**BAB II**

**LANDASAN TEORI**

**2.1 Jaringan Komputer**

Jaringan Komputer adalah suatu sistem yang didalamnya terdiri dari dua atau lebih perangkat komputer serta perangkat - perangkat lainnya yang dibuat atau dirancang untuk dapat berkerja sama dengan tujuan agar dapat berkomunikasi, mengakses informasi, meminta serta memberikan layanan atau service antara komputer satu dengan yang lainnya.

## 2.1.1 Jenis-Jenis Jaringan Komputer

**1. Berdasarkan Letak Geografisnya Atau Jangkauan**

**a. LAN ( Local Area Network )**

Merupakan jaringan yang mencakup wilayah kecil, salah satu contoh adalah jaringan komputer yang berada dilingkup sekolah, kampus atau kantor.

**b. MAN ( Metropolitan Area Network )**

Merupakan sebuah jaringan yang berada di dalam satu kota dengan kecepatan transfer data tinggi yang menghubungkan beberapa kantor tetapi masih dalam satu wilayah kota.

**c. WAN ( Wide Area Network )**

Merupakan jaringan komputer yang mencakup area yang sangat luas, salah satu contoh dari WAN adalah jaringan antar wilayah, daerah, kota atau bisa jadi antar negara.

**2.1.2 Berdasarkan Fungsinya**

#### a. Jaringan Komputer Peer to Peer

Merupakan model jaringan komputer dimana dalam jaringan tersebut, setiap komputer dapat difungsikan sebagai Client dan juga sebagai Server.

#### b. Jaringan Komputer Client Server

Merupakan sebuah model jaringan komputer dimana salah satu dari komputer difungsikan sebagai Server yang bertugas melayani komputer lain yang difungsikan sebagai Client. jadi dalam model jaringan ini komputer server biasanya didisain khusus dan hanya bertugas sebagai penyedia layanan yang dibutuhkan Client.

**2.1.3 Berdasarkan Media Transmisinya**

#### a. Jaringan Komputer Menggunakan Media Kabel ( Wired Network )

Jenis jaringan komputer yang satu ini biasanya menggunakan media kabel sebagai media transmisinya ada Jenis jaringan ini disebut juga dengan jenis jaringan menggunakan media transmisi terpadu ( Guided Transmission Media ). beberapa kabel yang bisa digunakan untuk membuat model jaringan seperti ini diantaranya, Kabel Coaxial, Kabel TP ( STP dan UTP ), serta Kabel Fiber Optic.

#### b. Jaringan Komputer Tanpa Menggunakan Kabel ( Nirkable )

Jenis jaringan komputer ini menggunakan sistem gelombang sebagai media Transmisinya, jenis jaringan ini juga disebut sebagai jenis jaringan yang menggunakan media transmisi tidak terpandu ( Unguided transmission media ), beberapa contoh media yang bisa digunakan antara lain : Gelombang Mikro, Satelit dan Sinar Infra Merah.

**2.1.4 Berdasarkan Distribusi Sumber Transmisi Datanya**

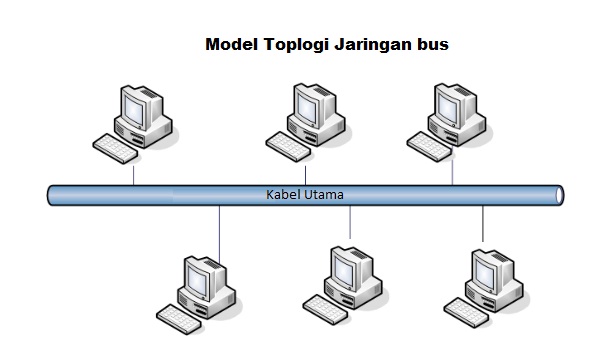
#### a. Jaringan Komputer Terpusat (Host Based Network)

Jenis Jaringan ini biasanya terdiri dari komputer client dan server dimana salah satu komputer client yang berfungsi sebagai perantara untuk dapat mengakses sumber informasi/data yang berasal dari komputer server

#### b. Jaringan Komputer Terdistribusi ( Distributed Network )

Jenis jaringan yang satu ini merupakan perpaduan antara beberapa jaringan terpusat sehingga terdapat beberapa komputer server yang saling berhubungan dengan klient dan membentuk sistem jaringan tertentu.

**2.1.5 Berdasarkan Topologinya**

**a. Topologi Bus**

**Gambar 2.1 Topology Bus**

**Topologi bus** merupakan sebuah topologi yang menggunakan kabel tunggal sebagai media transmisinya atau kabel pusat tempat dimana seluruh client dan server dihubungkan.

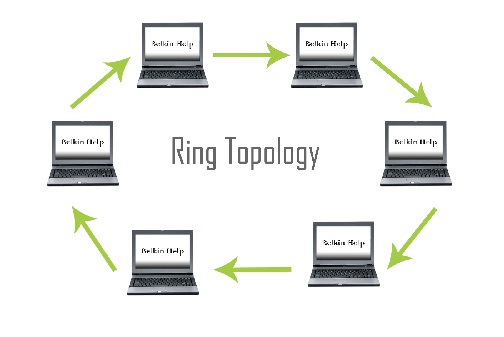
1. Keuntungan topologi bus

* Hemat kabel, karena pada topologi bus hanya menggunakan kabel tunggal dan terpusat sebagai media transmisi sehingga tidak membutuhkan banyak kabel.
* Layout kabel sederhana, pada pemasangan topologi bus rancangan dan skema kabel yang digunakan sangat sederhana sehingga mudah dalam pemasangannya.
* Pengembangan jaringan komputer atau penambahan komputer baru baik sebagai server maupun client dapat dilakukan dengan mudah tanpa mengganggu komputer atau workstation yang lain.

2. Kerugian topologi bus

* Deteksi dan isolasi kesalahan sangat kecil sehingga jika jaringan mengalami gangguan, maka akan lebih sulit untuk mengidentifikasi kesalahan yang ada.
* Kepadatan lalu lintas pada jalur utama, karena topologi bus menggunakan kabel terpusat sebagai media transmisi maka lalu lintas data akan sangat padat pada kabel utama.
* Jika kabel utama mengalami gangguan maka seluruh jaringan akan mengalami gangguan pula.
* Diperlukan repeater sebagai penguat sinyal jika akan menambahkan workstation dengan lokasi yang jauh.

**b. Topologi Ring**

****

Gambar 2.2 Topology Ring

Topologi cincin atau yang disebut topologi ring adalah topologi jaringan yang bentuknya rangkaian yang masing-masing tersambung ke dua titik yang lainnya, sehingga bisa membentuk jalur lingkaran yang menyerupai cincin. Kabel yang digunakan dalam topologi cincin merupakan kabel BNC, Oleh sebab itu tidak mempunyai ujung maka tidak dibutuhkan terminator. Tetapi topologi ini sudah banyak ditinggalkan karena mempunyai kelemahan yang serupa dengan topologi bus selain itu, pengembangan jaringan dengan menggunakan topologi ring ini relatif sulit dilakukan. Pada topologi Cincin semua node/ titik berfungsi sebagai repeater yang akan memperkuat sinyal di sepanjang sirkulasinya. Maksudnya setiap perangkat saling bekerja sama untuk menerima sinyal dari perangkat sebelumnya setelah itu diteruskan pada perangkat sesudahnya.

Kelebihan Topologi Cincin (Ring):

1. Lebih hemat kabel.

2. Tidak akan mengalami tabrakan pengiriman data (collision), karena di satu waktu hanya satu node yang bisa mengirimkan data/ data mengalir dalam satu arah.

3. Setiap komputer memiliki hak akses yang sama terhadap token sehinnga tidak ada komputer yang memonopoli jaringan.

Kekurangan Topologi Cincin (Ring):

1. Peka kesalahan, tiap node pada jaringan akan selalu ikut serta mengelola informasi yang dilewatkan dalam jaringan, sehingga jika di suatu node ditemukan gangguan maka semua jaringan akan mengalami gangguan.

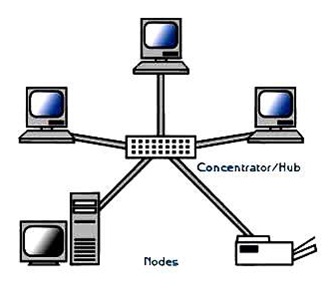
2. Jika terjadi kerusakan di jaringan topologi ring Sulit untuk diatasi.

3. Jika Ingin menambah komputer atau mengurangi komputer dapat mengacaukan jaringan.

4. Sulit untuk melakukan konfigurasi ulang.

5. Pengembangan jaringan lebih kaku.

**c. Topologi Star**

****

Gambar 2.3 Topology Star

Topologi star merupakan bentuk topologi jaringan yang berupa konvergensi dari node tengah ke setiap node atau pengguna. Topologi jaringan bintang termasuk topologi jaringan dengan biaya menengah.

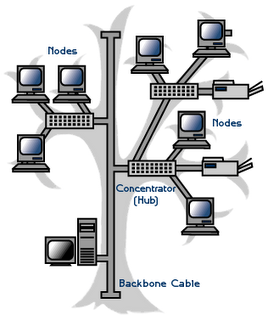
**Kelebihan dari topologi star :**

* Kerusakan pada satu saluran hanya akan memengaruhi jaringan pada saluran tersebut dan station yang terpaut.
* Tingkat keamanan termasuk tinggi.
* Tahan terhadap lalu lintas jaringan yang sibuk.
* Penambahan dan pengurangan station dapat dilakukan dengan mudah.
* Akses Kontrol terpusat.
* Kemudahan deteksi dan isolasi kesalahan/kerusakan pengelolaan jaringan.

**Kekurangan dari topologi star :**

* Jika node tengah mengalami kerusakan, maka seluruh rangkaian akan berhenti.
* Boros dalam pemakaian kabel.
* HUB/SWITCH jadi elemen kritis karena kontrol terpusat.
* Peran hub sangat sensitif sehingga ketika terdapat masalah dengan hub maka jaringan tersebut akan down.
* Jaringan tergantung pada terminal pusat.
* Jika menggunakan HUB dan lalu lintas data padat dapat menyebabkan jaringan lambat.
* Biaya jaringan lebih mahal daripada bus atau ring.

**d. Topologi Tree**

****

Gambar 2.4 Topology Tree

Topologi Pohon adalah kombinasi karakteristik antara topologi bintang dan topologi bus. Topologi ini terdiri atas kumpulan topologi bintang yang dihubungkan dalam satu topologi bus sebagai jalur tulang punggung atau *backbone*. Komputer-komputer dihubungkan ke hub, sedangkan hub lain di hubungkan sebagai jalur tulang punggung.

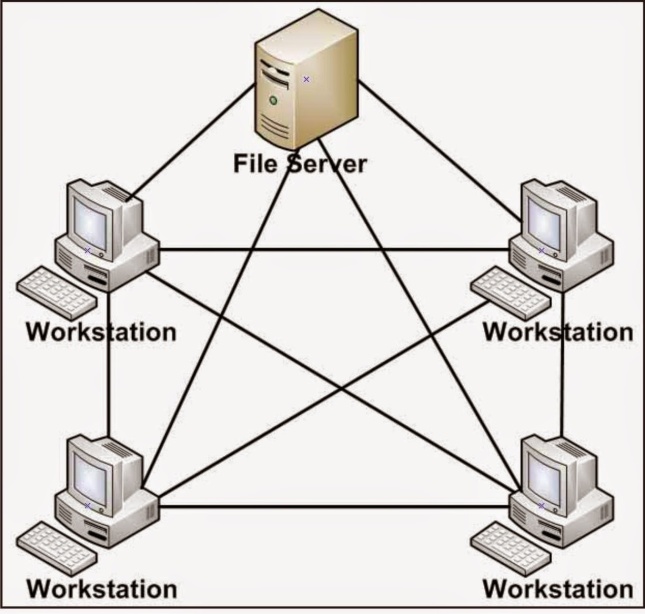
Kelebihan dari topologi Tree :

* Scalable, level-level dibawah level utama dapat menambahkan node baru dengan mudah.
* Koneksi terjadi secara point to point.
* Manajemen mudah karena mudah melakukan identifikasi dan isolasi kesalahan dalam jaringan.
* Mudah di kembangkan

Kekurangan dari topologi Tree :

* Pada area yang luas sulit untuk melakukan perawatan jaringan.
* Karena topologi ini adalah varian dari topologi BUS maka jika kabel backbone (kabel utama penyedia arus data) rusak maka seluruh jaringan akan down).
* Dapat terjadi tabrakan file data (collision).
* Lebih sulit untuk mengkonfigurasi dan memasang kabel dari pada topologi lain.
* Jika salah satu node rusak, maka node yang berada di jenjang bagian bawahnya akan rusak.
* Kabel yang digunakan menjadi lebih banyak sehingga diperlukan perencanaan yang matang dalam pengaturannya, termasuk di dalamnya adalah tata letak ruangan.

**e. Topology Mesh**

****

Gambar 2.5 Topology Mesh

Topologi Meshmerupakan sebuah perangkat yang saling berhubungan antara satu dengan yang lainnya.Topologi jenis ini memiliki kemampuan yaitu bisa berkomunikasi dengan perangkat yang dituju dengan cepat.Biasanya topologi ini digunakan pada sebuah [jaringan komputer](http://komputermesh.blogspot.com/2015/01/pengertian-jaringan-komputer.html) yang tidak besar.Memiiliki hubungan yang berlebihan antar peralatan yang ada,setiap peralatan saling terhubung dalam sebuah susunan dan semakin banyak jumlah perlatan maka semakin sulit pula cara mengendalkannya merupakan beberapa karakteristik topologi mesh.

Kekurangan dari topologi mesh : Terlalu boros kabel,pemasangan yang rumit,biaya yang cukup besar untuk merawat hubungan yang berlebih dan ketika jumlah komputer dan peralatan yang saling terhubung maka akan semakin sulit dalam melakukan instalasi dan konfigurasi ulang.

Kelebihan dari topologi mesh : Terjaminya kaspasitas channel komunikasi,karena memiliki hubungan berlebih,Relatif lebih mudah dalam Troubelshooting.sharing file akan lebih cepat sampai karena memiliki jalur masing-masing.

* 1. **Sistem Keamanan Jaringan**
     1. Pegertian keamanan jaringan

Keamanan jaringan adalah suatu cara atau suatu system yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan.

* + 1. Elemne pembentukan keaman jaringan

Ada dua elemen utama pembentuk keamanan jaringan :

* + - * Tembok pengamanan (baik secara fisik maupun maya), yaitu suatu cara untuk memberikan proteksi atau perlindugan pada jarigan, baik secara fisik (kenyataan) maupun maya (menggunakan software).
      * Rencana pengamanan, yaitu suatu rancagan yang nantinya akan di implementasiakan untuk melindugi jaringan agar terhindar dari berbagai ancaman dalam jaringan.
    1. Alasan keaman jaringan sangat penting

Alasan keaman jaringan sangat penting karena

* 1. Privacy / Confidentiality
     + - Defenisi : menjaga informasi dari orang yang tidak berhak mengakses.
       - Privacy : lebih kearah data-data yang sifatnya privat , Contoh : e-mail seorang pemakai (user) tidak boleh dibaca oleh administrator.
       - Confidentiality : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.
       - Contoh : 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) harus dapat diproteksi dalam penggunaan dan penyebarannya.
       - Bentuk Serangan : usaha penyadapan (dengan program sniffer).
       - Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.
  2. Integrity
     + - Defenisi : informasi tidak boleh diubah tanpa seijin pemilik informasi.
       - Contoh : e-mail di intercept di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.
       - Bentuk serangan : Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin, “man in the middle attack” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.
  3. Authentication
     + - Defenisi : metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.
       - Dukungan :
* Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking(untuk menjaga “intellectual property”, yaitu dengan menandai dokumen atau hasil karya dengan “tanda tangan” pembuat ) dan digital signature.
* Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.
  1. Availability
     + - Defenisi : berhubungan dengan ketersediaan informasi ketika dibutuhkan.
       - Contoh hambatan :
* “denial of service attack” (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.
* mailbomb, dimana seorang pemakai dikirimi 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.
  1. Access Control
     + - Defenisi : cara pengaturan akses kepada informasi berhubungan dengan masalah.
       - authentication dan juga privacy.
       - Metode : menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain.
  2. Non-repudiation
     + - Defenisi : Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce.
     1. Dasar-Dasar Keamanan Jaringan
        + - availability / ketersedian

hanya user tertentu saja yang mempunyai hak akses atau authorized diberi akses tepat waktu dan tidak terkendala apapun.

* + - * + Reliability / Kehandalan

Object tetap orisinil atau tidak diragukan keasliannya dan tidak dimodifikasi dalam perjalanannya dari sumber menuju penerimanya.

* + - * + Confidentiality / Kerahasiaan

Object tidak diumbar / dibocorkan kepada subject yang tidak seharusnya berhak terhadap object tersebut, lazim disebut tidak authorize.

* + 1. Syarat keaman jaringan
       - * Prevention (pencegahan).

Kebanyakan dari ancaman akan dapat ditepis dengan mudah, walaupun keadaan yang benarbenar 100% aman belum tentu dapat dicapai. Akses yang tidak diinginkan kedalam jaringan komputer dapat dicegah dengan memilih dan melakukan konfigurasi layanan (services) yang berjalan dengan hati-hati.

* + - * + Observation (observasi).

Ketika sebuah jaringan komputer sedang berjalan, dan sebuah akses yang tidak diinginkandicegah, maka proses perawatan dilakukan. Perawatan jaringan komputer harus termasuk melihat isi log yang tidak normal yang dapat merujuk ke masalah keamanan yang tidak terpantau. System IDS dapat digunakan sebagai bagian dari proses observasi tetapi menggunakan IDS seharusnya tidak merujuk kepada ketidak-pedulian pada informasi log yang disediakan.

* + - * + Response (respon)

Bila sesuatu yang tidak diinginkan terjadi dan keamanan suatu system telah berhasil disusupi,maka personil perawatan harus segera mengambil tindakan. Tergantung pada proses produktifitas dan masalah yang menyangkut dengan keamanan maka tindakan yang tepat harus segera dilaksanakan. Bila sebuah proses sangat vital pengaruhnya kepada fungsi system dan apabila di-shutdown akan menyebabkan lebih banyak kerugian daripada membiarkan system yang telah berhasil disusupi tetap dibiarkan berjalan, maka harus dipertimbangkan untuk direncakan perawatan pada saat yang tepat [1]. Ini merupakan masalah yang sulit dikarenakan tidak seorangpun akan segera tahu apa yang menjadi celah begitu system telah berhasil disusupi dari luar.

* + 1. Katagori keaman jaringan
       - * Interruption

Suatu aset dari suatu sistem diserang sehingga menjadi tidak tersedia atau tidak dapat dipakai oleh yang berwenang. Contohnya adalah perusakan/modifikasi terhadap piranti keras atau saluran jaringan.

* + - * + Interception

Suatu pihak yang tidak berwenang mendapatkan akses pada suatu aset. Pihak yang dimaksud bisa berupa orang, program, atau sistem yang lain. Contohnya adalah penyadapan terhadap data dalam suatu jaringan.

* + - * + Modification

Suatu pihak yang tidak berwenang dapat melakukan perubahan terhadap suatu aset. Contohnya adalah perubahan nilai pada file data, modifikasi program sehingga berjalan dengan tidak semestinya, dan modifikasi pesan yang sedang ditransmisikan dalam jaringan.

* + - * + Fabrication

Suatu pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contohnya adalah pengiriman pesan palsu kepada orang lain.

* + 1. Jenis – jenis seragan atau gagguan dalam jaringan
       - * ***DOS / DDOS,*** Denial of Services dan Distributed Denial of Services adalah sebuah metode serangan yangbertujuan untuk menghabiskan sumber daya sebuah peralatan jaringan komputer sehingga layanan jaringan komputer menjadi terganggu.
         * ***Paket Sniffing,*** 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.
         * ***IP Spoofing,*** sebuah model serangan yang bertujuan untuk menipu seseorang. Serangan ini dilakukan dengan cara mengubah alamat asal sebuah paket, sehingga dapat melewati perlindungan firewall dan menipu host penerima data.
         * ***DNS Forgery,*** 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.
         * ***Trojan Horse,*** program yang disisipkn tanpa pengetahuan si pemilik komputer, dapat dikendalikan dari jarak jauh & memakai timer.
         * ***Probe :*** Usaha yang tak lazim untuk memperoleh akses ke dalam suatu sistem/ untuk menemukan informasi tentang sistem tersebut. Dapat dianalogikan sebagai usaha untuk memasuki sebuah ruangan dengan mencoba-coba apakah pintunya terkunci atau tidak.
         * ***Scan :*** kegiatan probe dalam jumlah besar dengan menggunakan tool secara otomatis. Tool tersebut secara otomatis dapat mengetahui port-port yang terbuka pada host lokal/host remote, IP address yang aktif bahkan bisa untuk mengetahui sistem operasi yang digunakan pada host yang dituju.
         * ***Account Compromise :*** penggunaan account sebuah komputer secara ilegal oleh seseorang yang bukan pemilik account tersebut. Account Compromise dapat mengakibatkan korban mengalami kehilangan atau kerusakan data.
         * ***Root Compromise :*** mirip dengan account compromise, dengan perbedaan account yang digunakan secara ilegal adalah account yang mempunyai privelege sebagai administrator sistem. Akibat yang ditimbulkan bisa mengubah kinerja sistem, menjalankan program yang tidak sah.
    2. Perbedaan hacker dengan cracker
       - * Hacker

Hacker adalah sebutan untuk mereka yang memberikan sumbangan yang bermanfaat kepada jaringan komputer, membuat program kecil dan membagikannya dengan orang-orang di Internet. Sebagai contoh : digigumi (Grup Digital) adalah sebuah kelompok yang mengkhususkan diri bergerak dalam bidang game dan komputer. Digigumi ini menggunakan teknik teknik hexadecimal untuk mengubah teks yang terdapat di dalam game. Contohnya, game Chrono Trigger berbahasa Inggris dapat diubah menjadi bahasa Indonesia. Oleh karena itu, status Digigumi adalah hacker, namun bukan sebagai perusak. Hacker disini artinya, mencari, mempelajari dan mengubah sesuatu untuk keperluan hobi dan pengembangan dengan mengikuti legalitas yang telah ditentukan oleh developer game. Para hacker biasanya melakukan penyusupan-penyusupan dengan maksud memuaskan pengetahuan dan teknik. Rata - rata perusahaan yang bergerak di dunia jaringan global (internet) juga memiliki hacker. Tugasnya yaitu untuk menjaga jaringan dari kemungkinan perusakan pihak luar "cracker", menguji jaringan dari kemungkinan lobang yang menjadi peluang para cracker mengobrak - abrik jaringannya, sebagai contoh : perusahaan asuransi dan auditing "Price Waterhouse". Ia memiliki team hacker yang disebut dengan Tiger Team. Mereka bekerja untuk menguji sistem sekuriti client mereka.

* + - * + Cracker

Cracker adalah sebutan untuk mereka yang masuk ke sistem orang lain dan cracker lebih bersifat destruktif, biasanya di jaringan komputer, mem-bypass password atau lisensi program komputer, secara sengaja melawan keamanan komputer, men-deface (merubah halaman muka web) milik orang lain bahkan hingga men-delete data orang lain, mencuri data dan umumnya melakukan cracking untuk keuntungan sendiri, maksud jahat, atau karena sebab lainnya karena ada tantangan. Beberapa proses pembobolan dilakukan untuk menunjukan kelemahan keamanan sistem.

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

IDS [Intrusion Detection System](http://bocahsoenyi.blogspot.com/2010/11/ids-intrusion-detection-system.html) adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan traffic jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Dalam banyak kasus IDS juga merespon terhadap traffic yang tidak normal/ anomali melalui aksi pemblokiran seorang user atau alamat IP ([Internet](http://bocahsoenyi.blogspot.com/) Protocol).

IDS sendiri muncul dengan beberapa jenis dan pendekatan yang berbeda yang intinya berfungsi untuk mendeteksi traffic yang mencurigakan didalam sebuah jaringan. Beberapa jenis IDS adalah : yang berbasis jaringan (NIDS) dan berbasis host (HIDS).

Ada IDS yang bekerja dengan cara mendeteksi berdasarkan pada pencarian ciri-ciri khusus dari percobaan yang sering dilakukan. Cara ini hampir sama dengan cara kerja perangkat lunak antivirus dalam mendeteksi dan melindungi sistem terhadap ancaman. Kemudian ada juga IDS yang bekerja dengan cara mendeteksi berdasarkan pada pembandingan pola traffic normal yang ada dan kemudian mencari ketidaknormalan traffic yang ada. Ada IDS yang fungsinya hanya sebagai pengawas dan pemberi peringatan ketika terjadi serangan dan ada juga IDS yang bekerja tidak hanya sebagai pengawas dan pemberi peringatan melainkan juga dapat melakukan sebuah kegiatan yang merespon adanya percobaan serangan terhadap sistem jaringan dan komputer.

* + 1. Jenis-jenis IDS
       - *NIDS (Network Intrusion Detection System)*

IDS jenis ini ditempatkan disebuah tempat/ titik yang strategis atau sebuah titik didalam sebuah jaringan untuk melakukan pengawasan terhadap traffic yang menuju dan berasal dari semua alat-alat (devices) dalam jaringan. Idealnya semua traffic yang berasal dari luar dan dalam jaringan di lakukan di scan, namun cara ini dapat menyebabkan bottleneck yang mengganggu kecepatan akses di seluruh jaringan.

* + - * *HIDS (Host Intrusion Detection System)*

IDS jenis ini berjalan pada host yang berdiri sendiri atau perlengkapan dalam sebuah jaringan. Sebuah HIDS melakukan pengawasan terhadap paket-paket yang berasal dari dalam maupun dari luar hanya pada satu alat saja dan kemudian memberi peringatan kepada user atau administrator sistem jaringan akan adanya kegiatan-kegiatan yang mencurigakan yang terdeteksi oleh HIDS.

* 1. Signature Based

IDS yang berbasis pada signature akan melakukan pengawasan terhadap paket-paket dalam jaringan dan melakukan pembandingan terhadap paket-paket tersebut dengan basis data signature yang dimiliki oleh sistem IDS ini atau atribut yang dimiliki oleh percobaan serangan yang pernah diketahui. Cara ini hampir sama dengan cara kerja aplikasi antivirus dalam melakukan deteksi terhadap malware. Intinya adalah akan terjadi keterlambatan antara terdeteksinya sebuah serangan di internet dengan signature yang digunakan untuk melakukan deteksi yang diimplementasikan didalam basis data IDS yang digunakan. Jadi bisa saja basis data signature yang digunakan dalam sistem IDS ini tidak mampu mendeteksi adanya sebuah percobaan serangan terhadap jaringan karena informasi jenis serangan ini tidak terdapat dalam basis data signature sistem IDS ini. Selama waktu keterlambatan tersebut sistem IDS tidak dapat mendeteksi adanya jenis serangan baru.

* 1. Anomaly Based

IDS jenis ini akan mengawasi traffic dalam jaringan dan melakukan perbandingan traffic yang terjadi dengan rata-rata traffic yang ada (stabil). Sistem akan melakukan  identifikasi apa yang dimaksud dengan jaringan “normal” dalam jaringan tersebut, berapa banyak bandwidth yang biasanya digunakan di jaringan tersebut, protolkol apa yang digunakan, port-port dan alat-alat apa saja yang biasanya saling berhubungan satu sama lain didalam jaringan tersebut, dan memberi peringatan kepada administrator ketika dideteksi ada yang tidak normal, atau secara signifikan berbeda dari kebiasaan yang ada.

* 1. Passive IDS

IDS jenis ini hanya berfungsi sebagai pendeteksi dan pemberi peringatan. Ketika traffic yang  mencurigakan atau membahayakan terdeteksi oleh IDS maka IDS akan membangkitkan sistem pemberi peringatan yang dimiliki dan dikirimkan ke administrator atau user dan selanjutnya terserah kepada administrator apa tindakan yang akan dilakukan terhadap hasil laporan IDS.

* 1. Reactive IDS

IDS jenis ini tidak hanya melakukan deteksi terhadap traffic yang mencurigakan dan membahayakan kemudian memberi peringatan kepada administrator tetapi juga mengambil tindakan proaktif untuk  merespon terhadap serangan yang ada. Biasanya dengan melakukan pemblokiran terhadap traffic jaringan selanjutnya dari alamat IP sumber atau user jika alamat IP sumber atau user tersebut mencoba  melakukan serangan lagi terhadap sistem jaringan di waktu selanjutnya.

* + 1. Kelebihan dan kekurangan IDS
       - * Kelebihan
* Dapat mendeteksi “external hackers” dan serangan jaringan internal.
* Dapat disesuaikan dengan mudah dalam menyediakan perlindungan untuk keseluruhan jaringan.
* Dapat dikelola secara terpusat dalam menangani serangan yang tersebar dan bersama-sama.
* Menyediakan pertahanan pada bagian dalam.
* Menyediakan layer tambahan untuk perlindungan.
* IDS memonitor Internet untuk mendeteksi serangan.
* IDS membantu organisasi utnuk mengembangkan dan menerapkan kebijakan keamanan yang efektif.
* IDS  memungkinkan anggota non-technical untuk melakukan pengelolaan keamanan menyeluruh.
* Adanya pemeriksaan integritas data dan laporan perubahan pada file data.
* IDS  melacak aktivitas pengguna dari saat masuk hingga saat keluar.
* IDS menyederhanakan sistem sumber informasi yang kompleks.
* DS memberikan integritas yang besar bagi infrastruktur keamanan lainnya.
  + - * + Kekurangan
* Lebih bereaksi pada serangan daripada mencegahnya.
* Menghasilkan data yang besar untuk dianalisis.
* Rentan terhadap serangan yang “rendah dan lambat”.
* Tidak dapat menangani trafik jaringan yang terenkripsi.
* IDS hanya melindungi dari karakteristik yang dikenal.
* IDS tidak turut bagian dalam kebijakan keamanan yang efektif, karena dia harus diset terlebih dahulu.
* IDS tidak menyediakan penanganan kecelakaaN.
* IDS tidak mengidentifikasikan asal serangan.
* IDS hanya seakurat informasi yang menjadi dasarnya.
* Network-based IDS rentan terhadap “overload”.
* Network-based IDS dapat menyalahartikan hasil dari transaksi yang mencurigakan.
* Paket terfragmantasi dapat bersifat problematis
  1. **Portsentry**

PortSentry adalah sebuah perangkat lunak yang di rancang untuk mendeteksi adanya port scanning & meresponds secara aktif jika ada port scanning. Port scan adalah proses scanning berbagai aplikasi servis yang dijalankan di server Internet. Port scan adalah langkah paling awal sebelum sebuah serangan di lakukan. Cara kerja port sentry dengan melakukan melihat komputer yang melakukan scan dan secara aktif akan memblokir mesin penyerang agar tidak dapat masuk & melakukan transaksi dengan Server kita.

Kelebihan atau Keuntungan Portsentry :

1. Deteksi portscan TCP/UDP berbasis hostbased dan mengaktifkan sistem pertahanan.
2. Deteksi Stealth scan.
3. Bereaksi ke portscan dengan memblok host.
4. Internal state engine untuk mengingat host yang terkoneksi sebelumnya Semua kejadian akan disimpan ke syslog.

Kekurangan Portsentry :

1. Portsentry dibinding ke port sehingga diperlukan pengecekan menyeluruh.
2. Tidak dapat mendeteksi spoofing.
   1. **Honeypot**

Honeypot merupakan sumber sistem informasi yang bersifat terbuka (opensif) yang memfocuskan pada proses pemgumpulan informasi tentang aktifitas ilegal si Attacker yang mencoba menyusup dan mengeksplorasi authorisasi system komputer (server). Dengan Honeypot kita bisa mengetahui tingkah laku si Attacker diantaranya : port yang diserang, perintah-perintah yang dipergunakan, dan jenis aktifitas lainnya yang bisa direkam. Honeypot akan melindungi server asli yang kita miliki karena kita mendirikan server palsu yang tanpa disadari sebenarnya si Attacker sedang menyerang sistem yang bukan sebenarnya sehingga terperangkap.

Kelebihan Honeypot :

1. Riset : mempelajari tool dan metode yang digunakan si black-hat, membantu pakar keamanan IT membuat sistem yang lebih baik.
2. Proteksi : membuat penyerang jauh dari sistem yang asli.
3. Deteksi : seharusnya tidak ada lalu lintas jaringan pada sebuah honeypot.
4. Evidence : sekali sipenyerang terindentifikasi, semua bukti dapat digunakan secara ilegal.

Kekurangan Honeypot :

1. Limited View : hanya menangkan aktivitas dari sistem tersebut dan tidak pada sistem lain dalam jaringan.
2. High Risk : resiko yang besar untuk digunakan sebagai lompatan untuk menyerang sistem lain.
3. Skill Intensive : butuh waktu lama untuk mengembangkan, memaintain dan menganalis “Legal Issue”. Jika kita gunakan untuk menyerang sistem lain, maka itu akan membahayakan kita.
   1. **Snort**

Snort adalah NIDS yang bekerja dengan menggunakan signature detection, berfungsi juga sebagai sniffer dan packet logger. Snort pertama kali di buat dan dikembangkan oleh Marti Roesh, lalu menjadi sebuah opensource project

. Salah satu aplikasi Linux yang dapat dipakai untuk meningkatkan keamanan komputer adalah Snort.  Secara garis besar, Snort adalah sebuah program yang memiliki tiga fungsi atau tiga modus operasi.  Snort dapat dipakai dalam ***packet sniffer mode*** sehingga bekerja sebagai sniffer sama seperti Wireshark.  Sama seperti Wireshark, Snort juga dapat menyimpan setiap packet yang di-capture ke dalam media penyimpan di modus ***packet logger mode***.  Akan tetapi berbeda dengan Wireshark, Snort dapat dipakai sebagai komponen NIDS dengan menjalankannya pada ***Network Intrusion Detection System (NIDS) mode***.  Pada modus yang terakhir ini, Snort akan menganalisa packet  berdasarkan rule yang ada untuk mengenali adanya upaya serangan hacker.

* 1. **Tripwire**

Tripwire adalah termasuk kategori Host Intrusion Detection System (IDS). Yang mendeteksi perubahan file di mesin yang mungkin dilakukan oleh penyerang. Logika bekerja tripwire adalah dengan membuat baseline database dari file yang ada di system. Jika file tersebut berubah maka tripwire akan mencatat dan atau memberitahukan administrator mesin. Integrity checker pada Tripwire bekerja dengan cara menghitung checksum (menghitung integritas) dari daftar-daftar direktory yang sudah dienkripsi dan menyimpannya di dalam sebuah database. Kemudian secara periodik atau ketika user memerintahkan untuk melakukan pengecekan, checksum dari program-program tersebut akan dihitung ulang dan dibandingkan dengan database checksum tersebut.

* 1. **Personal Komputer**

Personal Computeradalah seperangkat komputer yang digunakan oleh satu orang saja / pribadi. Biasanya komputer ini adanya dilingkungan rumah, kantor, toko, dan dimana saja karena harga PC sudah relatif terjangkau dan banyak macamnya. Fungsi utama dari PC adalah untuk mengolah data input dan menghasilkan output berupa data/informasi sesuai dengan keinginan *user* (pengguna).

* 1. **TCP/IP**

Internet protokol dikembangkan pertama kali oleh defense Advance Research project Agency(DARPA) pada tahun 1970 sebagai awal dari usaha untuk mengembangkan yang dapat melakukan interkoneksi berbagai jaringan komputer yang terpisah,yang masing-masing jaringan tersebut menggunakan teknologi yang berbeda.Protokol utama yang dihasilkan proyek ini adalah internet protokol(IP),Riset yang sama dikembangkan yaitu beberapa protokol level tinggi yang di desain dapat bekerja dengan IP.

Yang paling penting dari proyek tersebut adalah Transmision Control Protokol(TCP),dan semua grup protokol diganti dengan TCP/IP suite.

* + 1. Susunan TCP/IP protokol

TCP/IP protokol suite terdiri dari 4 layers : Application, Transport, Network, dan Physical.Layer Tersebut dapat dilihat sebagai hirarki seperti diabawah ini :

1. Application layer

Pada layer ini terletak semua aplikasi yang menggunakan TCP/IP ini. Lapisan ini melayani permintaan pemakai untuk mengirim dan menerima data. Data tersebut kemudian disampaikan ke lapisan transport untuk diproses lebih lanjut.

1. Transport layer

Berisi protokol yang bertanggung jawab untuk mengadakan komunikasi antara dua host/komputer. Kedua protokol tersebut ialah TCP (Transmission Control Protocol) dan UDP (User Datagram Protocol). Protokol ini bertugas mengatur komunikasi antara host dan pengecekan kesalahan. Data dibagi ke dalam beberapa aket yang dikirim ke lapisan internet dengan sebuah header yang mengandung alamat tujuan atau sumber dan checksum. Pada penerima checksum akan diperiksa apakah paket tersebut ada yang hilang di perjalanan.

1. Network layer (internet layer)

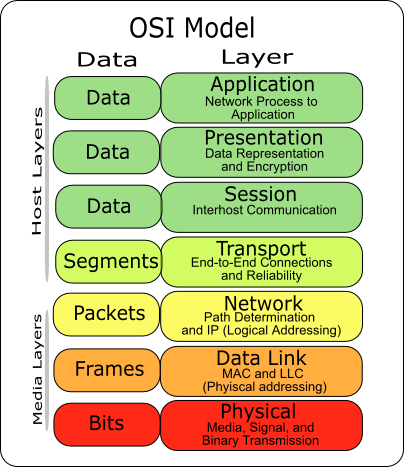
Protokol yang berada pada layer ini bertaggung jawab dalam proses pengiriman paket ke alamat yang tepat. Pada layer ini terdapat tiga macam protokol, yaitu IP, ARP, dan ICMP.

1. Physical layer (network interface layer)

Bertanggung jawab mengirim dan menerima data ke dan dari media fisik. Media fisiknya dapat berupa Ethernet, token ring, kabel, serat optik, frame relay, atau gelombang radio. Protokol pada layer ini harus mampu menerjemahkan sinyal listrik menjadi data digital yang dimengerti komputer yang berasal dari peralatan.

* 1. **OSI Layer**

Layer OSI adalah model arsitektural jaringan yang dikembangkan oleh Badan International Organization of Standardization (ISO) di wilayah Eropa pada tahun 1977. OSI nama kependekan dari nama aslinya yaitu Open System Interconnection. Model OSI biasa disebut dengan model "Model Tujuh Lapis OSI" .



Gambar 2.6 lapisan-lapisan OSI layer

1. Application

Application layer menyediakan jasa untuk aplikasi pengguna, layer ini bertanggungjawab atas pertukaran informasi antara program computer, seperti program e-mail dan servis lain yang berjalan di jaringan seperti server printer atau aplikasi computer lainnya.Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan. Mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protocol yanmg berada dalam lapisan ini adalah HTTP, FTP, SMTP, dan NFS.

1. Presentation

Presentation layer bertanggung jawab bagaimana data dikonversi dan di format untuk transfer data. Contoh konversi format text ASCII untuk dokumen, .GIF dan .JPG untuk gambar layer ini membentuk kode konversi, trnslasi data, enkripsi dan konversi. Berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi kedalam format yang dapat ditransmisikan melalui jaringan. Protocol yang berada dalam level ini adalah perangkat lunak director (redictor Software). Seperti llayanan worksatation (dalam Windows NT) dan juga Network Shell ( semacam Virtual Network Computing) (VNC) atau RemoteDekstopProtocol(RDP).

1. Session

Session layer menentukan bagaimna dua terminal menjaga, memelihara dan mengatur koneksi. Bagaimna mereka saling berhubungan satu sama lain. Koneksi di layer di sebut “session”.Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat.

1. Transport

Transport layer bertanggung jawab membagi data menjadi segmen, menjaga koneksi logika “end – to \_ end” antar terminal, dan menyediakan penanganan error (error handling).  
Berfungsi untuk memecahkan data kedalam paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan yang telah diterima. Selain itu, pada level ini juga membuat tanda bahwa paket diterima dengan sukses (acknowledgement) dan mentransmisikan ulang terhadap paket-paket yang hilang di tengah jalan.

1. Network

Network layer bertanggung jawab menentukan alamat jaringan, menentukan rute yang harus diambil selama perjalanan, menjaga antrian tafik di jaringan. Data pada layer ini berbentuk “Paket”. Berfungsi untuk mendefinisikan alamat-alamat IP, membuat Header untuk paket-paket dan kemudian melakukan routing melalui internet-working dengan menggunakan router dan switch layer 3.

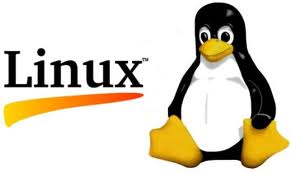
1. Datalink

Data link layer menyediakan link untuk data. Memaketkannya menjadi frame yang berhubungan dengan “hardware” kemudian diangkut melalui media komunikasinya dengan kartu jaringan, mengatur komunikasi layer physical antara system koneksi dengan penaganan error.Berfungsi untuk menentukan bagaimana bit-bit data dikelompokan menjadi format yang disebut sebagai frame. Selain itu, pada level ini terjadi koreksi kesalahan, flow control, pengalamatan perangkat keras( seperti halnya di Media Access Control Address ( MAC Address), dan menetukan bagaimna perangkat perangkat jaringan seperti hub, bridge, repeater dan switch layer 2 beroperasi. Spesifikasi IEEE 802, membagi level; ini menjadi dua level anak, yaitu lapisan Logical Link Control (LLC)dan lapisan Media AccessControl(MAC).

1. Physical

Physical layer bertyanggung jawab atas proses data menjadi bit dan mentransfernya melalui media (seperti kabel) dan menjaga koneksi fisik antar system.Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya Ethernet atau token Ring), topologi jaringan dan pengkabelan. Selain itu, level ini juga mendefinisikan bagaimana Networl Interface Card (NIC) dapat berinteraksi dengan media kabel atau radio.

* 1. **Linux (Sistem Operasi)**

****

Gambar 2.7 Sistem Operasi Linux

Linux merupakan sistem operasi yang bersifat *multi user* dan *multi tasking*. Artinya lebih dari satu user dapat masuk ke Linux yang sama pada waktu yang sama dan aplikasi yang berbeda. Linux juga multi-tasking, artinya user dapat mengeksekusi lebih dari satu proses (program) pada waktu yang sama.

Linux menggunakan sebuah license yang bernama ***GNU General Public License*** (GNU/GPL). **Apa itu GNU GPL?** Singkatnya GNU General Public License memungkinkan suatu aplikasi ( termasuk sistem operasi ) secara bebas digunakan dan disebarluaskan dimana pengguna/penerima software berhak menerima kode asal ( source code) dari aplikasi tersebut beserta semua hak yang diijinkan oleh penulis asli.

License dari aplikasi yang mengalami perubahan/baru masih tetap berada pada GNU GPL. Sang penulis asli hanyalah bertanggung jawab atas kode asli dan tidak bertanggung jawab atas perubahan yang telah dibuat. Penyebarluasan aplikasi yang telah dirubah tetap mencantumkan penulis asli , kode asli, kode perubahan yang ditambahkan dan penanggungjawab perubahan tersebut.

Dengan adanya license GNU GPL ini, bukan berarti tidak memungkinkan adanya komersial, paling tidak biaya dapat ditarik dari biaya kopi media distribusi. Jasa layanan seperti dukungan teknis dapat merupakan produk komersial.

* + 1. Jenis-Jenis Sistem Operasi Linux

1. Red Hat Linux

RedHat Linux merupakan salah satu GNU/Linux yang tergolong sudah tua, menawarkan kemudahan, mode tampilan yang sepenuhnya grafis mulai saat instalasi, dan pemakaian yang ramah. Versi terakhir Red Hat adalah Distribusi RedHat Linux 9.0, ini merupakan versi stabil dan perbaikan serta peningkatan administrasi sistem yang dilengkapi dengan desktop manager terbaru seperti KDE 3.1 dan GNOME 2.2 dan aplikasi terbaru seperti grafis GIMP 1.2.3, OpenOffice, KOffice, Diagram, aplikasi Multimedia Player, dll. Kemudahan penggunaan yang ditawarkan RedHat Linux 9.0 hampir sama dengan lingkungan yang disediakan oleh sistem operasi Windows. Kemudahan tersebut antara lain dalam melakukan instalasi software, pengenalan deteksi hardware, konfigurasi dan pengelolaan sistem dan harddisk, serta penggunaan aplikasi-aplikasi yang semuanya dapat dilakukan dengan sangat mudah dan didukung dengan menu grafis serta perintah yang gampang untuk diikuti.

1. Debian Linux

Salah satu distro Linux, dari websitenya saja (.org), tampak kalau distro ini sebetulnya tidak mengedepankan sebagai suatu distro yang komersial. Debian linux merupakan hasil usaha para sukarelawan untuk membuat distro dengan kualitas tinggi dan nonkomersial. Keunggulan menggunakan Debian adalah mudah di-upgrade, depedensi paket didefinisikan dengan baik, dan dikembangkan secara terbuka. Merupakan satu-satunya distro yang dikembangkan bersama-sama melalui Internet dengan lebih dari 400 pengelola paket menggarap lebih dari 1500 paket dalam mengembangkan Debian. Merupakan distro yang sangat dinamis.

1. Mandrake Linux / Mandriva

Salah satu distribusi Linux, lahir diinspirasi oleh RedHat Linux, dengan banyak pengembangan dan aplikasi prakonfigurasi sehingga memudahkan untuk para pemula, baik dari proses awal instalasinya yang berbasis Xwindow, sampai penggunaannya dan didukung oleh berbagai bahasa. Di dalam Mandrake, semua paket telah dikompilasi dengan optimasi CPU untuk kelas Pentium (intel, amd, cyrixm winchip) dan prosesor di atasnya dan menghasilkan optimasi lebih dari 30%. Menggunakan paket manajer disebut **urpmi.** Sampai versi 8.0 masih menggunakan nama mandrake, versi 8.1 – 9.2 menggunakan nama mandriva.

1. SuSE Linux

Salah satu keunggulan utama dari OpenSUSE dibandingkan distro Linux lainnya adalah kelengkapan pustaka dan berlimpahnya software yang disertakan. Bersama [Red Hat](http://www.redhat.com/), SUSE adalah distro Linux versi awal yang terus bertahan dan berkembang hingga sekarang. Fiturnya antara lain : instalasi berbasis menu(CD-ROM), disket boot modular, ratusan halaman buku referensi, dan YAST, tool admnistrasi dalam SuSe. Mendukung kartu grafis baru dan mode demo secara langsung. Paket SuSe dinamakan SPM(SuSe Package Manager). SUSE merupakan distro Linux yang stabil, mudah dalam melakukan deteksi perangkat keras, mudah dikelola dan didukung penuh oleh komunitas pengembang di seluruh dunia serta memiliki dukungan sponsor dari perusahaan besar.

1. Xandros Linux

Xandros Linux adalah sebuah [distro Linux](http://id.wikipedia.org/wiki/Distro_Linux) yang berdasarkan pada sistim KDE. Tampilannya sangat mirip dengan [Microsoft](http://id.wikipedia.org/wiki/Microsoft) [Windows](http://id.wikipedia.org/wiki/Windows), jadi apabila dioperasikan sangat mudah dan nyaman. Selain itu pun, sistim operasi ini pun murah. Di toko-toko, CD LinuXandros biasa dijual dengan harga kurang lebih 15.000 - 30.000 [Rupiah](http://id.wikipedia.org/wiki/Rupiah). Sistim operasi ini pun sangat *user-friendly* dan tidak menyulitkan bagi para pemula. Saat ini, Xandros telah mencapai versi 4.

1. Gentoo Linux

Gentoo Linux adalah suatu distribusi [Linux](http://id.wikipedia.org/wiki/Linux) yang memakai paket sistem manajemen Portage. [Debian yang menggunakan paket .deb, RedHat / Mandrake yang menggunakan paket .rpm]. Manajemen paket ini dirancang untuk modular (mudah ditambah-tambah), portabel (dapat di port ke distro lain), mudah ditata, fleksibel, dan dioptimalkan untuk masing-masing komputer pengguna. Nama proyek pengembangan dan produknya diambil dari jenis penguin bernama Gentoo. Distribusi yang mempunyai keunikan tersendiri dan dapat dioptimisasi dan dikustomisasi untuk hampir segala jenis aplikasi atau kegunaan. Konfigurasi yang sangat ekstrim, dukungan dari sesama user dan developer yang sangat bagus adalah salah satu kelebihan Gentoo. Berkat adanya teknologi bernama Portage, Gentoo Linux dapat menjadi server yang aman, sistem develop, profesional desktop, game sistem, solosi buat 'embedded' atau apa pun sesuai yang kita ingini.

1. Knoppix

Knoppix adalah [distro Linux](http://id.wikipedia.org/wiki/Distro_Linux) live-cd yang dapat dijalankan melalui [CD-ROM](http://id.wikipedia.org/wiki/CD-ROM) tanpa instalasi di [hard disk](http://id.wikipedia.org/wiki/Hard_disk). Distro ini berbasis [Debian](http://id.wikipedia.org/wiki/Debian) [Linux](http://id.wikipedia.org/wiki/Linux) dan diciptakan oleh [Klaus Knopper](http://id.wikipedia.org/w/index.php?title=Klaus_Knopper&action=edit&redlink=1). Knoppix memiliki ragam aplikasi yang cukup lengkap dan dapat dipergunakan sebagai demo atau sarana belajar Linux bagi yang belum mempunyai ruang pada hard disknya. Knoppix juga dapat dipergunakan sebagai CD rescue. Kelemahan dari Knoppix adalah diperlukannya [memori](http://id.wikipedia.org/wiki/Memori_%28komputer%29) yang besar untuk menggunakan modus grafisnya yaitu 96 MB walaupun bisa juga dijalankan pada memori 64 MB dengan swap pada hard disk.

1. Ubuntu Linux

Ubuntu adalah salah satu distribusi [Linux](http://id.wikipedia.org/wiki/Linux) yang berbasiskan pada [Debian](http://id.wikipedia.org/wiki/Debian). Proyek Ubuntu disponsori oleh [Canonical Ltd](http://id.wikipedia.org/w/index.php?title=Canonical_Ltd&action=edit&redlink=1) (perusahaan milik [Mark Shuttleworth](http://id.wikipedia.org/w/index.php?title=Mark_Shuttleworth&action=edit&redlink=1)). Nama Ubuntu diambil dari nama sebuah konsep [ideologi](http://id.wikipedia.org/wiki/Ideologi) di [Afrika Selatan](http://id.wikipedia.org/wiki/Afrika_Selatan). "Ubuntu" berasal dari bahasa kuno Afrika, yang berarti "rasa perikemanusian terhadap sesama manusia". Versi terbaru adalah 8.10, dengan beberapa kelebihan yaitu : **Settingan Network Manager lebih mudah, dapat membuat Startup Disk di USB Flashdisk, Unmount media lebih mudah, versi desktop Gnome 2.24.1.**

1. **Fedora**

Fedora (sebelumnya bernama Fedora Core, terkadang disebut juga dengan Fedora Linux) adalah sebuah [distro Linux](http://id.wikipedia.org/wiki/Distro_Linux) berbasis [RPM](http://id.wikipedia.org/wiki/RPM_Package_Manager) dan [yum](http://id.wikipedia.org/w/index.php?title=Yum&action=edit&redlink=1) yang dikembangkan oleh [Fedora Project](http://id.wikipedia.org/wiki/Fedora_Project) yang didukung oleh komunitas pemrogram serta disponsori oleh [Red Hat](http://id.wikipedia.org/wiki/Red_Hat). Versi terbarunya adalah Fedora 10, yg memiliki beberapa kelebihan yaitu : desktop GNOME 2.24.1, KDE 4.1.2, OpenOffice 3.0, Firefox 3.0.4, Linux 2.6.27.5, X.org-X-Server 1.5.3, Glibc 2.9 dan RPM 4.6. Banyak fitur baru seperti versi 'Glitch-Free' untuk PulseAudio, sistem Security, Audit dan Intrusion-Detection Sectool, PackageKit-Framework, software konfigurasi printer dengan fitur baru dan dukungan untuk Adhoc-Network/Connection Sharing melengkapi NetworkManager, menjadikan Cambridge sebagai salah satu distro dengan fitur terdepan yang dipastikan akan diikuti distro-distro lainnya.

1. Free BSD

FreeBSD adalah sebuah sistim operasi komputer berbasiskan 4.4BSD-Lite2, sebuah versi dari UNIX yang dikembangkan oleh University of California di Berkeley. Sebuah bagian penting dalam sistim operasi FreeBSD adalah koleksi Ports, yang saat ini memiliki jumlah 8.633 buah dari aplikasi UNIX yang populer digunakan. Koleksi ports memberikan otomatisasi proses porting aplikasi untuk digunakan pada sistim FreeBSD. FreeBSD memiliki stabilitas tinggi sistem operasi, open source dan mendukung penuh teknologi networking TCP/IP.

1. CentOS

CentOS adalah [sistem operasi](http://id.wikipedia.org/wiki/Sistem_operasi) bebas yang didasarkan pada [Red Hat Enterprise Linux (RHEL)](http://id.wikipedia.org/wiki/Red_Hat_Linux). Proyek ini berusaha untuk 100% binari kompatibel dengan produk hulunya (RHEL). Arsip perangkat lunak tambahan menyediakan versi terbaru paket-paketnya, berbasis paket [RPM](http://id.wikipedia.org/w/index.php?title=RPM&action=edit&redlink=1). CentOS singkatan dari Community ENTerprise Operating System (Sistem Operasi Perusahaan buatan Komunitas/Masyarakat). Salah satu kekurangan CentOS adalah sedikitnya sistem file yang didukung oleh kernelnya, antara lain CentOS tidak bisa membaca [ReiserFS](http://www.namesys.com/) dan [NTFS](http://en.wikipedia.org/wiki/NTFS).

1. Turbo Linux

Turbo Linux menargetkan pada produk berbasis Linux dengan kinerja tinggi untuk pasar workstation dan server terutama untuk penggunaan clustering dan orientasinya ke perusahaan. Beberapa produk-produknya: TurboLinux Workstation untuk dekstopnya, TurboLinux Server untuk backend server dengan kinerja tinggi terutama untuk penggunaan bisnis di perusahaan, e-commerce dan transaksi B2B (Business-to-Business).Salah satu produknya TurboCluster Server ditargetkan untuk pembuatan server cluster yang berskala luas dan dapat digunakan 25 cluster node atau lebih. Salah satu aplikasinya yang berbasis pada konsep sederhana dan powerful yang dinamakan ' parametric execution'. enFuzion akan merubah jaringan komputer perusahaan menjadi super computer dengan kecepatan tinggi dan ' fault tolerant'. Pengguna produk dan layanan TurboLinux terbanyak adalah perusahaan dan perorangan di Jepang dan Asia.

1. Linux Mint

Linux Mint adalah [sistem operasi](http://id.wikipedia.org/wiki/Sistem_operasi) berbasis [Linux](http://id.wikipedia.org/wiki/Linux) untuk [PC](http://id.wikipedia.org/wiki/PC). Inti dari LinuxMint adalah [Ubuntu](http://id.wikipedia.org/wiki/Ubuntu), sehingga aplikasi yang dapat berjalan di [Ubuntu](http://id.wikipedia.org/wiki/Ubuntu), juga bisa berjalan pada LinuxMint. LinuxMint dilengkapi dengan pencarian dan aplikasi favorit. LinuxMint sudah terintegrasi dengan [codec](http://id.wikipedia.org/w/index.php?title=Codec&action=edit&redlink=1) [multimedia](http://id.wikipedia.org/wiki/Multimedia) yang umum digunakan dan terintegrasi [Java Runtime](http://id.wikipedia.org/w/index.php?title=Java_Runtime&action=edit&redlink=1).

1. Sabayon Linux

Sabayon linux adalah live DVD berbasis Gentoo Linux. Walaupun di release dalam live DVD namun tetap dapat di install ke dalam harddisk. Berasal dari Trentino, Italia dan dinamakan mengikuti sebuah hidangan penutup Italia yang disebut Sabayon. Sabayon dibuat dari telur kuning, gula dan alkohol manis.Dari segi tampilan, Sabayon memiliki ciri khas tersendiri, dengan warna merah hitam dan [logo tapak kaki ayam](http://www.sabayonlinux.org/sabayon/press/logos/2007/logo_only_small.png). Namun kebanyakan themes dan wallpapernya masih bawaan KDE yang bisa dikustomisasi, dan dengan setting Compiz/Beryl yang mudah diaktifkan.

1. Damn Small Linux (DSL)

[Damn Small Linux](http://www.damnsmalllinux.org/) seperti namanya merupakan linux yang berukuran ringan, hanya 50MB sehingga dapat di[install](http://www.damnsmalllinux.org/dsl-hd-install.html) dikomputer yang sudah tua atau bahkan dijalankan melalui USB. Dikatakan ringan karena aplikasi - aplikasi yang diusungnya adalah program - program kecil namun powerfull. Sebagian besar adalah aplikasi berbasis GTK. Selain bisa berfungsi untuk pemakaian desktop, DSL juga bisa berfungsi sebagai server kecil karena telah dilengkapi aplikasi semacam http server, ssh server dan ftp server. Distribusi ini juga bisa diinstall pada harddisk atau Flashdisk. Proses instalasinya tidak perlu manual, karena scriptnya telah disediakan dalam distribusi ini.

1. Linspire

Linspire, dahulunya LindowsOS, adalah [sistem operasi](http://id.wikipedia.org/wiki/Sistem_operasi) komersial (tidak gratis) berbasis [Debian](http://id.wikipedia.org/wiki/Debian) dan kemudian [Ubuntu](http://id.wikipedia.org/wiki/Ubuntu). Linspire diterbitkan oleh Linspire, Inc. Linspire membundel piranti lunak, driver dan codecs proprietary yang tidak memiliki alternatif handal di pihak Open Source. Termasuk yang dicontohkan adalah yang terkait dengan MP3, Real, Java, Flash, ATI, nVidia, WiFi, dan banyak lain. Linspire 6.0 disebut sebagai Linux pertama yang mengandung teknologi Microsoft seperti Windows Media, True Type Fonts, dan juga penerjemah Open XML sehingga OpenOffice bisa membuka dan menyunting format Microsoft Word .docx alias Office Open XML (OOXML).

1. Freespire

[Freespire](http://gudanglinux.net/gmc/component/option,com_wikidoc/task,viewcontent/docid,5/Itemid,109/sid,146/cid,146/) merupakan edisi asal Linspire yang dikembangkan bersama komunitas dan di sponsori oleh Linspire. FreeSpire adalah Linux yang mengandung baik komponen open source maupun free software lainnya (community driven, freely distributed, open source code, etc.), tapi memberi peluang kepada pengguna untuk menambahkan pilihan software seperti proprietary codecs, drivers dan aplikasi yang dibutuhkan.. Setelah sempat berbasis Ubuntu, freespire kembali ke basis Debian. Tapi tetap "sharing repository" dgn ubuntu.

1. Zencafe

Zencafe GNU/Linux atau singkatnya Zencafe, adalah salah satu anggota keluarga distro Zenwalk. Zencafe dikembangkan di Indonesia didisain khusus untuk kebutuhan WarNet (Warung Internet) dan telah menjadi pelopor distro Internet Cafe berkiprah Internasional. Zencafe dipoles sedemikian rupa agar mudah digunakan, meskipun untuk pemakai yang tidak memiliki pengetahuan teknis. Termasuk didalamnya autorecovery dan internet cafe management software / billing system.

1. Trustix Merdeka

Trustix Merdeka, merupakan sebuah distribusi **Linux** untuk desktop dengan mengambil basis Trustix Secure **Linux**. Dengan penekanan pada security, paket-paket aplikasi yang disertakan di dalam Trustix Merdeka merupakan paket pilihan, dengan auditing yang cukup ketat untuk setiap sumber yang disertakan. Distribusi Made in Indonesia ini bertujuan lebih dari sekedar distro **Linux** saja. Ditargetkan menjadi jalur komunikasi masyarakat **Linux** dan IT. Bahasa Indonesia yang digunakan dapat dikatakan sebagai faktor pemersatu. TM berisi kumpulan artikel tentang Linux, dan membuka siapapun yang ingin berkontribusi. Tiap programmer di Indonesia dapat menyertakan program buatannya, dan didistribusikan secara masal bersama TM.

1. BlankOn

BlankOn Linux adalah distro Linux yang dikembangkan oleh [Yayasan Penggerak Linux Indonesia (YPLI)](http://www.ypli.or.id/) dan [Komunitas Ubuntu Indonesia](http://www.ubuntu-id.org/) demi menghasilkan distro Linux yang sesuai dengan kebutuhan pengguna komputer umum di Indonesia. Dengan menghadirkan filosofi, kemudahan, dan kehandalan yang ditawarkan Ubuntu Linux sebagai distribusi aslinya, BlankOn Linux dikembangkan secara terbuka dan bersama-sama untuk menghasilkan distro Linux khas Indonesia, khususnya untuk dunia pendidikan, perkantoran dan pemerintahan.