BAB 2
LANDASAN TEORI

Bab ini berisi pembahasan mengenai teori dasar yang melandasi permasalahan serta penyelesaian yang ada dalam penelitian ini. Dasar teori yang diberikan meliputi keamanan jaringan, Konsep IDS dan IPS, Snort, pfSense dan teori pendukung lainnya.

1.1 Jaringan Komputer

Jaringan Komputer adalah himpunan antara dua computer *autonomus* atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*). Dua computer dikatakan terkoneksi apabila keduanya dapat melakukan pertukaran data atau informasi, berbagi resource yang dimiliki. [10]. Data atau informasi tersebut bergerak melalui media kabel atau tanpa kabel sehingga memungkinkan pengguna komputer dalam jaringan komputer dapat saling bertukar file atau data.

Jaringan komputer bertujuan membawa informasi secara tepat dan tanpa ada kesalahan dari pengirim menuju penerima melalui media komunikasi. Tujuan dibangunnya jaringan komputer bagi user dapat dibagi menjadi dua, yaitu kebutuhan perusahaan dan jaringan untuk umum. Berikut tujuan dibangunnya suatu jaringan komputer pada suatu perusahaan :

1. Resource Sharing, bertujuan agar seluruh program, peralatan, khusunya data, dapat digunakan oleh setiap user pada jaringan tanpa terpengaruh lokasi resource dan pemakai.
2. High reliability, tersedianya sumber daya alternatif, misalnya, semua data atau file dapat disalin ke semua mesin, sehingga jika salah satu mesin mati, maka data atau file tetap dapat di akses dari mesin lainnya yang masih aktif.
3. Saving Money, komputer berukuran kecil mempunyai rasio kinerja yang lebih baik daripada komputer. Komputer mainframe memiliki kecepatan 10 kali lipat tetapi harga komputer mainframe 10 kali lipat lebih mahal dari komputer pribadi. Hal ini menyebabkan perancang sistem merasa lebih baik membangun sistem yang terdiri dari komputer kecil, seperti PC Desktop.

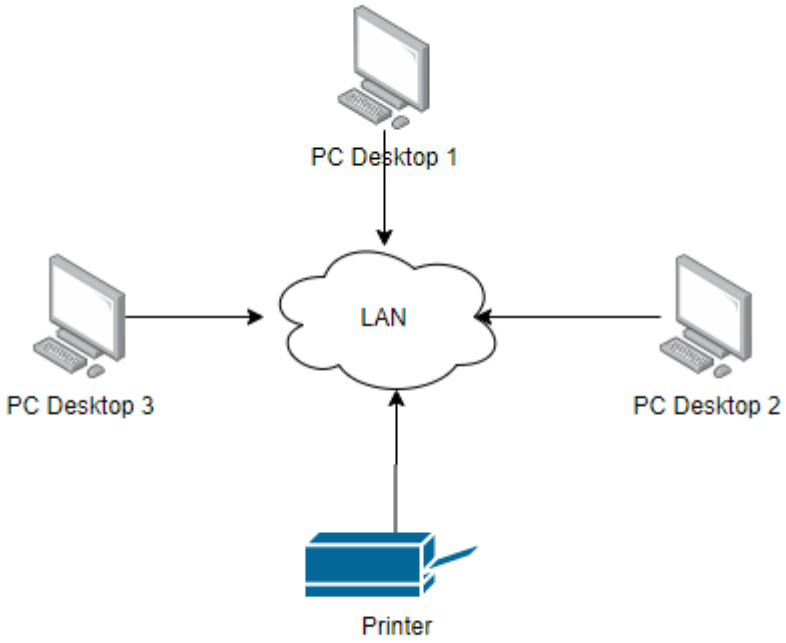
Adapun beberapa tujuan dibangunnya sesuatu jaringan komputer untuk umum :

1. Akses ke informasi yang berada di tempat lain lebih mudah
2. Komunikasi orang ke orang (seperti email, chatting, video conference)
3. Hiburan interaktif (seperti video streaming, download lagu dll)

Jaringan Komputer dapat dibedakan berdasarkan area cangkupannya. Ada tiga kategori utama yang menajdi pembeda jaringan komputer menurut area cangkupannya, yaitu :

1. LAN (*Local Area Network*)

   Local Area Network adalah jaringan yang cangkupannya relatif kecil, umumnya dibatasi oleh area lingkungan, seperti kantor pada suatu gedung, tiap ruangan pada sekolah [10]. Biasanya jarak antarnode tidak lebih dari sekitar 200 meter. Berikut adalah gambar skema jaringan LAN yang dapat dilihat pada gambar 2.1.



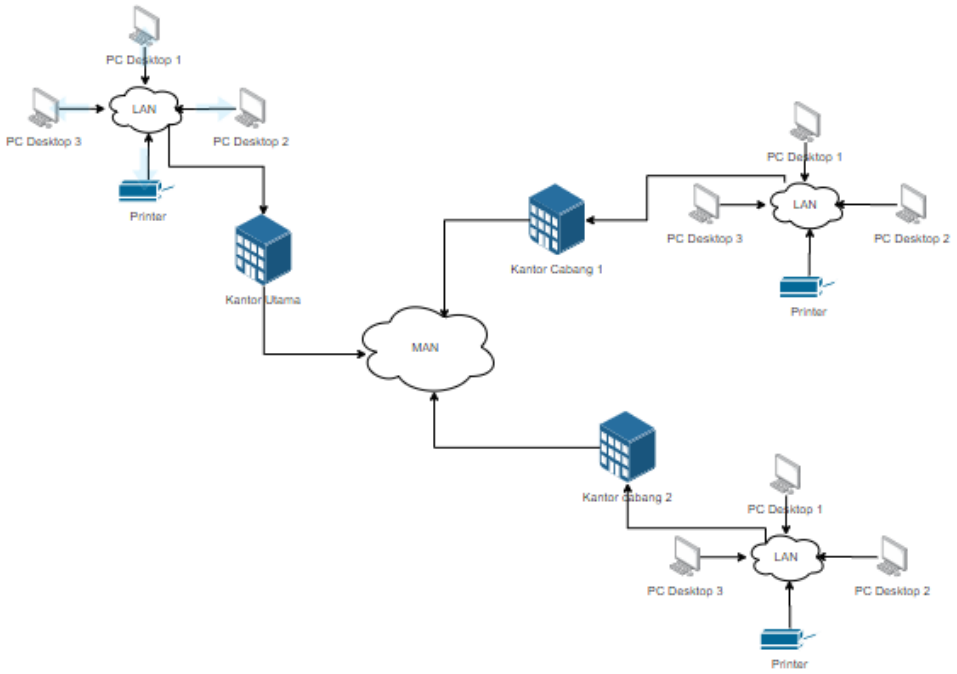
Gambar 2. 1 Jaringan Local Area Network

2. MAN (*Metropolitan Area Network*)

   Metropolitan Area Network adalah jaringan yang cangkupan jaringannya lebih besar dari LAN, misalnya antargedung yang saling berdekatan. Dalam hal ini MAN menghubungkan beberapa jaringan kecil (LAN) ke cangkupan area yang

lebih besar. Sebagai contoh, jaringan beberapa kantor cabang didalam kota besar yang dihubungkan antar satu dengan yang lainnya.

Berikut adalah gambar skema jaringan MAN yang dapat dilihat pada gambar 2.2.



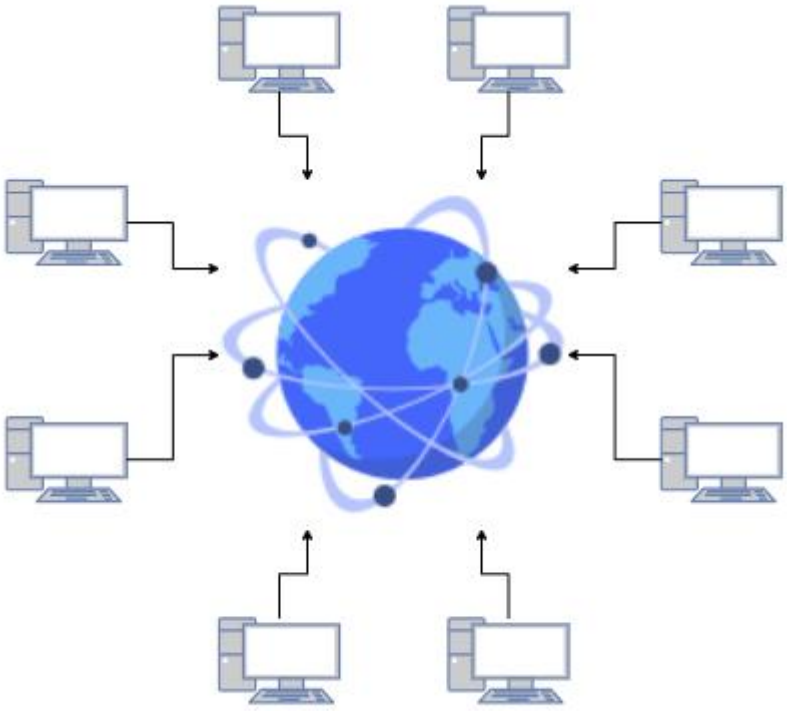
Gambar 2. 2 Jaringan Metropolitan Area Network

3. WAN (*Wide Area Network*)

   Wide Area Network adalah jaringan yang cangkupannya sangat luas, biasanya menggunakan media *wireless*, satelit, ataupun kabel serat optik, *Wide Area Network* bukan hanya meliputi satu kota atau antarkota dalam suatu wilayah, tetapi sudah menjangkau area otoritas negara. Sebagai contoh, jaringan komputer ATM Master Card, Visa Card yang ada di Indonesia ataupun yang ada di negara lain yang saling berhubungan.

   Wide Area Network lebih rumit dan lebih kompleks dibandingkan dengan *Local Area Netwok* maupun *Metropolitan Area Network*. Meski demikian LAN, MAN dan WAN tidak banyak berbeda, hanya area cangkupannya saja yang berbeda satu sama lain.

Berikut adalah gambar skema jaringan WAN yang dapat dilihat pada gambar 2.3.



Gambar 2. 3 Jaringan Wide Area Network

Selain berdasarkan area cangkupannya, jaringan komputer juga dapat dibedakan berdasarkan media trasnmisinya. media transmisi adalah perangkat yang digunakan sebagai jalur penyampaian dari data yang dikirimkan. Hampir 85% kegagalan yang terjadi pada jaringan komputer disebabkan karena adanya sekalah pada media komunikasi yang digunakan [10] Salah satu media transmisi pada jaringan komputer adalah kabel. Berikut beberapa kabel yang menjadi media transmisi pada jaringan komputer :

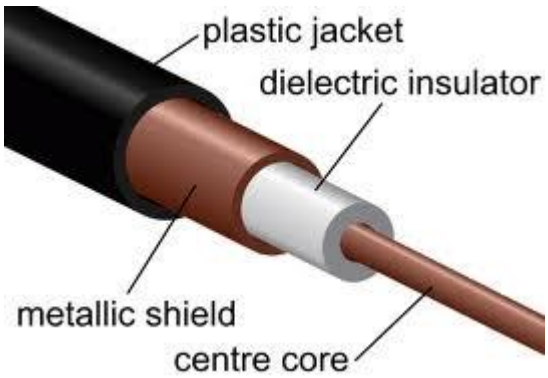
1. Kabel Coaxial

   Kabel Coaxial memiliki dua jenis tipe berbeda yang digunakan pada jaringan komputer, yaitu :

   a. *Thick Coax* (Kabel Coaxial “Gemuk”)

Kabel coaxial jenis ini dispesifikasikan berdasarkan standar IEEE 802.3 – 10BASE5, dimana kabel ini mimiliki diameter rata – rata 12mm. jenis kabel ini biasa digunakan untuk jaringan dengan *Bandwidth* tinggi.

Berikut adalah gambar kabel *Thick Coaxial* yang dapat dilihat pada gambar 2.4.

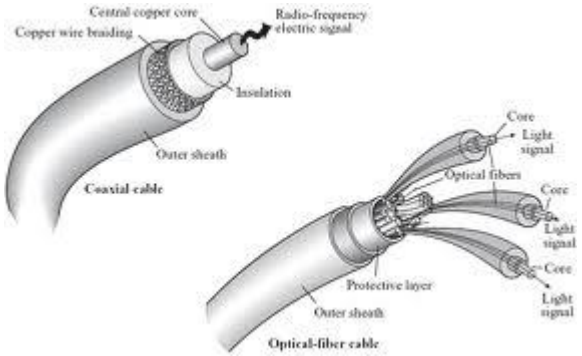


Gambar 2. 4 Kabel *Thick Coaxial*

b. *Thin Coax* (Kabel Coaxial "Kurus")

Kabel coaxial jenis ini sering digunakan oleh radio amatir, terutama untuk transceiver yang tidak memerlukan output daya yang besar. Jenis kabel untuk antena televisi juga termasuk jenis *thin coaxial*.

Berikut adalah gambar kabel *Thick Coaxial* yang dapat dilihat pada gambar 2.5.

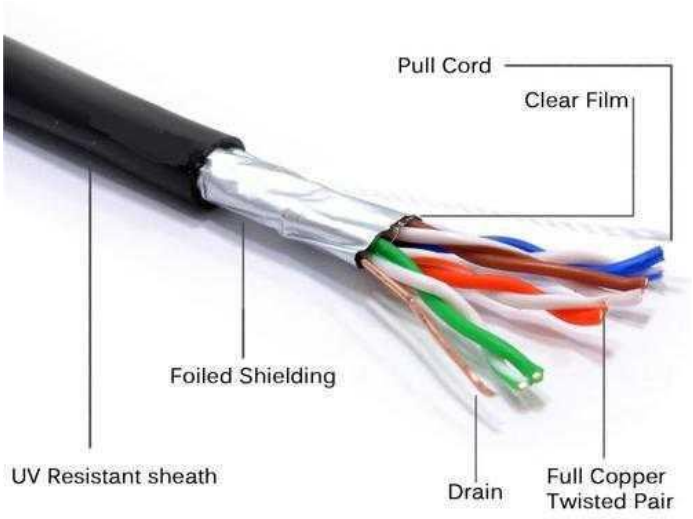


Gambar 2. 5 Kabel *Thin Coaxial*

2. Kabel *Unshielded Twisted Pair*

   Unshielded Twisted Pair biasa disebut kabel UTP adalah kabel yang terdiri dari 4 pasang kabel yang terpilin dimana masing – masing pasang mempunyai kode warna berbeda.

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

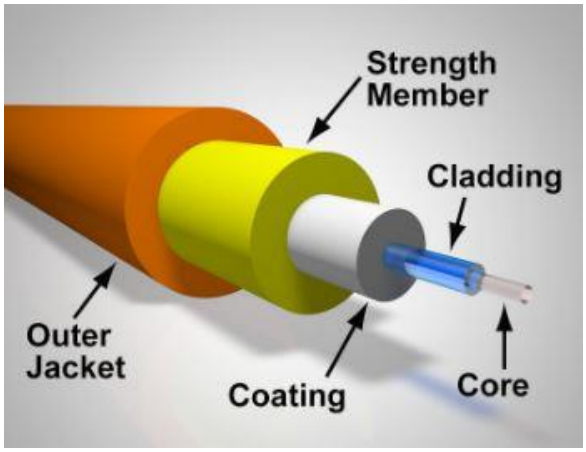


Gambar 2. 6 Kabel UTP

3. Kabel Fiber Optic

   Kabel fiber optic adalah kabel yang memiliki serat kaca sebagai saluran untuk menyalurkan sinyal antarterminal yang sering digunakan sebagai saluran BACKBONE karena *realiability* nya yang tinggi dibandingkan dengan kabel coaxial atau kabel UTP.

   Berikut adalah gambar kabel Fiber Optic yang dapat dilihat pada gambar 2.7.



Gambar 2. 7 Kabel Fiber Optic

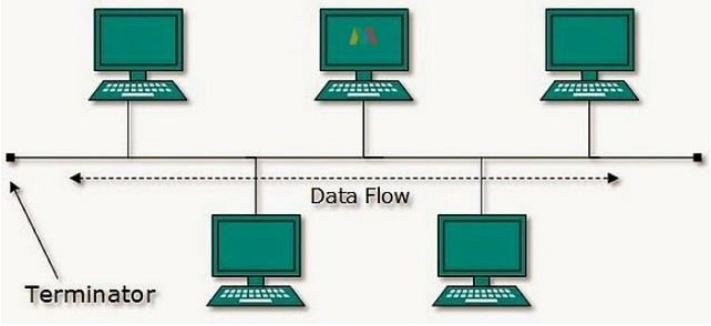
1.2 Topologi

Topologi jaringan adalah konsep untuk menghubungkan dua komputer atau lebih, berdasarkan geometris, antara unsur – unsur dasar penyusun jaringan, yaitu node, link, dan station [10].

Berikut adalah jenis – jenis topologi yang biasa digunakan untuk membangun suatu jaringan :

1. Topologi Bus

   Topologi Bus adalah konsep jaringan dimana beberapa client berhubungan menggunakan line komunikasi yang terbagi yang disebut BUS. Pada topologi bus biasanya menggunakan kabel coaxial. Seluruh jaringan biasanya merupakan satu saluran kabel yang kedua ujungnya dipisahkan dengan alat berupa Terminator. Topologi bus rentan terhadap collision atau tabrakan data apabila 2 *client* mentrasmisikan data pada saat yang sama. Beberapa sistem yang menggunakan topologi bus umumnya memiliki skema *collision handling* untuk mencegah tabrakan data. Model topologi bus dapat dilihat pada gambar 2.8.



Gambar 2. 8 Topologi BUS

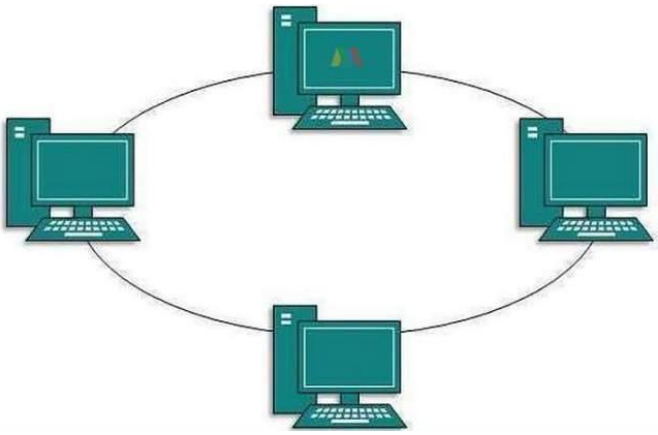
Berikut ini adalah kelebihan dan kekurangan penerapan topologi bus yang dijabarkan pada tabel 2.1.

Tabel 2. 1 Kelebihan dan Kekurangan Topologi Bus

Kelebihan	Kekurangan
1. Mudah di implementasikan dan diperluas 2. Kabel yang diperlukan sedikit 3. Cocok untuk jaringan komputer kecil karena mudah di *setup* 4. Layout kabel sederhana	1. Deteksi dan isolasi kesalahan sangat kecil 2. Bila salah satu client rusak, maka jaringan tidak dapat berfungsi. 3. Jika komputer banyak, maka jumlah data yang mengalir akan memperlambat jaringan. 4. Diperlukan repeater untuk jarak jauh. 5. Operasional jaringan bergantung pada setiap terminal

2. Topologi Ring

   Topologi Ring adalah topologi jaringan dimana tiap simpul akan terhubung ke simpul lainnya sehingga membentuk lingkarang yang berfungsi sebagai line untuk trasnmisi data. Data akan dijalankan dari simpul ke simpul yang konsekuensinya tiap simpul akan menangani tiap paket. Model topologi Ring dapat dilihat pada gambar 2.9.



Gambar 2. 9 Topologi Ring

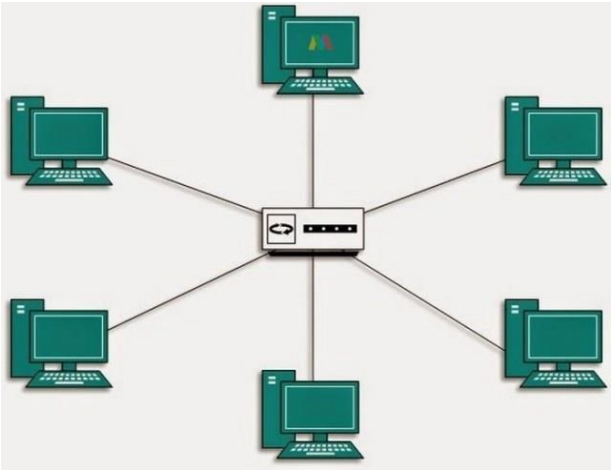
Berikut ini adalah kelebihan dan kekurangan penerapan topologi Ring yang dijabarkan pada tabel 2.2.

Tabel 2. 2 Kelebihan dan Kekurangan Topologi Ring

Kelebihan	Kekurangan
1. Data mengalir dalam satu arah sehingga terjadinya tabrakan data dapat dihindari. 2. Dapat melayani aliran lalulintas data yang padat 3. Waktu untuk mengakses data lebih optimal	1. Jika salah satu komputer gagal berfungsi, maka akan memper=ngaruhi keseluruhan jaringan. 2. Sulit melakukan konfigurasi ulang. 3. Menambah atau mengurangi komputer akan mengacaukan jaringan.

3. Topologi Star

   Topologi Star adalah konsep yang sering digunakan saat membangun suatu jaringan. Jaringan ini memiliki bentuk paling sederhana. Jaringan ini terdiri dari switch atau hub yang berfungsi sebagai pusat untuk melakukan transmisi data. Topologi star menggunakan satu terminal sebagai terminal pusat yang mengubungkan ke semua terminal client. Apabila salah satu terminal client tidak berfungsi maka tidak akan mempengaruhi kerja dari jaringan, karena ganguan tersebut hanya mempengaruhi terminal yang bersangkutan. Model topologi Star dapat dilihat pada gambar 2.10.



Gambar 2. 10 Topologi Star

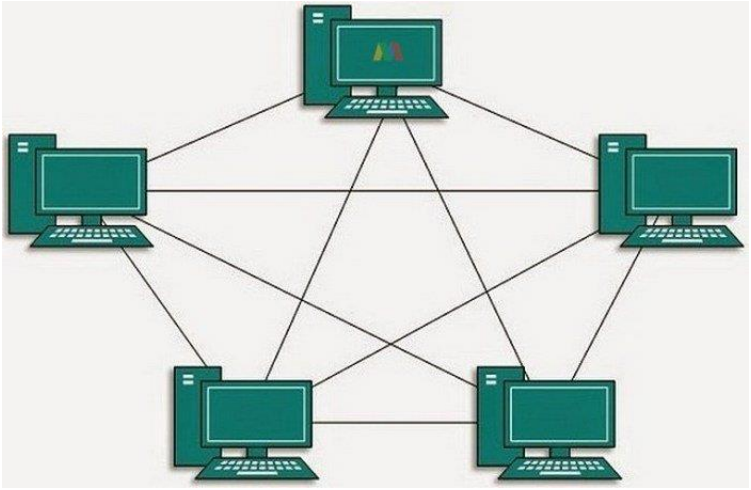
Berikut ini adalah kelebihan dan kekurangan penerapan topologi Ring yang dijabarkan pada tabel 2.3.

Tabel 2. 3 Kelebihan dan Kekurangan Topologi Star

Kelebihan	Kekurangan
1. Fleksibel 2. Pemasangan atau perubahan stasiun sangan mudah dan tidak mengganggu bagian jaringan lain. 3. Kontrol terpusat 4. Mudah mendeteksi dan isolasi kesalahan atau kerusakan 5. Mudah dalam pengelolaan jaringan.	1. Boros kabel 2. Perlu penanganan khusus 3. Kontrol terpusat menjadi elemen kritis.

4. Topologi Mesh

   Topologi Mesh adalah sebuah cara untuk melakukan routing data, suara dan instruksi antar simpul. Topologi mesh memungkinkan koneksi continue dan rekonfigurasi di jalur yang putus atau terblok. Topologi mes berbeda dengan topologi lain dimana komponen dari topologi ini bisa saling terhubung menggunakan rute yang berlainan. Model topologi mesh dapat dilihat pada gambar 2.11.



Gambar 2. 11 Topologi Mesh

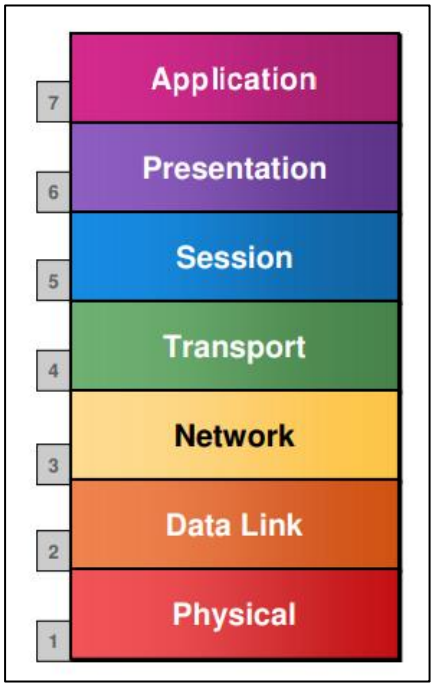
Berikut ini adalah kelebihan dan kekurangan penerapan topologi Mesh yang dijabarkan pada tabel 2.4.

Tabel 2. 4 Kelebihan dan Kekurangan Topologi Mesh

Kelebihan	Kekurangan
1. Fault Tolerance 2. Terjaminnya kapasitas channel komunikasi 3. Relatif lebih mudah untuk troubleshoot	1. Sulit pada saat melakukan instalasi dan konfigurasi ulang. 2. Biaya besar untuk maintenance

1.3 *Open System Interconnection* (OSI)

Open System Interconnection atau OSI adalah model referensi komunikasi antar entitas principle terdiri atas tujuh lapisan. Ketujuh lapisan tersebut mempunyai peranan dan fungsi berbeda antara satu terhadap lainnya. Setiap layer bertanggung jawab secara khusus pada proses komunikasi. Tujuan utama model OSI adalah membantu memahami fungsi dari tiap-tiap layer yang berhubungan dengan aliran komunikasi data, termasuk jenis protokol jaringan dan metode transmisi. Model OSI dibagi menjadi tujuh layer, dengan karekteristik dan fungsinya masing masing. Tiap layer harus dapat berkomunikasi dengan layer di atas maupun dibawahnya secara langsung melayani beberapa protokol dan standar. Berikut adalah layer OSI yang dapat dilihat pada gambar 2.12.



Gambar 2. 12 Layer Open System Interconnection (OSI)

Berikut ini merupakan penjabaran tujuh model Layer OSI, yang mana pada setiap lapisan mempunyai tugas dan fungsi masing – masing sesuai dengan penggunaannya terkait dengan kebutuhan koneksi :

1. Physical Layer (Lapisan ke-1)

   Lapisan ini digunakan untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan dan pengabelan.

2. Data-Link Layer (Lapisan ke-2)

   Lapisan ini bertugas untuk menentukan setiap bit data dikelompokkan menjadi format yang disebut dengan frame. Pada lapisan ini juga terjadi koreksi kesalahan, flow control, pengalamatan hardware atau perangkat keras (seperti halnya pada MAC Address)

3. Network Layer (Lapisan ke-3)

   Lapisan ini betugas membuat header untuk paket yang berisi informasi IP (Internet Protocol), baik IP pengirim atau IP tujuan data. Pada suatu kondisi, network layer juga melakukan proses routing melalui internetworking dengan menggunakan bantuan router dan switch pada layer ke-3.

4. Transport Layer (Lapisan ke-4)

   Lapisan ini bertugas untuk memecah data menjadi paket – paket data, serta memberikan nomor urut untuk setiap paketnya. Sehingga, nantinya dapat disusun kembali saat sampai pada tujuan. Pada lapisan ini juga menentukan protokol yang akan digunakan untuk mentransmisikan data, seperti protokol TCP. Protokol tersebut akan mengirimkan paket data, sekaligus memastikan bahwa setiap paket telah diterima dengan sukses dan tepat sasaran.

5. Session Layer (Lapisan ke-5)

   Lapisan ini berfungsi untuk mendefinisikan bagaimana sebuah koneksi dapat dibuat, dikelola, dan dikembangkan. Contoh protokol yang berada pada session layer adalah NFS, SMB, RTP, dan lain – lain.

6. Presentation Layer (Lapisan ke-6)

   Lapisan ini mempunyai fungsi untuk mentranslasikan format data yang akan ditransmisikan oleh aplikasi melalui jaringan, ke dalam format yang dapat ditransmisikan oleh sebuah jaringan. Pada Lapisan ini, data juga akan ter-enkripsi dan dekripsi melalui sistem

7. Application Layer (Lapisan ke-7)

   Lapisan ini adalah lapisan yang menjadi pusat (center) terjadinya suatu interaksi antara pengguna (end user) dengan aplikasi yang bekerja menggunakan fungsionalitas sebuah jaringan. Selain itu juga mempunyai fungsi untuk melakukan konfigurasi mengenai bagaimana cara aplikasi dapat bekerja menggunakan resource jaringan yang kemudian, dapat memberikan pesan saat terjadi sebuah kesalahan pada proses pengaturan jaringan.

1.4 TCP/IP

TCP/IP adalah sekumpulan prokol yang terdapat didalam network yang digunakan untuk berkomunikasi atau bertukar data antarkomputer. TCP/IP merupakan protokol standar pada jaringan internet yang menghubungkan banyak komputer yang berbeda jenis mesin maupun sistem operasi agar dapat berinteraksi

satu sama lain. TCP/IP memiliki nilai biner 32-bit yang diberikan kesetiap *host* dalam sebuah jaringan. Nilai ini digunakan untuk mengidentifikasi jaringan mana Host dan mengidentifikasi nomor host unik di jaringan tertentu. Setiap host yang terhubung ke host di Internet harus memiliki host Alamat TCP / IP unik.

Tabel 2. 5 Klasifikasi Alamat IP

Kelas	Jumlah Host	Jumlah Oktet Pertama	Jumlah Network
A	16.777.216	1-126	126
B	16.536	128-191	16,384
C	256	192-233	2,097,151

Setiap komputer di jaringan biasanya ingin mengirim data Langsung ke komputer lain. Komputer pengiriman harus memastikan Penerima berada di jaringan yang sama atau di luar jaringan itu. Gunakan subnet mask Tentukan host akan berkomunikasi melalui protokol TCP / IP Di jaringan lokal yang sama atau di jaringan jarak jauh.

Tabel 2. 6 Klasifikasi Subnet Mask

Kelas	Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

1.5 IP Address

IP (*Internet Protocol*) adalah standar protokol dalam internetworking. Alamat IP merupakan representasi 32 bit bilangan unsigned biner yang biasa ditampilkan dalam bentuk desimal dengan titik [11]. Contoh 192.168.10.0 merupakan contoh valid dari IP. Untuk mengidentifikasi suatu host pada internet, maka tiap host diberi IP address atau internet address.

Bit pertama dari IP address memberikan spesifikasi terhadap sisa alamat dari IP. Selain itu juga dapat memisahkan suatu alamat IP dari jaringan. Network (network address) biasa disebut juga sebagai netID, sedangkan untuk alamat host (host address) biasa disebut juga sebagai hostID. Ada 5 pembagian kelas IP Address :

1. Kelas A : Menggunakan 7 bit network address dan 24 bit hostID, dengan ini memungkinkan adanya 2 juta alamat.
2. Kelas B : Menggunakan 14 bit alamat network dan 16 bit untuk alamat host. Dengan ini memungkinkan adanya 1 juta alamat.
3. Kelas C : Menggunakan 21 bit alamat network dan 8 bit untuk alamat host. Dengan ini memungkinkan adanya sekitar setengah juta alamat.
4. Kelas D : Biasa digunakan untuk multicast
5. Kelas E : Digunakan untuk selanjutnya

1.6 Port

Port digunakan untuk melakukan proses komunikasi dengan proses lain pada jaringan TCP/IP. Port menggunakan nomer 16 bit, digunakan untuk komunikasi host-to-host. Tipe port ada 2 macam yaitu :

1. Well-known : port yang sudah dimiliki oleh server. Contoh : telnet menggunakan port 23. Well-known port memiliki range dari 1 hingga 1023. Port Well-known diatur oleh Internet Assigned Number Authority (IANA) dan dapat digunakan oleh proses sistem dengan user tertentu yang mendapatkan akses.
2. Ephemeral : client tidak menggunakan port well-known karena untuk berkomunikasi dengan server, mereka sudah melakukan perjanjian terlebih dahulu untuk menggunakan port mana. Ephemeral port memiliki range dari 1023 hingga 65535.

1.7 Perangkat Jaringan

Perangkat jaringan adalah peranti yang digunakan untuk membangun suatu jaringan baik peranti keras maupun peranti lunak. Perangkat jaringan memiliki fungsi dan tujuan tersendiri dalam suatu jaringan. Perangkat jaringan adapt dipilih bersdasarkan kebutuhan saat membangun suatu jaringan.

1.7.1 Hub

Hub merupakan alat untuk menggabungkan beberapa komputer atau jaringan lainnya secara bersama-sama untuk membentuk segmen jaringan tunggal.

Pada segmen jaringan, semua komputer dapat berkomunikasi langsung pada setiap hub. Hub mencakup serangkaian port yang masing – masing menerima kabel jaringan. Hub digolongkan sebagai perangkat lapisan 1 pada model OSI. Hub hanya menerima *incomingpackets* dan menyebarkan paket ini ke semua komputer dan perangkat pada jaringan. Berikut adalah hub yang dapat dilihat pada gambar 2.13.

Gambar 2. 13 Hub

1.7.2 Repeater

Repeater adalah untuk menerima sinyal yang kemudian meneruskan kembali sinyal yang diterima dengan kekuatan yang sama. Dengan adanya reperater, sinyal dari suatu komputer dapat dikirim ke komputer lain yang letaknya berjauhan. Berikut adalah repeater yang dapat dilihat pada gambar 2.14.

Gambar 2. 14 Repeater

1.7.3 Bridge

Bridge berfungsi seperti repeater atau hub, tetapi lebih pintar karena bridge bekerja pada lapisan data link sehingga mempunyai kemampuan untuk menggunakan MAC Address dalam proses pengiriman frame ke alamat yang dituju. Bridge berfungsi untuk menghubungkan dua buah LAN yang mempunyai perbedaan pada lapisan OSI 1 dan 2, contohnya LAN dengan Ethernet akan dihubungkan dengan LAN yang menggunakan metode token bus. Berikut adalah bridge yang dapat dilihat pada gambar 2.15.

Gambar 2. 15 Bridge

1.7.4 Switch

Switch terdiri dari beberapa port sehingga switch disebut *multiport bridge*. Fungsi switch hampir sama dengan bridge. Switch memiliki kemampuan dimana, jika salah satu port pada switch sibuk maka port yang lain masih tetap berfungsi dengan normal. Namun switch tidak dapat meneruskan paket IP yang ditujukan ke komputer lain jika berbeda jaringan (*network address*). Berikut adalah switch yang dapat dilihat pada gambar 2.16.

Gambar 2. 16 Switch

1.7.5 Router

Router adalah perangkat jaringan yang berfungsi sebagai penghubung dua buah jaringan ang memiliki perbedaan pada lapisan OSI 1 , 2 dan 3, contohnya LAN dengan Netware akan dihubungkan dengan jaringan yang menggunakan UNIX. Berikut adalah router yang dapat dilihat pada gambar 2.17.

Gambar 2. 17 Router

1.8 Keamanan Jaringan Komputer

Keamanan jaringan komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaanlayanan bagi penggunaannya [3]. Sistem keamanan jaringan komputer harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak.

Komputer Yang Terhubung ke Jaringan Mengalami ancaman keamanan yang lebih besar daripada hosted yang tidak terhubung keamanan. Dengan Mengendalikan keamanan jaringan, resiko tersebut dapat dikurangi. Namun keamanan jaringan biasanya bertentangan dengan akses jaringan, keamanan jaringan akan semakin rawan. Bila keamanan jaringan *backbone area*, *network access* semakin terbatas. Suatu Jaringan di desain sebagai komunikasi data highway dengan tujuan meningkatkan ke sistem komputer, sementara keamanan dirancang untuk mengontrol akses. Penyediaan keamanan jaringan adalah sebagai penyeimbang antara is open access dengan keamanan.

Pada dasarnya keamanan adalah perlindungan atas sumber fisik dan konseptual dari ancaman - ancaman. Keamanan terhadap sumber konseptual meliputi data dan informasi. Namun disamping itu banyak sekali upaya penyerangan, untuk menjaga keamanan atas sumber fisik maupun konseptual dengan berbagai macam cara. Keamanan harus memiliki beberapa hal yang harus dipenuhi, yaitu :

1. Confidentiality

   Confidentiality (rahasia) berarti menjaga kerahasiaan informasi dengan melakukan pembatasan hak akses seseorang, yang paling umum dengan menggunakan enkripsi. Contoh data-data yang harus dijaga kerahasiaannya seperti data-data yang sifatnya pribadi (nama, tanggal lahir, penyakit yang pernah diderita, nomor kartu kredit, nama ibu kandung, dan sebagainya), data-data milik organisasi atau perusahaan.

2. Integrity

   Integrity (keaslian) berarti menjamin bahwa data/informasi yang dimiliki terjaga keasliannya, tidak berubah tanpa pemilik informasi. Integrity

merujuk pada tingkat kepercayaan terhadap suatu informasi. Di dalam integrity terdapat 2 mekanisme pengamanan yaitu mekanisme priventif dan mekanisme detektif. Mekanisme priventif merupakan kontrol akses untuk menghalangi terjadinya modifikasi data. Sedangkan mekanisme detektif adalah untuk melakukan deteksi terhadap modifikasi yang telah dilakukan oleh orang lain

3. Availability

   Availability (ketersediaan) berhubungan dengan ketersediaan informasi ketika dibutuhkan. Artinya, informasi harus selalu tersedia saat dibutuhkan oleh user, dan dapat dengan cepat diakses. Serangan yang paling lazim untuk jenis keamanan ini adalah Distributed Denial of Service (DDoS). Serangan ini memenuhi resource atau sumber informasi (server) dengan permintaan yang banyak atau permintaan diluar perkiraan sehingga server tidak dapat melayani permintaan lain atau bahkan down.

1.9 Model Serangan Keamanan Jaringan

Model serangan jaringan adalah model yang digunakan penyerang untuk menyerang suatu jaringan. Terdapat beberapa model yang biasa digunakan penyerang untuk merusak suatu jaringan. Berikut model serangan terhadap suatu jaringan :

1. Interruption

   Interruption adalah model serangan yang ditujukan untuk aspek ketersediaan (availability), yang menjadikan sistem tidak tersedia atau rusak. Contoh serangan *denial of service attack*.

2. Interception

   Interception adalah model serangan berupa pihak yang tidak memiliki wewenang berhasil mengakses data / informasi. Misalnya dengan melakukan penyadapan (wiretapping).

3. Modification

Modification adalah model serangan berupa pihak yang tidak memiliki wewenang berhasil memodifikasi aset atau data/informasi yang dimiliki organisasi/perusahaan.

4. Fabrication

   Fabrication adalah model serangan berupa pihak yang tidak berwenang menjadi seolah-olah pengguna sah dan mengirimkan pesan palsu kedalam sistem. Menyerang aspek autentikasi. Contoh dengan memasukkan pesan-pesan palsu seperti e-mail palsu ke jaringan komputer

1.10 Distributed Denial Of Service (DDoS)

DDoS (Denial Of Service) merupakan jenis serangan yang menyerang server komputer dengan cara mengambil sumber daya dari server yang menyebabkan pelemahan sehingga komputer server tidak dapat menjalankan fungsinya dengan baik dan pengguna dari luar bias leluasa untuk mengakses layanan pada komputer server yang di serang dalam jaringan tersebut [12].

Konsep sederhana DDoS attacks adalah membanjiri lalu lintas jaringan dengan banyak data. Konsep DDoS attacks bisa dibagi menjadi 3 tipe penggunaan, sebagai berikut :

1. Request Flooding

   Request Flooding adalah cara yang digunakan penyerang dengan membanjiri jaringan dengan menggunakan banyak request. Hal ini mengakibatkan pengguna lain yang terdaftar tidak dapat layanan dari server.

2. Traffic Flooding

   Traffic Flooding adalah cara ynag digunakan penyerang dengan membanjiri lalu lintas jaringan dengan banyak data. Hal ini mengakibatkan pengguna lain yang terdaftar tidak dapat layanan dari server.

3. Merubah Konfigurasi Sistem

Serangan terakhir ini dengan melakukan perubahan sistem konfigurasi atau bisa saja dengan merusak komponen serta server tertarget. Namun serangan ini jarang dilakukan karena terbilang rumit.

1.11 Malware

Malware merupakan perangkat lunak yang dirancang untuk merusak atau menggangu komputer, sistem komputer, atau jaringan. Malware mengacu pada program yang disisipikan secara teselubung dengan tujuan untuk melihat informasi korban baik berbentuk data, aplikasi ataupun sistem operasi. Penyisipan malware bisa terjadi karena beberapa kemungkinan, seperti kesalahan pengguna yang tidak sengaja mengakses website yang berisi malware. Malware tidak sama dengan perangkat lunak cacat (defective software), yaitu, perangkat lunak yang mempunyai tujuan sah tetapi berisi bug yang berbahaya

1.12 Intrusion Detection System (IDS)

Intrusion Detection System (IDS) merupakan perangkat lunak atau perangkat keras sistem yang secara otomatis melakukan proses pemantauan (monitoring) insiden yang terjadi dalam sistem komputer atau jaringan serta menganalisis tanda-tanda adanya masalah terhadap keamanan sistem. Jika terindikasi adanya aktifitas yang mencurigakan terhadap aliran (traffic) paket-paket yang keluar dan masuk pada sistem, maka IDS akan merekam aktifitas tersebut.

1.12.1 Klasifikasi Intrusion Detection System (IDS)

Penerapan IDS dapat dilakukan diberbagai tempat pada suatu jaringan di sebuah instansi atau perusahaan dengan tujuan tercapainya keamanan sistem. IDS sendiri dapat diklasifikasikan menjadi dua jenis yaitu Host-based Intrusion Detection System (HIDS) dan Network-based Intrusion Detection System (NIDS).

1. Host-based Instrusion Detection System (HIDS)

   IDS tipe ini diterapkan dan beroperasi pada sebuah komputer server yang dianggap kritis atau rawan. Dalam pengertian lainnya, HIDS sesuai untuk arsitektur yang berupa single server yang memberikan layanan seperti web server, mail server, maupun layanan lainnya. Tujuan HIDS untuk memantau

serta mendeteksi aliran paket-paket yang masuk dan keluar yang terindikasi berbahaya pada host sehingga tipe ini disebut juga host-based IDS

2. Network-based Instrusion Detection System (NIDS)

   Pada IDS jenis ini diterapkan dan beroperasi dengan melihat semua lalu lintas aliran yang melewati jaringan sehingga disebut network-based IDS. Pada klasifikasi ini semua paket yang keluar maupun masuk pada sebuah jaringan komputer akan terlebih dahulu dianalisa dengan tujuan untuk menemukan adanya percobaan penyusupan ke dalam sistem jaringan. Hal ini efektif untuk menganalisa traffic diantara host maupun segmen jaringan lokal. Berbeda dengan HIDS, pada jenis ini NIDS akan ditempatkan pada pintu masuk jaringan (gateway).

1.12.2 Snort

Snort merupakan sebuah *open-source* yang dikembangkan oleh Marty Roesch. Snort bisa digunakan pada sistem operasi Linux, Windows, BSD, Solaris dan sistem operasi lainnya. Snort merupakan IDS berbasis jaringan yang menggunakan metode deteksi *rule-based*, menganalisis paket data apakah sesuai dengan jenis serangan yang sudah diketahui olehnya [7]. Snort digunakan karena memiliki beberapa kelebihan berikut: mudah dalam konfigurasi dan penambahan aturan-aturan, gratis, dapat berjalan pada sistem operasi yang berbeda-beda.

1.12.3 Anomaly-Based

IDS dengan pendekatan anomaly-based adalah Sebuah metode untuk mendeteksi serangan melalui pola lalu lintas jaringan yang tidak biasa. Jenis IDS ini memantau setiap lalu lintas jaringan dengan membandingkan aliran terkontrol untuk lalu lintas normal yang ada [4]. Lalu lintas jaringan normal merupakan penggunaan bandwidth yang biasa digunakan, protocol, port, dan perangkat yang terhubung

1.12.4 Signatured Based

IDS dengan metode signature based merupakan metode dalam mendeteksi serangan melalui pola atau paket data yang dibaca kemudian dibandingkan dengan

data atau paket yang sudah tersimpan dalam database yang ada atau rule yang sudah ada [4]. IDS berbasis signature mempunyai berbagai macam signature atau pola – pola serangan yang dapat dijadikan sebagai pembanding. IDS jenis ini bekerja dengan menyadap paket yang melalui lalu lintas jaringan, kemudian membandingkan dengan pola serangan yang ada, jika paket data mempunyai pola yang sama dengan salah satu pola yang terdapat pada rule database, maka paket tersebut dianggap sebagai sebuah serangan. Jika tidak mempunyai kesamaan, maka paket tersebut dianggap bukan sebagai serangan.

1.13 Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) adalah sebuah perangkat lunak atau perangkat keras yang bekerja untuk monitoring trafik jaringan, mendeteksi aktivitas yang mencurigakan dan melakukan pencegahan dini terhadap penyusupan atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti sebagaimana mestinya [13]. IPS merupakan pendekatan yang sering digunakan untuk membangun sistem keamanan komputer, IPS mengombinasikan teknik firewall dan metode intrusion detection system (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor saat seragan teridentifikasi. Jadi IPS bertindak seperti layaknya firewall yang akan mengizinkan atau menghalang paket data IPS memiliki empat komponen utama, yaitu :

1. Normalisasi Traffic: menginterpretasikan traffic jaringan dan melakukan analisa terhadap paket yang disusun kembali, seperti halnya fungsi block sederhana.
2. Detection Engine: mendeteksi traffic jaringan dan melakukan patternmatchingterhadap tabel acuan dan respon yang sesuai.
3. Service Scanner: membangun suatu tabel acuan untuk mengelompokkan informasi.
4. Traffic Shaper: membentuk dan mengatur traffic jaringan.

1.13.1 pfSense

PfSense adalah open-source yang secara khusus dairancang untuk digunakan sebagai firewall dan router yang sepenuhnya dikelola melalui antarmuka web [8]. Selain menjadi firewall dan router yang kuat dan fleksibel, PfSense mencakup sistem paket yang memungkinkan perluasan lebih lanjut tanpa menambahkan potensi kerentanan keamanan ke dalam distribusi dasar.

1.14 Virtual Machine

Virtual Machine adalah sebuah perangkat lunak yang memungkinkan suatu perangkat keras menjalankan beberapa sistem operasi beserta sumber daya secara bersamaan. Virtual machine dibuat untuk menghindari pemborosan sumber daya yang mahal, dengan kata lain meningkatkan efisiensi [14]. Virtual Machine juga merupakan kunci untuk membangun komputasi awan (*Cloud Computing*) yang memungkinkan *application isolation, mobility*, dan *patitioning* dari individual server di *cloud*. Sebagai contoh, saat menjalankan sistem operasi linux diatas sistem operasi Windows, menjalankan sistem Operasi FreeBSD diatas Linux dan sebagainya.

1.14.1 Vmware Workstation

VMware Workstation adalah rangkaian produk hypervisor desktop yang memungkinkan pengguna menjalankan mesin virtual, container, dan cluster Kubernetes. VMware Workstation menggunakan fitur khusus dalam CPU x86 64-bit modern untuk membuat mesin virtual yang sepenuhnya terisolasi dan aman yang merangkum sistem operasi dan aplikasinya. Lapisan virtualisasi VMware memetakan sumber daya perangkat keras fisik ke sumber daya virtual mesin virtual, sehingga setiap mesin virtual memiliki CPU, memori, disk, dan perangkat I/O sendiri, serta setara lengkap dengan mesin x86 standar. VMware Workstation diinstal pada sistem operasi host dan menyediakan dukungan perangkat keras yang ekstensif dengan mewarisi dukungan perangkat dari host.

Gambar 2. 18 Logo Vmware Workstation

1.15 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 dibagikan.

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.

1.15.1 Windows

Microsoft windows adalah salah satu sistem operasi. Sistem operasi windows telah berkembang dari MS-DOS, sistem operasi yang berbasis teks dan

command line. Windows pertama yang menggunakan sistem GUI adalah Windows Graphic Encirontment 1.0 yang dikenal dengan Windows 1.0 dikenalkan pertama kali pada 10 novembar 1983. Windows 1.0 merupakan perangkat lunak 16-bit yang berjalan di atas MS-DOS (dan beberapa varian dari MS-DOS), sehingga ia tidak dapat berjalan tanpa adanya sistem operasi DOS. Berikut adalah logo sistem operasi windows dapat dilihat pada gambar 2.18.

Gambar 2. 19 Logo Sistem Operasi Windows

1.15.2 Linux

Linux adalah varian dari sistem operasi Unix. Linux dikembangkan oleh Linus Torvlads pada tahun 1990, yang berkeinginan memiliki sistem operasi sendiri untuk komputernya, seolah program komputer biasa. Berikut adalah logo sistem operasi linux dapat dilihat pada gambar 2.19.

Gambar 2. 20 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.

1.15.2.1 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. Berikut adalah logo sistem operasi Ubuntu Linux dapat dilihat pada gambar 2.20

Gambar 2. 21 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.

1.15.2.2 Kali Linux

Kali linux adalah salah satu distribusi dari sistem operasi linux untuk melakukan penetration testing dan audit keamanan. Kali linux pengembangan dari BackTrack linux secara sempurna. Semua infrastruktur baru telah dimasukan kedalam satu tempat, tools, dan lainnya.Kali linux dirilis pada tanggal 13 maret

2013, kali linux memiliki dasar dari debian dan FHS-compliant filesystem. Berikut adalah logo sistem operasi Ubuntu Linux dapat dilihat pada gambar 2.21.

Gambar 2. 22 Sistem Operasi Kali Linux

Kali linux memiliki lebih banyak keuntungan dari pendahulunya, karena kali linux hadir dengan lebih banyak tools yang telah di-update, tools dengan standar repositori debian dan disingkronisasi empat kali dalam sehari. Yang artinya pengguna dapatkan update paket dan security fixes terbaru.