BAB 2

LANDASAN TEORI

Landasan teori merupakan bagian yang akan membahas tentang uraian pemecahan masalah yang akan ditemukan solusinya melalui pembahasan-pembahasan teoritis. Teori-teori yang akan dikemukakan merupakan dasar-dasar penulis untuk meneliti masalah-masalah yang akan dihadapi penulis pada pelaksanaan penelitian.

2.1 Tinjauan Perusahaan

Tinjauan Perusahaan adalah untuk mengetauhi keadaan perussahaan diantanya adalah sejarah perusahaan dan stuktur organisasi perusahaan.

2.1.1 Profil Diskominfo Kabupaten Garut

Profil Diskominfo Kabupaten Garut merupakan pembahasan mengenai sejarah, visi dan misi, struktur organisasi serta deskriptif jabatan pada Diskominfo yang akan menjadi tempat pembangunan sistem ini.

2.1.2 Sejarah Perusahaan

Dinas Komunikasi, Informasi dan Statistik Kabupaten Garut merupakan salah satu Satuan Kerja Perangkat Daerah yang dimiliki oleh Pemerintah Kabupaten Garut yang berfokus pada “Layanan pengelolaan informasi TIK, layanan E-Government dan layanan statistik dan persandian”. Pada periode-periode sebelumnya Dinas Komunikasi, Informasi dan Statistik berasal dari BAPAPSI yang dibentuk berdasarkan Peraturan Daerah Kabupaten Garut No.21 tahun 2007 tentang Pembentukan Organisasi Lembaga Teknis Daerah Kabupaten Garut Terhitung 1 April 2008. Berdasarkan Perda No.21 tahun 2017 ini Kantor Perpustakaan Daerah, Kantor Arsip Daerah, Badan Pengembangan Informasi Darah dan Kantor Pengolahan Data Elektronik digabungkan menjadi SKPD baru dengan nama BAPAPSI (Badan Perpustakaan, Arsip dan Pengembangan Sistem Informasi) yang kemudian terpecah kembali menjadi beberapa dinas dan salah-satunya adalah DISKOMINFO (Dinas Komunikasi, Informasi dan Statistik) yang didirikan di masa transisi pada tahun 2016 hingga 2017 awal.

2.1.3 Visi dan Misi

DIKOMINFO memiliki Visi dan Misi sebagai berikut :

1. Visi : "**Terwujudnya masyarakat informasi Jawa Barat melalui penyelenggaraan komunikasi dan informatika yang efektif dan efisien**".
2. Misi :
    a. Meningkatkan sarana dan prasarana dan profesionalisme sumber daya aparatur bidang Komunikasi dan Informatika.
    b. Mengoptimalkan pengelolaan pos dan telekomunikasi.
    c. Mengoptimalkan pemanfaatan sarana komunikasi dan informasi pemerintah dan masyarakat, serta melakukan diseminasi informasi.
    d. Mewujudkan layanan online dalam penyelenggaraan pemeritah berbasis teknologi informasi dan komunikasi serta mewujudkan pengadaan barang dan jasa secara elektronik.
    e. Mewujudkan pengelolaan data menuju satu data pembangunan untuk Jawa Barat.

1.1.1 Logo Perusahaan

Logo Diskominfo Kabupaten Garut menggunakan logo dari Provinsi Jawa Barat. Logo Diskominfo dapat terlihat pada Gambar 2.1.

Gambar 2.1 Logo Diskominfo Kabupaten Garut

Makna bentuk dan motif yang terdapat dalam logo ini ialah:

1. Bentuk bulat telur pada lambang Jawa Barat diambil dari bentuk perisai yang biasa digunakan oleh laskar-laskar pada zaman baheula (dahulu).
2. Ditengah-tengah terlihat ada sebilah kujang. Kujang ini merupakan alat serbaguna yang selama ini dianggap senjata khas masyarakat Sunda. Lima lubang pada kujang melambangkan dasar Negara Indonesia yaitu Garuda Pancasila.
3. Padi satu tangkai yang terdapat di sisi sebelah kiri melambangkan bahan makanan pokok masyarakat Jawa Barat sekaligus juga melambangkan kesuburan pangan, dan jumlah padi yaitu 17 menggambarkan tanggal Proklamasi Republik Indonesia.
4. Kapas satu tangkai yang berada di sebelah kanan melambangkan kesuburan sandang, dan 8 kuntum bunga menggambarkan bulan proklamasi Republik Indonesia.
5. Gunung yang terdapat di bawah padi dan kapas melambangkan bahwa daerah Jawa Barat terdiri atas daerah pegunungan.
6. Sungai dan terusan yang terdapat di bawah gunung sebelah kiri melambangkan di Jawa Barat banyak terdapat sungai dan saluran air yang sangat berguna untuk pertanian.
7. Petak-petak yang terdapat di bawah gunung sebelah kanan melambangkan banyaknya pesawahan dan perkebunan. Masyarakat Jawa Barat umumnya hidup mengandalkan kesuburan tanahnya yang diolah menjadi lahan pertanian.
8. Dan atau bendungan yang terdapat di tengah-tengah bagian bawah antara gambar sungai dan petak, melambangkan kegiatan di bidang irigasi yang merupakan salah satu perhatian pokok mengingat Jawa Barat merupakan daerah agraris. Hal ini juga melambangkan dam-dam yang berada di Jawa Barat seperti Waduk Jatiluhur.
9. Tulisan GEMAH RIPAH REPEH RAPIH, melambangkan sebuah pepatah lama dikalangan sunda yang menyatakan bahwa yang padat yang hidup rukun dan damai.

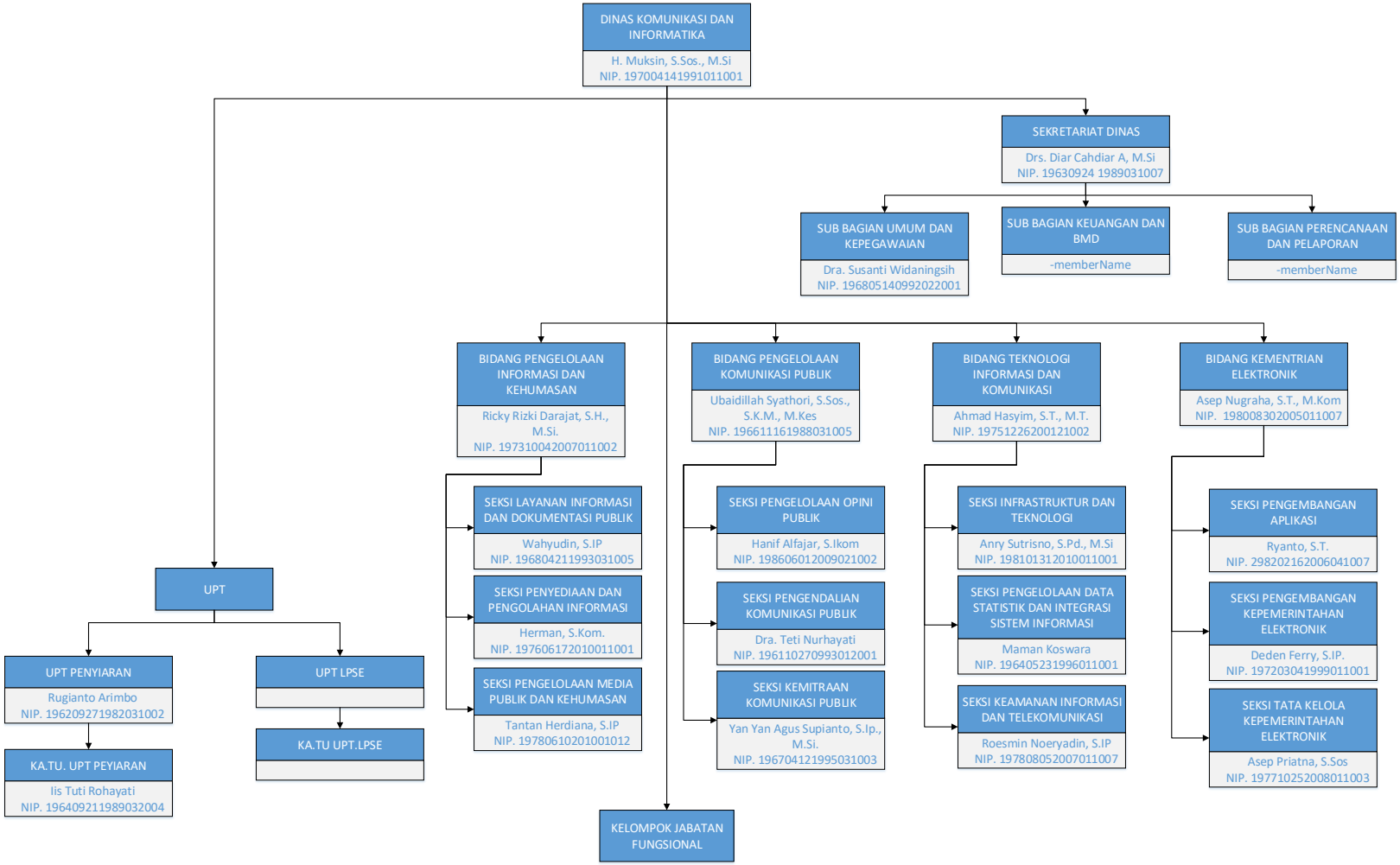
10. Dua garis putih bergelombang dengan warna dasar biru yang terdapat dibagian bawah melambangkan sungai, terusan, saluran dan laut.

Logo Diskominfo Kabupaten Garut memiliki beberapa warna yaitu hijau, kuning, hitam, biru, merah, dan putih. Warna-warna ini memiliki arti khusus. Arti khusus warna-warna pada logo Diskominfo ialah:

1. Warna hijau artinya melambangkan kesuburan dan kemakmuran tanah Jawa Barat.
2. Warna Kuning artinya melambangkan keagungan, kemuliaan dan kekayaan.
3. Warna Hitam artinya melambangkan keteguhan dan keabadian.
4. Biru artinya melambangkan ketentraman atau kedamaian.
5. Merah artinya melambangkan keberanian.
6. Putih artinya melambangkan kemurnian, kesucian atau kejujuran.

1.1.2 Struktur Organisasi

Struktur Organisasi merupakan penggambaran secara grafik seperti struktur kerja dari setiap bagian yang mempunyai wewenang dan tanggung jawab untuk masing masing pejabat di lingkungan Diskominfo Kabupaten Garut. Berikut gambar Struktur organisasi Diskominfo Kabupaten Garut pada Gambar 2.2.



Gambar 2.2 Struktur Organisasi

2.2 Jaringan Komputer

Jaringan komputer adalah himpunan “interkoneksi” antara 2 komputer autonomous atau lebih yang terhubung dengan media tranmisi kabel atau tanpa kabel (wireless). Bila sebuah komputer dapat membuat komputer lainnya restart, shutdown, atau melakukan control lainya, maka komputer-komputer tersebut bukan autonomous (tidak melakukan kontrol terhadap komputer lain dengan akses penuh).

Sedangkan jaringan komputer menurut probeyekti Jaringan komputer merupakan sekumpulan komputer berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya. Dua buah komputer misalnya dikatakan terkoneksi bila keduanya dapat saling bertukar informasi. Berdasarkan Pengertian dari sandyhkara dan probeyekti dapat di simpulkan bahwa jaringan komputer adalah sistem yang terpisah untuk melakukan komunikasi agar dapat bertukar informasi.[4]

2.2.1 Manfaat Jaringan Komputer

Adapun manfaat yang didapat dalam membangun jaringan komputer adalah sebagai berikut.[4]

a. Sharing Resource, bertujuan agar seluruh program, peralatan lainya dapat dimanfaatkan oleh setiap orang yang ada pada jaringan komputer tanpa terpengaruh oleh lokasi maupun pemakaian.
b. Media komunikasi, jaringan komputer memungkinkan terjadinya hubungan antara komputer pengguna, baik untuk teleconference maupun untuk mengirim pesan atau informasi penting lainya. Dengan menggunakan jaringan komputer dua orang atau lebih yang jaraknya sangat jauh akan lebih mudah bekerja.
c. Integrasi data, pembangunan jaringan komputer dapat mencegah ketergantungan pada komputer pusat, setiap proses data tidak harus dilakukan pada satu komputer saja, melainkan dapat didistribusikan ke tempat lainnya.

d. Pengembangan dan pemeliharaan, dengan adanya jaringan komputer ini, maka pengembangan peralatan dapat dilakukan dengan mudah dan menghemat biaya. Jaringan komputer juga bisa memudahkan pemakai dalam merawat hard disk dan peralatan lainnya, seperti memberikan perlindungan terhadap serangan virus maka pemakai cukup memusatkan perhatian pada hard disk uang ada di komputer pusat.
e. Keamanan data, memberikan perlindungan terhadap data. Jaminan keamanan data tersebut diberikan melalui pengaturan hak akses para pemakai dan password, serta teknik perlindungan terhadap hard disk sehingga data mendapatkan perlindungan yang efektif.

2.2.2 Jenis Jaringan Komputer

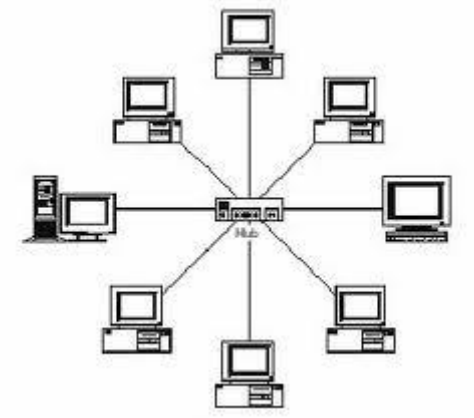
Secara umum tipe jaringan komputer dibagi menjadi 2 bagian yaitu *peer to peer* dan *client server*. perbedaan yang paling mendasar diantra dua tipe jaringan ini adalah *client – server* terdapat sebuah komputer yang bertugas sebagai *server* yang melayani *client-client* yang lain sedangkan *peer to peer* tidak ada komputer yang bertindak sebagai *server* ataupun *client*, setiap komputer bisa bertindak menjadi *client* ataupun *server*.

2.2.2.1 Jaringan LAN

Local Area Network (LAN) adalah jarigan yang di batasi oleh area yang relative kecil, umumnya dibatasi oleh area lingkungan seperti sebuah gedung perkantoran, atau sebuah sekolah, dan biasanya tidak jauh dari sekitar 1 kolometer persegi.beberapa model konfigurasi LAN biasanya berupa, satu komputer biasanya dijadikan sebuah dile server, yang digunakan untuk menyimpan perangkat lunak (Software yang mengatur aktifitas jaringan), ataupun sebagai perangkat lunak yang dapat digunakan oleh komputer-komputer yang terhubung kedalam jaringan lokal.[4]

LAN kebanyakan menggunakan media kabel untuk menghubungkan antara LAN kebanyakan menggunakan media kabel untuk menghubungkan antara satu komputer dengan komputer lainnya. LAN merupakan jaringan komunikasi yang

terbatas pada daerah yang kecil, misalkan sau gedung atau sekelompok bangunan kecil.

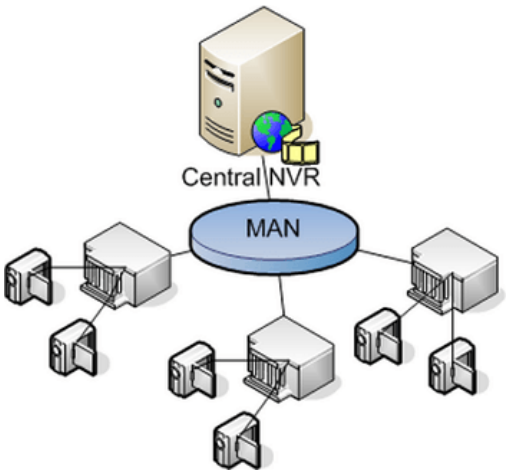


Gambar 2.3 Skema Jaringan LAN

2.2.2.2 Jaringan MAN

Metropolitan area network pada dasaranya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.[4]

Berikut ini adalah gambar skema jaringan MAN yang dapat dilihat pada Gambar 2.4.

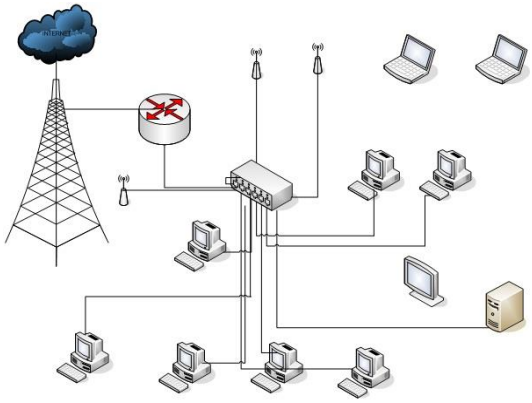


Gambar 2.4 Skema Jaringan MAN

2.2.2.3 Jaringan WAN

Wide Area Network (WAN) merupakan jaringan yang lebih besar dari MAN dan mencakup daerah geografis yang luas, seringkali mencakup sebuah negara atau benua. WAN terdiri dari kumpulan mesin yang bertujuan unuk menjalankan program-program (aplikasi) pemakai. Pada sebagian besar WAN, jaringan terdiri dari sejumlah banyak kabel atau saluran telepon yang menghubungkan sepasang router. Bila dua router yang tidak menggunakan kabel yang sama akan melakukan komunikasi, keduanya harus berkomunikasi secara tidak langsung melalui router lainnya. Ketika sebuah paket dikirimkan dari sebuah router ke router lainnya melalui sebuah router perantara atau lebih, maka paket akan diterima router perantara dalam keadaan lengkap, disimpan sampai saluran output menjadi bebas, dan kemudian baru diteruskan.[4].

Berikut ini adalah gambar skema jaringan WAN yang dapat dilihat pada Gambar 2.5.



Gambar 2.5 Skema Jaringan WAN

2.2.3 Jenis-Jenis Media Transmisi

Media adalah suatu bentuk atau benda yang digunakan untuk menyampaikan informasi atau pesan, sedangkan transmisi adalah komunikasi data melalui penyebaran dan pemrosesan sinyal-sinyal. Sehingga media transmisi dapat diartikan perangkat yang digunakan sebagai jalur transmisi dari data yang dikirimkan. Berdasarkan media transmisinya, jaringan komputer dapat dibagi menjadi dua jenis[4], yaitu:

1. Wire Network (Guided Media)

   Wire Network adalah jaringan komputer yang menggunakan kabel sebagai media transmisinya, kabel yang digunakan pun bermacam-macam, antara lain:

a. Kabel Unshielded Twisted Pair

   unshielded twisted pair yaitu jenis kabel ini terbuat dari bahan penghantar tembaga, mempunyai isolasi dari plastik & terbungkus oleh bahan isolasi yang dapat melindungi dari api dan juga kerusakan fisik, kabel UTP sendiri terdiri dari 4 pasang inti kabel yang saling berbelit dimana masing-masing pasang mempunyai kode warna berbeda.

   Berikut ini adalah gambar kabel UTP yang dapat dilihat pada Gambar 2.6.

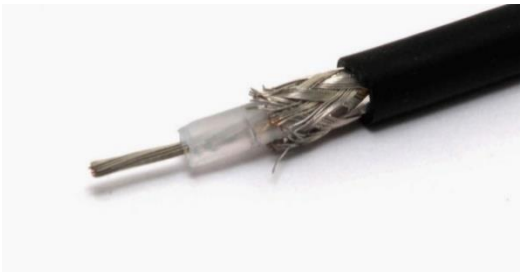
Gambar 2.6 Kabel UTP

b. Kabel Coaxial

   Coaxial adalah suatu jenis kabel yang menggunakan dua buah konduktor. Pusatnya berupa inti kawat padat yang dilingkupi oleh sekat yang kemudian dililiti lagi oleh kawat berselaput konduktor. Jenis kabel ini biasa digunakan untuk jaringan dengan bandwith yang tinggi. Kabel coaxial mempunyai pengalir tembaga di tengah (centre core). Lapisan plastik (dielectric insulator) yang mengelilingi tembaga berfungsi sebagai penebat di antara tembaga dan lapisan metal (metallic shield). Lapisan metal berfungsi untuk menghalang sembarang gangguan luar, sedangkan lapisan paling luar

adalah lapisan plastik yang disebut jacket plastic. Lapisan ini berfungsi seperti jaket yaitu sebagai pelindung bagian terluar.

Berikut ini adalah gambar kabel coaxcial yang dapat dilihat pada Gambar 2.7.

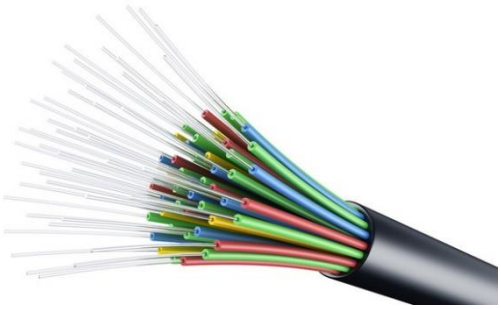


Gambar 2.7 Kabel Coaxial

c. Kabel Fiber Optic

Kabel Fiber optic adalah sebuah kabel yang terbuat dari serat kaca dengan teknologi canggih dan mempunyai kecepatan transfer data yang lebih cepat daripada kabel biasa, biasanya fiber optic digunakan pada jaringan backbone (Tulang Punggung) karena dibutuhkan kecepatan yang lebih dalam jaringan ini,namun pada saat ini sudah banyak yang menggunakan fiber optic untuk jaringan biasa baik LAN, WAN maupun MAN karena dapat memberikan dampak yang lebih pada kecepatan dan bandwith karena fiber optic ini menggunakan bias cahaya untuk mentransfer data yang melewatinya dan sudah barang tentu kecepatan cahaya tidak diragukan lagi namun untuk membangun jaringan dengan fiber optic dibutuhkan biaya yang cukup mahal dikarenakan dibutuhkan alat khusus dalam pembangunannya.

Berikut ini adalah gambar kabel fiber optic yang dapat dilihat pada Gambar 2.8.



Gambar 2.8 Kabel Fiber Optik

2. Wireless Nerwork (Unguided Media)

   Wireless Network adalah jaringan komputer yang menggunakan media gelombang radio, infrared, ataupun microwave sebagai media transmisinya. Spektrum yang digunakan pada wireless network antara 3kHz hingga 900 THz.

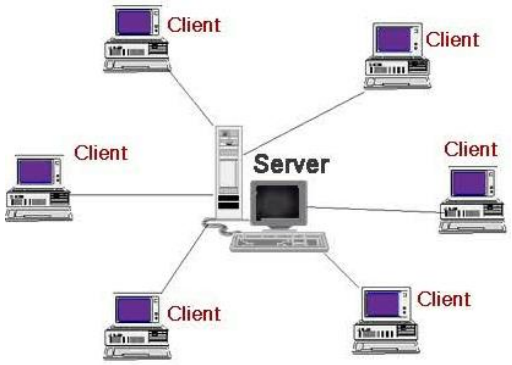
2.2.4 Fungsi Jaringan Komputer

Berdasarkan fungsinya, jaringan komputer dibagi menjadi dua jenis [4], yaitu:

1. Client Server

   Jenis jaringan ini terdapat komputer yang bertindak sebagai server dan komputer yang berperan sebagai client (workstation). Secara normal komputer server dapat mengontrol sepenuhnya komputer client. Server biasanya mempunyai kemampuan yang lebih besar dari pada client (Wahidin, 2007 : 1).

   Berikut ini adalah gambar contoh jaringan client server yang dapat dilihat pada Gambar 2.9.

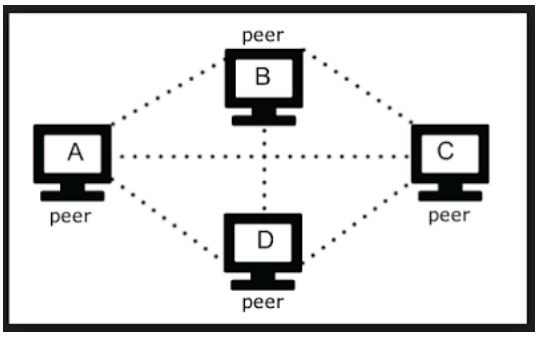


Gambar 2.9 Jaringan Client Server

2. Peer to Peer

   Peer to Peer merupakan jenis jaringan yang tidak memerlukan server secara khusus, karena komputer yang terhubung pada jaringan dapat bertindak sebagai server ataupun client. Contoh: hubungan komputer ke komputer (Wahidin, 2007 : 1).

   Berikut ini adalah contoh jaringan peer to peer yang dapat dilihat pada Gambar 2.10.



Gambar 2.10 Jaringan Peer to Peer

2.2.5 Topologi Jaringan Komputer

Topologi menggambarkan struktur dari suatu jaringan atau bagaimana sebuah jaringan didesain. Dalam definisi topologi terbagi menjadi dua, yaitu topologi fisik (Topologi menggambarkan struktur dari suatu jaringan atau bagaimana sebuah jaringan didesain. Dalam definisi topologi terbagi menjadi dua, yaitu topologi fisik (physical topology) yang menunjukan posisi pemasangan kabel secara fisik dan

topologi logic (logical topology) yang menunjukan bagaimana suatu media diakses oleh host[4].

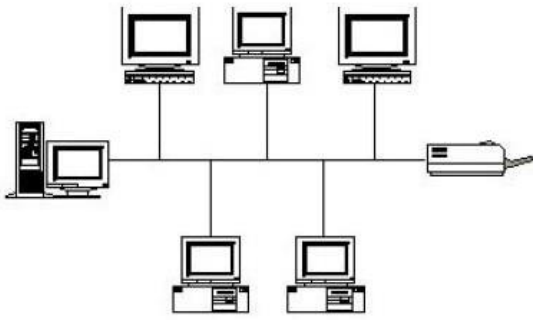
2.2.5.1 Topologi Fisik

Topologi fisik adalah desain suatu jaringan komputer dengan melihat bentuk nyata pada posisi dan letak node atau komputer, topologi fisik memerlukan kabel jaringan dan peralatan pendukung seperti kondensator, hub, switch, dan lainnya [4].

Berikut ini adalah jenis-jenis topologi fisik yang digunakan pada sebuah jaringan, yaitu :

1. Topologi Bus

   Topologi Bus terdiri dari satu jalur kabel utama dimana pada setiap ujungnya dipasang sebuah terminator. Semua node pada jaringan terkoneksi kabel utama (backbone). Contoh model topologi bus dapat dilihat pada Gambar 2.11.



Gambar 2.11 Topologi BUS

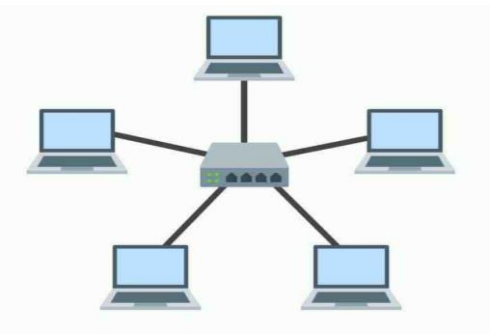
Berikut ini adalah keuntungan-keuntungan dan kerugian-kerugian dalam menggunakan topologi bus yang dijabarkan pada tabel Tabel 2.1 Kelebihan dan kekurangan Topologi BUS.

Tabel 2.1 Kelebihan dan kekurangan Topologi BUS

Kelebihan	Kekurangan
1. Mudah dikembangkan. 2. Jarak LAN tidak terbatas. 3. Keterandalan jaringan tinggi. 4. Kecepatan pengiriman tinggi. 5. Jumlah terminal dapat ditambah ataupun dikurangi tanpa mengganggu operasi yang telah berjalan. 6. Tidak diperlukan pengendalian pusat. 7. Kondusif untuk konfigurasi jaringan pada gedung bertingkat	1. Jika *traffic* data terlalu tinggi atau padat dapat terjadi kemacetan (*congestion*). 2. Diperlukan *repeater* untuk menguatkan sinyal pada pemasangan jarak jauh. 3. Oprasional jaringan LAN bergantung pada setiap terminal. 4. Jika terjadi gangguan atau kerusakan pada salah satu *node* dalam jaringan maka akan mempengaruhi jaringan secara keseluruhan, bahkan ada kemungkinan jaringan akan terhenti.

2. Topologi Star

   Topologi ini dirancang agar setiap node yang terhubung pada jaringan terkoneksi melalui konsentrator seperti hub atau switch. Semua data yang akan dikirim akan melawati konsetrator terlebih dahulu sebelum dikirim ke tujuan. Konsetrator ini berfungsi untuk mengendalikan jaringan itu da bertindak juga sebagai repeater. Contoh model topologi star dapat dilihat pada Gambar 2.12.



Gambar 2.12 Topologi Star

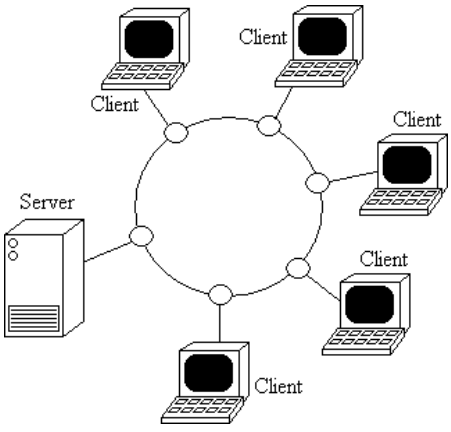
Berikut ini adalah keuntungan-keuntungan dan kerugian-kerugian dalam menggunakan topologi star yang dijabarkan pada Tabel 2.2, yaitu sebagai berikut :

Tabel 2.2 Kelebihan dan Kekurangan Topologi Star

Kelebihan	Kekurangan
1. Kehandalan topologi ini lebih besar dari topologi lainnya. 2. Mudah dikembangkan. 3. Keamanan data tinggi. 4. Kemudahan akses ke jaringan LAN lainnya.	1. Traffic data yang padat menyebabkan jaringan lambat. 2. Jaringan tergantung pada terminal pusat atau konsentrator.

3. Topologi Ring

Topologi ring mempunyai konfigurasi yang mirip dengan topologi star, namun tanpa adanya konsentrator. Sehingga media transmisi akan menyerupai cincin. Contoh model topologi ring dapat dilihat pada Gambar 2.13.



Gambar 2.13 Topologi Ring

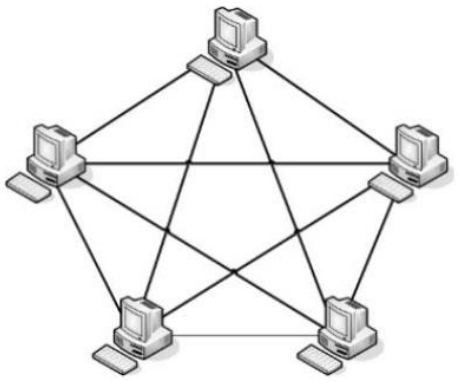
Berikut ini adalah keuntungan-keuntungan dan kerugian-kerugian dalam menggunakan topologi ring yang dijabarkan pada Tabel 2.3, yaitu sebagai berikut :

Tabel 2.3 Kelebihan dan Kekurangan Topologi Star

Kelebihan	Kekurangan
1. Laju data (*transfer rate*) tinggi. 2. Dapat melayani *traffic* data yang padat. 3. Tidak diperlukan *host*, relatif lebih mudah. 4. Dapat melayani berbagai media pengiriman. 5. Komunikasi antar terminal mudah. 6. Waktu yang diperlukan untuk mengakses data optimal.	1. Penambahan atau pengurangan terminal cukup sulit. 2. Kerusakan pada media pengiriman data menghentikan kerja seluruh jaringan. 3. Harus ada kemampuan untuk mendeteksi kesalahan dan metode pengisolasian kesalahan. 4. Tidak kondusif untuk pengiriman suara, gambar, dan data.

4. Topologi Mesh

Topologi mesh memberi setiap perangkat koneksi khusus point-to-point terhadap semua perangkat lain yang berada dalam satu jaringan. Maksud dari koneksi khusus ini adalah bahwa satu koneksi hanya membawa paket antara dua perangkat yang saling terkoneksi. Contoh model topologi mesh dapat dilihat pada Gambar 1.1.



Gambar 2.14 Topologi Mesh

Berikut ini adalah keuntungan-keuntungan dan kerugian-kerugian dalam menggunakan topologi ring yang dijabarkan pada Tabel 2.4, yaitu sebagai berikut:

Tabel 2.4 Kelebihan dan Kekurangan Topologi Mesh

Kelebihan	Kekurangan
1. Dapat melayani berbagai media pengiriman. 2. Tidak diperlukan pengendalian pusat.	1. Penambahan atau pengurangan terminal sangat sulit. 2. Kerusakan pada salah satu terminal dapat mengakibatkan kelumpuhan jaringan. 3. Kerusakan pada salah satu terminal membuat *traffic* data terhambat.

2.3 Keamanan Jaringan Komputer

Keamanan dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan, segi-segi keamanan didefinisikan lima poin[5], yaitu:

1. confidentiality Mensyaratkan bahwa informasi (data) hanya bisa di akses oleh pihak yang memiliki wewenang.
2. Intergrity, mensyaratkan bahwa informasi hanya dapat di ubah oleh pihak yang memiliki
3. Availability, mensyaratkan bahwa informasi tersedia untuk pihak yang memiliki wewenang ketika di butuhkan.
4. Authentication, Mensyaratkan bahwa pengirim suatu informasi dapat diindentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu.
5. Nonrepudiation, Mensyaratkan bahwa baik pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan.

Serangan (gangguan) terhadap keamanan dapat dikategorikan dalam empat kategori utama, yaitu 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.

Penggunaan sistem jaringan komputer dalam skala kecil maupun luas akan membutuhkan pengaturanpengaturan mulai dari tingkat fisik maupun non fisik. Pengaturan-pengaturan tersebut melibatkan proses pengontrolan. Ada beberapa definisi mengenai administrasi jaringan ini antara lain : Controlling corporate strategic (assets), Controlling complekxity, Improving service, Balancing various needs, Reducing downtime dan Controlling costs.

Pemahaman tentang routing teori maupun konfigurasi harus di kuasai dengan baik agar mampu membangun jaringan dengan baik hal ini sangat diperlukan terutama jika komputer ataupun sub organisasi perusahaan sangat banyak. Pengetahuan tentang sistem keamanan komputer terutama jaringannya (network security) akan sangat membantu dan memberikan nilai lebih. Selain kemampuan teori maupun praktek yang harus dikuasai dengan baik hal lain adalah memiliki etika profesional, tanpa etika dan sikap seorang profesional yang baik maka semua kemampuan teori maupun praktek yang dikuasai tidak akan berarti banyak.

Keamanan jaringan secara umum adalah komputer yang terhubung ke network, mempunyai ancaman keamanan lebih besar dari pada komputer yang tidak terhubung kemana-mana. Dengan pengendalian yang teliti, resiko tersebut dapat dikurangi, namun network security biasanya bertentangan dengan network access, dimana bila network access semakin mudah, maka network security semakin rawan, begitu pula sebaliknya.

Seperti yang di ungkapkan oleh Kevin Mitnick(seorang craker terkenal), sebagian besar celah diperoleh melalui rekayasa social yang menunjukan kelemahan user. Saat ini di Indonesia masih banyak praktik di pengguna yang sangat mengabaikan faktor keamanan (bahkan di bank). Banyak user tergolong

sensitive (missal bank) saling menukar password, bahkan sering menuliskan password dan menempel di dekat monitornya.

2.3.1 Macam-macam keamanan jaringan

Keamanan jaringan dibagi menjadi 2 yaitu keamanan physical dan logic, serangan langsung maupun serangan tidak langsung, oleh karna itu penulis akan membahas tantang keamanan jaringan[5].

1. Keamanan jaringan secara physical atau keamanan fisik yang sering mengacu pada tindakan yang diambil untuk melindungi sistem, gedung dan infrastuktur pendukung yang terkait terhadap ancaman yang berhubungan dengan lingkungan fisik, contoh-contoh dalam keamanan fisik yaitu company surroundings, reception, server, workstation area, wireless access point, access control, computer equipment maintence, wiretapping, remote access.
2. Kemanan jaringan secara logic adalah hal yang paling rawan terjadi sehingga harus lebih memperhatikan lagi keamanan logic dalam jaringan komputer kita, dalam hal ini keamanan logic ini sering mendapatkan serangan secara tidak langsung seperti yang di alami oleh fisik tetapi serangan secara logic menimbulkan dampak yang cukup serius.

2.3.2 Ancaman keamanan

Ancaman keamanan yang terjadi bisa di kelompokan menjadi beberapa ancaman yaitu:

a. Interruption adalah ancaman terhadap availability informasi, data yang ada dalam sistem komputer dirusak atau di hapus sehingga jika data atau informasi tersebut di butuhkan maka pemiliknya akan mengalami kesulitan mengaksesnya, bahkan mungkin informasi itu hilang.
b. Interception adalah ancaman terhadap kerahasiaan (secrecy). Informasi disadap sehingga orang yang tidak berhak dapat mengakses komputer dimana informasi tersebut disimpan.

c. Modification adalah ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu-lintas informasi yang sedang dikirim dan kemudian mengubahnya sesuai keinginan orang tersebut.
d. Fabrication adalah ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru atau memalsukan informasi sehingga orang yang menerima informasi tersebut menyangka bahwa informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi.

2.3.3 Penyebab serangan

Penyerang menggunkan teknik yang telah dipublikasijan, yang biasa di akses dengan mudah ke suatu sistem . jika sytem terhubung dengan jaringan publik tidak mempunyai pertahanan yang baik, Karena tidak dikoreksi dengan naik, walaupun vendor memiliki produk yang mempunyai lubang-lubang keamanan, yang apabila tidak di perhatikan dengan baik maka akan banyak situasi yang menyebabkan ada begitu banyak lubang keamanan, seperti [5]:

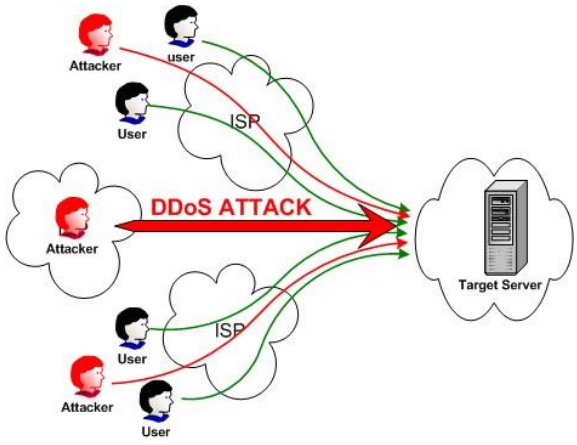
a. Banyak dari legacy sistem, sistem oprasi tidak patch maupun update.
b. Patch yang digunakan tidak diperhatikan dengan baik kebanyakan dari patch yang ada tidak diperiksa keamanannya sehingga menambahkan masalah baru dalam hal keamanan.
c. User yang melakukan kegiatan oprasional terhadap permintaan service jaringan dan protocol tidak memahami sistem, step-step yang harus dilakukan sehingga jaringan dan protocol yang mereka gunakan memiliki lubang keamanan.
d. User dan administrator membuat kesalahan dalam konfigurasi dan dalam menggunakan sistem.
e. Mekanisme konfigurasi akses control sistem tidak mempunyai policy yang baik.

2.4 Jenis Serangan Terhadap Jaringan Komputer

Jenis jenis serangan / tipe tipe serangan adalah macam macam teknik penyerangan terhadap keamanan jaringan yang memiliki tujuan yang berbeda-beda berikut adalah jenis jenis serangan .

2.4.1 Denial of service (DOS)

Serangan Denial Of Service (DOS) atau Denial of service (DOS) Attack merupakan suatu serangan yang dimana bertujuan untuk mendapatkan hak akses penuh pada server misalnya penyerangan ingin mendapatkan suatu data di database server, menginstall program jahat (malware), dan lain-lain yang pada intinya melumpuhkan compute target[6]. Denial of service (DOS) dilakukan dengan cara membanjiri server target dengan pesan-pesan ataupun permintaan secara terus-menerus pada satu waktu, sehingga mengakibatkan server menjadi overload Karena sumber daya (memory, CPU useg, bandwith) yang memiliki server tersebut habis terpakai melayani pesan dan permintaan datang. Seperti pada Gambar 2.15.



Gambar 2.15 Serangan DOS

Tujuan dari DoS attack tidak untuk mendapatkan hak akses yang legal untuk masuk ke dalam sistem, melainkan untuk mencegah user untuk mengakses servis. Agar serangan tersebut dapat berjalan, penyerang akan melakukan berbagai cara antara lain[6] :

1. Mencoba untuk membajiri traffic data pada jaringan yang ditargetkan, sehingga membuat jaringan tidak dapat memberi user konektivitas.

2. Mencoba untuk mengganggu koneksi antara dua mesin dalam suatu jaringan yang berdampak servis tidak dapat dipergunakan.
3. Mencoba untuk mencegah beberapa individu dari menakses servis atau mengganggu salah satu servis yang spesifik agar tidak dapat diakses.

2.4.2 Scanning

Scanning adalah proses dimana penyerang akan menggali informasi tentang alamat IP target, sistem operasi yang digunakan, arsitektur jaringan yang digunakan, dan servis yang sedang berjalan pada komputer pun dapat di peroleh. Tidak seperti footprinting yang hanya mengali informasi secara pasif dari pihak ketiga dalam berbagai sumber, scanning secara aktif berhadapan dengan target untuk menperoleh informasi[6].

Dalam melakukan scanning, terdapat beberapa tipe scanning diantaranya sebagai berikut :

1. *Port scanning*

   Port scanning meliputi pengiriman beberapa pesan pada komputer target untuk memperoleh tipe servis jaringan apakah yang sedang berjalan pada jaringan tersebut. Dikarenakan servis tersebut berkaitan dengan nomor port, maka dengan melakukan port scan pada target akan menampilkan seluruh port yang terbuka.

2. *Network scanning*

   Network scanning adalah suatu prosedur untuk mengidentifikasi host yang sedang aktif pada jaringan target yang bertujuang untuk melakukan serangan pada target ataupun untuk menilai keamanan jaringan. Dalam langkah ini akan memungkinkan penyerang untuk membuat daftar host-host yang dapat diserang secara langsung atau menggunakan host tersebut untuk menyerang host lain secara tidak langsung.

3. *Vulnerability scanning*

   Vulnerability scanning berhubungan dengan penggunaan tools otomastis yang dikenal dengan vulnerability scanner yang secara otomatis mengidentifikasi kelemahan-kelemahan keamanan pada sistem komputer di

jaringan tersebut. Tools ini akan melacak target untuk mencari tahu celah keamanan manakah yang dapat di eksploitasi.

2.4.3 Malware

Malware adalah perangkat lunak (software) yang diciptakan untuk menyusup atau merusak sistem komputer. Perangkat lunak dianggap sebagai perangkat perusak berdasarkan maksud yang terlihat dari pencipta dan bukan berdasarkan ciri-ciri tertentu. *S*alah satu teknik kemanan jaringan dimana penyadap menempatkan dirinya berada di tengah-tengah perangkat yang saling berkomunikasi.[7] Malware mencakup virus komputer, worm, Trojan horse, rootkit, spyware, adware, dan perangkat lunak lainnya yang berniat jahat dan tidak diinginkan. Malware tidak sama dengan perangkat lunak cacat *(defective software)*, yaitu, perangkat lunak yang mempunyai tujuan sah tetapi berisi bug yang berbahaya[6].

2.5 IDPS (Intrusion Detection and Prevention System)

Cara kerja IDPS *(Intrusion Detection and Prevention System)* adalah dengan memonitor karakteristik dan peristiwa yang terjadi pada host. Pemonitoran tersebut untuk medeteksi adanya aktivitas mencurigakan. Host-based IDPS melakukan pemeriksaaan terhadap lalulintas jaringan terhadap host, sistem log, proses yang sedang berjalan, akses file, modifikasi file, serta perubahan pengaturan sistem dan aplikasi[8].

2.5.1 Komponen dan Arsitektur

1. Komponen Utama

Host-based IDPS berupa software pendeteksi (agent) yang terinstall pada host dan dalam bentuk alat yang menjalankan software pendeteksi (agent). Alat tersebut diletakkan didepan host pada jaringan. Satu agent mengawasi hanya satu aplikasi spesifik, misalkan web server atau database server. Setiap agent didisain khusun untuk melindungi salah satu hal berikut: [8]

a. Server

   Pemantauan meliputi OS dan aplikasi pada server.

b. Client host (berupa destop atau laptop)

   Pemantauan meliputi OS dan Aplikasi (misalkan e-mail client dan Web browser) yang terinstall di host

c. Layanan aplikasi

   Contoh layanan tersebut berupa Web server program dan database server program. Produk yang tersedia umumnya tidak memiliki agent untuk host lainnya, semacam network device(firewalls, routers, switches)

2. Arsitektur Jaringan

Agent dipasang pada host yang tersambung pada jaringan suatu organisasi. Oleh karena itu, agent pada umummya berkomunikasi melalui jaringan tersebut daripada menggunakan jaringan yang terpisah. Produk host-based IDPS yang dijual umunnya melakukan enkripsi terhadap komuikasi tersebut.

3. Lokasi Agent

Host-based IDPS agent paling sering dipasang pada host yang sangat rawan. Hal tersebut misalnya server yang dapat diakses oleh publik dan server yang memiliki informasi penting. Setiap server dan host dapat dipasangi agent ini. Host-based IDPS ini digunakan untuk mengawasi aktifitas yang tidak bisa dilakukan IDPS lain. pengawasan tersebut misalnya dilakukan terhadap komunikasi terenkripsi pada jaringan. Host merupakan end-point komuikasi sehingga dapat melakun dekripsi.

Kriteria pemilihan tempat pemasangan agent:

a. Biaya pemasangan, perawatan, dan pengawasan
b. OS dan aplikasi yang dapat didukung agent
c. Tingkat kepentingan data dan layanan pada host
d. Kemampuan infrastruktur mendukung agent
e. Ketersediaan bandwidth jarigan untuk mengirim data peringatan dari agnet ke server pusat serta pembaruan perangkat lunak dan kebijakan dari server pusat ke agent

4. Arsitektur Host

Untuk menyediakan kemampuan pencegahan, kebanyakan agent dari IDPS merubah arsitektur internal host. Hal ini dlikakan misalnya dalam penggunaan shim. Shim adalah suatu layer yang diletakkan diantara layer-layer code program. Shim ini dapat melakuakan analisa data antar layer tersebut dan menentukan apakah hal tersebut diperbolehkan atau ditolak. Agent dari host-based IDPS mungkin menggunakan shim untuk pemantauan lalulistas jaringan, aktivitas filesystem, system call, aktivitas register window, serta aplikasi umum seperti e-maildan Web.

Selain hal diatas, ada juag agent host-based IDPS yang tidak merubah arsitektur internal host. Agent-agent ini melakukan pemantauan tanpa menggunakan shim. Sebagai gantinya mereka menggunakan jejak dari aktivitas intrusi, misalnya catatan log dan perubahan file. Walaupun demikian, metode ini lebih tidak efektif mendeteksi ancaman dibandingkan dengan metode sebelumnya. Selain itu, dengan penggunaan metode ini kita tidak bisa melakukan pencegahan intrusi. [8]

Selain pemilihan metode diatas, pemilihan lain yang penting adalah apakah host-based IDPS ini diintall pada host atau menggunakan device fisik. Agent yang di-install di host memiliki sejumlah keuntungan dilihat dari segi pendeteksian dan pencegahan. Agent medapatkan akses langsung terhadap host sehingga dapat melakukan pedetesian dan pencegahan secara lebih lengkap dan akurat.

Namun demikian, tidak semua agent dapat di install pada OS yang digunakan. Disini, agent dalam bentuk device fisik lebih cocok digunakan. Pertimbangan lainnya adalah beban di host. Bila agent di-intall di host, beban di host bertambah banyak dan bisa menyebakan penurunan performa host.

2.5.2 Security Capabilities

1. Logging Capabilities

   Agent melakukan pencatatan terhadap kejadian yang terdeteksi. Data ini digunakan untuk mengecek validitas sinyal peringatan, menghubungkan kejadian antara host-based IDPS dan sumber log yang lain[8].

   Jenis data yang biasanya dicatat adalah:

a. Timestamp
b. Kejadian atau jenis sinyal peringatan
c. Tingkat prioritas, serangan, dampak, dan kepercayaan
d. Aksi pencegahan yang dilakukan bila ada

2. Detection Capabilities

Agent mendeteksi sejumlah aktivitas jahatan. Teknik yang digunakan merupakan kombinasi dari:

a. Teknik pendeteksian berdasarkan signature serangan yang pernah terjadi
b. Teknik pendeteksian berdasarkan kejanggalan. Digunakan untuk mendeteksi serangan yang belum pernah terjadi.

Aspek yang berkaitan dengan kemampuan pendeteteksian host-based IDPS

a. Jenis kejadian yang terdeteksi
b. Akurasi pendeteksian
c. Penyetelan dan kustomisasi
d. Keterbatasan teknologi

3. Prevention Capabilities

Kemampuan pencegahan intrusi beragam tergantung teknik pendeteksian yang digunakan. Teknik yang digunakan misalkan analisa code. Dengan teknik ini dapat dicegah pengeksekusian code berupa malware dan unauthorized aplication. Teknik lainnya adalah analisa lalulintas jaringan, penyaringan lalulintas jaringan, dan pemantauan sistem file

2.6 Simulasi

Simulasi berasal dari bahasa inggris, yaitu : *to simulate*, yang artinya untuk memperoleh intisari dari sesuatu tanpa melibatkan kenyataan. Simulasi mempunyai banyak pengertian bila dilihat dari berbagai sudut pandang yang berbeda. Klasifikasi atau pengelompokan dari teknik simulasi dibagi menjadi tiga kelompok, yaitu : [9]

1. Simulasi statis dan dinamis

   Simulasi statis merupakan representasi dari sebuah sistem pada suatu waktu tertentu, atau digunakan pada sistem dimana waktu tidak mempunyai peran. Penerapan paling sederhana pada simulasi ini adalah saat memasukan nilai variable pada suatu rumus untuk memperoleh nilai akhirnya. Sedangkan simulasi dinamis mewakili sistem yang berubah-ubah seturut waktu. Contohnya sistem ban berjalan pada pabrik.

2. Simulasi deterministik dan stochastic

   Simulasi deterministik adalah bila sistem simulasi tidak mempunyai komponen probabilitas. Contoh dari simulasi ini adalah persamaan diferensial yang menghitung reaksi kimia. Simulasi stochastic adalah bila sistem tersebut memiliki beberapa komponen input acak *(random)*, hasil akhir dari simulasi ini juga berupa komponen acak. Kebanyakan sistem antrian *(queueing)* dan persediaan *(inventory)* merupakan model simulasi stochastic.

3. Simulasi kontinyu dan diskrit

   Simulasi kontinyu merupakan model sistem yang kondisi status variablenya berubah-ubah terus menerus sesuai dengan waktu, simulasi model ini melibatkan persamaan diferensial yang merupakan relasi dari tingkat perubahan status variable sistem terhadap waktu, contohnya simulasi aliran air dari beberapa sungai ke danau. Simulasi diskrit adalah dimana status variabelnya berubah seketika pada satu titik waktu yang terpisah, dengan kata lain sistem berubah hanya pada waktu tertentu. Contoh dari simulasi ini adalah sistem antrian, sistem sirkulasi parker.

2.7 Sistem Operasi Komputer

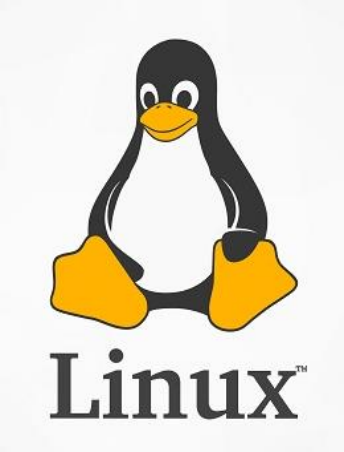
Sistem operasi komputer merupakan bagian yang terpenting dalam suatu sistem komputer, merupakan jantung dari komputer itu sendiri. Sistem operasi komputer merupakan program yang figunakan untuk mengendalikan sistem input/output, seperti keyboard, diskdrive, dan juga digunakan untuk membaca dan menjalankan program atau aplikasi. Sistem operasi juga merupakan sekumpulan

mekanisme dan kebijakan yang membantu mendefinsikan pengendalian sumberdaya yang di-share[10].

Sistem operasi dibedakan berdasarkan kemampuan untuk menangani proses dan pemakaian komputer pada saat yang bersamaan menjadi sistem operasi standalone dan multiuser. Pada sistem operasi standalone, komputer hanya dapat digunakan untuk satu pemakai saja pada saat yang bersamaan, tetapi proses yang di tanganinya bias lebih dari satu pada saat yang bersamaan. Sedangkan dengan sistem operasi multiuser, komputer dapat digunakan untuk melayani proses dari banyak pemakai pada saat yang bersamaan.

2.7.1 Linux

Linux adalah varian dari sistem operasi Unix. Linux dikembangkan oleh Linus Torvlads, pada saat itu masih merupakan mahasiswa di Finlandia, tahun 1990, yang berkeinginan memiliki sistem operasi sendiri untuk komputernya yang bias dengan mudah dimodifikasi, seolah program komputer biasa[10]. Berikut ini adalah logo sistem operasi linux dapat dilihat pada Gambar 2.16.



Gambar 2.16 Logo Sistem Operasi Linux

Versi awal dari linux kemudian disebarluaskan secara bebas, untuk mendapatkan masukan dari pengguna dan pengembang software yang memang mencari sistem operasi alternatif. Sambutan yang sangat antusias diterima dari komunitas yang mencoba sistem operasi baru ini, ternyata kemudian mereka menyokong dan membantu mengembangkan sistem operasi ini.

2.7.2 Debian

Debian pertama kali diperkenalkan oleh Ian Murdock, seorang mahasiswa dari universitas Purdue, Amerika Serikat. Debian dikenal karena pilihannya yang beragam. Rilis stabil saat ini memuat lebih dari 29 ribu paket perangkat lunak untuk 9 arsitektur komputer. Debian menggunakan kernel linux dan juga menggunakan 2 kernel FreeBSD. Arsitektur komputer ini mulai dari Intel/AMD yang umumnya ditemukan di sistem embedded dan server mainframe IBM Zseries[10]. Berikut ini adalah logo sistem operasi debian dapat dilihat pada Gambar 2.17.

Gambar 2.17 Logo Sistem Operasi Debian

Fitur yang menonjol dari debian adalah APT sistem pengaturan paket, repository dengan jumlah paket yang banyak, kebijakan paket yang ketat, dan kualitas rilis, begitupun untuk penghapusan paket. Standar instalasi debian menggunakan GNOME desktop environtment.

2.7.3 Ubuntu

Salah satu komponen utama dalam jaringan adalah sistem operasi komputer. Sistem operasi ini berfungsi untuk mengatur komunikasi jaringan berupa dokumen, printer. Scanner dan perangkat-perangkat lainnya. Sistem operasi dapat membedakan arsitektur dalam pemanfaatan fasilitas-fasilitas yang ada di jaringan. Misalkan membedakan perangkat jaringan seperti Ethernet dan token ring atau arsitektur lainnya [10]. Berikut ini adalah logo sistem operasi Ubuntu dapat dilihat pada Gambar 2.18.

Gambar 2.18 Logo Sistem Operasi Ubuntu

Sistem operasi Ubuntu merupakan turunan dari sistem operasi linux yang lain, yakni Debian. Ubuntu itu sendiri dibuat dengan tujuan selalu gratis tanpa adanya biaya lisensi, bersifat open source, dan siap untuk dipergunakan dalam kondisi yang stabil. Ubuntu didukung oleh perusahaan bernama canonical, Ltd yang memiliki tujuan untuk membantu perkembangan, distribusi, dan promosi dari produk-produk yang bersifat open source. Perusahaan ini bermarkas di eropa dan dipimpin oleh seseorang bernama Mark Shuttleworth. Sejak pertama kali diluncurkan, Ubuntu mendapatkan perhatian yang sangat besar dari pengguna linux yang lain. Hai ini disebabkan karena kestabilan yang dimiliki oleh Ubuntu itu sendiri. Selain itu kenyamanan dan kemudahan yang dimiliki Ubuntu menjadi daya tarik yang besar bagi pengguna linux di seluruh belahan dunia.

2.7.4 Windows

Microsoft windows atau yang lebih dikenal dengan sebutan windows adalah salah satu dari keluarga sistem operasi. Sistem operasi windows telah berevolusi dari MS-DOS, sebuah sistem operasi yang berbasis modus teks dan command-line. Windows pertama yang menggunakan sistem GUI adalah Windows Graphic Encirontment 1.0 atau yang biasa dikenal dengan Windows 1.0 dikenalkan pertama kali pada 10 novembar 1983. Windows 1.0 merupakan perangkat lunak 16-bit tambahan (bukan merupakan sistem operasi) yang berjalan di atas MS-DOS (dan beberapa varian dari MS-DOS), sehingga ia tidak dapat berjalan tanpa adanya

sistem operasi DOS[10]. Berikut ini adalah logo sistem operasi windows dapat dilihat pada Gambar 2.19.

Gambar 2.19 Logo Sistem Operasi Windows

Dimulai dari DosShell untuk DOS 6 buatan Microsoft dan inginya Microsoft bersaing terhadap larisnya penjualan apple macintosh yang menggunakan GUI, Microsoft menciptakan windows 1.0. nama ini berasal dari kelatahan karyawan Microsoft yang menyebutkan nama aplikasi tersebut sebagai program windows (jendela program). Windows versi 2 adalah versi windows pertama yang bisa diinstal program.

2.8 Perangkat Lunak Pendukung

Perangkat lunak pendukung ialah beberapa perangkat lunak yang digunakan oleh penulis dalam merancang aplikasi ini.

2.8.1 VirtualBox

VirtualBox pertamakali dikembangkan oleh perusahaan Jerman (Innotek GmbH). Pada February 2008, Innotek GmbH diakusisi oleh Sun Microsystems. dan menjadi milik Oracle saat pengakuisisian Sun Microsystems. Oracle VM VirtualBox adalah perangkat lunak virtualisasi, yang dapat digunakan untuk mengeksekusi sistem operasi "tambahan" di dalam sistem operasi "utama". Sebagai contoh, jika seseorang mempunyai sistem operasi MS Windows yang terpasang di komputernya, maka seseorang tersebut dapat pula menjalankan sistem operasi lain yang diinginkan di dalam sistem operasi MS Windows[10].

Fungsi ini sangat penting jika seseorang ingin melakukan ujicoba dan simulasi instalasi suatu sistem tanpa harus kehilangan sistem yang ada. Aplikasi dengan fungsi sejenis VirtualBox lainnya adalah VMware dan Microsoft Virtual PC. Sistem operasi yang dapat menjalankannya antara lain Linux, Mac OS X, Windows XP, Windows Vista, Windows 7, Windows 8, Solaris, dan OpenSolaris

Gambar 2.20 Logo VirtualBox

2.8.2 Suricata

Suricata adalah mesin pendeteksi ancaman jaringan yang bebas dan open source, matang, cepat dan tangguh. Mesin Suricata mampu mendeteksi intrusi waktu nyata (IDS), pencegahan intrusi sebaris (IPS), pemantauan keamanan jaringan (NSM) dan pemrosesan pcap offline. Suricata memeriksa lalu lintas jaringan menggunakan aturan dan bahasa tanda tangan yang kuat dan luas, dan memiliki dukungan skrip Lua yang kuat untuk mendeteksi ancaman yang kompleks. Dengan format input dan output standar seperti integrasi YAML dan JSON dengan alat-alat seperti SIEM yang ada, Splunk, Logstash / Elasticsearch, Kibana, dan basis data lainnya menjadi mudah[11].

Pembangunan yang didorong oleh masyarakat Suricata yang cepat berfokus pada keamanan, kegunaan, dan efisiensi.Proyek dan kode Suricata dimiliki dan didukung oleh Open Security Security Foundation (OISF), sebuah yayasan nirlaba yang berkomitmen untuk memastikan pengembangan Suricata dan kesuksesan berkelanjutan sebagai proyek sumber terbuka.

2.8.3 Barnyard2

Barnyard2 adalah tool open source sebagai penerjemah alert unified dan log dari snort. Barnyard dapat meningkatkan efisiensi Suricata dengan cara mengurangi beban pada sensor deteksi. Barnyard2 bekerja dengan membaca Suricata unified logging output files dan memasukkannya ke dalam database. Jika database tidak tersedia maka Barnyard2 akan memasukkan semua data ketika database tersedia kembali sehingga tidak ada alert atau log yang hilang [12]

2.8.4 Snorby

Snorby adalah alat pemantauan jaringan berbasis ruby yang merupakan platform open source. Keuntungan utama adalah fleksibilitasnya, dengan kata lain, Anda dapat menambahkan kode ke aplikasi dan memodifikasinya sesuai kebutuhan Anda. Snorby adalah antarmuka web modern untuk Pemantauan Keamanan Jaringan yang juga menyediakan sistem pencegahan intrusi berbasis perangkat lunak.[13]

2.8.5 Nmap

Nmap adalah utilitas keamanan open-source kuat yang dapat digunakan untuk meng-audit keamanan dan mengeksplorasi jaringan, tetapi dapat juga digunakan untuk komputer yang tidak terhubung dengan jaringan[14]. Nmap didesain untuk melakukan scanning jaringan besar ataupun kecil dengan menggunakan paket raw IP untuk mengetahui host yang sedang aktif dalam jaringan, service yang dijalankan , dan port yang terbuka. Berikut ini adalah bentuk umum perintah yang digunakan dalam melakukan scanning : nmap [tipe scan] [opsi scan] [alamat target]. Sebagai contoh berikut adalah perintah dan pengertian opsi untuk scanning dasar : nmap –sS –P0 –sV –o 192.168.1.1. Untuk opsi yang digunakan memiliki fungsi sebagai berikut, -sS opsi untuk menggunakan fitur TCP SYN scan, -P0 adalah opsi untuk melakukan scanning terhadap protocol tertentu berdasarkan nomor protokolnya, sedangkan –sV adalah opsi untuk mencari versi dari service yang aktif pada port tertentu, dan –o adalah opsi untuk mengetahui sistem operasi apa yang digunakan oleh target. Nmap dapat digunakan untuk

melakukan fingerprinting yang bisa membandingkan dan memberikan estimasi jenis istem operasi apa yang digunakan target. Nmap juga mempunyai banyak kelebihan atau flags yang akan memanipulasi cara scanning

2.8.6 Hping3

Hping adalah sebuat TCP/IP assembler dan juga merupakan command-line yang berorientasi pada pemrosesan paket TCP/IP. Hping dapat digunakan untuk membuat paket IP yang berisi TCP. UDP atau ICMP payloads. Semua field header dapat dimodifikasi dan dikontrol dengan menggunakan baris perintah (command-line) [15].

Berikut ini adalah bentuk umum perintah yang digunakan hping untuk menyerang targetnya : hping3 [opsi] [alamat target], dan berikut adalah contoh perintah untuk melakukan serangan pada target yang beralamat 192.168.1.1 : hping3 –c 100000 –d 12000 –S –w 128 –p 21,80,443,3306 –flood 192.168.1.1 dari perintah diatas dapat diartikan hping3 menyerang target yang beralamat di 192.168.1.1 dengan menggunakan opsi –c yang berarti jumlah paket yang akan dikirimnya sebanyak 100000 byte, kemudian –d yang berarti ukuran data yang dikirim sebesar 12000 byte, -S yang berarti menggunakan SYN flag, -w berarti winsize yang digunakan berukuran 128, -p adalah opsi ke port mana saja serangan akan dituju, dan opsi terakhir --flood yaitu mengirim paket secepat-cepatnya agar target menjadi lebih sulit untuk merespon.