,106,12,73
200 PORT Command successful.
RETR samdump.dll
150 Opening ASCII mode data connection for samdump.dll
(36864 bytes).
226 Transfer complete.
QUIT
221 Buh bye, you seeksi hax0r j00 :|
```

Gambar 2.5 Contoh data session FTP dari high-interaction NT honeyspot

Karena mekanisme control yan luas, high-interaction honeypot sangatlah sulit dan menghabiskan waktu untuk dinstal dan dikonfigurasikan. Berbagai macam teknologi yang berbeda terllibat disini seperti firewall atau Intrusion Detection System (IDS) haruslah disesuaikan dengan seksama. Pemeliharaannya pun menghabiskan waktu, seperti mengupdate rulebase firewall dan signature database IDS serta mengawasi honeyspot terus menerus. High-interaction Honeypot akan menjadi solusi yang baik apabila diimplementasikan dengan benar, dan begitu pula kebalikannya jika high-interaction honeypot tidak diimplementasikan dengan benar maka penyerang dapat mengambil alih dan ia akan menjadi bumerang yang berbahaya.

Honeypot juga dapat dibedakan menjadi dua yaitu *Physical* yaitu Mesin sungguhan dalam jaringan dengan alamat IP sendiri. dan Virtual yaitu honeypots yang disimulasikan oleh mesin lain yang berespon pada traffic jaringan yang dikirim ke
virtual honeypot.

Suatu honeypots merupakan sumber system informasi yang menghasilkan nilai palsu pada saat terjadi penggunaan sumber daya yang tidak sah tidak diijinkan.

2.7 Intrusion Detection System(IDS)

Intrusion detection system adalah suatu perangkat lunak (software) atau suatu system perangkat keras (hardware) yang bekerja secara otomatis untuk memonitor kejadian pada jaringan komputer dan dapat

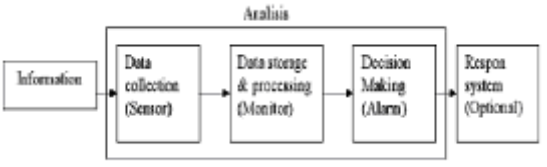
menganalisa masalah keamanan jaringan. IDS memiliki 3 (tiga) komponen fungsi fundamental yang merupakan proses utama dalam
IDS. Komponen fungsi itu antara lain :

i. Pengambilan Data (Information Sources).
Komponen ini merupakan fungsi untuk melakukan pengambilan data dari berbagai sumber yang ada pada sistem yang diamati.

ii. Analisis. Bagian ini melakukan organisasi terhadap data yang diperoleh, mengambil kesimpulan terhadap pelanggaran / intrusion baik yang sedang terjadi maupun yang telah terjadi.

Komponen ini melakukan beberapa aksi pada sistem setelah pelanggaran yang terjadi telah terdeteksi. Respon ini dapat dikelompokkan menjadi 2 (dua), yaitu respon aktif dan respon pasif.

Respon aktif dalam hal ini berarti melakukan beberapa aksi secara otomatis untuk mengintervensi sistem yang ada, sedangkan pasif adalah memberikan report pada administrator yang akan melakukan respon terhadap sistem.



Gambar 2.6 Blog Diagram Intruksion Deteksion Sistem

2.8 SQL Injection

Injeksi *SQL* adalah sebuah teknik yang menyalahgunakan sebuah celah keamanan
terjadi dalam lapisan basis data Celah ini terjadi ketika masukan pengguna tidak
disaring secara benar dari karakterbentukan string yang diimbuhkan dalam pernyataan
SQL atau masukan pengguna tidak karenanya dijalankan tidak sesuai harapan. Pada
dasarnya sql injection adalah sebuah contoh dari sebuah kategori celah keamanan yang lebih umum yang dapat terjadi setiap kali sebuah bahasa pemrograman atau skrip diimbuhkan di dalam bahasa yang lain.

2.9 Denial Of Service (DOS)

Denial of Service adalah aktifitas menghambat kerja sebuah layanan (servis) atau mematikannya sehingga user yang berhak/berkepentingan tidak dapat menggunakan layanan tersebut. Dampak akhir dari aktifitas ini menjurus kepada tehambatnya 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 membingungkan antara layanan dan kenyamanan terhadap keamanan. Seperti yang
kita tahu, keyamanan berbanding terbalik dengan keamanan. Maka resiko yang mungkin timbul selalu mengikuti hukum ini.

Wood (2003) DoS attack ditandai oleh usaha attacker untuk

mencegah legitimate user dari penggunaan resource yang diinginkan. Adapun beberapa metode untuk melakukan DoS attack sebagai berikut:

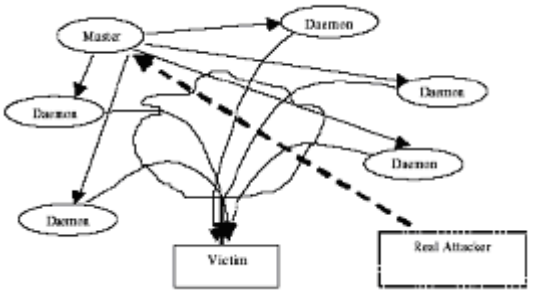
i. Mencoba untuk membanjiri (flood) network, dengan demikian mencegah lalu lintas yanglegitimate pada network.

ii. Mencoba mengganggu koneksi antara dua mesin, dengan demikian mencegah suatu akses layanan.

iii. Mencoba untuk mencegah individu tertentu dari mengakses layanan.

iv. Mencoba untuk mengganggu layanan system yang spesifik atau layanan itu sendiri.

Format terdistribusi membuat dimensi menjadi .*many to one*., dimana jenis serangan ini lebih sulit untuk dicegah. DDoS adalah terdiri dari 4 elemen seperti gambar 2.6 dibawah ini .



Gambar 2.7 Gambar 4element DDos attack.

Empat elemen tersebut adalah:

1. Korban (victim) yakni host yang dipilihuntuk diserang.

2. Attack Daemon Agents, merupakan program agen yang benar serangan pada target korban. Serangan daemon biasanya menyebar ke computer komputer host. Daemon ini mempengaruhi target dan computer Manfaat serangan daemon ini dipergunakan attacker untuk untuk memperoleh akses dan menyusup ke kompute

3. Kendali Program Master, Yakni Tugasnya adalah untuk mengkoordinir serangan.

4. Attacker (penyerang), yakni penyerang riil, dalang di belakang serangan. Dengan penggunaan kendali master program, penyerang riil dapat berdiri dibelakang layer serangan. Langkah-Langkah yang berikut berlangsung pada saat serangan terdistribusi:

i. Penyerang riil mengirimkan suatu .execute. pesan kepada kendali master program.

ii. Kendali master program menerima .execute. pesan kemudian menyebarkan perintah ini kepada attack daemons dibawah kendalinya.

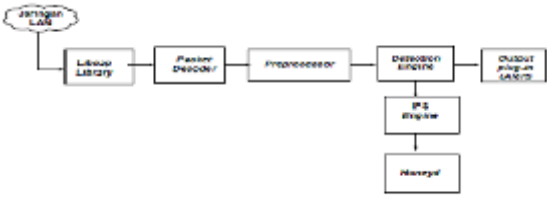
iii. Ketika menerima perintah penyerangan, attack daemons mulai menyerang korban (victim). Walaupun nampaknya penyerang riil hanya melakukan sedikit pekerjaan disini, namun dengan melakukan pengiriman .execute. command, sebenarnya telah merencanakan pelaksanaan DDoS attacks. Attacker harus menyusup ke semua komputer host dan network dimana daemon attacker dapat

disebar. Attacker harus mempelajari topologi jaringan target, kemudian melakukan pencarian bottlenecks dan kelemahan jaringan untuk dimanfaatkan selama serangan. Oleh karena penggunaan attack daemon dan kendali master program, penyerang real tidak secara langsung
dilibatkan sepanjang searangan, dimana keadaan ini membuat dia sulit dilacak sebagai pembuat serangan.

BAB III
METODOLOGI PENELITIAN

3.1 Diagram Blok Sistem Snort IDS dan Honeyd

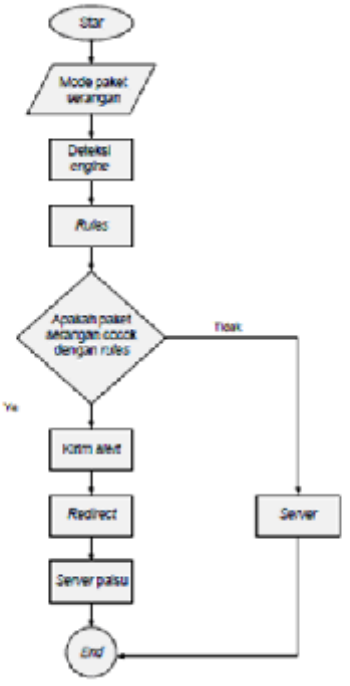
Gambar 1 merupakan diagram blok sistem pencegahan penyusupan yang dimana libpcap library, packet decoder, dan preproccesor bekerja untuk menangkap dan mengelompokan paket data yang ada dalam suatu jaringan. Detection engine bekerja menentukan apakah paket data tersebut terdeteksi serangan atau bukan. IPS engine bekerja membaca alert pada database lalu memerintahkan iptables membelokan (redirect) serangan. Honeyd bekerja sebagai server palsu dimana mensimulasikan tingkah laku sebuah komputer beserta sistem operasinya, sedangkan output plug-in bekerja menghasilkan report atau alert.



Gambar 3.1 Diagram Blok Pencegahan Penyusupan

3.2 Flowchart Sistem Pencegahan Penyusupan

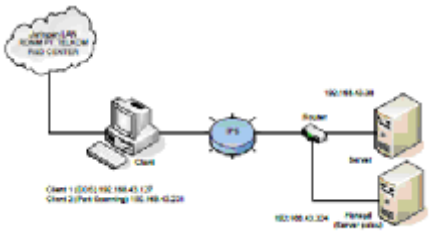
Untuk mengetahui prinsip kerja dari sistem yang akan dirancang, maka agar lebih mudah dalam pemahamannya dibuatlah terlebih dahulu diagram alir (flowchart) dari sistem tersebut. Gambar 2 menjelaskan apabila ada paket data yang masuk, sistem ini akan mulai bekerja yaitu dengan mengidentifikasi mode paket serangan apakah paket data tersebut. Setelah diketahui mode paketnya, pada detection engine akan membandingkan apakah sama dengan rules yang telah ada pada Snort, jika sama maka Snort akan mengeluarkan alert lalu membelokkan serangan tersebut ke Honeyd, jika tidak paket data tersebut langsung di kirim ke server.



Gambar 3.2 Flowchart Sisrem pencegahan penyusup.

3.3 Topologi

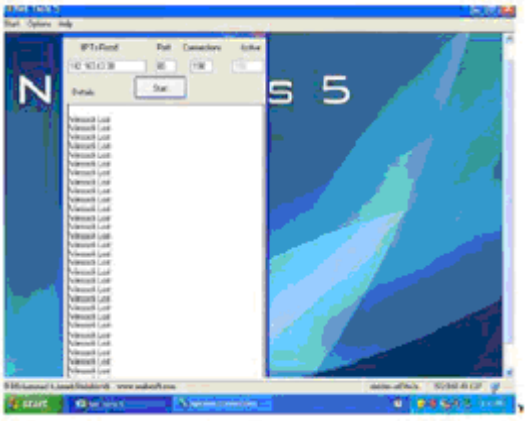
Topologi yang dirancang dapat diilustrasikan pada Gambar 3 yaitu terdapat Jaringan Lan yang terdapat pada PT.Telkom, client berupa DOS dan Port Scanning, IPS yang terdiri dari Snort IDS dan blockit, server, dan Honeyd (server palsu)(fauzi, 2010).



Gambar 3.3 Topologi system pencegahan penyusup

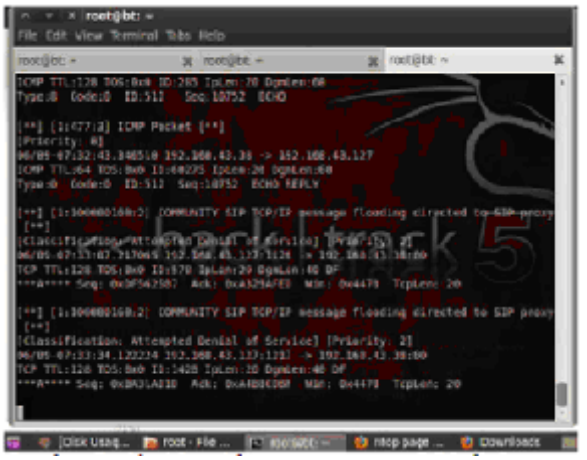
3.4 Pengujian Sistem Pencegahan Penyusupan Jaringan

Untuk menguji sistem pencegahan penyusupan yaitu dengan cara melancarkan paket serangan dari client ke server. Dalam perancangan ini, serangan yang digunakan adalah Port Scanning dan DOS.



Gambar 3.4 Paket serangan DOS (Daniel Of Service)

Serangan DOS dibangkitkan oleh Net-Tools pada client 1 dengan IP 192.168.43.127, pada Gambar 3.4 memperlihatkan bahwa client 1 telah mengirimkan paket serangan. Setelah serangan dikirim, Snort di server mengeluarkan alert bahwa IP 192.168.43.127 melakukan serangan berupa DOS dapat dilihat pada Gambar 5 yang terdiri dari IP penyerang, IP yang diserang dan bentuk serangan (Rafiudin, 2010).

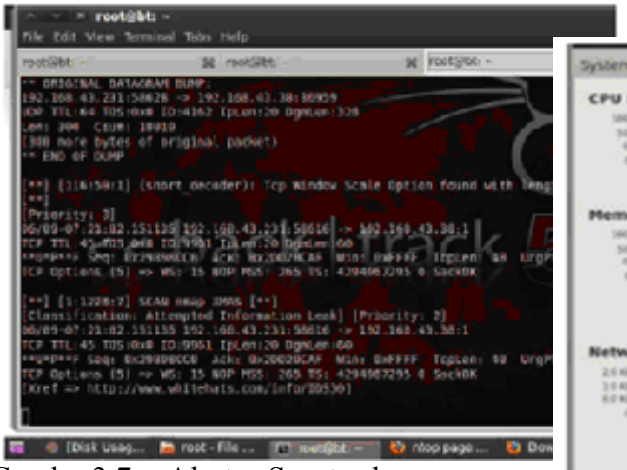


Gambar3.5 Alert Snort berupa serangan DOS di Server

Gambar3.6 Paket Serangan Port Scanning (nmap)

Serangan Port Scanning dibangkitkan oleh nmap berupa Zenmap pada client 2 dengan IP 192.168.43.231, pada Gambar 6 memperlihatkan bahwa client 2 telah mengirimkan paket serangan. Setelah serangan dikirim, Snort di

server mengeluarkan alert bahwa IP 192.168.43.127 melakukan serangan berupa Port
Scanning (nmap) yang dapat dilihat pada Gambar 7 yang terdiri dari IP penyerang, IP yang diserang dan bentuk serangan.



Gambar3.7 Alert Snort berupa serangan Port Scanning di Server

BAB IV

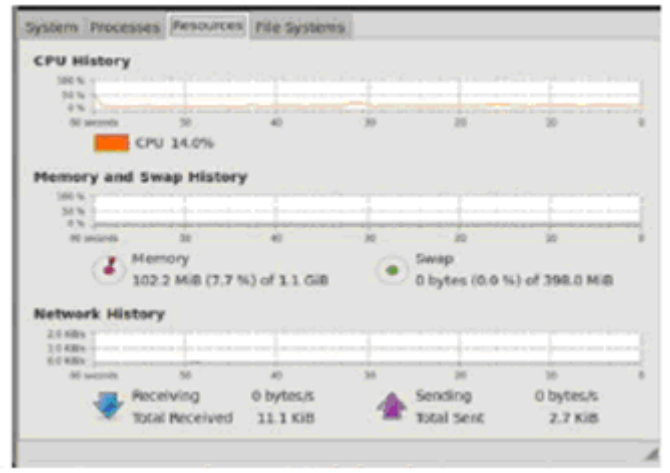
Hasil Pengujian

Pengujian dilakukan dengan beberapa tahap. Berikut ini tahap-tahap hasil pengujian yang dilakukan:

4.1. Hasil pengujian saat tidak ada serangan .

Pada pengujian ini, sistem pencegahan penyusupan dalam keadaan normal yaitu tidak ada paket data yang dikirim berupa serangan port scanning dan DOS dengan topologi pada Gambar 4.1 Hasil dari pengujian sebelum adanya serangan dapat dilihat pada Gambar 4.2 yaitu kapasitas memory 102,2 MB.

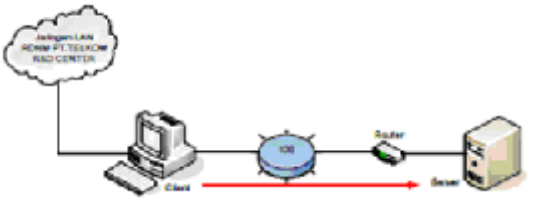
Gambar 4.1 Topologi pengujian saat tidak ada serangan penyusup (intruder)



Gambar 4.2 Keadaan server pada saat tidak ada serangan penyusup (intruder)

4.2. Hasil pengujian saat ada serangan penyusup (intruder)

Pada pengujian ini, serangan berupa port scanning dan DOS langsung menuju server tanpa adanya pencegahan penyusupan dengan topologi pada Gambar 4.3 Hasil dari pengujian setelah adanya serangan dapat dilihat pada Gambar 4.4 yaitu kapasitas memory naik menjadi 330,2 MB.



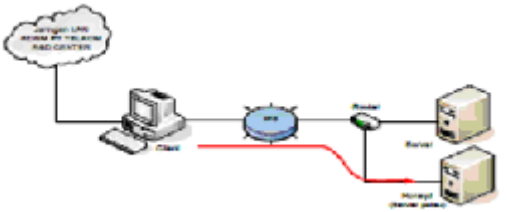
Gambar 4.3 Topologi pengujian saat terjadi serangan penyusup (intruder)

Gambar 4.4 Keadaan server saat terjadi serangan penyusup (intruder)

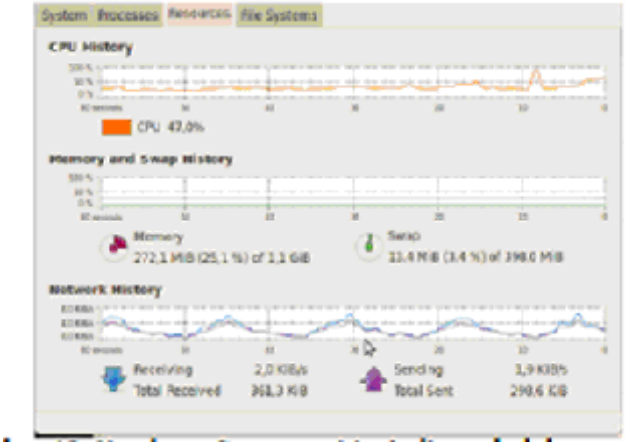
4.3. Hasil pengujian pembelokan serangan penyusup

Pada pengujian ini, serangan yang berupa port scanning dan DOS akan dibelokan (redirect) menuju server palsu (Honeyd) dengan toplogi pada Gambar 4.5. Hasil dari pengujian setelah adanya pembelokan serangan penyusup dapat dilihat pada Gambar 4.6 yaitu keadaan kapasitas memory turun menjadi 272,1 MB.

Jaringan LAN RDNM

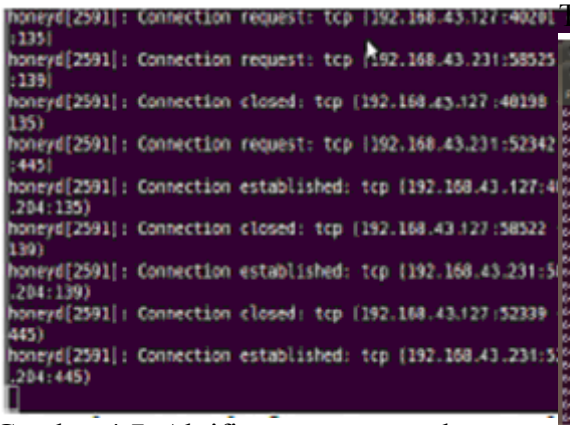


Gambar 4.5 Topologi pengujian saat terjadi pembelokan serangan penyusup



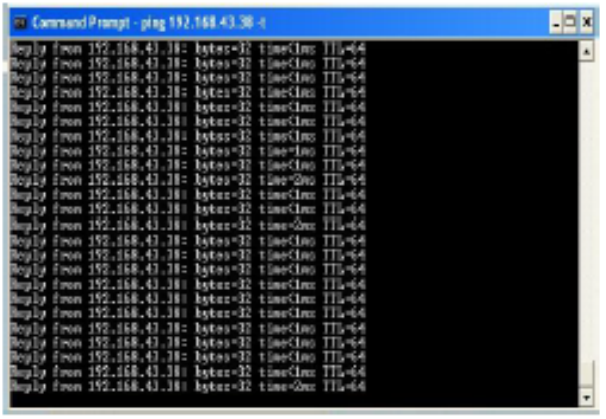
Gambar 4.6 keadaan server saat terjadi pembelokan serangan penyusup

Setelah mendapatkan serangan penyusup (intruder) berupa port scanning dan DOS, Snort akan mengeluarkan alert. Alert yang keluar dari Snort akan dibaca oleh IPS engine berupa blockit (Isnan, 2011) yang bertugas untuk memerintahkan iptables untuk membelokan akses penyusupan ke server palsu (Honeyd) dengan sintaks seperti berikut:



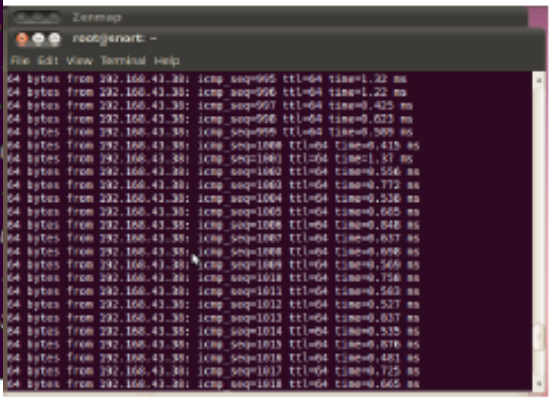
Gambar 4.7 Aktifitas serangan pada honeyd

Pada Honeyd (server palsu) akan menampilkan aktifitas serangan yang terdiri IP serangan port scanning dan IP DOS seperti pada Gambar 4.7 (Utdirartatmo, 2005). Pembelokan serangan pada server palsu, tidak memberikan kecurigaan pada intruder (penyusup), karena penyusup (intruder) dengan IP 192.168.43.127 dan 192.168.43.231 masih bisa mengakses IP 192.168.43.38 dapat dilihat pada Gambar 4.8 (a) bukti bahwa DOS masih terhubung pada server dan (b) bukti bahwa port scanning masih terhubung pada server.



(a)

Gambar 4.8 (a) Bukti Bahwa DOS (Denial Of Service) Masih Terhubung



(b)

Gambar 4.8 (b) Bukti Bahwa Port Scanning Masih Terhubung ke Server