BAB II

LANDASAN TEORI

2.1 Tinjauan Pustaka

Menurut penelitian Mangunkusumo et al (2013) Zimbra adalah aplikasi *email* yang berbasis *open source* dengan fitur yang lengkap, mudah dalam instalasi dan manajemen *mail server* itu sendiri, meskipun keamanan *mail server* menjadi masalah utama. Perancangan keamanan untuk *mail server* sangatlah penting dimana dapat menghindari terjadinya serangan *cracking* pada jaringan komputer seperti *port scanning*, *brute force* dan *virus*. Keamanan yang baik dapat mengoptimalisasikan kinerja dari *mail server* itu sendiri.

Proyek ini untuk merancang keamanan jaringan mail server zimbra pada jaringan lokal. Selanjutnya mail server zimbra akan dianalisa tentang kelebihan dan kekurangan pada keamanannya dalam suatu jaringan komputer.

Banyak kerugian yang didapat akibat serbuan ratusan bahkan ribuan *spam* dan *virus* pada *mail server*. Habisnya konsumsi *resource* jaringan, CPU dan ruang *harddisk* akan menggangu pelayanan *mail server* bagi suatu organisasi. Sistem yang hang atau *bandwidth* yang harus dibayar mahal sebagai akibat dari *mail spam* dan *virus* telah membuat banyak organisasi mengalami pemborosan yang tidak sedikit. Banyak solusi yang telah ditawarkan untuk mengatasi masalah seperti ini. Salah

satunya adalah dengan menggunakan penyaring *spam* "*Untange Gateway*". *Untange Gateway* adalah solusi jaringan berbasis *open source* yang telah terintegrasi dengan modul – modul untuk memfilter *spam* dan *virus*. (Primartha & Sukemi, 2010)

Menurut Ellysa Rahajeng et al (2013) Keamanan dan privasi basis data pada aplikasi *web* sangat beragam jenisnya untuk terhindar dari serangan. Hal ini dikarenakan banyaknya kebutuhan manusia berupa layanan yang berbasis *web*, seperti *online banking*, toko *online*, dan lain-lain. Salah satu jenis serangan yang sangat banyak dilakukan oleh penyerang adalah SQL *injection*. Dimana serangan tersebut dapat menyebabkan kerugian besar terhadap vendor komersil yang mengelola aplikasi *web*, dikarenakan SQL *injection* dapat memanipulasi basis data, bahkan sampai merusak sistem aplikasi *web* tersebut.

2.2 Landasan Teori

2.2.1 Definisi Jaringan Komputer

Jaringan komputer adalah kumpulan komputer serta perangkat - perangkat lain pendukung komputer yang saling terhubung dalam suatu kesatuan. Media jaringan komputer dapat melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling melakukan pertukaran informasi seperti dokumen dan data. Dapat juga melakukan pencetakan pada printer yang sama dan bersama-sama memakai perangkat keras dan perangkat lunak yang terhubung dengan jaringan. (Muallifah & Yulianto, 2013).

2.2.2 Jenis – jenis Jaringan Komputer

1. LAN (*Local Area Network*)

Merupakan jaringan lokal yang dibuat pada area tertutup. Misalkan dalam satu gedung atau dalam satu ruangan. LAN biasa digunakan untuk jaringan kecil yang menggunakan *resource* bersama. Seperti penggunaan printer secara bersama. LAN dapat menggunakan media komunikasi seperti kabel dan *wireless*.

2. MAN (*Metropolitan Area Network*)

Merupakan jaringan antara LAN satu dengan LAN lain yang dipisahkan daerah lokasi yang cukup jauh. Contoh penggunaan MAN adalah hubungan antara kantor pusat dengan kantor cabang yang ada di daerah-daerah. Dapat dikatakan MAN merupakan pengembangan dari LAN.

3. WAN (*Wide Area Network*)

Merupakan jaringan yang cakupannya lebih luas dari pada MAN. Cakupan WAN meliputi satu kawasan, satu negara, satu pulau, bahkan satu benua. Metode yang digunakan WAN hampir sama dengan LAN dan MAN. (Sofana, 2012).

2.2.3 OSI (*Open System Interconnection)* Layer

Model referensi OSI dibuat pada akhit tahun 1970, model ini dibuat sebagai solusi untuk mengatasi masalah kompatibilitas antar vendor komputer maupun jaringan. Sehingga dalam membuat *hardware* atau *software* yang bisa saling kerja sama, dalam bentuk protokol-protokol sehingga *hardware* maupun *software* yang dibuat oleh vendor yang berbeda bisa saling kerja sama. (Sotyohadi, 2012)

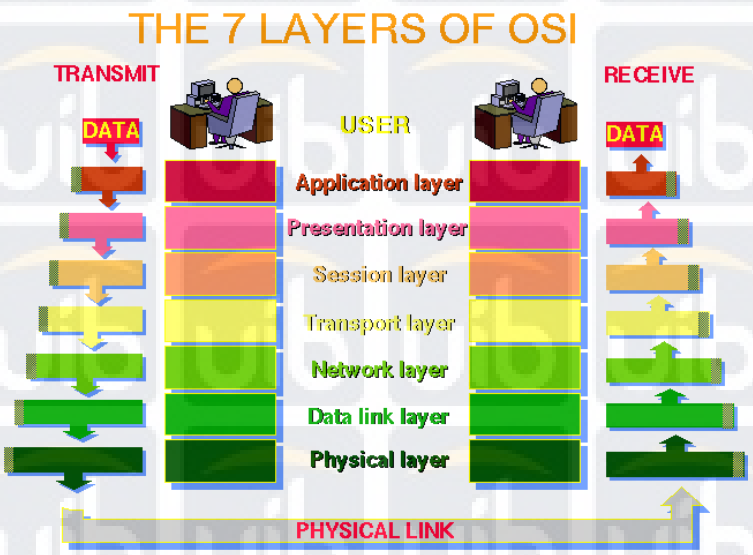
Model OSI menjadi semacam referensi atau acuan bagi siapa saja yang ingin memahami cara kerja jaringan komputer. Walaupun OSI merupakan sebuah model yang diakui didunia saat ini, namun tidak ada paksaan bagi pengembang *Hardware* atau *Software* dan *user* untuk menggunakannya. Sebagai contoh, jaringan internet

menggunakan model DARPA (*Defence Advanced Research Projects Agency*) yang berbeda dengan model OSI. Bahkan internet bisa berkembang sangat pesat walaupun tidak menggunakan model OSI.

Perlu dipahami bahwa model OSI bukanlah sebuah protocol. Protokol adalah sekumpulan aturan yang digunakan pada komunitas data. Protokol untuk jaringan komputer cukup banyak, beberapa yang popular seperti: TCP/IP, IPX, NetBIOS, PPP, AppleTalk, dan sebagainya. Model OSI dibuat setelah teknologi jaringan komputer hadir diantara kita.

Model OSI terdiri atas layer – layer atau lapisan – lapisan berjumlah 7 buah. Ketujuh layer tersebut yaitu:

1. Phsycal
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application



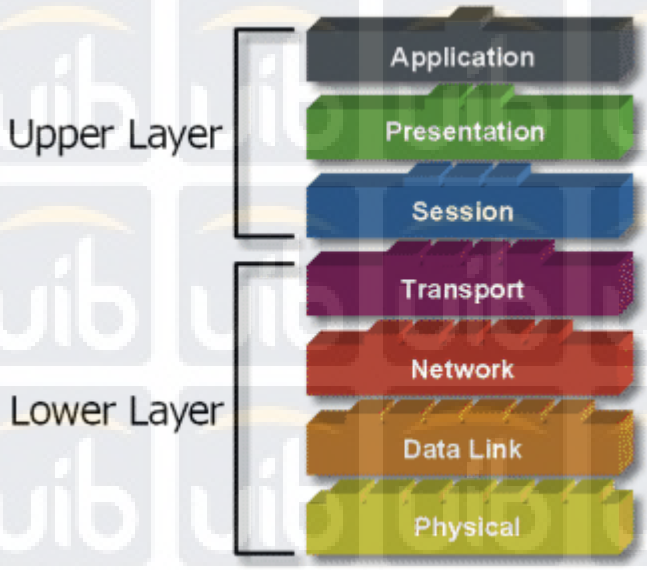
Gambar 2.1 7 *OSI Layer*

Ketujuh layer ini jika dilihat secara fungsional dapat dibedakan menjadi dua saja, yaitu:

1. Layer 5 s.d. 7 dikelompokkan sebagai application layers atau *upper layers*. Segala sesuatu yang berkaitan dengan user interface, data formatting, dan communication sessions ditangani layer ini. *Upper layers* banyak diimplementasikan dalam bentuk software (aplikasi).

2. Layer 1 s.d. 4 dikelompokkan sebagai data *flow layers* atau *lower layers*. Bagaimana data mengalir pada *network* ditangani oleh layer ini. *Lower layers* dapat diimplementasikan dalam bentuk *hardware* maupun *software*. (Sofana, 2012)

OSI Layers:



Gambar 2.2 Upper dan Lower Layer

2.2.4 Perangkat Network dan OSI

Menurut Sofana (2012). Jika perangkat – perangkat network tersebut kita kaitkan dengan layer – layer OSI maka kita dapat mengelompokkannya menjadi beberapa perangkat yang umum, yaitu:

- Router

Router bekerja pada layer 3 (Model OSI) atau layer network. Pada layer ini disedikan protokol yang bertanggung jawab mengatur pengelamatan (addressing) dan penentuan rute (routing). Saat ini sudah dikembangkan router yang dapat bekerja

pada layer 4 atau layer transport. Router semacam ini memiliki fungsi tambahan, yaitu sebagai firewall.

- Bridge

  Bridge bekerja pada layer 2 (Model OSI) atau layer data link. Layer ini tidak menyediakan protokol routing dan addressing (disebut alamat logika). Namun bridge dapat mengenali alamat hardware (disebut alamat fisik atau MAC Address). Biasanya bridge digunakan untuk menghubungkan network yang menggunakan teknologi sejenis.

- Switch

  Switch juga bekerja pada layer 2. Switch berfungsi sebagai central atau konsentrator. Switch dapat dipandang sebagai multiport bridge.

  Selain switch tradisional, saat ini sudah dikembangkan MLS atau Multi Layer Switch yang dapat beroperasi pada layer 2 hingga layer 7. Switch semacam ini memiliki beberapa fitur tambahan yang tidak dijumpai pada switch tradisional

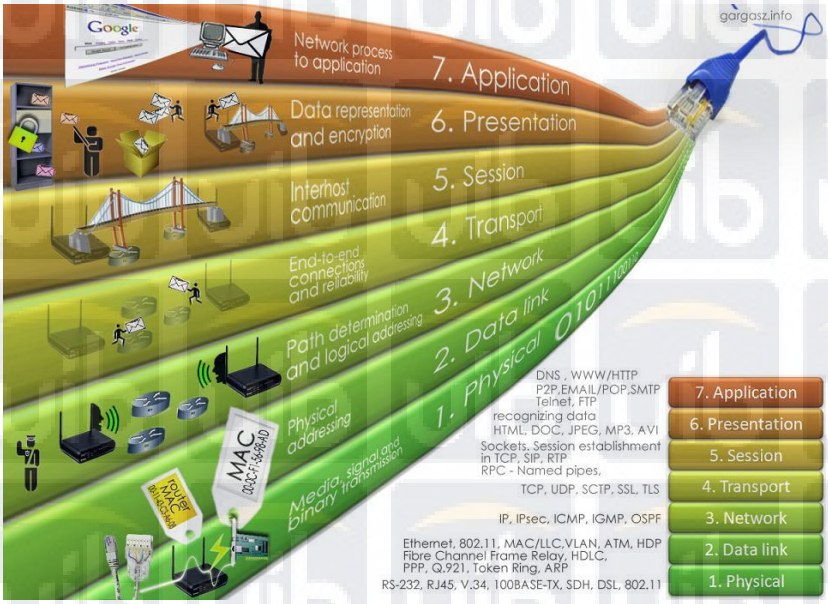
- Hub

  Hub bekerja pada layer 1 (Model OSI) atau layer phisycal. Hub berfungsi sebagai konsentrator. Namun Hub tidak dapat mempelajari hardware sehingga informasi dating ke Hub akan diteruskan keseluruh Host. Jadi setiap host akan menerima

informasi dari Hub. Kondisi semacam ini disebut sebagai “banjir broadcast” dan sangat mempengaruhi performa network. Saat ini Hub semakin jarang dijumpai.

- Repeater

Repeater bekerja pada layer 1 (Model OSI) atau layer physical. Repeater digunakan untuk “memperkuat” signal agar informasi dapat sampai ke host lain yang lokasinya cukup jauh. Saat ini repeater sudah jarang dipasarkan. Apalagi harga switch saat ini sudah semakin terjangkau.



Gambar 2.3 OSI Layer dan Media

2.2.5 IP Address

IP Address dibentuk oleh sekumpulan bilangan biner sepanjang 32 bit, yang dibagi atas 4 bagian. Setiap bagian panjangnya 8 bit. *IP Address* merupakan identifikasi setiap host pada jaringan internet. Artinya tidak boleh ada host lain (yang tergantung ke internet) menggunakan *IP Address* yang sama. Contoh *IP Address* sebagai berikut:

01000100 10000001 11111111 00000001

Apabila setiap bagian kita konversikan kebilangan desimal maka IP Address diatas menjadi:

68.129.255.1

Bentuk penulisan *IP Address* diatas dikenal dengan notasi "*noted decimal*". Dalam prakteknya, IP Address bentuk decimal inilah yang kita gunakan sebagai alamat host.

Saat ini alokasi IP Address versi 4 sudah semakin berkurang. IPv4 sudah digunakan hampir 20 tahun. Untuk mengatasinya, telah dikembangkan IP Address versi 6 IPng (IP next generation). Salah satu keunggulan IPv6 adalah jumlahnya yang sangat besar. Sehingga bisa mengantisipasi lonjakan permintaan IP Address dimasa yang akan datang.

IPv4 menggunakan 32 bit, sedangkan IPv6 menggunakan 128 bit. Sehingga kurang lebih memiliki 4 milyar (4e+9) komputer yang dapat terhubung ke internet menggunakan IPv4. Sedangkan jika menggunakan IPv6 bisa mencapai 3,4e+38 komputer. Secara teori kira – kira terdapat 6,65e+23 Address untuk setiap meter persegi diseluruh permukaan bumi. Namun semakin meningkatnya kebutuhan IP Address untuk perangkat genggam, seperti PDA, handphone, Blackberry, dan sebagainya, maka paling sedikit terdapat sebanyak 1564 address tiap meter persegi diseluruh permukaan bumi.

Sedangkan IP Address selain yang dicantumkan diatas dapat digunakan untuk internet. IP Address yang digunakan untuk keperluan LAN/Internet disebut sebagai IP Address Private. Sedangkan IP Address yang digunakan untuk keperluan internet disebut IP Address Public.

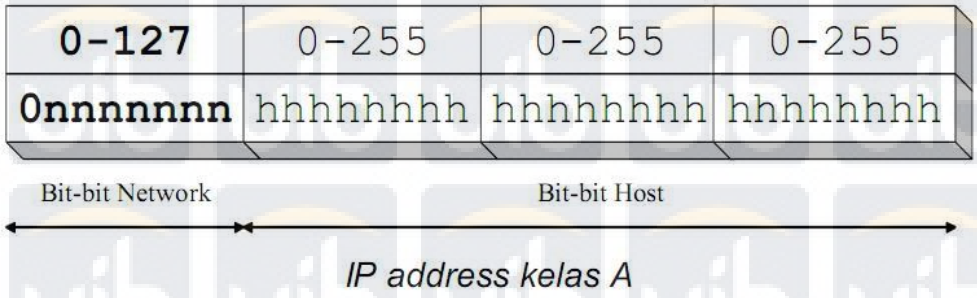
Secara umum, IP Address dapat dibagi menjadi 5 buah kelas. Kelas A, B, C, D, dan E. Namun dalam prakteknya hanya kelas A,B dan C yang dipakai untuk keperluan umum. Ketiga kelas IP Address ini disebut *IP Address unicast*. IP Address kelas D dan E digunakan untuk keperluan khusus. IP Address kelas D disebut juga *IP Address Multicast*. Sedangkan IP Address kelas E digunakan untuk keperluan *research.*

Berikut ini penjelasan masing – masing kelas IP Address

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

1. Kelas A

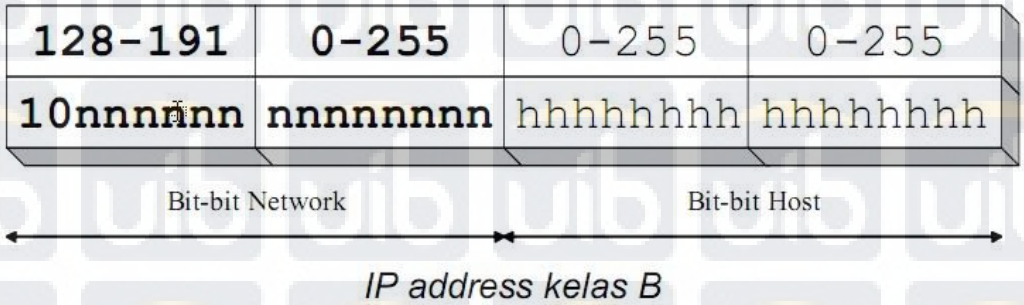
Bagian IP Address kelas A sebagai berikut;



IP address kelas A

Bit pertama bernilai 0. Bit ini dan 7 bit berikutnya (8bit pertama) merupakan bit – bit network (*network bit*) dan boleh bernilai berapa saja (kombinasi angka 1 dan 0). Sisanya, yaitu 24 bit terakhir merupakan bit – bit untuk host.

2. Kelas B



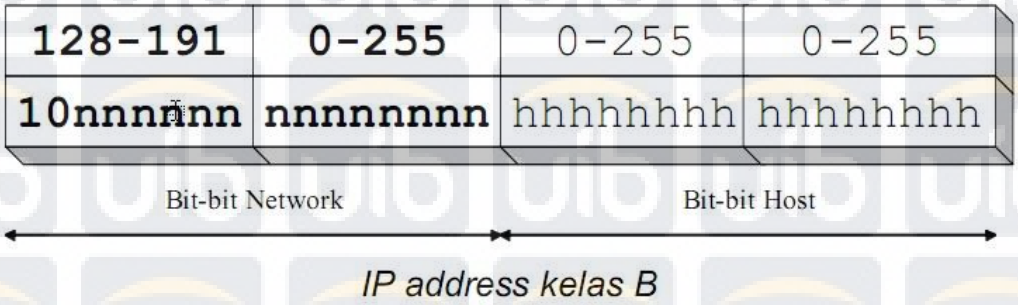
IP address kelas B

Bagian IP Address kelas B sebagai berikut:

2 Bit pertama bernilai 10. 2 Bit ini dan 14 bit berikutnya (16 bit pertama) merupakan bit network dan boleh bernilai berapa saja (kombinasi angka 1 dan 0). Sisanya, yaitu 16 bit terakhir merupakan bit – bit host.

3. Kelas C

Bagian IP Address kelas C sebagai berikut:



IP address kelas B

3 Bit pertama bernilai 110. 3 Bit ini dan 21 bit berikutnya (24 bit pertama) merupakan bit network dan boleh bernilai berapa saja (kombinasi angka 1 dan 0). Sisanya, yaitu 8 bit terakhir merupakan bit – bit host.

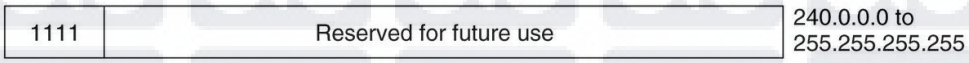
4. Kelas D

Bagian IP Address kelas D sebagai berikut:

Bit pertama bernilai 1110. IP Address Kelas D merupakan *multicast address*. Salah satu aplikasi yang memanfaatkan *multicast address* adalah *real time video conferencing*. Pada IP Address kela D tidak dikenal bit – bit network dan host.

5. Kelas E

Bagian IP Address kelas E sebagai berikut:



4 Bit pertama bernilai 1111. *IP Address* Kelas E dicadangkan untuk kegiatan research atau ekperimental. Pada IP Address kelas E juga tidak dikenal Bit – bit network dan host. (Sofana, 2012)

2.2.6 DNS Server

DNS adalah server yang berfungsi untuk menerjemahkan *IP Address* ke sebuah nama alamat dan sebaliknya dari nama alamat ke *IP Address*. *DNS Server* memberikan nama sebuah komputer, sedangkan dalam internet nama yang diterjemahkan oleh *DNS Server* merupakan *IP Address* dimana *web* dapat diakses. (Khairil, 2013)

2.2.7 Pengenalan Email

Menurut Athailah (2012). Email adalah layanan pengiriman surat melalui jalur jaringankomputer (misalnya internet). Email dikirim dari suatu alamat email yang terdapat pada sebuah mail server kepada alamat email yang lain yang terdapat pada mail server yang sama maupun pada mail server yang berbeda. Untuk mengirim surat elektronik diperlukan suatu program *mail-client*. Protocol yang dipakai untuk layanan email adalah layanan SMTP dan POP3.

Email adalah singkatan dari *electronic Mail*. Sebuah pesan elektronik baik berupa text maupun gambar, yang dikirimkan dari suatu alamat kealamat lain di jaringan internet. Perkembangan email ini seiring dengan laju perkembangan internet, karena pengguna lebih tertarik dari kelebihan email itu sendiri yaitu kemudahan dan cepat dalam penyampaian informasi.

Contoh Penulisan E-mail

dewa@batam.tcm.com

2.2.8 Pengenalan Email Server

Menurut Athailah (2012). Mail server merupakan sebuah server yang berurusan dengan lalu lintas *e-mail*, *email* dapat dianalogikan dengan surat yang akan di kantor POS sedangkan *mail server* dapat diibaratkan sebagai kantor POS dengan analogi ini sebuah mail server dapat memiliki banyak *account email* yang ada didalamnya.

Didalam pengiriman email terdapat tiga aplikasi yang diperlukan yaitu MTA (*Mail Transfer Agent*), MDA (*Mail Delivery Agent*), dan MUA (Mail User Agent). Kerja sama antara MUA, MDA dan MTA dapat diibaratkan seorang agen perjalanan dan perusahaan yang bergerak di bidang perjalanan, yang mana *email* merupakan orang yang melakukan perjalanan.

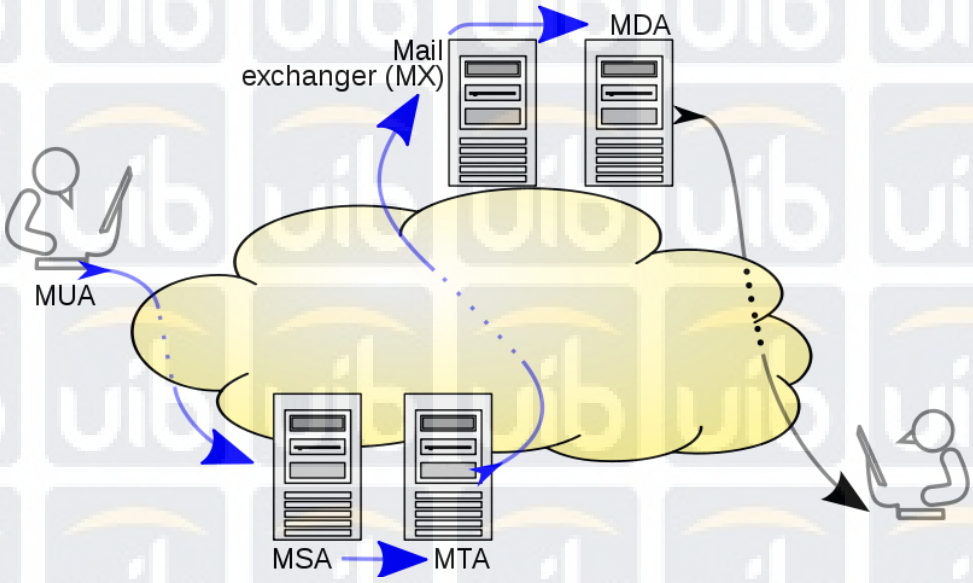
Mail Transfer Agent atau *relay* adalah perangkat lunak yang mengantar pesan surat elektronik dari suatu komputer ke komputer lainnya menggunakan arsitektur aplikasi *client server*. Suatu MTA mengimplementasikan apa yang dikenal sebagai *Simple Mail Transfer Protocol* (SMNP) baik pada bagian klien (mengirimkan) dan *server* (menerima).

MDA (*Mail Delivery Agent*) adalah perangkat lunak komputer yang bertanggung jawab mengantarkan pesan *email* ke *mailbox user*. Didalam sebuah arsitektur *email Internet*, pengantaran pesan dilakukan dari sebuah proses penanganan

pesan dari *Message Transfer Agent* (MTA), dan kemudian menyimpan *email* tersebut ke dalam *mail box*.

Mail User Agent (MUA), adalah sebuah program komputer yang digunakan untuk memanajemen *email user*. Istilah *email client* dapat merujuk pada sistem apa saja yang dapat digunakan untuk mengakses *mailbox email user*, sebuah *relaying server*. Suatu aplikasi web yang menyediakan fungsi manajemen, pembuat dan penerimaan email seringkali juga dianggap sebagai *email client*, tetapi secara umum disebut sebagai *webmail*.

Gambaran umum cara kerja MTA-MDA-MUA, adalah sebagai berikut:



Gambar 2.4 Cara kerja MTA-MDA-MUA

2.2.9 Zimbra dan Komponen Zimbra

Zimbra adalah *software open source* untuk *email server* dan kolaborasi (*groupware*), yang menyediakan solusi *email server* yang *powerful*, penjadwalan, kalender grup, kontak dan manajemen penyimpanan dokumen via web. Zimbra server tersedia untuk Linux, Mac OS X dan platform virtualisasi. Zimbra menggunakan klien Ajax Web 2.0 yang dapat dijalankan pada browser *Firefox, safari* dan *Internet Explorer* (6.0+) dan IE serta mudah diintegrasikan dengan portal web API, aplikasi bisnis dan VoIP menggunakan *web services*.

Zimbra pada dasarnya sekelas dengan aplikasi *Microsoft Exchange Server*. Bedanya, Zimbra tersedia dalam 2 edisi, yaitu *Open Source Edition* dan *Network Edition*. *Zimbra Open Source Edition* menggunakan lisensi *Mozilla Public License* yang salah satu butir lisensinya menyatakan bahwa perubahan atau modifikasi yang dilakukan pada kode sumber Zimbra harus dikembalikan pada komunitas. Zimbra Server terdiri dari gabungan berbagai *software Open Source*, yaitu *postfix, MySQL, OpenLDAP, Anti Virus Clamav dan Anti Spam Assassin*.

Adapun aplikasi – aplikasi open source yang digunakan zimbra collaboration suite yang merupakan aplikasi standar yang dipakai di dunia industry (Zaida, 2010) antara lain:

1. Jetty yaitu aplikasi web server yang menjalankan aplikasi zimbra.
2. Postfix, aplikasi open source MTA (Mail Transfer Agent) yang menjalankan e-mail server zimbra.
3. Open LDAP, aplikasi open source sebagai lightweight directory access protocol (LDAP) yang berguna untuk autentifikasi user.
4. MySQL sebagai aplikasi database.
5. Lucene, aplikasi open source powerfull text index dan search engine.
6. Anti virus dan anti spam, aplikasi open source yang terdiri dari: clan AV sebagai anti virus scanner yang melindungi file dari serangn virus, Spam Assassin sebagai mail filter yang mengindetifikasi adanya spam. (Tuxkeren, 2012)

2.2.10 Kriptografi

Kriptografi adalah ilmu yang mempelajari mengenai bagaimana cara mengamankan suatu informasi. Pengamanan ini dilakukan dengan mengenkrip informasi tersebut dengan suatu kunci khusus. Informasi ini sebelum dienkrip dinamakan *plaintext*. Setelah dienkrip dengan suatu kunci dinamakan *ciphertext*. Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

1. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
2. Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
3. Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
4. Non-repudiasi., adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat. Istilah-istilah yang digunakan dalam bidang kriptografi :

a. *Plaintext* (M) adalah pesan yang hendak dikirimkan (berisi data asli).

b. *Ciphertext* (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.

c. Enkripsi (fungsi E) adalah proses pengubahan plaintext menjadi *ciphertext*.

d. Dekripsi (fungsi D) adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi plaintext, sehingga berupa data awal/asli. (Dharmawan Eka Adhitya)

2.2.11 SQL Injection

SQL *injection* merupakan sebuah teknik yang menyalahgunakan sebuah celah keamanan yang terjadi dalam lapisan basis data suatu aplikasi. Dengan menggunakan perintah SQL seperti *Select*, *Where*, *Insert*, *Delete*, dan *Update*, seorang penyerang dapat mengubah struktur (memanipulasi) kode SQL sebenarnya dan mengeksekusi kode injeksi tersebut kedalam aplikasi *web*. Jika serangan ini berhasil dilakukan, penyerang dapat dengan mudah mengakses data-data yang bersifat sensitif, memodifikasi data yang terproteksi, mengeksekusi data, dan bahkan penyerang dapat merusak keseluruhan aplikasi, sehingga tidak dapat memberi layanan kepada *web server*.

Metode SQL *injection* ada bermacam-macam, yang paling umum digunakan adalah memanfaatkan kesalahan pada pentrasmisian parameter, jenis penanganan (*handling*), dan penggunaan kode SQL, seperti („ OR) 1 = -- ’). Jenis SQL *injection* juga bermacam-macam, antara lain tautologi, ilegal *query*, UNION *query*, *Piggy-*

backed query, *Stored Procedures*, *Blind SQL*, *Timing Attack*, *Alternate Encoding*, dan lain-lain

2.2.12 *Protocol HTTP*

HTTP atau *Hypertext Transfer Protocol* adalah sebuah protokol jaringan pada lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan menggunakan hipermedia. Pada umumnya, HTTP merupakan sebuah protokol yang memproses permintaan dari *client* dan jawaban dari *server*, atau sebaliknya. Protokol tersebut mengirimkan data maya (disebut *resources*) pada World Wide Web (WWW).

HTTP berkomunikasi melalui TCP/IP. Sebuah *client* HTTP seperti *web browser*, biasanya memulai permintaan dengan membuat hubungan ke *port* tertentu (biasanya *port* 80). Sebuah *server* HTTP yang mendengarkan *port* tersebut, menunggu *client* mengirimkan kode permintaan yang akan meminta halaman yang sudah ditentukan, lalu diikuti dengan pesan MIME yang memiliki beberapa informasi kode kepala yang menjelaskan permintaan tersebut dan badan pesan.

2.2.13 Keamanan Jaringan

Menurut Syariful Ikhwan (2014), Internet dan *World Wide Web* (WWW) menjadi bagian yang penting bagi kehidupan banyak orang. Secara teratur, beragam transaksi terjadi melalui web yang melibatkan informasi pribadi. Transaksi ini meliputi *online banking*, *e-edukasi*, *e-commerce* dan lain-lain. Setiap orang yang berkomunikasi meng-inginkan transaksi yang aman dan terjamin. Menurut Ammar Yassir dan Smitha Nayak, serangan terhadap mesin yang terhubung ke internet mengalami peningkatan 260% sejak tahun 1994 dan membuat kerugian sekitar 1.290 juta dollar setiap tahun di Amerika . Oleh karena itu, keamanan jaringan menjadi signifikan bagi setiap pengguna internet .

Keamanan jaringan pada intinya adalah mengendalikan akses terhadap sumberdaya jaringan. Akses jaringan dikontrol agar bisa diakses oleh siapa saja yang berhak dan menghalangi orang atau subjek yang tidak terdaftar untuk mengaksesnya.

Prinsip keamanan jaringan di klasifikasikan menjadi 3 bagian :

1. *Confidentiality* (Kerahasiaan)

Confidentiality mengacu pada kerahasiaan sebuah objek, dimana sebuah objek dijaga agar tidak diakses oleh subjek yang tidak berhak. Istilah ini juga mengacu pada data pribadi yang diberikan kepada pihak lain untuk keperluan tertentu dan hanya digunakan untuk keperluan tersebut. Contoh data-data yang sifatnya pribadi itu adalah nama, nomor kartu kredit, nomor paspor, nomor telepon, password komputer, agama, status perkawinan dan lain-lain .

Ada banyak tool yang digunakan untuk menjaga agar kerahasiaan sebuah subjek terjaga dengan baik, diantaranya Enkripsi, Akses Kontrol, otentifikasi, otorisasi dan keamanan fisik.

2. *Integrity* (Integritas)

Integrity mengacu pada objek yang tetap asli (original), dimana objek tidak berubah di perjalanan hingga sampai ke tujuan dari objek tersebut. Sebagai contoh, email yang dikirim oleh seseorang bisa dicegat ditengah jalan kemudian diubah isinya dan selanjutnya baru dikirim ke penerima sebenarnya sehingga data yang diterima oleh penerima telah berubah dari yang diinginkan oleh pengirim. Bentuk serangan terhadap aspek integrity diantaranya adalah virus, *trojan horse*, atau pemakai lain yang berada ditengah komunikasi.

Untuk mengatasi hal tersebut, maka perlu dibuat mekanisme proteksi agar data tidak bisa diubah oleh pihak-pihak yang tak diizinkan. Tool yang digunakan untuk menjaga hal itu terlaksana diantaranya adalah *Checksums*, *Data correcting codes* dan *backup*.

3. Availability (Ketersediaan)

Availability mengacu pada ketersediaan *resource* dengan tepat, dimana user mempunyai hak akses tepat waktu dan tidak terkendala apapun.

Salah satu serangan terhadap aspek availability adalah serangan *Distributed Denial of Service* (DDoS Attack). Tujuan utama dari *DDoS attack* adalah memenuhi

resource yang dibutuhkan oleh *user* sehingga *user* tidak bisa menggunakan *resource* tersebut sebagaimana harusnya. Selain *DDoS attack*, faktor lain yang mempengaruhi berkurangnya aspek *availability* adalah kelalaian manusia dan bencana alam. *Tool* yang digunakan untuk hal ini bisa jadi adalah perlindungan secara fisik dan penyimpanan redundan pada storage. Sedangkan untuk data-data yang sifatnya memiliki ketersediaan yang sangat penting, perlu adanya *server* cadangan yang senantiasa siap digunakan apabila *server* utama mengaami kerusakan.

2.2.14 Spamming

Spam adalah penyalahgunaan sistem email untuk mengirim pesan massal yang tidak diminta. Dalam hal ini spam pada email dalam volume besar yang menyebabkan masalah serius bagi pengguna, dan layanan internet. Seperti, mendegradasi pengalaman pencarian pengguna, membantu penyebaran virus di jaringan, meningkatkan beban pada lalu lintas jaringan, membuang-buang sumber daya seperti bandwidth, penyimpanan, dan daya komputasi, juga membuang-buang waktu pengguna dan energi. saran umum untuk menghindari spam yang menggunakan filter spam, Jangan pernah membalas spam, Jangan posting alamat email anda di situs web Anda, dan tidak pernah membeli sesuatu dari spam.

Pendefinisian spam *e-mail* berbeda-beda. Undang-undang CAN-SPAM memberikan definisi utama spam dengan menjelaskan apa yang (dan apa yang tidak) diperbolehkan bila mengirim *e-mail* komersial pemasaran. Undang-undang tersebut

disahkan pada tahun 2004 oleh Federal Trade Commission, yang diperbarui tahun 2008. Selain FTC terdapat badan-badan lain yang mengklasifikasikan spam, yaitu *Internet Service Provider* (ISP*). Internet Service Provider* juga memiliki bagian besar dalam menentukan apa yang dianggap spam. ISP tidak mengandalkan CAN-SPAM sendirian untuk mendefinisikan spam karena di mata mereka spam .didefinisikan oleh pengguna. Jika penerima *e-mail* mengelompokkan pesan *e-mail* sebagai spam dengan cara meletakkan di daftar pengirim yang diblokir mereka, menjatuhkannya di folder spam atau sekadar tidak konsisten membukanya, maka itu dianggap spam oleh ISP terlepas dari apakah itu melekat pada masing-masing dan setiap CAN-SPAM aturan. Berikut adalah tipe-tipe *e-mail* spam

1. Untuk Iklan: Spam dapat digunakan untuk mempromosikan suatu produk ataupun layanan, mulai dari produk software, perumahan real estate hingga produk kesehatan dan produk vitamin.

2. Untuk Mengirimkan Malware: Spam adalah salah satu cara utama untuk mendistribusikan virus dan malware. Dengan target yang bersifat individual, akan memperdaya korban untuk mempercayai bahwa mereka menerima dokumen penting atau file tertentu, yang sebenarnya mengandung malware.

3. Phishing: Bersembunyi dibalik namanama besar perusahaan besar, lembaga keuangan, lembaga pemerintah, lembaga amal, para phisher mencoba memikat korban untuk mengunjungi website palsu, dimana melalui website tersebut mereka dapat mencuri data keuangan pribadi atau informasi dengan mengenai identitas korbannya.

4. Scam: Mengirimkan *e-mail* sebagai pangeran dari Nigeria, pegawai bank dari Swiss, seorang anak kecil yang sakit keras, dan beberapa tipe lainnya, para scammer berusaha memperoleh simpati.
5. Pesan yang tak berarti: Sebuah potongan pesan sampah seperti ini dapat memenuhi inbox mail kita. Bahkan beberapa pesan seperti ini dapat mengkelabui teknologi spam filter, banyak pesan tak berarti ini dikirimkan tanpa tujuan yang jelas.

Cara bagaimana orang melakukan komunikasi menggunakan alat-alat modern membuka peluang besar untuk orang-orang yang tidak hanya melihatnya cara untuk melakukan komunikasi, tetapi cara untuk memperluas bisnis dan mendapatkan uang. Informasi adalah cara bagaimana orang membujuk orang lain untuk tertarik dengan produk yang ditawarkan, dan mengejar untuk lebih banyak orang mendapatkan mengirim sebagian besar pesan dalam waktu yang sama dengan konten yang sama ke banyak orang karena mereka memiliki. Sebagian besar pesan yang diterima disebut spam / spamming. Spamming didefinisikan oleh dua karakteristik yaitu, karakteristik utama dan karakteristik sekunder. karakteristik utama yang termasuk pesan elektronik, mengirim dalam jumlah besar, tidak diminta, dan komersial. Dengan melihat semua karakteristik pada orang-orang karakteristik utama akan langsung menganggap bahwa itu spam. Syarat di kata Spam:

1. Spam adalah pesan elektronik.
2. Spam adalah tidak diminta. Ketika penerima tidak memiliki komentar dan hanya setuju dengan pesan sehingga tidak spam.

3. Spam dikirim dalam jumlah besar. Ini berarti bahwa pengirim informasi mengirim pesan dalam jumlah besar dengan isi yang sama.
4. Komersial, ini menyiratkan bahwa pesan penerima mendapat adalah komersial meminta orang untuk membeli produk yang ditawarkan. Karakteristik yang tersisa yang sekunder sering dikaitkan dengan spam, tetapi belum tentu terkait dengan spam.