BAB II
KAJIAN PUSTAKA

2.1 Teori Dasar

2.1.1 Jaringan Komputer

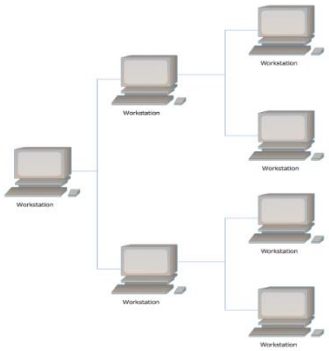
Jaringan komputer adalah *interkoneksi* antara dua komputer *autonomous* atau lebih, yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*) (Wongkar, Sinsuw, & Najoan, 2015). Dalam defenisi *networking autonomous* dijelaskan sebagai jaringan yang independent dengan manajemen sistem sendiri, memiliki topologi jaringan, *hardware* dan *software* sendiri, dan dikoneksikan dengan jaringan *autonomous* yang lain. Dua unit komputer dikatakan terkoneksi apabila keduanya bisa saling bertukar data/informasi, berbagi *resource* yang dimiliki, seperti *file*, *printer*, *hardisk*, *cd-rom*, *flashdisk*, *camera* dll).

Dalam membangun jaringan komputer dibutuhkan beberapa komponen jaringan, komponen jaringan adalah suatu alat yang digunakana dalam membangun suatu jaringan komputer.

Berdasarkan topologi nya secara umum jaringan komputer dibagi menjadi 5 yaitu:

1. *Topologi Tree*

Topologi Tree menggabungkan beberapa *topologi star* kedalam sebuah *bus.* Dalam bentuk sederhana, hanya *hub* yang dikoneksikan secara langsung ke pohon *bus* dan setiap *hub* berfungsi sebagai akar dari kumpulan *node.* Dalam hal ini *node* tersebut dapat juga berupa *hub* ataupun perangkat-perangkat lainnya (Prama Wira Ginta, Galih Putra Kusuma, 2013).



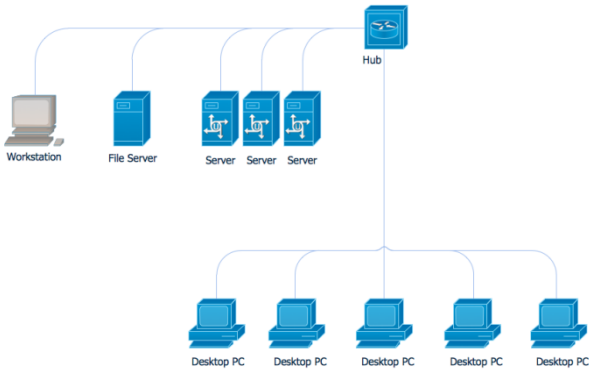
Gambar 2.1 *Topologi Three*
(Sumber : Peneliti)

2. *Topologi BUS*

Topologi bus menggunakan sebuah kabel untuk menghubungkan keseluruhan jaringan. Setiap *node* yang ada pada jaringan akan dikoneksikan menggunakan sebuah konektor pada kabel tersebut dan setiap sinyal/pesan akan dikirimkan melalui kabel tersebut.

Sebuah *node* yang ingin melakukan komunikasi dengan *node* lainnya pada jaringan akan mengirimkan pesan secara *broadcast* melalui kabel yang kemudian akan diterima oleh semua *node* yang ada pada jaringan tersebut. Jika *IP address* dan *Mac address* dari tujuan pengiriman pesan sama dengan *node*, makan pesan

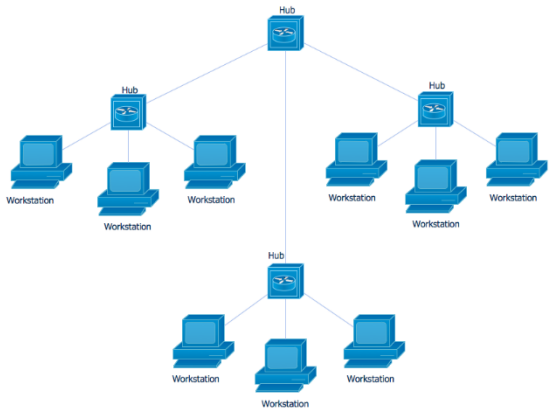
akan diproses oleh *node* tersebut. Tetapi jika tidak cocok, maka *node* akan mengabaikan dan tidak memproses pesan tersebut (Prama Wira Ginta, Galih Putra Kusuma, 2013).



Gambar 2.2 *Topologi BUS*
(Sumber : Peneliti)

3. *Topologi Star*

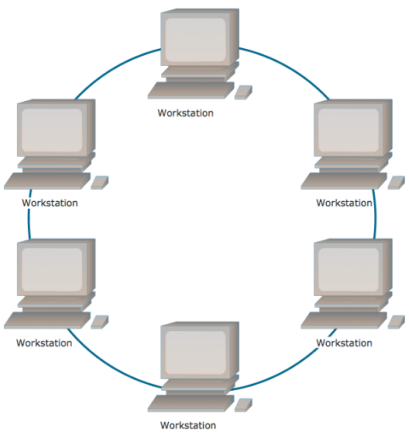
Pada *topologi Star* setiap *node* terkoneksi ke sebuah titik pusat koneksi yang biasanya disebut dengan *hub* (dapat berupa *hub, switch* atau *router*). Berbeda dengan *topologi bus, topologi star* memungkinkan setiap *node* pada jaringan untuk memiliki koneksi *point to point* ke *hub* pusat. Semua lalu lintas yang dikirimkan ke jaringan akan melewati hub tersebut dan sekaligus akan menjadi penguat dari pesan agar dapat dikirimkan ke *node* lain (Prama Wira Ginta, Galih Putra Kusuma, 2013).



Gambar 2.3 *Topologi Star*
(Sumber : Peneliti)

4. *Topologi Ring*

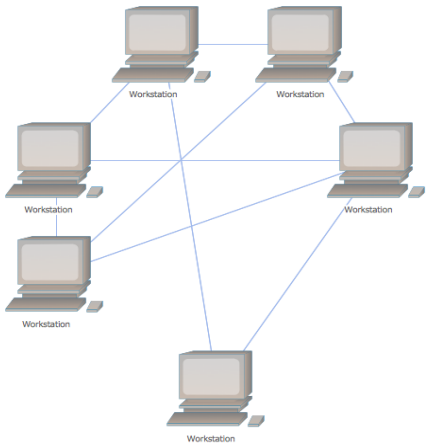
Di dalam *topologi Ring* semua *workstation* dan *server* dihubungkan sehingga terbentuk suatu pola lingkaran atau cincin. Tiap *workstation* ataupun *server* akan menerima dan melewatkan informasi dari satu komputer ke komputer lain, bila alamat-alamat yang dimaksud sesuai maka informasi diterima dan bila tidak informasi akan dilewatkan (Prama Wira Ginta, Galih Putra Kusuma, 2013).



Gambar 2.4 *Topologi Ring*
(Sumber : Peneliti)

5. *Topologi Mesh*

Topologi Mesh menggunakan konsep rute yang berbeda dari topologi lainnya. Pesan yang dikirimkan pada topologi ini bisa melewati beberapa jalur yang mungkin dari sumber sampai tujuan. Topologi ini juga digunakan pada *Wide Area Network* (WAN) yang kita kenal sebagai internet (Prama Wira Ginta, Galih Putra Kusuma, 2013).



Gambar 2.5 *Topologi Mesh*
(Sumber : Peneliti)

Sedangkan berdasarkan cakupan area, jaringan komputer dibagi menjadi 4 yaitu :

1. *LAN (Local Area Network)* yatu jaringan lokal di dalam gedung perkantoran ataupun kampus dll.

2. *MAN (Metropolitan Area Network)* jaringan ini menghubungkan beberapa jaringan LAN yang berada dalam gedung yang berbeda tapi masih dalam satu kota yang sama.

3. *WAN (Wide Area Network)* mencakup area jaringan yang sangat luas, bisa mencakup 1 negara bahkan benua.

4. *Internet (Interconnected Network)* merupaka gabungan dari semua jaringan *LAN, MAN, dan WAN*.

2.1.2 Standar jaringan komputer

Standar adalah suatu hal yang penting dalam penciptaan dan pemeliharaan sebuah kompetisi pasar daripada manufaktur perangkat komunikasi dan menjadi jaminan *interoperability* data dalam proses komunikasi. Standar komunikasi data dapat dikategorikan dalam 2 kategori yakni kategori *de facto* (konvensi) dan *de jure* (secara hukum atau *regulasi*) (Nethanel, Junior, & Harianto, 2009).

Adapun penjelasan lain tentang standar adalah Standar, patokan, norma, ukuran yang berlaku secara umum. Standar adalah persetujuan terhadap format, prosedur, dan antar muka yang mengijinkan perancang *Hardware, software*, basis data dan fasilitas telekomunikasi untuk membuat produk-produk dan sistem yang mandiri atau independen satu terhadap lainnya dengan jaminan bahwa produk-produk tersebut akan saling kompatibel dengan produk atau sistem lain yang merujuk pada standar yang sama. Standar merupakan elemen tunggal yang paling penting dalam mencapai integrasi informasi perusahaan dan sumber daya komunikasi. Proses penetapan standar, karena melibatkan negoisasi di antara provider IT dan pemakai, persetujuan formal dan rumusan-rumusan, sertifikasi

dan prosedur pengujian, serta dokumentasi dan publikasi, bisa berjalan dalam waktu dan proses yang cukup panjang. Bahkan untuk menyelesaikan penetapan sebuah standard menerapkannya pada produk-produk komersial dapat memakan waktu lebih dari 1 dekade.Berikut beberapa organsasi Pembuat Standar Jaringan Komputer :

1. IEEE

Menurut (Nethanel et al., 2009) IEEE adalah organisasi nirlaba internasional, yang merupakan asosiasi profesional utama untuk peningkatan teknologi. Sebelumnya, IEEE merupakan kepanjangan dari *Institute of Electrical and Electronics Engineers*. Namun berkembangnya cakupan bidang ilmu dan aplikasi yang diperdalam organisasi ini membuat nama-nama kelektroan dianggap tidak relevan lagi, sehingga IEEE tidak dianggap memiliki kepanjangan lagi, selain sebuah nama yang dieja sebagai *Eye-triple-E*.

Di samping *society*, IEEE memiliki badan standard (Standard Association, IEEE-SA). IEEE-SA memiliki wibawa cukup besar untuk bisa mempersatukan substandard industri membentuk standardisasi internasional yang diakui seluruh industri.

Beberapa standar IEEE yaitu :

1. IEEE 802.3 — *Ethernet* akses LAN.
2. IEEE 802.11 — *Wifi*, akses *wireless* LAN.
3. IEEE 802.16 — *WiMAX*, akses *wireless* MAN.

Sedikit mengenail *WiMAX* : *WiMAX* (*Worldwide Interoperability for Microwave Access*) adalah sebuah tanda sertifikasi untuk produk-produk yang lulus tes cocok dan sesuai dengan standar IEEE 802.16. *WiMAX* merupakan teknologi nirkabel yang menyediakan hubungan jalur lebar dalam jarak jauh. *WiMAX* merupakan teknologi broadband yang memiliki kecepatan akses yang tinggi dan jangkauan yang luas. *WiMAX* merupakan evolusi dari teknologi BWA sebelumnya dengan fitur-fitur yang lebih menarik. Disamping kecepatan data yang tinggi mampu diberikan, *WiMAX* juga membawa isu open standar. Dalam arti komunikasi perangkat *WiMAX* diantara beberapa vendor yang berbeda tetap dapat dilakukan. Dengan kecepatan data yang besar (sampai 70 MBps).

2. ANSI

Menurut (Nethanel et al., 2009) ANSI (*American National Standards Institute)* adalah sebuah kelompok yang mendefinisikan standar Amerika Serikat untuk industri pemrosesan informasi. ANSI berpartisipasi dalam mendefinisikan standar protokol jaringan dan merepresentasikan Amerika Serikat dalam hubungannya dengan badan-badan penentu standar International lain, misalnya ISO Ansi adalah organisasi sukarela yang terdiri atas anggota dari sektor usaha, pemerintah, dan lain-lain yang mengkoordinasikan aktivitas yang berhubungan dengan standar, dan memperkuat posisi Amerika Serikat dalam organisasi standar nasional. ANSI membantu dengan komunikasi dan jaringan (selain banyak hal lainnya). ANSI adalah anggota IEC dan ISO. ANSI adalah lembaga amerika yang mengeluarkan standard ASCII (*American Standard Code for Information Interchange*).ASCII *(American Standard Code for Information Interchange)*

merupakan suatu standar internasional dalam kode huruf dan simbol seperti Hex dan Unicode tetapi ASCII lebih bersifat universal, contohnya 124 adalah untuk karakter "|". Ia selalu digunakan oleh komputer dan alat komunikasi lain untuk menunjukkan teks. Kode ASCII sebenarnya memiliki komposisi bilangan biner sebanyak 8 bit. Dimulai dari 00000000 hingga 11111111. Total kombinasi yang dihasilkan sebanyak 256, dimulai dari kode 0 hingga 255 dalam sistem bilangan Desimal. *SQL* adalah standar ANSI (American National Standards Institute) bahasa pemrograman untuk mengakses dan memanipulasi database. Statemen *SQL* digunakan untuk menerima, mengubah dan menghapus data. *SQL* bekerja dengan berbagai sistem database antara lain MS Access, DB2, Informix, *MS SQL Server, Oracle, Sybase,* dll. Sesuai kegunaan dan perkembangannya, *SQL* memiliki beberapa versi, tetapi agar tidak terjadi kekeliruan dibuat standar oleh ANSI, mereka harus memiliki *keywords* utama yang dipakai secara umum yaitu (*SELECT, UPDATE, DELETE, INSERT, WHERE*, dan sebagainya). ANSI C adalah standar bahasa C pertama.

3. ISO

Menurut (Nethanel et al., 2009) Organisasi Internasional untuk Standardisasi, *International Organization for Standardization (ISO)* adalah badan penetap standar internasional yang terdiri dari wakil-wakil dari badan standar nasional setiap negara. Pada awalnya, singkatan dari nama lembaga tersebut adalah IOS, bukan ISO. Tetapi sekarang lebih sering memakai singkatan ISO, karena dalam bahasa yunani sos berarti sama (equal). Penggunaan ini dapat dilihat

pada kata isometrik atau isonomi. Didirikan pada 23 February 1947 ISO menetapkan standar-standar industrial dan komersial dunia. ISO, yang merupakan lembaga nirlaba internasional, pada awalnya dibentuk untuk membuat dan memperkenalkan standardisasi internasional untuk apa saja.Dalam menetapkan suatu standar tersebut mereka mengundang wakil anggotanya dari 130 negara untuk duduk dalam Komite Teknis (TC), Sub Komite (SC) dan Kelompok Kerja (WG). Meski ISO adalah organisasi nonpemerintah, kemampuannya untuk menetapkan standar yang sering menjadi hukum melalui persetujuan atau standar nasional membuatnya lebih berpengaruh daripada kebanyakan organisasi non-pemerintah lainnya, dan dalam prakteknya ISO menjadi konsorsium dengan hubungan yang kuat dengan pihak-pihak pemerintah. Peserta ISO termasuk satu badan standar nasional dari setiap negara dan perusahaan-perusahaan besar. ISO bekerja sama dengan Komisi Elektroteknik Internasional (IEC) yang bertanggung jawab terhadap standardisasi peralatan elektronik. Penerapan ISO di suatu perusahaan berguna untuk:

1. Meningkatkan citra perusahaan
2. Meningkatkan kinerja lingkungan perusahaan
3. Meningkatkan efisiensi kegiatan
4. Memperbaiki manajemen organisasi dengan menerapkan perencanaan, pelaksanaan, pengukuran dan tindakan perbaikan (plan, do, check, act)
5. Meningkatkan penataan terhadap ketentuan peraturan perundang-undangan dalam hal pengelolaan lingkungan
6. Mengurangi resiko usaha

7. Meningkatkan daya saing
8. Meningkatkan komunikasi internal dan hubungan baik dengan berbagai pihak yang berkepentingan
9. Mendapat kepercayaan dari konsumen/mitra kerja/pemodal

Contoh : Standarisasi Protokol (ISO 7498) ISO *(International Standard Organization)* mengajukan struktur dan fungsi protocol komunikasi data. Model tersebut dikenal sebagai OSI *(Open System Interconnection) Reference Model*. Terdiri atas 7 *layer* (lapisan) yang mendefinisikan fungsi. Untuk tiap layernya dapat terdiri atas sejumlah protocol yang berbeda, masing-masing menyediakan pelayanan yang sesuai dengan fungsi layer tersebut.

4. IETF

Menurut (Nethanel et al., 2009) IETF adalah ebuah organisasi yang berwenang dan bertanggung jawab dalam mengatur dan menetapkan protocol-protocol standard yang digunakan di internet. *Internet Engineering Task Force* (disingkat IETF), merupakan sebuah organisasi yang menjaring banyak pihak (baik itu individual ataupun organisasional) yang tertarik dalam pengembangan jaringan komputer dan Internet. Organisasi ini diatur oleh IESG *(Internet Engineering Steering Group),* dan diberi tugas untuk mempelajari masalah-masalah teknik yang terjadi dalam jaringan komputer dan Internet, dan kemudian mengusulkan solusi dari masalah tersebut kepada IAB *(Internet Architecture Board*). Pekerjaan IETF dilakukan oleh banyak kelompok kerja (disebut sebagai *Working Groups*) yang berkonsentrasi di satu bagian topik saja, seperti halnya

keamanan, routing, dan lainnya. IETF merupakan pihak yang mempublikasikan spesifikasi yang membuat standar protokol TCP/IP. Kebijakan protokol QoS *(Quality of Service)* yang diusulkan sebagai standar IETF untuk mengkomunikasikan informasi kebijakan QoS dalam jaringan.

2.1.3 Jenis Jaringan Komputer

Suatu jaringan komputer umumnya terdiri dari L*ocal Area Network* (LAN), *Metropolitan Area Network* (MAN), *WideArea Network* (WAN).

Berikut 3 jenis jaringan tersebut :

1. *Local Area Network* (LAN)

Menurut (Nethanel et al., 2009) LAN adalah jaringan yang dibatasi oleh area yang relative kecil, umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran di sebuah gedung, atau sebuah sekolah, dan biasanya tidak jauh dari sekitar 1 km persegi.

2. *Metropolitan Area Network* (MAN)

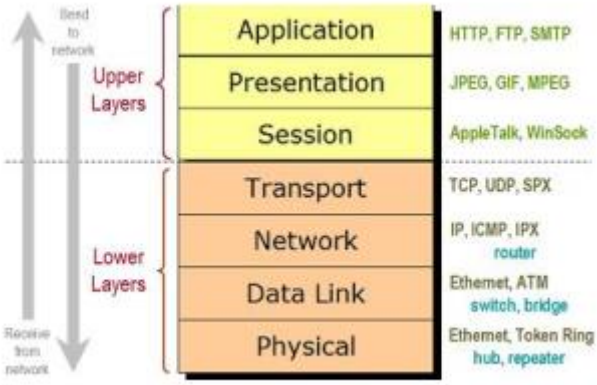
Menurut (Nethanel et al., 2009) MAN biasanya meliputi area yang lebih besar dari LAN, misalnya antar wilayah dalam satu propinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu jaringan Bank dimana beberapa kantor cabang sebuah Bank di dalam sebuah kota besar dihubungkan antara satu dengan lainnya.

3. *Wide Area Network* (WAN)

Menurut (Nethanel et al., 2009) WAN adalah jaringan yang lingkupnya biasanya sudah menggunakan sarana Satelit ataupun kabel bawah laut sebagai contoh keseluruhan jaringan BANK BNI yang ada di Indonesia ataupun yang ada di Negara-negara lain.

2.1.4 Model OSI Layer

Menurut (Sri Supatmi, Taufiq Nuzwir Nizar, 2014) Standar yang paling populer untuk menggambarkan arsitektur jaringan adalah model referensi *Open System Interconnect* (OSI) yang dikembangkan oleh *International Organization for Standarization* (ISO) pada tahun 1977 dan diperkenalkan pada tahun 1984. Pada model referensi OSI terdapat 7 buah lapisan yang setiap lapis-nya mengilustrasikan fungsi – fungsi jaringan. Pembagian fungsi – fungsi jaringan ini antara lain:



Gambar 2.6 OSI Layer
(Sumber : Aprianti Putri Sujana, 2014)

1. Lapisan ke-1 – *Physical*

Menurut (Sri Supatmi, Taufiq Nuzwir Nizar, 2014) Lapisan ini bertugas menangani transmisi data dalam bentuk *bit* melalui jalur komunikasi. Lapisan ini menjamin transmisi data berjalan dengan baik dengan cara mengatur karakteristik tinggi tegangan, periode perubahan tegangan, lebar jalur komunikasi, jarak maksimum komunikasi dan koneksi

2. Lapisan ke-2 – *Data Link*

Menurut (Sri Supatmi, Taufiq Nuzwir Nizar, 2014) Lapisan ini berfungsi mengubah paket – paket data menjadi bentuk *frame*, menghasilkan alamat fisik, pesan – pesan kesalahan, pemesanan pengiriman data. Lapisan Data Link mengupayakan agar lapisan Physical dapat bekerja dengan baik dengan menyediakan layanan untuk mengaktifkan, mempertahankan dan menonaktifkan hubungan.

3. Lapisan ke-3 – *Network*

Menurut (Sri Supatmi, Taufiq Nuzwir Nizar, 2014) Lapisan ini menyediakan transfer informasi di antara ujung sistem melewati beberapa jaringan komunikasi berurutan. Lapisan ini melakukan pemilihan jalur terbaik dalam komunikasi jaringan yang terpisah secara *geografis*.

4. Lapisan ke-4 – *Transport*

Menurut (Sri Supatmi, Taufiq Nuzwir Nizar, 2014) Lapisan ini berfungsi sebagai pemecah informasi menjadi paket – paket data yang akan dikirim dan menyusun kembali paket – paket data menjadi sebuah informasi yang dapat diterima. Dua protokol umum pada lapisan ini adalah *Transfer Control Protocol* (TCP) yang berorientasi koneksi dan *User Datagram Protocol* (UDP) yang tidak berorientasi koneksi.

5. Lapisan ke-5 – *Session*

Menurut (Sri Supatmi, Taufiq Nuzwir Nizar, 2014) Lapisan ini berfungsi untuk menyelenggarakan, mengatur dan memutuskan sesi komunikasi. Lapisan Session menyediakan layanan kepada lapisan Presentation dan juga mensinkronisasi dialog di antara dua computer lapisan Presentation dan mengatur pertukaran data.

6. Lapisan ke-6 – *Presentation*

Menurut (Sri Supatmi, Taufiq Nuzwir Nizar, 2014) Lapisan ini menentukan format data yang dipindahkan di antara aplikasi dan mengelola informasi yang disediakan oleh lapisan *Application* supaya informasi yang dikirimkan dapat dibaca oleh lapisan *Application* pada sistem lain. Lapisan ini menyediakan layanan berupa transformasi format data, enkripsi dan kompresi.

7. Lapisan ke-7 – *Application*

Menurut (Sri Supatmi, Taufiq Nuzwir Nizar, 2014) Lapisan yang paling dekat dengan pengguna dan memiliki fungsi untuk menyediakan sebuah layanan jaringan kepada pengguna aplikasi, berisi protocol - protokol yang umum digunakan oleh pengguna, lapisan ini berbeda dengan lapisan lainnya yang dapat menyediakan layanan kepada lapisan lain.

Contoh : Simple *Mail Transfer Protocol* (SMTP), *Hypertext Transfer Protocol* (HTTP) dan *File Transfer Protocol* (FTP).

2.2 Teori Khusus

2.2.1 *Intrusion Detection System* (IDS)

Menurut (A.Masse, Nurul Hidayat, & Badrianto, 2015) *Intrusion Detection System* (*IDS)* adalah usaha mengidentifikasi adanya penyusup yang memasuki sistem tanpa otorisasi (misal *cracker*) atau seorang *user* yang sah tetapi menyalahgunakan (*abuse*) sumberdaya sistem.

Dalam melakukan tugasnya *Intrusion Detection System* (*IDS)* berada pada lapisan jaringan OSI *(Open System Interconnection)* model yang terdapat pada lapisan ketiga yaitu pada lapisan network dan sensor jaringan pasif yang secara khusus diposisikan pada choke point pada jaringan metode dari lapisan OSI.

A. Fungsi *Intrusion Detection System* (*IDS)*

Beberapa alasan untuk memperoleh dan menggunakan *Intrusion Detection System* (*IDS)* (A.Masse et al., 2015) diantaranya adalah:

1. Mencegah resiko keamanan yang terus meningkat, karena banyak ditemukan kegiatan ilegal yang diperbuat oleh orang-orang yang tidak bertanggung jawab dan hukuman yang diberikan atas kegiatan tersebut.
2. Mendeteksi serangan dan pelanggaran keamanan sistem jaringan yang tidak bisa dicegah oleh sistem, seperti *firewall*. Sehingga banyak menyebabkan adanya begitu banyak lubang keamanan, seperti:
    a) Banyak dari legacy sistem, sistem operasi tidak *patch* maupun *update*.
    b) *Patch* tidak diperhatikan dengan baik, sehingga menimbulkan masalah baru dalam hal keamanan.
    c) *User* yang tidak memahami sistem, sehingga jaringan dan protokol yang mereka gunakan memiliki lubang keamana.
    d) *User* dan *administrator* membuat kesalahan dalm konfigurasi dan dalam menggunakan sistem.
3. Mendeteksi serangan awal. Penyerang akan menyerang suatu siste yang biasanya melakukan langkah-langkah awal yang mudah diketahui yaitu dengan melakukan penyelidikan atau menguji sistem jaringan yang akan menjadi target, untuk mendapatkan titik- titik dimana mereka akan masuk.
4. Mengamankan file yang keluar dari jaringan.

5. Sebagai pengendali untuk rancangan keamanan dan administrator, terutama bagi perusahaan yang besat
6. Menyediakan informasi yang akurat terhadap ganguan secara langsung, meningkatkan diagnosis, recovery, dan mengoreksi faktor-faktor penyebab serangan.

B. Peran *Intrusion Detection System* (*IDS)*

Menurut (A.Masse et al., 2015) IDS (*Intrusion detection system*) juga memiliki peran penting untuk mendapatkan arsitektur defence-in-depth (pertahanan yang mendalam) dengan melindungi akses jaringan internal, sebagai tambahan dari parameter defence. Hal-hal yang dilakukan *Intrusion Detection System* (*IDS)* pada jaringan internal adalah sebagai berikut:

a) Memonitor akses *database* : ketika mempetimbangkan pemilihan kandidat untuk penyimpanan data, suatu perusahaan akan memilih database sebagai solusi untuk menyimpan data-data yang berharga.
b) Melindungi *e-mail server* : *Intrusion Detection System* (*IDS)* juga berfungsi untuk mendeteksi *virus e-mail* seperti *QAZ, Worm, NAVIDAD Worm*, dan versi terbaru dari *ExploreZip*.
c) Memonitor *policy security* : jika ada pelanggaran terhadap *policy security* maka IDS (*intrusion detection system*) akan memberitahu bahwa telah terjadi sesuatu yang tidak sesuai dengan aturan yang ada.

C. Tipe *Intrusion Detection System* (*IDS)*

Menurut (A.Masse et al., 2015) Pada dasarnya terdapat tiga macam *Intrusion Detection System* (*IDS)*, yaitu:

1. *Network based Intrusion Detection System* (NIDS) : Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. NIDS umumnya terletak di dalam segmen jaringan penting di mana server berada atau terdapat pada "pintu masuk" jaringan. Kelemahan NIDS adalah bahwa NIDS agak rumit diimplementasikan dalam sebuah jaringan yang menggunakan switch Ethernet, meskipun beberapa *vendor switch Ethernet* sekarang telah menerapkan fungsi IDS di dalam *switch* buatannya untuk memonitor port atau koneksi.
2. *Host based Intrusion Detection System (HIDS)*: Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya *firewall, web server*, atau *server* yang terkoneksi ke *Internet*.
3. *Distributed Intrusion Detection System (DIDS)* : sekumpulan sensor IDS yang saling terhubung satu sama lain dan berfungsi sebagai remotet sensor (sensor jarak jauh) yang memberikann pelaporanpada manajemen sistem terpusat.

Menurut (A.Masse et al., 2015) Pembagian jenis-jenis *Intrusion Detection System* (*IDS)* yang ada saat ini didasarkan pada beberapa terminologi di antaranya:

1. Arsitektur sistem

Dibedakan menurut komponen fungsional *Intrusion Detection System* (*IDS)*, bagaimana diatur satu sama lainnya.

a) *Host-Target Co-Location* : IDS dijalankan pada sistem yang akan dilindungi. Kelemahan sistem ini adalah jika penyusup berhasil memperoleh akses ke sistem maka penyusup dapat dengan mudah mematikan IDS tipe ini.
b) *Host-Target Separation* : *Intrusion Detection System* (*IDS)* diletakkan pada komputer yang berbeda dengan komputer yang akan dilindungi.

2. Tujuan Sistem

Ada dua bagian tujuan *Intrusion Detection System* (IDS), diantaranya adalah:

a) Tanggung jawab : adalah kemampuan untuk menghubungkan suatu kegiatan dan bertanggung jawab terhadap semua yang terjadi, diantaranya adalah serangan.
b) Respons : suatu kemampuan untuk mengendalikan aktivitas yang merugikan dalam suatu sistem komputer.

3. Strategi Pengendalian

Pada tahap ini *Intrusion Detection System* (*IDS)* dibedakan berdasarkan yang dikendalikan, baik input maupun outputnya. Jenis-jenis IDS menurut terminologi ini adalah:

a) Terpusat : seluruh kendalai pada *Intrusion Detection System* (*IDS)*, baik monitoring, deteksi, dan pelaporannya dikendalikan secara terpusat.
b) Terdistribusi Parsial : monitoring dan deteksi dikendalikan dari node lokal dengan hierarki pelaporan pada satu atau beberapa pusat lokasi.
c) Terdistribusi Total : monitoring dan deteksi menggunakan pendekatan berbasis agen, dimana keputusan respons dibuat pada kode analisis.

4. Waktu

Waktu dalam hal ini berarti waktu antara kejadian, baik monitoring atau analisis. Jenisnya adalah:

a) *Interval-Based (Batch Mode)* : informasi dikumpulka terlebih dahulu, kemudian dievaluasi menurut interval waktu yang telah ditemtukan.
b) *Realtime (Continues)* : *Intrusion Detection System* (*IDS)* memperoleh data terus menerus dan dapat mengetahui bahwa penyerangan sedang terjadi sehingga secara cepat dapat melekukan respons terhadap penyerangan.

5. Sumber Informasi

Intrusion Detection System (*IDS)* dibedakan menurut sumber daya yang diperoleh. Jenis-jenis *Intrusion Detection System* (*IDS)* menurut terminologi ini di antaranya:

a) *Host-Based* : *Intrusion Detection System* (*IDS)* memperoleh informasi dari data yang dihasilkan oleh sistem pada sebuah komputer yang diamati. Biasanya informasi yang diperoleh berupa log yang dihasilkan dengan memonitor sistem file, event, dan keamanan pada Windows NT san syslog pada lingkungan sistem opersi UNIX.

b) *Network-Based* : *Intrusion Detection System* (*IDS)* memperoleh informasi dari paket-paket jaringan yang ada. Network-Based menggunakan raw packet yang ada pada jaringan sebagai sumber datanya, menggunakan network adapter yang bejalan pada mode prosmicuous sebagai alat untuk menangkap paket-paket yang akan di pantau.

Dari jenis-jenis *Intrusion Detection System* (*IDS)* tersebut, sistem *Intrusion Detection System* (*IDS)* yang digunakan adalah yang berbasis pada jaringan *(Network-Based)* untuk memantau paket-paket data yang berjalan didalam jaringan. Snort merupakan aplikasi yang dapat digunakan pada tingkat network, karena cara kerja snort hampir sama dengan alarm yaitu memberitahukan adanya penyusup yang akan masuk kejaringan.

D. Keuntungan dan Kekurangan *Intrusion Detection System* (*IDS)*

Berikut ini beberapa keuntungan dari penerapan *Intrusion Detection System* (*IDS)* pada sistem jaringan komputer :

1. Secara efektif mendeteksi aktifitas penyusupan, penyerangan atau tindak pelanggaran lainnya yang mengacam aset atau sumber daya sistem jaringan.
2. *Intrusion Detection System* (*IDS)* membuat *administrator* diinformasikan tentang status keamanan.
3. *Intrusion Detection System* (*IDS)* secara berkesinambungan mengamati *traffic* dari sistem jaringa komputer dan secara rinci menginformasikan setiap *event* yang berhubungan dengan aspek keamanan.
4. *Intrusion Detection System* (*IDS)* menyediakan informasi akurat terhadap gangguan secara langsung, meningkatkan diagnosis, pemulihan, mengoreksi sejumlah faktor penyebab intursi atau serangan.
5. Sejumlah file log yang berisi catatan aktifitas kinerja *Intrusion Detection System* (*IDS)* adalah bagian penting dari forensik komputer yang dapat digunakan sebagai sumber informasi untuk proses penelusuran aktivitas serangan yang terjadi, analisis dan audit kinerja sensor *Intrusion Detection System* (*IDS)* serta sebagai barang bukti untuk tindakan hukum.

Ada pula kekeurangan yang terdapat pada penerapan sensor *Intrusion Detection System* (*IDS)*, sebagai berikut :

1. Rentang waktu antara pengembangan teknik penyerangan atau intrusi dan pembuatan signature, memungkinkan penyerang untuk mengeksploitasi *Intrusion Detection System* (*IDS)* yang tidak mengenali jenis serangan

spesifik. Karena signature tidak dapat dibuat tanpa mempelajari traffic seranagan.

2. *False Negative* adalah serangan sesungguhnya yang tidak terdeteksi maka tidak ada peringatan atau notification mengenai peristiwa ini.
3. *False Positive* adalah kesalahan *Intrusion Detection System* (*IDS)* dalam mendeteksi traffic *network* normal sebagai suatu serangan. Jika terjadi dalam jumlah besar berkemungkinan menutupi kejadian intrusi sesungguhnya.

Intrusion Detection System (*IDS)* merupakan program atau aplikasi yang dapat mendeteksi adanya gangguan pada sistem kita. Pada saat ini ada beberapa *Intrusion Detection System* (*IDS)* yang umum digunakan pada jaringan, salah satunya adalah *SNORT*. Adapun tujuan dari *tools* ini diantaranya: mengawasi jika terjadi penetrasi kedalam sistem, mengawasi *traffic* yang terjadi pada jaringan, mendeteksi anomali terjadinya penyimpangan dari sistem yang normal atau tingkah laku user, mendeteksi signature dan membedakan pola antara *signature user* dengan *attacker*.

2.2.2 *Snort*

Menurut (Triandini, 2016) *Snort* merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisa paket yang melintasi jaringan secara langsung dan melakukan pencatatan ke dalam penyimpanan data serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan. Snort merupakan sebuah produk terbuka yang dikembangkan oleh *Marty Roesch* dan tersedia gratis di *www.snort.org*. *Snort* bisa digunakan pada sistem operasi *Linux*,

Windows, BSD, Solaris dan sistem operasi lainnya. *Snort* merupakan *Intrusion Detection System* (*IDS)* berbasis jaringan yang menggunakan metode deteksi *rule based*, menganalisis paket data apakah sesuai dengan jenis serangan yang sudah diketahui olehnya. *Snort* digunakan karena memiliki beberapa kelebihan berikut :

Mudah dalam konfigurasi dan penambahan aturan-aturan

1. Gratis
2. Dapat berjalan pada sistem operasi yang berbeda – beda
3. Pembaharuan pola serangan secara berkala

Menurut (Triandini, 2016) *Snort* dapat berjalan dalam tiga mode antara lain:

1. *Paket Sniffer*, melihat paket yang lewat di jaringan.
2. *Paket Logger*, mencatat semua paket yang lewat di jaringan untuk dianalisis.
3. *NIDS* mendeteksi serangan yang dilakukan melalui jaringan komputer dengan konfigurasi dari berbagai aturan yang akan membedakan sebuah paket normal dengan paket serangan.

Menurut (Triandini, 2016) *Snort* terdiri dari komponen – komponen yang mempunyai tugas dan fungsinya sendiri – sendiri yaitu:

1. *Packet capture library*

Packet capture library adalah sebuah perangkat lunak yang terpisah yang mengambil paket data dari NIC. Paket – paket data itu adalah paket data Lapisan Data Link (OSI model) yang biasanya disebut *frame* yang masih belum diproses.

Pada sistem *Linux* dan *UNIX*, *Snort* menggunakan *libpcap*, sedangkan pada *System Windows*, *Snort* menggunakan *winpcap*.

2. *Packet decoder*

Packet decoder mengambil *frame* lapisan 2 *(Data Link)* yang dikirimkan oleh packet capture library dan kemudian memecahnya. Pertama – tama komponen ini membaca kode sandi terhadap *frame* lapisan 2, kemudian paket lapisan 3 (*protokol IP*), lalu kemudian paket lapisan 4 (paket TCP atau UDP). Setelah proses selesai dilakukan, *Snort* mempunyai semua informasi masing – masing protokol untuk pemrosesan lebih lanjut.

3. *Preprocessor*

Preprocessor pada *Snort* memiliki beberapa fitur tambahan yang dapat dimatikan atau dinyalakan. *Preprocessor* bekerja pada paket yang sudah dibaca kode sandinya dan kemudian melakukan transformasi pada data itu supaya lebih mudah untuk diproses oleh *Snort*.

4. *Detection engine*

Komponen ini mengambil informasi dari packet decoder dan preprocessor yang kemudian memproses data itu pada lapisan *Transport* dan *Application*, membandingkan data yang terkandung dalam paket dengan aturan-aturan yang juga merupakan fitur tambahan dari komponen ini.

5. *Output*

Ketika *preprocessor* terpancing karena adanya data yang cocok dengan definisi jenis serangan, Snort kemudian menghasilkan peringatan dan kemudian melakukan pencatatan. Snort mendukung beberapa macam keluaran, seperti keluaran dalam format teks atau biner. Pencatatan juga bisa dilakukan ke dalam penyimpanan data ataupun syslog.

2.2.3 *Raspberry Pi*

Menurut (Kurniawan Dayat, 2016: 7) *Raspberry Pi* adalah sebuah perangkat komputer seukuran kartu kredit, benar-benar praktis dan harganya Rp.470.000. Sistem operasinya ditanam pada sebuah *SD Flash Card*, yang menjadikannya sangat mudah untuk diganti dan ditukar. Potensinya luar biasa, dari yang sudah maupun belum pernah dieksplorasi, tetapi telah diuji sebagai *multimedia player* dengan kemampuan *streaming*, sebagai perangkat *game machine, internet browsing* dan sebagai *mainboard* pengembangan *hardware*. Hal tersebut memungkinkan perangkat ini digunakan sebagai perangkat pendidikan bagi orang-orang dari segala usia dan tingkat keterampilan.

A. Spesifikasi Raspberry Pi 3

Tabel 2.1 Spesifikasi Raspberry Pi 3

Spesifikasi Raspberry Pi 3	
1.SoC	**Broadcom BCM2837**
2.CPU	**4× ARM Cortex-A53, 1.2GHz**
3.GPU	**Broadcom VideoCore IV**
4.RAM	**1GB LPDDR2 (900 MHz)**
5.Networking	**10/100 Ethernet, 2.4GHz 802.11n wireless**
6.Bluetooth	**Bluetooth 4.1 Classic, Bluetooth Low Energy**
7.GPIO	**40-pin header, populated**
8.Ports	**HDMI, 3.5mm analogue audio-video jack, 4× USB 2.0, Ethernet, Camera Serial Interface (CSI), Display Serial Interface (DSI)**
9.Storage	**microSD**

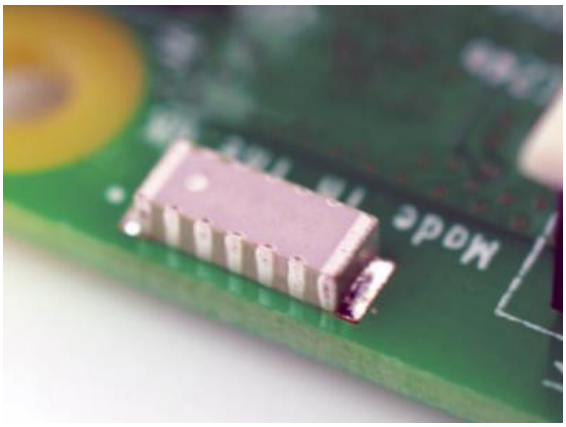
B. Radio Nirkabel

Bagian ini ukurannya sangat kecil, hanya bisa dilihat dengan menggunakan *mikroskop* atau kaca pembesar, *chip Broadcom* BCM43438 menyediakan LAN nirkabel standar 2,4GHz 802.11n, *Bluetooth* rendah daya, dan dukungan *Bluetooth* 4.1 klasik. Dengan apiknya dibenamkan dalam boardnya Raspi untuk tetap menjaga biaya seminim mungkin, dari pada menggunakan modul-modul umum yang mesti dibeli terpisah dan harganya cukup mahal, fitur dari komponen ini yang tidak digunakan hanyalah bagian penerima radio FM.

Gambar 2.7 Radio Nirkabel
(Sumber : Peneliti)

C. Antenna Radio/Wi-Fi

Kita tidak perlu menggunakan *antenna eksternal* pada Raspi 3. *Chip* radionya sudah terhubung dengan *chip* antenna ini yang disolder langsung ke board, untuk menjaga ukurannya tetap ramping dan minimum. Meskipun bentuknya kurang meyakinkan, tetapi antenna ini mestinya lebih dari cukup untuk bisa menangkap sinyal *Wi-Fi* dan *Bluetooth* meskipun terhalang dinding.



Gambar 2.8 Antena Radio
(Sumber : Peneliti)

D. SoC (System on Chip)

Dibuat khusus untuk *Raspberry Pi* 3 yang baru, *system-on-chip* (Soc) dari *Broadcom* BCM2837 dipersenjatai dengan *prosesor* berperforma tinggi ARM Cortex-A53 yang memiliki empat *core* berkecepatan 1.2GHz dengan cache *memory* Level 1 sebesar 32kB dan Level 2 512kB, sebuah *prosesor* grafis *VideoCore* IV, dan terhubung dengan modul *memory* 1GB LPDDR2 pada bagian belakang *board.*

Gambar 2.9 SoC
(Sumber : Peneliti)

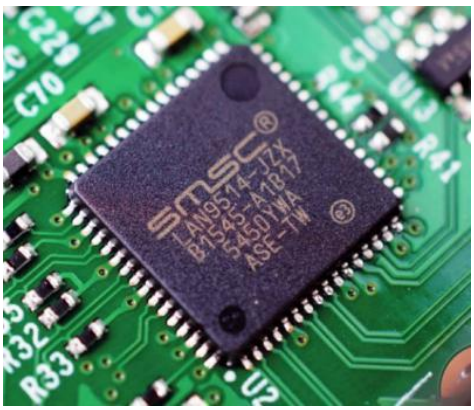
E. GPIO

Raspberry Pi 3 menggunakan *pin header general purpose input output (GPIO)* yang sama dengan versi sebelumnya yaitu Model B+ dan Model A+. Perangkat-perangkat sebelumnya yang menggunakan *GPIO* versi ini akan tetap bisa digunakan tanpa modifikasi apapun; perubahan yang ada pada versi ini hanyalah *switch* untuk UART yang terekspos pada pin *GPIO*, tapi penanganannya sekarang secara internal oleh sistem operasi.

Gambar 2.10 GPIO
(Sumber : Peneliti)

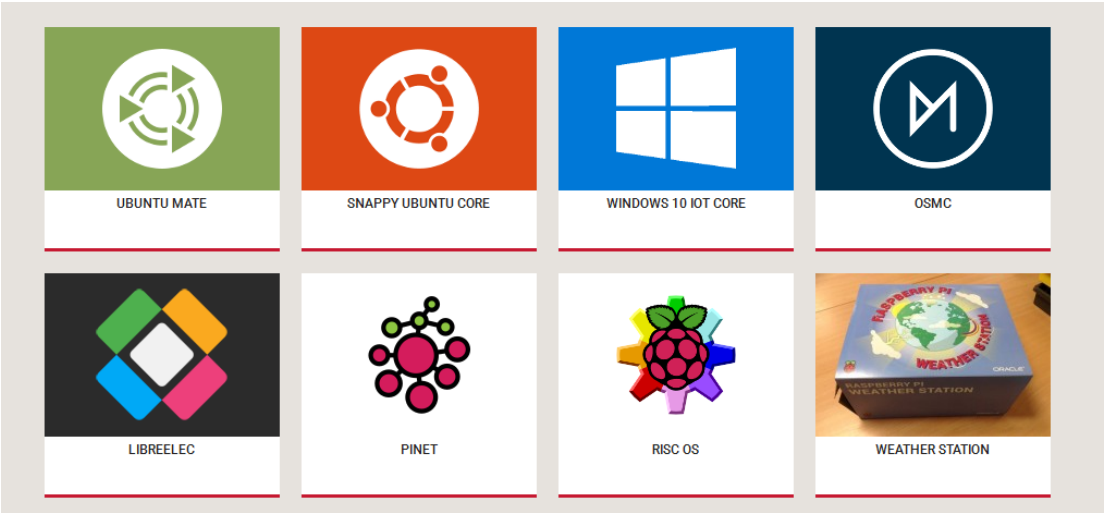
F. Chip USB

Raspberry Pi 3 menggunakan *chip* SMSC LAN9514 yang sama dengan pendahulunya, *Raspberry Pi* 2, mendukung konektifitas *Ethernet* dan USB empat channel pada board. Seperti sebelumnya, chip SMSC terhubung ke SoC melalui satu channel USB, beroperasi sebagai adaptor USB ke *Ethernet* dan USB hub.



Gambar 2.11 Chip
(Sumber : Peneliti)

G. Operating System



Gambar 2.12 *Operating System*
(Sumber : Peneliti)

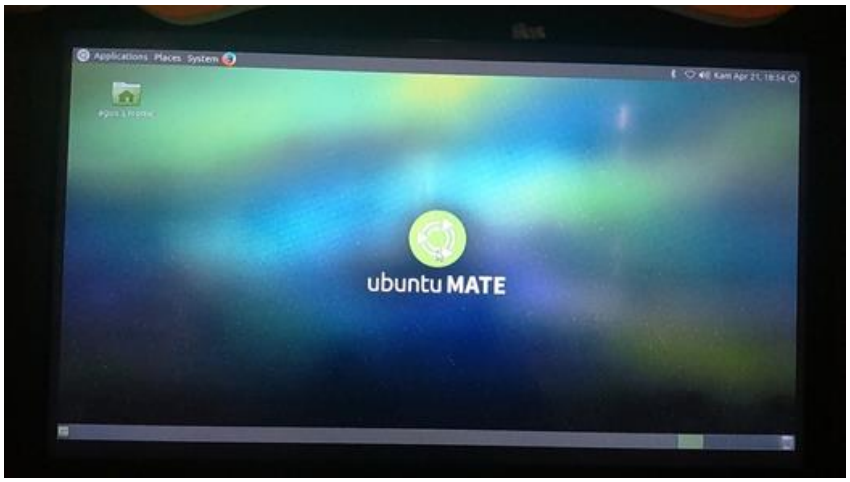
Raspberry Pi mempunya beberapa OS varian dari *Ubuntu MATE* , *Snappy Ubuntu Core* , *Win10 IOT*, dll. Pada pembuatan skripsi ini penulis menggunakan *OS Ubuntu Mate.*

2.3 Tools

2.3.1 *Ubuntu Mate*

Ubuntu MATE merupakan Remix sistem operasi *open source* yang diturunkan berdasarkan *Ubuntu* dan fitur utama MATE, yaitu *fork* dari lingkungan desktop GNOME klasik sebagai default dan antarmuka grafis tunggal. Banyak yang menklaim distro ini sebagai penjelmaan *MATE* yang paling indah yang pernah dibuat sampai saat ini! *Ubuntu MATE* ini tidak hanya berbasis kernel sistem operasi *Linux Ubuntu* dan dibangun di sekitar lingkungan *Desktop MATE*

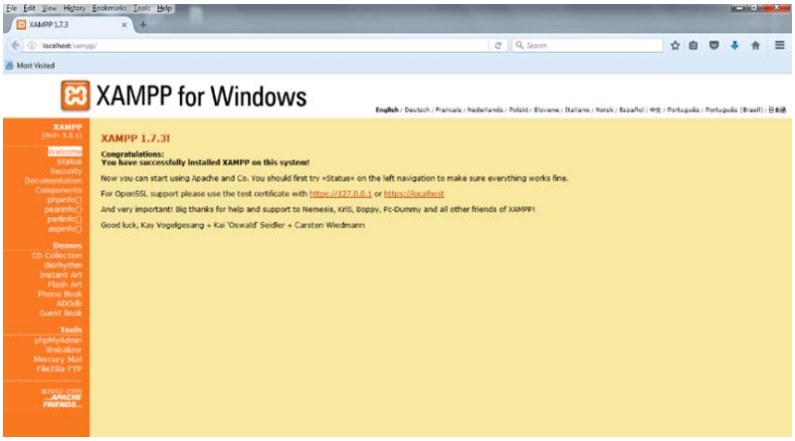
yang tampil sangat menarik, namun pada saat yang sama menjadi sistem yang sangat ringan dan sehat untuk “Komputer Usia Lanjut” atau Kompula**.**



Gambar 2.13 *Ubuntu Mate*
(Sumber : Peneliti)

2.3.2 *XAMPP*

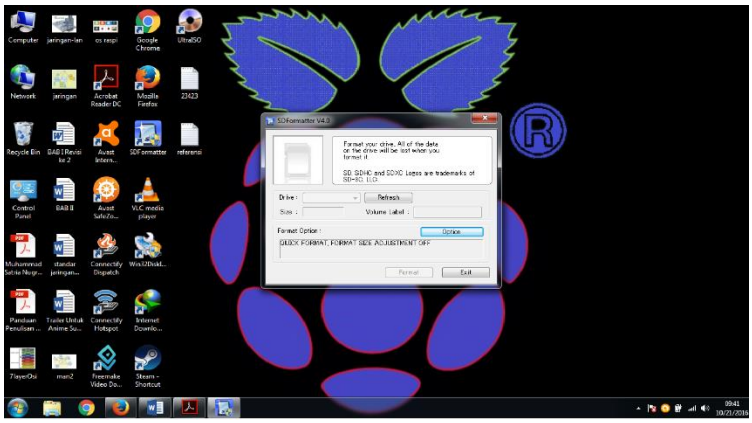
XAMPP adalah perangkat lunak dengan lisensi terbuka yang di dalamnya terdiri dari kompilasi beberapa perangkat lunak lainya. X adalah singkatan dari *cross platform* atau mendukung lintas *platform*, kemudian *AMPP* adalah singkatan dari nama beberapa perangkat lunak *Apache, My SQL,* dan penerjemah bahasa *PHP* dan *Pearl. Apache* digunakan sebagai *local webserver* , dan *MySQL* digunakan sebagai database managemen system (DBMS) (Henry Februariyanti, 2012).



Gambar 2.14 *XAMPP*
(Sumber : Peneliti)

2.3.3 *SD Formatter*

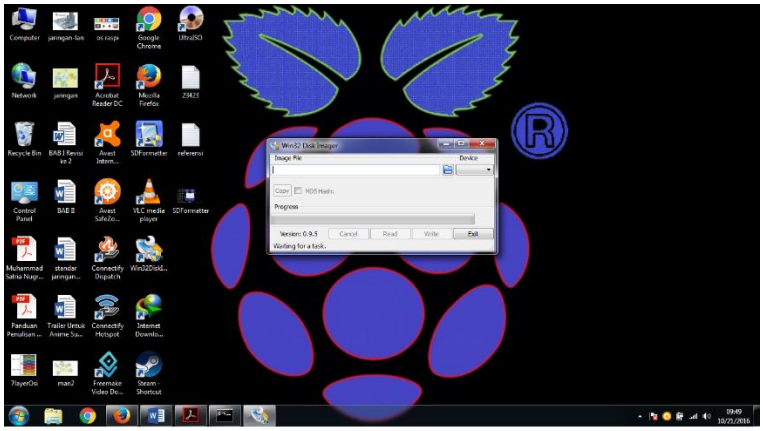
SD Card Formatter adalah sebuah program yang memyediakan akses mudah dan cepat ke semua kartu memori, seperti SD, SDHC dan SCCX. Program ini telah didesain agar Anda bisa membuang semua konten yang tersimpan di kartu SD Anda sekali jalan (Kurniawan, 2016: 15).



Gambar 2.15 SD Formatter
(Sumber : Peneliti)

2.3.4 *Win32 Disk Imager*

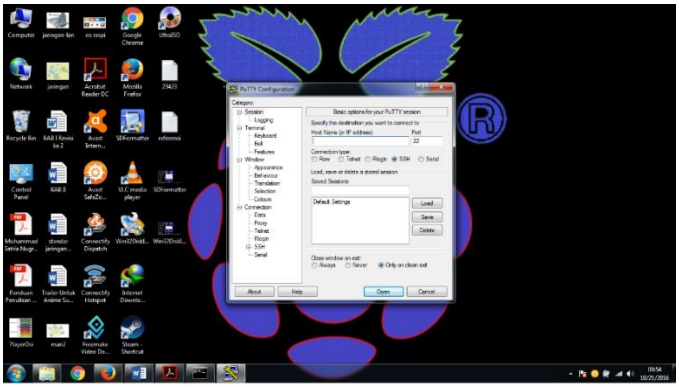
Win32 Disk Imager ini adalah aplikasi *open source* yang bisa dipakai untuk menulis berkas *image* CD atau DVD ke USB atau kartu SD, membuat *drive* berisi *disk* virtual (Kurniawan, 2016: 23).



Gambar 2.16 *Win32 Disk Imager*
(Sumber : Peneliti)

2.3.5 *Putty*

Putty adalah *Software SSH client* gratis untuk *Windows*, protokol SSH adalah cara aman untuk membuat sambungan aman ke sistem *remote*. Putty dapat meremote server yang menggunkan sistem operasi *linux*, sedangkan sistem operasi computer menggunakan *windows*. Dengan menggunakan *putty* dengan kata lain dapat melalukan komunikasi antara dua sistem (komputer dan *remote* server *vps*) (Kurniawan, 2016: 32).



Gambar 2.17 Putty
(Sumber : Peneliti)

2.4 Penelitian terdahulu

Beberapa penelitian yang telah dilakukan mengenai Implementasi *Intrusion detection system (IDS)* adalah :

(Budiman dan Iswahyudi, 2014) dalam penelitiannya yang berjudul Implementasi *Intrusion detection system (IDS)* menggunakan jejaring sosial sebagai media notifikasi menjelaskan bahwa setiap ada serangan yang datang dari luar menuju host atau server yang didalamnya terdapat IDS yang sedang berjalan, maka secara otomatis akan mendeteksi dan memberitahukan kepada administrator.

(Arif dan Huri. 2015) dalam penelitiannya yang berjudul Penerapan Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang menjelaskan bahwa IDS menggunakan *portsentry* cukup efektif dalam menangkal serangan *port scanning* (misalnya menggunakan *ipscan*, *nmap*, *LANspy*, *nessus* dan *superscan*) yang merupakan langkah awal dari serangan ke sistem jaringan. Hasil pengujian

penyerangan yang dilakukan oleh semua port scanner yang menjadi tool pengujian sistem dan informasi portsentry yang diintegrasikan dengan *syslog-notify*, memperlihatkan bahwa syslognotify berhasil menampilkan informasi portsentry yang ada di *file syslog* dalam bentuk *pop up windows* yang dapat muncul secara *real time* ketika *portsentry* menangkap aktifitas penyerangan yang dilakukan oleh alat serang dalam pengujian sistem IDS.*Syslog notify* membantu *administrator* dalam memonitoring jaringan dan menganalisa ketika terjadi serangan. *Syslog-notify* dalam menampilkan informasi *pop up window* dilakukan secara bertahap dengan melihat informasi yang ada di file *syslog* yang menjadi tempat informasi sistem komputer saat bekerja terutama *portsentry* dalam melakukan pendeteksian serangan *port scanning*

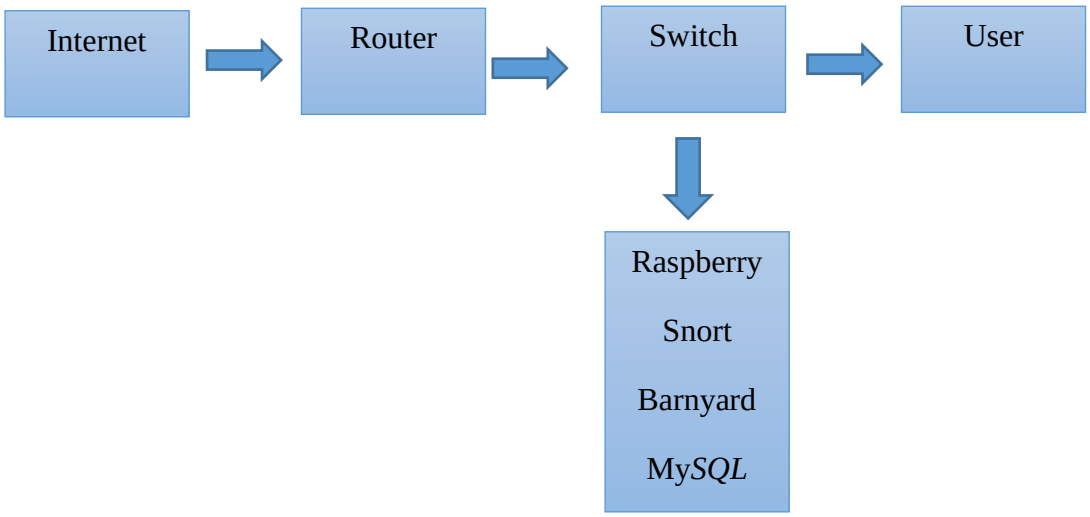
(Maria ulfa, 2013) dalam penelitiannya yang berjudul *Implementasi Intrusion Detection System (IDS)* di Jaringan Universitas Bina Darma menjelaskan bahwa Untuk menghindari dari bentuk serangan *flooding* maka di setiap server *firewall* melakukan proses pencegahan paket *flood syn Attack* dan paket *ping flood attack*. Kemudian untuk bentuk serangan *port scaning* yang terjadi agar melakukan pemblokiran terhadap *port-port* yang terbuka yang sudah dimasuki oleh penyusup melalui server *firewall*, selain itu juga dapat menggunakan perangkat lunak seperti *portsentry*.Serangan dapat terdeteksi atau tidak tergantung pola serangan tersebut ada didalam *rule IDS* (*Intrusion Detection System*) atau tidak. Oleh karena itu pengelola *Intrusion Detection System* (*IDS*) harus secara rutin meng-*update rule* terbaru. Oleh karena itu pengelola *Intrusion Detection System* (*IDS*) harus secara rutin meng-*update rule* terbaru.

(Alamsyah, 2011) dalam penelitiannya yang berjudul Implementasi Keamanan *Instrusion Detection System (IDS) dan Instrusion Prevention System (IPS)* menggunakan ClearOS menjelaskan bahwa Penerapan IDS (*Intrusion Detection System*) dan IPS *(Intrusion Prevention System)* menggunakan Snort dapat mendeteksi dan mencegah anomaly pada sistem komputer server dari penyusup.

(Nurhidayat dan Bata, 2015) dalam penelitiannya yang berjudul Penerapan Wireless intrusion detection system using open source tool menjelaskan bahwa *WIDS* mampu mendeteksi semua skenario serangan yang ada, selain mendeteksi serangan *WIDS* juga mampu mendeteksi semua aktifitas yang terjadi pada sebuah jaringan *wireless* mulai dari proses autentikasi sampai proses deautentikasi.

2.4 Kerangka Berpikir

Berdasarkan latar belakang penelitian diatas yaitu mengenai Penerapan *Instrusion Detection System (IDS)* dalam keamanan jaringan komputer maka penelti mencoba untuk merancang sebuah sistem dengan menggunakan *Raspberry Pi* yang akan di jadikan *Instrusion Detection System (IDS)*.



Gambar 2.18 Kerangka Berpikir
(sumber : peneliti)

Penjelasan dari gambar di atas adalah :

1. *Raspberry Pi* akan di install *OS Ubuntu Mate* yang akan digunakan untuk *Instrusion Detection System (IDS)* yang di dalamnya akan di *install Snort* dan *Barnyard*
2. *Raspberry Pi* yang telah di berikan *rule* untuk mendeteksi seangan akan di hubungkan ke *switch* dimana s*witch* akan dipantau oleh aplikasi *Snort* yang hasilnya berupa peringatan (alert) yang di simpan pada *database MySQL*.
3. *Raspberry Pi* akan menampilkan hasil dari pantauan tersebut melalui *Barnyard* dengan mengambil data dari *database MySQL*.