**BAB I**

**PENDAHULUAN**

* 1. **Latar Belakang**

Seiring dengan pertumbuhan teknologi, surat elektronik*(email)*menjadi sarana komunikasi yang semakin banyak digunakan. Di negara maju, surat elektronik bahkan sudah menjadi komunikasi utama di kantor atau antara pelanggan dan nasabahnya. Pemberitahuan rapat dan segala hal yang menyangkut urusan kantor menjadi sangat praktis dengan menggunakan surat elektronik. Dengan fungsinya yang sangat penting tersebut, maka sebagai pengguna harus benar-benar memperhatikan faktor keamanan surat elektroniknya.

Pada Satuan Kerja Teknologi InformasiPT Bukit Asam (Persero) merupakan tempat pusat informasi perusahaan dan mengelola jaringan di PT Bukit Asam (Persero) Tbk Tanjung Enim.Beberapa usaha yang sudah dijalankan oleh PT Bukit Asam (Persero) Tbk Tanjung Enim dalam upaya peningkatan sumber daya perusahaansalah satunya adalah dengan surat elektronik*.* Pada PT Bukit Asam (Persero) Tbk, fasilitas surat elektronik berfungsi sebagai roda penggerak bisnis perusahaan yang fungsi dari surat elektronik bagi perusahaan dibagi menjadi dua bagian yaitu fungsi internal dan fungsi eksternal. Namun ada beberapa hal yang harus *admisistratur*diperhatikan dalam mengenai suatukeamanan jaringan pada surat elektronik selama surat elektronik masih menggunakan jaringan internet sebagai media penghantarnya. Maka surat elektronik juga sangat rentan terhadap celah keamanan seperti yang ada pada jaringan, terdapat banyak serangan terhadap jaringan. Salah satu contoh serangan umum yang sering terjadi yaitu serangan *spam*.*Spam* merupakan pengiriman sejumlah pesan yang sama secara bertubi-tubi tanpa dikehendaki oleh penerimanya yang bertujuan untuk merusak sistem itu sendiri dan dapat menghambat dalam bisnis perusahaan.Jagat, (2010).

Melihat dari kondisi di atas dalam mengamankan jaringan dibutuhkan *email gateway.* Istilah gateway merujuk kepada perangkat keras atau perangkat lunakyang menjembatani dua aplikasi atau jaringan yang tidak kompatibel, sehingga *gateway* mengatur lalu lintas paket data antar jaringan yang di dalamnya terdapat mekanisme pembatasan atau pengamanan data untuk membantu memastikan terhadap integritas surat elektronik sebelum masuk *mail server*.Email Gateway yang sudah diterapkan PT Bukit Asam (Persero) Tbk menggunakan *Symantec Message Gateway 9.5* yangdapat meminimalisir terhadap serangan pada jaringan dan jenis surat yang tidak diinginkan dan di dalamnya terdapat anti*spam real time*, serta membatasi koneksi yang tidak diinginkan, melakukan penyaringan pesan untuk menghapus konten yang tidak diinginkan, dan pencegahan kehilangan data.

Sehingga dengan adanya *email gateway* dan anti*spam* yang telah diterapkan oleh PT Bukit Asam (Persero) Tbk dapat mengamankan keamanan jaringan pada surat elektronikdari serangan dari jaringan internetyang dapat menghambat proses bisnis perusahaan.

* 1. **Perumusan Masalah**

Berdasarkan latar belakang yang ada, maka penulis merumuskan permasalahan yang ada dengan rumusan masalah diantaranya “Bagaimana menganalisis keamanan jaringan menggunakan *Email Gateway* sebagai penyaringan suratelektronik pada Satuan Kerja Teknologi Informasi PT Bukit Asam (Persero) Tbk?”.

* 1. **Batasan Masalah**

Untuk lebih mengarahkan masalah yang ada serta tidak menyimpang dari permasalahan yang akan dilakukan dalam penelitian maka penulis hanya membatasi pada analisis *email gateway* yang dapat diketahui dari hasil *report*berupa cara kerja *Symantec Message Gateway 9.5*, selanjutnya konfigurasi pada fitur *Symantec Message Gaterway 9.5* dan uji coba pada sistem keamanan jaringan PT Bukit Asam (Persero) Tbk.

* 1. **Tujuan dan Manfaat Penelitian**
     1. **Tujuan Penelitian**

Berdasarkan dari latar belakang dan masalah yang diteliti maka tujuan dari penelitian ini adalah;

1. Melindungi sumber daya sebuah perusahaan salah satunya adalah jaringan komputer yang membuat kinerja karyawan menjadi meningkat,

2. Dapat mencegah ancaman dari hal-hal yang membahayakan jaringan di satuan kerja Teknologi Informasi PT Bukit Asam (Persero) Tbk,

3. Membuat analisa terhadap sistem yang diterapkan di perusahaan yang diharapkan dapat memberikan kesimpulan dan saran terhadap sistem tersebut,

4. Mendapatkan pengalaman kerja serta menerapkan teori dan pengetahuan yang telah diterima di dalam perkuliahan atau dengan situasi nyata di tempat perusahaan.

* + 1. **Manfaat Penelitian**

Manfaat yang bisa didapatkan dari penelitian ini adalah;

1. Meningkatkan efektifitas dari kinerja jaringan di Satuan Kerja Teknologi Informasi PT Bukit Asam (Persero) Tbk,
2. Sebagai usaha dalam meningkatkan sistem keamanan jaringan komputer di Satuan Kerja Teknologi Informasi PT Bukit Asam (Persero) Tbk,
3. Dapat mengetahui bentuk sistem keamanan yang digunakan pada dunia kerja sehingga dapat menambah pengetahuan dalam merancang dan membangun suatu sistem keamanan jaringan yang sesuai dengan permasalahan yang ada,
4. Dengan menggunakan *email gateway* akan mempermudah *administratur* jaringan untuk memantau aliran data yang masuk dan keluar di suatu jaringan.
   1. **Metodologi Penelitian**
      1. **Tempat dan Waktu Penelitian**

Penelitian dilakukan di satuan kerja Teknologi Informasi PT Bukit Asam (Persero) Tbk Tanjung Enim, dimulai pada 05 November sampai 05 Desember 2012 dari jam07.30 sampai dengan16.00 WIB.

* + 1. **Metode Penelitian**

Menurut Sugiyono (2007:9) penelitian tindakan merupakan penelitian yang bertujuan mengembangkan metode kerja yang paling efisien, sehingga biaya produksi dapat ditekan dan produktivitas lembaga dapat meningkat. Penelitian melibatkan peneliti dan karyawan untuk mengkaji bersama-sama tentang kelemahan dan kebaikan prosedur kerja dan alat-alat kerja yang digunakan selama ini dan selanjutnya mendapatkan metode kerja yang baru yang di pandang paling efisien. Jadi dapat dinyatakan disini bahwa, penelitian tindakan adalah suatu proses yang dilalui oleh perseorangan atau kelompok yang menghendaki perubahan dalam situasi tertentu untuk menguji prosedur yang diperkirakan akan menghasilkan perubahan tersebut dan kemudian setelah sampai pada tahap kesimpulan yang dapat dipertanggungjawabkan, melaksanakan prosedur ini. Tujuan utama penelitian ini adalah mengubah, evaluasi, perbaikan organisasi termasuk struktur mekanisme kerja. Adapun tahapan penelitian yang merupakan bagian dari *action research* ini, yaitu ;

Diagnosa,

Melakukan identifikasimasalah-masalah yang ada guna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan. Penulis melakukan diagnosa terhadap sistem keamanan jaringan komputer pada *administratur* yang ada pada pusat informasi di satuan kerja Teknologi Informasi PTBA.

Melakukan Rencana Tindakan,

Peneliti memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada. Pada tahap ini peneliti melakukan *survey* berkenaan masalah yang akan dianalisis tersebut apakah penelitian tersebut dapat dilaksanakan atau tidak di satuan kerja TI PT Bukit Asam (Persero) Tbk Tanjung Enim. Dalam hal ini penulis tertarik pada sistem keamanan jaringan komputer yang ada di PT Bukit Asam (Persero) Tbk Tanjung Enim.

Melakukan Tindakan,

Pada melakukan tindakan peneliti melakukan menganalisis kemananan jaringan menggunakan *email gateway* sebagai penyaringan surat elektronik yang dilihat dari hasil *report* dari sistem keamanan jaringan yang ada di Satuan Kerja Teknologi Informasi PT Bukit Asam (Persero) Tbk.

Evaluasi,

Peneliti melakukan evaluasi hasil dari analisis yang telah dilakukan tadi, dalam tahap ini dilihatpenerapan *email gateway* sebagai penyaringan surat elektronikapakah sudah berjalan dengan baik dalam mengamankan surat elektronikdengan melihathasil *report* dari sistem tersebut dalam mengatasi seranganyang terjadi pada sistem keamanan jaringan PT Bukit Asam (Persero) Tbk Tanjung Enim.

Pembelajaran.

Tahap ini merupakan bagian akhir yang telah dilalui dengan melaksanakan *review* tahap demi tahapan dan dapat memahami prinsip kerja dari hasil analisis.

* + 1. **Metode Pengumpulan Data**

Dalam melakukan penelitian untuk mendapatkan data dan informasi, maka metode yang digunakan dalam proses pengumpulan data adalah sebagai berikut;

1. Observasi,

Penulis mengadakan peninjauan langsung ke PT Bukit Asam (Persero) tbk Tanjung Enim khususnya di Satuan Kerja Teknologi Informasi yang merupakan tempat di mana pusatnya sistem informasi jaringan di perusahaan tersebut dengan mengamati, mencatat dan mengevaluasi jaringan yang ada di perusahaan tersebut dan bagaimana mengamankan sistem keamanan jaringan menggunakan *email gateway* sebagai penyaringan pesan pada PT Bukit Asam (Persero) Tbk Tanjung Enim.

1. Wawancara,  
   Dalam hal ini penulis mengajukan pertanyaan-pertanyaan kepada beberapa karyawan yang berada di satuan kerja Teknologi Informasi PT Bukit Asam (Persero) Tbk Tanjung Enim yang bertugas sebagai *administratur* jaringan pada perusahaan tersebut.
2. Dokumentasi,

Dalam hal ini penulis guna menyelesaikan penulisan, penulis mengumpulkan dokumentasi dalam bentuk data-data dan catatan.

Data sekunder yang sifatnya informasi diperoleh penulis dengan melakukan studi *literature* yang *relevan*, yaitu dengan cara mempelajari buku, *e-book*, dan jurnalyang erat kaitannya dengan penulisan penelitian.

* + 1. **Metode Analisis Sistem Keamanan Jaringan**
       1. **Metode Penetrasi**

Metode Penetrasi adalah suatu metode yang dilakukan guna mengevaluasi keamanan dari sebuah sistem komputer atau jaringan dengan cara melakukan simulasi serangan dari luar maupun internal sistem atau jaringan.Tujuan pengujian penetrasi adalah untuk menemukan setiap dan semua titik kerentanan di dalam sistem komputer. Pada dasarnya orang yang melakukan pengujian penetrasi sedang mencoba untuk kembali ke sistem. (Cymots, 2011)

**BAB II**

**TINJAUAN PUSTAKA**

* 1. **Landasan Teori**
     1. **Analisis**

Menurut (Komaruddin, 2012),Analisis adalah kegiatan berfikir untuk menguraikan suatu keseluruhan menjadi komponen sehingga dapat mengenal tanda-tanda komponen, hubungannya satu sama lain dan fungsi masing-masing dalam satu keseluruhan yang terpadu.

**2.1.2. Keamanan Jaringan**

Keamanan jaringan sebagai bagian dari keamanan sisteminformasi adalah sangat penting untuk menjaga keamanan data serta menjamin ketersediaan layanan bagi pengguna. (Simarmata,2006:131).

Keamanan jaringan melibatkan otorisasi akses ke data dalam jaringan, yang dikendalikan oleh *administratur* jaringan. Keamanan jaringan mencakup berbagai [jaringan komputer](http://agussale.com/category/komputer/jaringan-komputer), baik negeri maupun swasta, yang digunakan dalam pekerjaan sehari-hari melakukan transaksi dan komunikasi di kalangan bisnis, instansi pemerintah dan individu.

Jika diamati mengenai keamanan maka [keamanan jaringan komputer](http://agussale.com/keamanan-jaringan-komputer) dapat ditinjau dari segi bentuknya yaitu seperti berikut;

1. Keamanan Perangkat Keras

Keamanan perangkat keras sering dilupakan padahal merupakan hal utama untuk menjaga jaringan dari agar tetap stabil.Dalam keamanan perangkat keras*,server* dan tempat penyimpanan data harus menjadi perhatian utama. Akan lebih mudah bagi pencuri data untuk mengambil *harddisk* atau *tape backup* dari *server* dan tempat penyimpanannya daripada harus menyadap data secara perangkat lunakdari jaringan. Kabel-kabel jaringan harus dilindungi agar tidak mudah bagi *hacker* memotong kabel lalu menyambungkan ke komputernya.

1. Keamanan Perangkat Lunak

Perangkat lunak yang dimaksud di sini bisa berupa sistem operasi, sistem aplikasi, data dan informasi yang tersimpan dalam komputer jaringan terutama pada *server*.(Qbonk.2011).

Kegiatan dan hal-hal yang membahayakan keamanan jaringan antara lain adalah hal-hal sebagai berikut;

1. *Spam*

*Spam* adalah pengiriman sejumlah pesanyang sama yang memaksa orang lain yang tidak menginginkan adanya pesan itu mau tidak mau harus menerimanya. Kebanyakan *spam* yang ada di internet adalah berupa iklan, promosi dari suatu produk. *Spam* ini sangat menguntungkan bagi pengirim, karena hanya membutuhkan biaya yang kecil, sementara tidak sebaliknya jika kita memandang dari sisi penerima.Cara pencegahan dan penetralisir *spam* saat ini produsen aplikasi keamanan sudah menyediakan program anti *spam* yang handal. Beberapa diantaranya dipaket dalam aplikasi antivirus.

1. *Phising*

*Phising* adalah suatu bentuk penipuan yang dicirikan dengan percobaan untuk mendapatkan informasi, seperti kata sandi dan kartu kredit, dengan menyamar sebagai orang atau bisnis yang terpercaya dalam sebuah komunikasi elektronik resmi, seperti posnel atau pesan instan. Istilah *phising* dalam bahasa Inggris berasal dari kata *fishing* (memancing), dalam hal ini berarti memancing informasi keuangan dan kata sandi pengguna, *Phising* juga didefinisikan sebagai sebuah kegiatan memancing pemakai komputer di internetagar mau memberikan informasi data diri pemakai *(username)* dan kata sandinya *(password)* pada suatu *website* yang sudah di*deface.* Cara pencegahan dan penetralisir *phising* jangan pernah mengirimkan data pribadi seperti nomor kartu kredit, PIN ATM atau apapun melalui surat elektroniksekalipun diminta oleh bank, perusahaan kartu kredit atau apapun di mana anda terdaftar di dalamnya. Karena perusahaan tadi tidak akan pernah meminta data pribadi melalui surat elektronik*.*Kemudian jangan mudah percaya jika anda diminta membayar sesuatu atas hadiah yang telah anda menangkan tanpa melakukan pemeriksaan kepada pihak yang terkait.

1. *Denial of Service (DoS)*

*Denial of Service (DoS)* bertujuan untuk mencegah pengguna mendapatkanlayanan dari sistem. Serangan *DoS* dapat terjadi dalam banyak bentuk. penyerang dapat membanjiri *(flood)* jaringan dengan data yang sangat besar atau dengan sengaja menghabiskan sumber daya yang memang terbatas, seperti *pending network connection.* Penyerang juga mungkin saja mengacaukan komponen fisik dari jaringan atau memanipulasi data yang sedang dikirim termasuk data yang ter*enkripsi.*Meskipun cara pencegahan dan penetralisir seranganDoStidak ada cara terbaik untuk menghindari *DoS* namun identifikasi mana titik terlemah dalam jaringan serta penggunaan *firewall* yang mampu menghilangkan paket *DoS* secara otomatis adalah dua cara yang dapat dilakukan untuk melindungi sistem dari serangan ini. (Hong, 2012).

**2.1.3.*Email (Surat Elektronik)***

*Email* adalah singkatan dari *Electronic Mail*.Surat elektronik berfungsi sebagai sarana untuk mengirim surat atau pesan melalui jaringan internet, dengan surat elektronik kita hanya membutukan beberapa menit agar surat atau pesan kita sampai tujuan tidak perlu menunggu berhari-hari seperti mengirim surat atau pesan biasa(pos) dan dengan surat elektronikisi pesan dapat kita isi dengan konten gambar atau suara dan video. Surat elektronikmulai dipakai pada tahun 1960an, dan Pada saat itu internet belum terbentuk, yang ada hanyalah kumpulan *mainframe* yang terbentuk sebagai jaringan.(Ardians, 2012).

* + 1. ***Email Gateway***

Istilah *Email Gateway* merujuk kepada perangkat keras atau perangkat lunakyang menjembatani dua aplikasi atau jaringan yang tidak kompatibel, sehingga *gateway* mengatur lalu lintas surat elektronikantar jaringan. Maka di dalamnya bisa dipasangi meaknisme pembatasan atau pengamanan paket – paket data untuk membantu memastikan keamanansurat elektroniksebelum memasuki jaringan.

**2.1.4.1. Fungsi *Email Gateway***

1. Melakukan penerjemah bahasa mesin, agar dua arsitektur jaringan komputer yang berbeda dapat berkomunikasi,

2. *Email Gateway* berfungsi sebagai jembatan pelindung antara internetdan jaringan sehingga semua penyaringan dan pemblokiran terjadi sebelum lalu lintas surat elektronikmasuk ke jaringan*,*

3. Sebagai *rule* yang berguna untuk mendeteksi dan memf*ilter spam* dan memblokir virus,

4. *Email Gateway* ini merupakan layanan yang tersedia sebagai pilihan jaringan yang berbasis layanan *firewall.*

* + 1. **Packet Filtering**

Berbagai kebijakan dapat diterapkan dalam melakukan penyringan paket*.* Pada intinya, berupa mekanisme pengontrolan data yang diperbolehkan mengalir dari ke jaringan internal*,* dengan menggunakan beberapa parameter yang tercantum dalam *header* paket data, arah *(inbound atau outbound),address* asal dan tujuan, *port* asal dan tujuan, serta jenis *protokol transport*. *Router* akan mengevaluasi informasi ini dalam setiap paket data yang mengalir melaluinya, kemudian menetapkan aksi yang harus dilakukan terhadap paket tersebut, berdasarkan aturan program dalam penyringan paket. Sehingga keputusan *routing* dasar *router* tersebut, kemudian dilengkapi dengan bagian dari kebijakan keamananjaringan*.*(Eueung Mulyana dan Onno w. Purbo, 2010).

**2.1.6. *Symantec Messaging Gateway*9.5**

Penggunaan *Symantec Message Gateway 9.5* inidapat meminimalisirterhadap serangan pada jaringan dan jenis surat yang tidak diinginkan dan di dalamnya terdapat anti*spam real time*, serta konten penyaringan dan pencegahan dari kehilangan data-data penting*. Symantec Messaging Gateway* dapat melakukan hal berikut;

1. Mendeteksi *spam* padasurat elektronikyang masuk*,* dan mendeteksi adanya serangan *denial of service,*
2. Melakukukanpenyringan pesanyang digunakan untuk menghapus konten yang tidak diinginkan, dan hilangnya data melalui internet.(Symantec,2011).

Berikut adalah fiturdari *Symantec Message Gateway*9.5 yang terdapat pada tabel 2.1,

Table 2.1*.*Fitur*Symantec Messaging Gateway 9.5*

|  |  |
| --- | --- |
| **Fitur** | **Deskripsi** |
| *Policy groups* | Mekanisme yang dapat digunakan untuk mengatur [keamanan](http://id.wikipedia.org/wiki/Keamanan_komputer) dan beberapa kebijakan. *Policy Group* telah terintegrasi dengan [layanan](http://id.wikipedia.org/w/index.php?title=Layanan_direktori&action=edit&redlink=1)[*Active Directory*](http://id.wikipedia.org/wiki/Active_Directory) untuk menyederhankan konfigurasi dan manajemen sistem-sistem melalui [jaringan](http://id.wikipedia.org/wiki/Jaringan_komputer) yang luas, dan mencakup beberapa pilihan konfigurasi metode *autentikasi*, pengauditan sistem, pencatatan kejadian, pengaturan [*password*](http://id.wikipedia.org/wiki/Password), pengaksesan [*registry*](http://id.wikipedia.org/wiki/Windows_registry), *enkripsi* [*IPSec*](http://id.wikipedia.org/wiki/IPSec), dan masih banyak konfigurasilainnya. |
| Tabel 2.1Fitur*Symantec Messaging Gateway 9.5* Lanjutan 1 |  |
| **Fitur** | **Deskripsi** |
| *Scanners* | Mengumpulkan semua *logging* dan *statistic* dan mengontrol dan mengawasi peforma dari *Control Center* yang telah di *scanner.* |
| *Logs* | Dalam administrasi sistem, para *administratur* akan sering berhubungan dengan *logs*. *logs* adalah *file* yang berisi catatan *(log)* aktivitas dari sebuah program. |
| *Reports* | Merupakan *teks* yang isinya menggambarkan sesuatu secara apa adanya sebagai hasil pengamatan sistematis atau analisis. |
| *Appliance roles* | Dalam mengkonfigurasi sebuah peralatan dalam *Appliance Roles* ini untuk menjadi *Control Center* dan *Scanner*, sumber daya yang besar juga diperlukan untuk menyimpan data dalam mengkonfigurasi kedua peran tersebut agar tidak memperlambat kinerja dari sistem tersebut. |
| *Spam Quarantine* | Merupakan semua pesan yang mencurigakan terkait dengan *domain* saat ini disimpan. *Spam Quarantine* berisi pesan yang diblokir secara permanen oleh sistem anti*spam.* Pencarian pesan didasarkan pada nilai-nilai *Subject, Sender*atau *Recipient.*Pesan yang dapat dihapus atau dibebaskan. Jika mereka dilepaskan mereka akan muncul dalam kotak surat penerima. Pesan-pesan mencurigakan yang bersifat sementara ditolak tidak termasuk dalam sistem karantina. Pengiriman mereka akan secara otomatis *retried* oleh *server* pengirim |
| *Text-based attachment scanning* | *Symantec Messaging Gateway* dapat mengamati berbagai jenis lampiran pesandari *spam*.  Tabel 2.1 Fitur*Symantec Messaging Gateway 9.5* Lanjutan 2 |
| **Fitur** | **Deskripsi** |
| *DKIM (Domain Keys Identified Mail) signing* | Standar *authentication*pesan yang memungkinkan pengirim pesan untuk menandatangani pesandengan *domain* tertentu, dan untuk penerima pesanuntuk mengkonfirmasi bahwa pesan itu ditandatangani oleh *domain* tersebut dan belum diubah. |
| *SMTP authentication* | Skema yang digunakan untuk *authentication* pengirim yang sah sebelum mengizinkan pesanyang terhubung melalui *server email.* |

**2.1.7. Anti*Spam***

Anti*spam* itu sendiri adalah program yang meliputi alat atau perangkat lunak untuk mencegah *spam* masuk ke dalam *domain* tertentu. Program tersebut diperlukan terutama bagi pengguna surat elektronikkarena *spam* datang ke pesan masukmereka secara bertubi-tubi dengan pesan yang tidak mereka kehendaki. *Spam* muncul dalam berbagai bentuk dengan pesan yang beragam, mulai dari *junk mail* biasa, *junk mail* dengan *link* yang mengandung virus, *link* situs porno, *spam* mesin pencari informasi *web, spam blog,* dan lain-lain, yang mengakibatkan tidak nyamannya pengguna internet.(Jagat, 2010).

**2.1.7.1. Metode Anti *Spam***

Telah terdapat beberapa metode yang dapat digunakan untuk mencegah *spam* diantaranya;

* + - 1. *Address blocking*

Metode ini memblok *spam mail* berdasarkan *IP* atau *domain* atau alamat surat elektroniktertentu yang telah dikategorikan sebagai alamat *spammer.*

1. *White Listing*

Kebalikan dengan *black listing*, *white listing* berisi daftar alamat yang dikategorikan sebagai pengirim surat elektronik yang sah (*legitimate mail*). Alamat pengirim surat elektronikyang tidak termasuk dalam daftar ini akan diasumsikan sebagai *spam mail*.

1. *Signature Based Filtering*

Metode ini akan membandingkan surat elektronikyang datang dengan *spam mail* yang telah diketahui. Hal ini dilakukan dengan membuat beberapa alamat surat elektronikpalsu. *Spam mail* yang biasanya dikirim ke beratus-ratus alamat surat elektronik juga akan dikirim ke alamat-alamat palsu ini. Sehingga dengan membuat *list* alamat-alamat mana saja yang mengirim surat elektronik ke alamat palsu ini, *spammail* dapat diblok.

1. *Email minefield*

Metode ini dilakukan dengan menambahkan sejumlah alamat surat elektronikpalsu pada bagian alamat suatu situs, sehingga surat elektronik yang dikirimkan ke alamat tersebut dapat disimpulkan sebagai *spam*. *Spammers* biasanya mencoba untuk memalsukan *header message* atau *IP address* yang mereka gunakan. Tetapi pada transaksi *SMTP(Simple Mail Transfer Protokol)* dari *spammers* ke alamat *minefield,* terdapat suatu mekanisme tertentu yang mengharuskan *spammers* menyatakan *IP address* yang sebenarnya. Dengan mekanisme seperti ini, situs yang menjadi target *spamming* dan situs-situs lain yang terkait dengan situs target dapat mem*black-list IP address* tersebut secara bersamaan (*realtime sharedminefield*). Sehingga pemblokiran suatu *IP address spammer* dapat dilakukan dengan cepat. (Panjaitan, 2008).

**2.1.8. *Mail Server***

*Mail server* adalah suatu fasilitas yang berfungsi untuk mengatur penerimaan dan pengiriman surat elektronik*.* Agar surat elektronik dapat sampai ke tujuannya dengan baik dan cepat, di perlukan suatu sistem pengaturan surat elektronik yang tangguh. *Mail Server* harus mampu menangani surat - surat elektronik yang dikirimkan kepada pemakai di jaringan lain atau internet*.*(Keysha, 2008).

Berdasarkan pengalaman menangani *mail server klien-klien Excellent*, tips-tips berikut mungkin bisa bermanfaat bagi yang menjadi *administratur mail server*.

1. Pastikan selalu menggunakan *strong password* untuk semua *account.* Banyak terjadi serangan *flooding email spam* karena adanya *account-account* yang *password*nya *compromise* alias mudah di*hack.* Sebagai *admin,* kita bisa memaksa penggunauntuk menggunakan *password* yang *secure*,
2. Aktifkan akses *SSL.* Untuk keamanan data, jangan gunakan *protokol imap (*Internet *Mail Accses Protocol)*, *pop3(Post Office Protocol)*dan *smtp* standar (*port* 143, 110 dan 25). Gunakan *port SSL(Secure Sockets Layer)*untuk *protokol* tersebut, yaitu *port* 995 untuk *pop3 ssl,port* 993 untuk *imaps* dan *port* 465 atau 587 untuk *smtp SSL,*
3. Aktifkan *smtp-auth* untuk pengiriman surat elektronik.*Set klien* agar menggunakan *authentikasi* pada bagian *setting smtp* sehingga *user* harus melakukan *otorisasi* sebelum melakukan pengiriman surat elektronik,
4. Batasi isian *trusted network*. Jika *ip* tertentu di*set* sebagai *trusted network*, surat elektronikdari *ip* tersebut akan diperbolehkan mengirim surat elektronik tanpa *otorisasi,*
5. Aktifkan *policyD* untuk membatasi jumlah maksimum pengiriman atau penerimaan surat elektronik dalam suatu interval waktu tertentu. Tips ini bermanfaat untuk mengantisipasi adanya *flooding spam* yang bisa berakibat *black list* terhadap *ip public* yang digunakan,
6. Tutup semua *port* yang tidak digunakan. Selain *port* untuk konsumsi publik, tutup semua *port* yang lain menggunakan *firewall.* Bisa juga membatasi akses *port* tertentu hanya untuk akses dari *ip* tertentu,
7. Ubah *port default* untuk *SSH (Secure Shell).* Gunakan *port* selain *port* 22 (misalnya *port* 8622) agar *port ssh* tidak sibuk menerima *request* akses dari *spammer,*
8. Gunakan *appliance/instance* terpisah untuk anti *spam* dan *mail server* utama. Jadi modelnya adalah *front-end back-end* sehingga jika ada serangan besar-besaran, yang akan menjadi target adalah mesin *front-end,*
9. Aktifkan *Relay Block List (RBL)online* seperti *Barracudacentral* dan *zen.spamhaus.org*. *RBL* sangat membantu dalam melakukan *verifikasi IP* yang dicurigai sebagai *spammer,*
10. Aktifkan *Sender Policy Framework (SPF)* baik untuk *incoming* maupun *outgoing.SPF* bisa mengurangi kemungkinan adanya *email forgery*, meningkatkan performa *mail server* dalam menangkal *spam* dan meningkatkan *ranking spam* dimata *mail server* lain. (Masim,2011).
    * 1. ***DKIM (DomainKeys Identified Mail)***

*DomainKeys Identified Mail (DKIM)*adalah metode untuk menghubungkan sebuah [nama *domain*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Domain_name&usg=ALkJrhgUqg66kViBGXDCnXulJ-YiI1mT6A) ke sebuah [surat](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Email_message&usg=ALkJrhhNWiA-EyK_MeFbM83LhGf66O37MQ) elektronik, sehingga memungkinkan seseorang, atau organisasi untuk mengklaim beberapa tanggung. *Verifier* pulih penandatangan [kunci publik](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Public-key_cryptography&usg=ALkJrhjPPVYn7HABuAGH2evVg8dvrDF6sw) menggunakan [*DNS*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Domain_Name_System&usg=ALkJrhjDb58NZ2nUbP7kvf30esMHYXkMHg)*,* dan kemudian mem*verifikasi* bahwa tanda tangan sesuai isi pesan yang sebenarnya itu.

Sebuah tanda tangan *DKIM* dapat menutupi bidang bidang *header* pesan, seperti *From:* dan *Subject:* bidang, dan tubuh pesan (atau bagian awal). Bidang *DKIM Signature* sendiri selalu *implisit* tertutup, dan selain tanda tangan yang tepat, berisi data lain yang diidentifikasi oleh *tag,* seperti nama *domain*, daftar bidang yang dicakup, algoritma penandatanganan, dan metode yang potongan *teks* yang disederhanakan untuk menandatangani tujuan *(*[*canonicalization*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Canonicalization&usg=ALkJrhjzVCYsbyzHIjTad1HjxhM_R3KpHA)*).* Dengan demikian, kekuatan dari *Signature DKIM* dapat disetel sehingga memungkinkan modifikasi pesan mereka yang dianggap "normal".

* + - 1. **Cara Kerja *DKIM***

*DKIM* menambahkan *"DKIM-Signature"* untuk *header email*. Bidang ini berisi tanda tangan digital dari isi surat elektronik (berdasarkan pada kedua *header* dan tubuh surat elektronik*)*. Tanda tangan ini dibuat dengan cara *SHA-enkripsi 256* di mana penggunaan terbuat dari [*RSA*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=nl&twu=1&u=http://nl.wikipedia.org/wiki/RSA_%28cryptografie%29&usg=ALkJrhhhtiFRneKnk6VRz6p24B1RzjU4Ew)untuk menangani [*enkripsi*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=nl&twu=1&u=http://nl.wikipedia.org/wiki/Encryptie&usg=ALkJrhiFZ0B_fZu2d9KLodJYbX0u4GQ1Vg) dari [kunci](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=nl&twu=1&u=http://nl.wikipedia.org/wiki/Sleutel_%28cryptografie%29&usg=ALkJrhhGB0xLe3hDj-v8fFTSNGO1Jc8Csg). Para penerima [*SMTP*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=nl&twu=1&u=http://nl.wikipedia.org/wiki/SMTP&usg=ALkJrhimO_rOp3UlktI6vEggrTOKvEXDfw) *server* menggunakan nama *domain* pengirim, *string "\_domainkey"* dan pemilih dari bidang *DKIM-Signature* ke [*DNS*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=nl&twu=1&u=http://nl.wikipedia.org/wiki/Domain_Name_System&usg=ALkJrhiTS92rITsgorevDn3qMZQpKPxg8A)meminta untuk melakukannya. Dalam menanggapi permintaan *DNS*, kunci publik *server* pengirim. Penerima menggunakannya untuk menghitung ulang tanda tangan dan membandingkannya dengan nilai yang dikirim dalam pesan. Jika dua tanda tangan pertandingan membuktikan bahwa surat elektroniktersebut benar-benar dari *domain* tersebut dan tidak disesuaikan selama transportasi. *DKIM* memblok surat elektronik "palsu". Ini menandai mereka sebagai hanya *valid,* maka *filter spam* berdasarkan surat elektronik dapat memblokir atau menduga dapat mempertimbangkan. Untuk mencegah kunci publik catatan *DKIM* dapat dimanipulasi, dianjurkan untuk *file* zona nama *domain* aman dengan menggunakan [*DNSSEC*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=nl&twu=1&u=http://nl.wikipedia.org/w/index.php%3Ftitle%3DDNSSEC%26action%3Dedit%26redlink%3D1&usg=ALkJrhh8fKdmiOTzmrxtmJkuHSvLT2Vl3w) *.*

*"DKIM-Signature"*pada kolom *header* terdiri dari daftar *"value = tag"* bagian. *Tags* pendek, biasanya hanya satu atau dua huruf. Yang paling relevan “b” untuk tanda tangan digital yang sebenarnya dari isi (*header* dan tubuh)surat elektronik, “bh” untuk *hash* tubuh, “d” untuk *domain* penandatanganan, dan “s” untuk pemilih. Parameter *default* untuk [*otentikasi*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Authentication&usg=ALkJrhiRxyZpyI8VUaw1Mq-RAFPYgADmfw) mekanisme yang menggunakan [*SHA-256*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/SHA-256&usg=ALkJrhjX_kvwfebKC9qZ1s8RYGYPbuYmXQ) sebagai [*hash kriptografi*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Cryptographic_hash&usg=ALkJrhj4cFgDbMXDpyvVZoO6J86jrhPF8Q) dan [*RSA*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/RSA_%28algorithm%29&usg=ALkJrhjAdSkvXtWU932LOKr3NDktRklP4g) sebagai [*enkripsi* kunci publik](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Public_key_encryption&usg=ALkJrhj9HBNNesg83A9lCSARVSb75XKMkg) skema, dan menyandikan *hash* di*enkripsi* menggunakan [*Base64*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Base64&usg=ALkJrhgfJB--ijBmg6NNiAHe_f0c09HqKA).

Para penerima [*SMTP*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/SMTP&usg=ALkJrhiUuh14OZ5BF8WbIiIdC4plq7VnLg) *server* menggunakan nama *domain* dan pemilih untuk melakukan *lookup DNS*. Sebagai contoh, diberikan tanda tangan.

*DKIM-Signature: v = 1, a = rsa-SHA256, d = example.net, s = brisbane,*

c = santai / sederhana, q = *dns / txt*, l = 1234, t = 1117574938, x = 1118006938,

h = dari: ke: *subjek*: *date*: kata kunci: kata kunci,

bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=,

b= dzdVyOfAKCdLX dJOc9G 2q8LoXSlEniSbav + yuU 4zGeeruD00 lszZVoG4ZHRNiYzR.

Beberapa *tag* lebih terlihat dalam contoh: “v” merupakan versi, adalah algoritma penandatanganan, “c” adalah [*canonicalization*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Canonicalization&usg=ALkJrhjzVCYsbyzHIjTad1HjxhM_R3KpHA) algoritma “s” untuk *header* dan tubuh, “q” adalah metode *query default*, “l” adalah panjang bagian di*kanonikal* dari tubuh yang telah ditandatangani, “t” adalah *timestamp* tanda tangan, “x” adalah waktu berakhir, dan “h” adalah daftar *field header* ditandatangani, diulang untuk bidang yang terjadi beberapa kali. Perhatikan bahwa *DKIM Signature* kepala bidang itu sendiri selalu *implisit* termasuk dalam “h”.

* + - 1. **Keuntungan*DKIM***

Keuntungan utama dari sistem ini untuk surat elektronik, penerima memungkinkan *domain* penandatanganan untuk terpercaya mengidentifikasi aliran surat elektronik yang sah, sehingga memungkinkan *domain* berbasis *blacklist* dan *whitelist* agar lebih efektif. Hal ini juga mungkin untuk membuat beberapa jenis dari [*phising*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Phishing&usg=ALkJrhjj2ULEY3kLFm5EZngLlccxZDrh6A) serangan lebih mudah untuk dideteksi. Ada beberapa *insentif* bagi pengirim surat elektronik untuk menandatangani surat elektronik keluar yaitu memungkinkan penurunan yang besar dalam pekerjaan penyalahgunaan meja untuk *DKIM-enabled domain* jika surat elektronik penerima menggunakan sistem *DKIM* untuk mengidentifikasi ditempa surat elektronik yang mengaku dari *domain* tersebut. Kemudian pemilik *domain* kemudian dapat fokus penyalahgunaannya energi tim pada pengguna sendiri yang benar-benar membuat penggunaan yang tidak tepat dari *domain* tersebut.

*DKIM* dapat berguna sebagai anti [*phising*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Phishing&usg=ALkJrhjj2ULEY3kLFm5EZngLlccxZDrh6A) teknologi.*Mailer* dalam *domain* berat *phising* dapat menandatangani surat mereka untuk menunjukkan bahwa itu adalah asli. Penerima dapat mengambil tidak adanya tanda tangan yang *valid* pada surat elektronik dari *domain-domain* menjadi indikasi bahwa surat itu mungkin palsu. Cara terbaik untuk menentukan *set domain* yang pantas ini tingkat pengawasan tetap menjadi pertanyaan terbuka, *DKIM* kemungkinan akan memiliki fitur *opsional* yang disebut [*ADSP*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Author_Domain_Signing_Practices&usg=ALkJrhiZYuC9eLiOCRRJGo2ml3kqtvyA1w) yang memungkinkan penulis yang menandatangani semua surat mereka mengidentifikasi diri, tetapi efektivitas pendekatan ini masih harus diuji.

**2.1.9.3. Kelamahan *DKIM***

Tanda tangan *DKIM* tidak mencakup amplop pesan, yang memegang [kembali jalan](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Return-path&usg=ALkJrhiLH0eY4v2nGCCGLK1lZZhXkDjgvw) dan penerima pesan. Karena *DKIM* tidak berusaha untuk melindungi terhadap *mis*-menangani, hal ini tidak mempengaruhi kegunaannya. Keprihatinan untuk setiap solusi *kriptografi* akan [memutar ulang pesan](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/w/index.php%3Ftitle%3DMessage_replay%26action%3Dedit%26redlink%3D1&usg=ALkJrhgY_jQXwpH4DvN6TOzjOPYNnM2nxA) penyalahgunaan, yang *bypasses* teknik yang saat ini membatasi tingkat penyalahgunaan dari *domain* yang lebih besar. *Replay* dapat disimpulkan dengan menggunakan perpesan kunci publik, pelacakan *query DNS* untuk orang-orang kunci dan menyaring tingginya jumlah permintaan karena surat elektronikyang dikirim ke milis besar atau pertanyaan berbahaya oleh aktor yang buruk. Untuk perbandingan metode yang berbeda juga menangani masalah ini melihat [surat elektronik*otentikasi*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/E-mail_authentication&usg=ALkJrhigHdsc_G2XKU0VoBbl0sB_lPts6g).

* + 1. ***SPF (Sender Policy Framework)***

*SPF* adalah *validasi* sistem [surat](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Email&usg=ALkJrhiRX6O_k9skUVpWeFJ76SIUZGR_jQ) elektronikyang dirancang untuk mencegah [*spam*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Email_spam&usg=ALkJrhg4RoSFAVJnxFL81B1Pr13IB8Js5A) dengan mendeteksi [*spoofing*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Email_spoofing&usg=ALkJrhgexDU469l9buCDvdBTFUDalsknYw), dengan memverifikasi pengirim [alamat *IP*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/IP_address&usg=ALkJrhg58DrbrcvA8i8Wg5wqwd08TqF8KA).*SPF* memungkinkan *administratur* untuk menentukan [*host*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Host_%28network%29&usg=ALkJrhgk6riBmQR_O7_TVfcxvMY3BljNFg)yang diizinkan untuk mengirim [surat](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Email&usg=ALkJrhiRX6O_k9skUVpWeFJ76SIUZGR_jQ) elektronikdari *domain* yang diberikan dengan membuat tertentu [*record SPF*](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/List_of_DNS_record_types&usg=ALkJrhgFJUqwvAoQPjgDT6k22jBWh5iysw)atau *TXT record* dalam *DNS*. [penukar [surat](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Email&usg=ALkJrhiRX6O_k9skUVpWeFJ76SIUZGR_jQ) elektronik](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Mail_exchanger&usg=ALkJrhibk_UcbZH-AYaDf5AFFzVzdfJwqw) menggunakan *DNS* untuk memeriksa surat itu dari *domain* yang diberikan adalah dikirim oleh sejumlah sanksi oleh *administraturdomain* itu.

Sebuah *record SPF* adalah *file* dalam data *DNS* dari *domain*. *Register* yang alamat *IP* yang diizinkan untuk mengirim [surat](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Email&usg=ALkJrhiRX6O_k9skUVpWeFJ76SIUZGR_jQ) elektronik dari *domain* tersebut. Jadi jika seseorang ingin [surat](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Email&usg=ALkJrhiRX6O_k9skUVpWeFJ76SIUZGR_jQ) elektronik dari *contoh@ yahoo.com,* *DNS* harus memiliki *IP* mereka terdaftar. *Mail server* menerima memeriksa *SPF* secepat[surat](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Email&usg=ALkJrhiRX6O_k9skUVpWeFJ76SIUZGR_jQ) elektronik yang ditawarkan. Jika alamat *IP* tidak cocok, isi pesan tidak bahkan *download.*

Sementara *SPF* dan *SenderID* fokus pada pengirim [surat](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Email&usg=ALkJrhiRX6O_k9skUVpWeFJ76SIUZGR_jQ) elektronik*, DKIM* melihat keaslian dari pesan itu sendiri. *DKIM* menambahkan *header* terlihat [surat](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Email&usg=ALkJrhiRX6O_k9skUVpWeFJ76SIUZGR_jQ) elektronik yang terdiri dari tanda tangan digital.

Sebuah pesan [surat](http://translate.googleusercontent.com/translate_c?depth=1&ei=8PQFUbTaH8n_rAfOq4CgBw&hl=id&prev=/search%3Fq%3Dartikel%2Btentang%2Bdkim.%2Bwikipedia%26hl%3Did%26tbo%3Dd%26biw%3D1366%26bih%3D667&rurl=translate.google.co.id&sl=en&twu=1&u=http://en.wikipedia.org/wiki/Email&usg=ALkJrhiRX6O_k9skUVpWeFJ76SIUZGR_jQ) elektronik dengan semua konten dan *header* disertakan. Jumlah yang disertakan dalam tanda tangan digital dengan cara kode. *Mail server* penerima dapat membaca sandi pesan bahwa dengan mengambil kunci publik dari data *DNS*. Sementara itu, juga menghitung ulang jumlah pesan itu sendiri. Jika dihitung jumlah yang sama dengan jumlah pada tanda tangan, pesan itu asli.

* 1. **Penelitian Sebelumnya**

Penelitian Sebelumnya dilakukan oleh Teddy, 2011 dengan judul Studi dan Implementasi Teknologi *Flashdisk* dan *Email Gateway* dalam Penyewaan Alat pada Perusahaan X. Berdasarkan penelitan yang telah dilakukan dapat disimpulkan bahwa *Email Gate*way ini memungkinkan seseorang untuk memulai sebuah *skrip* dengan mengirim surat elektronikke alamat yang ingin kita tuju. *Email Gateway* bertindak seperti penerima surat elektronik *SMTP*. Namun,selain menyimpan atau meneruskan surat elektronikyang diterimanya, *email gateway* dapat menentukan skrip apa yang harus digunakan untuk memproses pesan surat elektronik. *Skrip* tersebut digunakan untuk menerima dan memproses isi surat elektronikataupun merespon surat elektronik, *log*, dan membuat prosedur penanganan kesalahan secara otomatis, yang dapat diubah sesuai dengan keinginan pengguna. Dengan menggunakan *email gateway*, laporan transaksi dapat dikirimkan secara otomatis kepada surat elektronik*administrator*.

Penelitian Selanjutnya dilakukan oleh Jason, 2011 dengan judul *GatewayServer.* Berdasarkan penelitan yang telah dilakukan dapat disimpulkan bahwa untuk dapat terhubung ke suatu jaringan dibutuhkan adanya suatu *gateway*. *Gateway* ini dapat dianalogikan sebagai suatu pintu masuk yang harus dilewati saat ingin masuk atau pun keluar ruangan. Pada *Gateway* juga dapat dijalankan beberapa fungsi lainnya yang dijalankan secara *pararel* disamping fungsi utamanya tersebut, seperti *dhcp, proxy.* Dengan adanya *gateway server* ini, akan mempermudah *administrator* jaringan untuk memantau aliran data yang masuk dan kelauar di suatu jaringan.

**BAB III**

**GAMBARAN UMUM**

* 1. **Sejarah Perusahaan**

Usaha penambangan Batubara di Indonesia dimulai pada tahun 1849 di Pengaron, Kalimantan Timur oleh NV. Oost Borneo Maatschappij dan tahun 1888, suatu perusahaan swasta juga memulai kegiatan penambangan di Pelarang sebelah Tenggara Samarinda, dan disusul oleh beberapa perusahaan kecil lainnya.

Di Sumatera Selatan, penyelidikan secara seksama antara tahun 1915-1918 menghasilkan dibukanya Tambang Batubara Bukit Asam di Tanjung Enim, Kabupaten Muara Enim tahun 1919 dengan nama BOEKIT ASAM MIJNEM STEEN KOLEN.

* 1. **Visi dan Misi Perusahaan**
     1. **Visi Perusahaan**

PT. Tambang Batubara Bukit Asam Tanjung Enim mempunyai Visi yaitu menjadi perusahaan energi berbasis batubara yang berdaya saing dan memberikan nilai optimal bagi *Stick Holders.*

* + 1. **Misi Perusahaan**

Sesuai dengan anggaran dasar perseroan yang ada, maksud dan tujuan didirikan PTBA yaitu untuk melaksanakan program perusahaan dan menunjang kebijaksanaan dibidang pertambangan bahan-bahan galian, terutama pertambangan batubara.Dalam upaya untuk mencapai maksud dan tujuan tersebut maka telah ditetapkannya misi jangka panjang perusahaan yang berbunyi sebagai berikut;

1. Memberikan nilai jangka panjang secara maksimal dan memproduksi batubara yang bernilai tambah secara komersial. Sebagai penjabaran misi jangka panjang tersebut ditetapkan misi bisnis perusahaan 5 tahun (1999-2003),
2. Memproduksi dan memasarkan batubara dengan cara dan harga terbaik serta berkembang harmonis bersama lingkungan,

Dengan misi diatas, PTBA dituntut untuk dapat memanfaatkan seluruh sumber daya yang ada termasuk batubara yang mempunyai kualitas rendah, sehingga hal ini memberikan nilai jangka panjang perusahaan secara maksimal.

Nilai jangka panjang perusahaan mencakup semua kekayaan PTBA, seperti;

* 1. Karyawan PTBA,
  2. Teknologi dan cadangan batubara,
  3. Peralatan tambang dan fasilitas penunjangnya,
  4. Bangunan perkantoran, perumahan dan infrastruktur lainnya.
  5. **Struktur Organisasi**

Organisasi adalah bentuk kerjasama manusia dalam bentuk kelompok untuk mencari tujuan yang telah ditentukan, bukan bersifat perorangan atau pribadi melainkan koordinasi kerjasama. Beriku adalah jenis-jenis organisasi :

Organisasi Garis

Organisasi Garis adalah suatu bentuk organisasi di mana di dalam terdapat garis dan wewenang yang berhubungan langsung secara vertikal antara atasan dan bawahan. Itu semua masing-masing dihubungkan dengan suatu garis wewenang atau garis komando. Tetapi pada perusahaan besar sistem organisasi seperti ini tidak dipergunakan, karena sebagai perusahaan yang besar tentu banyak mempunyai tugas dan tanggung jawab yang sesuai bagiannya.

Organisasi Fungsional

Organisasi Fungsional adalah suatu bentuk organisasi di mana wewenang dan pimpinan tertinggi dilimpahkan kepada kepala unit yang memimpin unit-unit pelaksanaan di bawahnya dalam suatu bidang pekerjaan tertentu tiap-tiap kepala unit ini mempunyai wewenang untuk memerintah pejabat dari unit-unit pelaksana bawahannya sepanjang masih menyangkut dibidang pekerjaannya.

Organisasi Garis dan Staff

Suatu bentuk organisasi di mana pelimpahan wewenang berlangsung secara vertikal dan sepenuhnya dari pimpinan tertinggi atau langsung di bawah masing-masing Kepala Unit.

Sedangkan, satuan kerja Teknologi Informasi ini merupakan pusat informasi jaringan komputer yang menghubungkan jaringan PT Bukit Asam (Persero) Tbk secara global karena di Tanjung Enim ini terdapat  *server* utama jaringan yang menghubungkan setiap cabang yang tersebar pada beberapa daerah di Indonesia. Pada satuan ini terbagi manjadi 3 devisi yaitu divisi layanan pengguna dan aplikasi, divisi pusat operasional dan jaringan, serta divisi perancangan dan pengembangan.

* + 1. **Struktur Organisasi PT Bukit Asam (Persero) Tbk**

Sumber: PT Bukit Asam (Persero) Tbk Tanjung Enim

Gambar 3.1.Struktur Organisasi PT Bukit Asam (Persero) Tbk

# Struktur Organisasi Satuan Kerja Teknologi Informasi

Sumber: PT Bukit Asam (Persero) Tbk Tanjung Enim

Gambar 3.2. Struktur Organisasi Satuan Kerja Teknologi Informasi

Dari gambar Struktur Organisasi PT Bukit Asam (Persero) Tbk, PT Bukit Asam (Persero) Tbk di pimpin oleh seorang direktur utama dan dibantu oleh lima direktur umum yang memiliki tanggung jawab mengawasi tujuh belas satuan kerja sesuai dengan tanggung jawab yang di bebankan mereka dalam mewujudkan visi dan misi PT Bukit Asam (Persero) Tbk yang terdiri dari lina unit yaitu Unit Pertambangan Tanjung Enim, Unit Pelabuhan Tarahan, Unit Dermaga Kertapati, Unit Pertambangan Ombilin dan Unit Pengusahaan Briket.

PT Bukit Asam (Persero) Tbk Tanjung Enim saat ini sudah menjadi salah satu perusahaan yang berskala internasional yang bergerak dalam bidang pertambangan.Untuk melakukan komunikasi dengan unit pertambangan yang tersebar dibeberapa wilayah itu PTBukit Asam (Persero) Tbk Tanjung Enim menggunakan jaringan komputer.PT. Bukit Asam (Persero) Tbk saat ini telah menggunakan sistem jaringan komputer *LAN* (*Local Area Network)* yaitu sebuah jaringan di mana dapat dilakukan pengiriman data antar komputer dalam satu gedung maupun satu area kerja. Jaringan komputer *LAN* di PT Bukit Asam (Persero) Tbk Tanjung Enim dapat terhubung dengan jaringan internetdengan menggunakan *router.*

Sumber: PT Bukit Asam (Persero) Tbk Tanjung Enim

Gambar 3.3.Topologi Jaringan *WAN* PT Bukit Asam (Persero) Tbk

Sumber: PT Bukit Asam (Persero) Tbk Tanjung Enim

Gambar 3.4Topologi Jaringan PT Bukit Asam (Persero) Tbk Tanjung Enim

PT Bukit Asam (Persero) Tbk menggunakan *Switch2950, 2960, dan 3750* dan *Router Cisco 3845* untuk koneksi ke jaringan *LAN* pada PT Bukit Asam (Persero) Tanjung Enim dan *ISP* (*Internet Service Provider*) Telkom yang mempunyai kecepatan akses2048 *kbps*. Koneksi seperti ini menyebabkan semua *workstation* dapat terkoneksi ke internetselama 24 jam. Selain itu, perusahaan ini juga menggunakan jaringan *WAN (Wide Area Network)*. *WAN* terdiri dari kumpulan *LAN* dan mesin-mesin yang bertujuan untuk menjalankan aplikasi pemakai. *WAN* PT. Bukit Asam (Persero) Tbk digunakan untuk menghubungkan jaringan antara beberapa unit kerja yang tersebar di beberapa daerah.

Pada PT Bukit Asam (Persero) Tbk, surat elektronik sendiri memiliki peran penting dalam perusahaan. Penggunaan surat elektronikbagi perusahaan PT Bukit Asam (Persero) Tbk adalah sebagai roda penggerak bisnis perusahaan. Fungsi dari surat elektronikitu sendiri memiliki fungsi utamanya bagi perusahaan dan di pisahkan menjadi dua bagian yaitu fungsi internal dan fungsi eksternal*.* Fungsi internal di sini di dalamnya berisi tentang persetujuan terhadap aplikasi pengadaan. Kemudian sebagai *ERP (Enterprise Resource Planning)* adalah sistem informasi yang diperuntukkan bagi perusahan maupun jasa yang berperan meng*integrasi*kan dan mengotomasikan proses bisnis yang berhubungan dengan aspek operasi, produksi maupun distribusi di perusahaan bersangkutan. Dan surat elektroniksebagai koordinasi dan informasi dan pemberitahuan yaitu proses saling mengerti antara dua orang atau lebih untuk melaksanakan suatu hal. Proses yang harus dijalani agar suatu kegiatan dapat dilaksanakan dengan lancar ataupun jika ada masalah tidak akan terlalu banyak kesulitan dalam mengatasi pengambilan keputusan. Selanjutnya Fungsi eksternalyaitumencakup koordinasi dengan pihak terkait dalam ruang lingkup perusahaan dan pemasok barang dan jasa.

Di Satuan kerja Teknologi Informasi ini merupakan pusat informasi jaringan komputer yang menghubungkan jaringan PT Bukit Asam (Persero) Tbk Tanjung Enim secara global terdapat  *server* utama jaringan yang menghubungkan setiap cabang yang tersebar pada beberapa daerah di Indonesia. Pada satuan ini terbagi manjadi 3 devisi yaitu divisi layanan pengguna dan aplikasi, divisipusat operasional dan jaringan, serta divisiperancangan dan pengembangan.

**BAB IV**

**METODE PENELITIAN**

**4.1. Melakukan Diagnosa**

Penulis melakukan diagnosa terhadap sistem keamanan jaringan komputer padasurat elektronikdi satuan kerja Teknologi Informasi PT Bukit Asam (Persero) Tbk Tanjung Enim.Untuk mengetahui gambaran sistem keamanan jaringan yang di PT Bukit Asam (Persero) Tbk Tanjung Enim dapat kita lihat dari gambar 4.1*topologi* sistem keamanan jaringan PT bukit Asam (Persero) Tbk.

Sumber: [PT](http://www.fortinet.com) Bukit Asam (Persero) Tbk Tanjung Enim

Gambar4.1. *Topologi* Sistem Keamanan Jaringan PT Bukit Asam (Persero) Tbk

Pada gambar 4.1 dapat dilihat bahwa sistem keamanan jaringan yang ada di PT Bukit Asam (Persero) Tbk Tanjung Enim *firewall*menggunakan *DMZ FortiGate-200B* dan *ISA Server* sebagai *firewall* guna menimimalisir penyusup untuk masuk ke jaringan PT Bukit Asam (Persero) Tbk Tanjung Enim.*DMZ FortiGate-200B* ini adalah perangkat keamanan dalam bentuk penyederhanaan dari beberapa komponen penting dalam sistem keamanan jaringan yang diantaranya yaitu *firewall, UTM (Unified Threat Management), VPN (Virtual Private Network), IDS (Intrution Detection System), IPS (Intrution Prevention System)d*an *antivirus.* Kemudian dibelakang *firewall* merupakan jaringan *internal* yaitu *mail server* milikPT Bukit Asam (Persero) Tbk Tanjung Enim*.*Pada PT. Bukit Asam (Persero) Tbk, *Mail Server* yang digunakan yaitu *Exchange Server 2003. Exchange Server 2003* merupakan *Mail Server* milik perusahaan *Microsoft*. Selain itu, tiga tahun yang lalu, PT. Bukit Asam (Persero) Tbk pernah terjadi kevakuman akibat *Threat Downadup32* yang biasanya *virus* ini menyerang pada akhir tahun dengan serangan *spam* 1000/detik sehingga mengakibatkan*lock* pada *password* surat elektronik *admin* dan *user*seperti digambarkan pada gambar 4.2.

Sumber: Admin Sistem Keamanan Jaringan Komputer PT Bukit Asam (Persero) Tbk

Gambar 4.2 Penyebaran Virus *Downadup32*

Pada PT Bukit Asam (Persero) Tbk, surat elektronik sendiri memiliki peran penting dalam perusahaan. Penggunaan surat elektronikbagi perusahaan PT Bukit Asam (Persero) Tbk adalah sebagai roda penggerak bisnis perusahaan. Namun ada beberapa hal yang perlu diperhatikan mengenai keamanan jaringan pada surat elektronik selama jalannya surat elektronikmasih menggunakan jaringan internet sebagai media penghantarnya dalam pengiriman. Maka surat elektronikjuga sangat rentan terhadap celah keamanan seperti yang ada pada jaringan, terdapat banyak serangan terhadap jaringan, sehingga serangan tersebut bisa berdampak buruk bagi perusahaan dan mengakibatkan proses bisnis terjadi terhambat apabila serangan tersebut berhasil menembus keamanan pada perusahaan.Serangan yang banyak terjadi yaitu serangan *spam, phising* dan *dos*.Anti *spam* yang digunakan PT Bukit Asam (Persero) Tbk adalah penggunaan *Symantec Messaging Gateway9.5*yangdibuatuntuk melindungi sumber daya perusahaan yaitu keamanan pada surat elektronik.*Symantec Messaging Gateway 9.5*inimemiliki banyak fungsi dan fitur di dalamnya dalam mengamankan jaringan pada surat elektronik*.*PT Bukit Asam (Persero) Tbk sudah menerapkan *Symantec Messaging Gateway 9.5* ini hampir 3 tahun dalam menggunakan jasa ini. Untuk *lisensi* suatu produk ini seharga 5$ per *user*.Jumlah penggunayang menggunakan lisensi ini pada PT Bukit Asam (Persero) Tbk lebih kurang 800 *user.*

* 1. **Membuat Rencana Tindakan (Action Planning)**

Peneliti memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada. Pada tahap ini peneliti melakukan *survey* berkenaan masalah yang akan dianalisis tersebut apakah penelitian tersebut dapat dilaksanakan atau tidak di satuan kerja TI PT Bukit Asam (Persero) Tbk Tanjung Enim. Dalam hal ini penulis tertarik pada sistem keamanan jaringan pada surat elektronikyang ada di PT Bukit Asam (Persero) Tbk Tanjung Enim.Pada perusahaan PT Bukit Asam (Persero) Tbk dalam menghadapi permasalahan terhadap serangan pada jaringan terutama pada keamanan surat elektronik*.*

Yang akan dilakukan dalam rencana tindakan ini adalah;

* 1. Penulis akan menjelaskan bagaimana cara kerja dari email gatewayyaitu Symantec Message Gateway 9.5yang digunakan oleh PTBA dalam mengamankan surat elektronikperusahaan,
  2. Kemudian bagaimana konfigurasi sistem yang digunakan,
  3. Serta melakukan pengujian terhadap sistem tersebut pada jaringan PTBA,
  4. Dengan melakukan rencana tindakan ini penulisakan mendapatkan hasil yang didapat berupa report dari sistem tersebut dan kemudian hasil report itu dilanjutkan dengan evaluasi.
     1. **Mengetahui Cara Kerja *Symantec Message Gateway 9.5***

Berikut adalah gambar *Mail Infrastruktur*PT Bukit Asam (Persero) Tbk serta bagaimana cara kerja *Symantec Message Gateway 9.5* dalam mengamankan sebuah surat elektronik.

Gambar 4.3.*Mail* Infrastruktur PT Bukit Asam (Persero) Tbk

Yang akan dilakukan pada tahap ini yaitu;

* + 1. Mengetahui bagaimana cara kerja dari sistem tersebut,
    2. Serta bagaimana tahapan-tahapan dalam mengamankan sebuah pesan.
    3. **Konfigurasi*Symantec Messaging Gateway 9.5***

Konfigurasisuatu sistem merupakan kewajiban yang harus dilakukan.Dengan melakukan konfigurasiini seorang *admin* dapat mengatur kebijakan yang dibuat sesuai dengan kepentingan yang digunakan guna untuk melindungi sumber daya perusahaan yang mereka kelola.

Yang akan dilakukan pada tahap ini yaitu;

* + - 1. Konfigurasi*Symantec Messaging Gateway 9.5*dalam mengatur koneksi pada *SMTP (Simple Mail Transfer Protokol),*
      2. Kemudian konfigurasi*feature*pada*Symantec Messaging Gateway 9.5.*
      3. **KonfigurasiKoneksi*SMTP Pada Symantec Messaging Gateway 9.5***

*SMTP(Simple Mail Transfer Protokol)* merupakan *protokol* yang digunakan sebagai pengelola dan pengatur lalu lintas keluar masuk surat elektronikpada suatu jaringan. *SMTP* berada pada *layer* aplikasi dengan *port* 25. Fungsi utama dari *SMTP* adalah menyampaikan pesan dari komputer pengirim ke komputer penerima, baik dalam jaringan yang sama*LAN* atau *WAN* maupun ke komputer penerima dalam suatu jaringan yang berbeda.

* + - 1. **Konfigurasi *Feature Pada Symantec Messaging Gateway 9.5***

*Symantec Message Gateway*9.5 mencakup beberapa fitur untuk memberikan perlindungan serta fitur penyaringan dan membuatnya lebih mudah untuk mengontrol data.Sehingga *administratur* dapat dengan mudah membangun kebijakan yang efektif dalam menegakkan suatu kepatuhan terhadap peraturan untuk melindungi terhadap hilangnya data-data penting.

*Symantec Messaging Gateway*9.5 juga termasuk dukungan *IPv6.*Dukungan *IPv6* adalah revisi keenam untuk *Internet Protocol* dan merupakan penerus dari *IPv4*. Kedua *protokol* tersebut menyediakan alamat *IP address* untuk perangkat yang terkoneksi ke internet. Namun bahwa [*IPv6*](http://www.ewawan.com/apa-itu-ipv6.html)bisa menampung jumlah *IP address* yang jauh lebih besar. Sebuah perbedaan yang signifikan antara *protokol IPv6* dan *IPv4* adalah struktur mereka berbeda dengan ruang alamat 32-*bit* lebih kecil dari *protokol IPv4*.*IPv6* menyediakan ruang 128-*bit* cukup besar.Hal ini memungkinkan pelanggan untuk memproses, memindai dan melaporkan pada lalu lintas surat elektronikberbasis *IPv6*.

* + 1. **Pengujian**

Penetrasi pengujianuntuk sistem komputermerupakan kunci untuk keberhasilan dalam perlindungan jaringan komputer. Pengujian memungkinkan perusahaan atau individu dengan beberapa komputer pada jaringan yang sama untuk melindungi komputer mereka dan untuk mencegah bahaya dari luar yang mempengaruhi sistem mereka.

Gambar 4.4.JaringanPT Bukit Asam (persero)Tbk Tanjung Enim

Yang akan dilakukan pada tahap ini yaitu;

* + - * 1. Melakukan pengujian pengiriman pesan melalui *Symantec Messaging Gateway,*
        2. Kemudian melakukan pengujian terhadap jaringan PTBA.
      1. **Pengujian Pengiriman Pesan Melalui *Symantec Message Gateway 9.5.***

Pada *Symantec Message Gateway9.5* ini terdapat 3 cara dalam melakukan penyampaian pesan dari *Symantec Message Gateway.* Yaitu di mana pesan yang disimpan dalam *spam* karantina untuk sehingga dengan melakukan pengujian ini kita dapat melihat hasil penyaringansurat elektronikitu sendiri.

* + - 1. **Pengujian Terhadap Jaringan PT. Bukit Asam (Persero) Tbk**

Untuk mengetahui apakah kemanan jaringan telah bekerja dengan baik atau tidak dalam mengamankan sistem keamanan jaringan PT Bukit Asam (Persero) Tbk Tanjung Enim, sehingga dapat mengetahui efektif atau tidaknya penerapan perangkat tersebut dengan melakukan penetrasi terhadap *server,* melalui beberapa trik pentrasi untuk menguji adakah celah pada sistem keamanan PT Bukit Asam (Persero) Tbk Tanjung Enim. Penetrasi pengujiansistem jaringan komputer adalah kunci keberhasilan untuk mengetahui kekuatan perlindungan jaringan komputer.

* + 1. **Hasil *Report* Dari Pem*filter*an *Email***

Hasil *report*merupakan kumpulan data yang di dapat dari sistem itu sendiri dalam melakukan pengamanan terhadap jaringan terutama pada surat elektronik.

Yang akan dilakukan pada tahap ini yaitu penulis akan mengevaluasi terhadap *report*yang di dapat.

Gambar 4.5.Status *report filter email*

Hasil *report* ini nantinya berisi tentang jenis-jenis serangan yang terdapat pada surat elektronikyang berhasil disaring*.*Pada *report* ini nanti akan tampil banyak jenis serangan yang didapat. Dari serangan inilah yang dapat merusak sistem keamanan jaringan apabila serangan tersebut berhasil menembus ke dalam sistem tersebut.

**BAB V**

**HASIL DAN PEMBAHASAN**

* 1. **Hasil Melakukan Tindakan *(Action Taking)***

Penelitimelakukan analisis sistem keamanan jaringan komputer menggunakan *email gateway*dalam dalam hal peningkatan sistem keamanan jaringan terutaman pada kemanan surat elektronikPT Bukit Asam (Persero) Tbk Tanjung Enim.

**5.1.1. Mengetahui Cara Kerja *Symantec Message Gateway 9.5***

Gambar 5.1.Cara Kerja*Symantec Message Gateway 9.5*

Pada gambar 5.1 terdapat 2 bagaimana cara pengiriman surat elektronik pada jaringan komputer*.* Pada contoh yang pertama, pada sebuah *user*akan mengirimkan sebuah surat elektronikmenuju ke *mail server*, kemudian surat elektroniktersebut akan memasuki gerbang *Symantec Message Gateway* tanpa melewati terowongan *TLS (Transport Layer Security)*. Selanjutnya *email* tadi langsung diteruskan tanpa di*encryption*dan tidak membawa *signature* atau *domain* dari *mail server*. Pada contoh ini merupakan contoh pengiriman surat elektronikyang tidak aman.

Kemudian contoh selanjutnya pada *Customer Network*, setiap *user* mengirimkan sebuah surat elektronik menuju ke *Mail Server,* di dalam *mail server* ini terdapat *DKIM(DomainKeys Multi Domain)dan SPF (Sender Policy Framework). S*elanjutnya surat elektronik tersebut menuju gerbang *Symantec Message Gateway* dan melewati terowongan *TLS (Transport Layer Security)* yang berfungsi untuk meningkatkan keamanan antara komunikasi *klien* dan *server*. Selanjutnya pesan tersebut die*ncription*. Pada *MailInfrastruktur* PT Bukit Asam (Persero) Tbk menggunakan *Symantec Content Encryption*dalammembantu menjaga kerahasiaan data penting dalam bertukar informasi dengan pelanggan dan mitra bisnis melalui surat elektronik*.Symantec Content Encryption*, yang disediakan oleh *Symantec Hosted*merupakan layanan, yang menyediakan cara mudah untuk mengontrol surat elektronik*.* Memanfaatkan industri terkemuka dari *Message Labs hostinfrastruktur*merupakan*host* yang sepenuhnya menggunakan layanan yang tidak memerlukan investasi *infrastruktur* tambahan, terlepas dari ukuran penyebaran. *Symantec Messaging Gateway* dengan *Symantec Content Encryption* dapat menghemat waktu dan sumber daya yang sebelumnya digunakan mencoba untuk memonitor lalu lintas surat elektronikdengan biaya rendah, jumlah kepemilikan diprediksi. Setelah pesan di*encryption*, apakah kata kunci yang ada dalam pesan tersebut pada saat dikirimkan sesuai maka pesan tersebut akan diteruskan menuju ke *klien,* akan tetapi masih melewati *Symantec Messaging Gateway*. Apabila pesan tadi pada saat di*encryption* tidak sesuai dengan kata kunci yang dibuat oleh *user,* maka pesan tersebut dimasukkan pada *Spam* Karantina. *Symantec.cloud*merupakan pilihan terbaikbagi pelangganyang tertarikdalam penawaranberbasis *cloud* dalam keamanan surat elektronikyang dikelolaoleh*Symantec.SymantecEmailSecurity.cloud*tidak memerlukan perangkat kerasatau perangkat lunak. Bagian daripendekatan terpadu yaitu untukmengamankandan mengelolasurat elektronik*, web,*dan lalu lintaspesan instan. *EmailSecurity.cloud*mencakup*SLA*industri terkemukayang mencakupperlindunganterhadap virusyang tidak dikenaldan *spam*.

Selanjutnya setelah mengetahui bagaimana cara kerja dari *Symantec Message Gateway 9.5* maka yang dilakukan selanjutnya adalah melakukan suatu konfigurasi pada *Symantec Message Gateway 9.5*

* + 1. ***Konfigurasi Symantec Messaging Gateway 9.5***

Berikut adalah carakonfigurasi *Symantec Messaging Gateway 9.5* dalam mengatur koneksi pada *SMTP (Simple Mail Transfer Protokol) dan* Konfigurasi *pada fitur Symantec Messaging Gateway 9.5.*

* + - 1. ***Konfigurasi* Koneksi*SMTP Pada Symantec Messaging Gateway 9.5***

Berikut adalah langkah-langkah untuk mengkonfigurasi*Symantec Message Gateway* untuk koneksi *SMTP (Simple Mail Transfer Protokol);*

Untuk memulaikonfigurasiyaitu dengan melakukan*Login* ke *Web Symantec Message Gateway* 9.5,

Gambar 5.2. L*ogin* ke *Web Symantec Message Gateway 9.5*

Layar *login*akan tampil ketika *Symantec Messaging Gateway* dijalankan. Layar ini dimaksud agar tidak semua orang dapat menggunakan aplikasi yang tersedia.Sehingga data-data dapat terlindungi dan terjamin keamanannya.Pada layar *login* sebelum memasuki program terdapat konten yang wajib di isi diantaranya berisi *user name* dan *password.*

Kemudian pilih pada tombol *Administration* pada menu paling kanan*,*

Gambar 5.3. *Administration*

3. Pilihpada bawah *link Certificates* padamenu kiri bagian bawah,pilih *Settings header* di *sidebar,*

Gambar 5.4. *Setting*

1. Pada halaman *Certificate Settings*, pilih pada salah satu tombol *Import* atau *Add* untuk pengaturan*sertifikat* pada *server Symantec Message Gateway 9.5*,

Gambar 5.5.*Certificate Settings*

1. Pilih pada *linkConfiguration*pada*headerHost* di *sidebar* di menu bawah bagian kiri,

Gambar 5.6. *Hosts*

1. Pilih pada *Scanner*yang ingin dirubah,

Gambar 5.7. *Host Configuration*

1. Pilih *tab SMTP (Simple Mail Transfer Protocol),*

Gambar 5.8. *Edit Host Configuration*

1. Di bawah *Inbound Mail Settings*centang kotak *Accept TLS (Transport Layer Security)encryption*dan pilih sertifikat dari daftar*drop-down,*

Gambar 5.9*Inbound Mail Setting*

1. Kemudian pilih tombol *Save*di bagian bawah halaman untuk menyimpan konfigurasitersebut.

Setelah melakukan konfigurasi pada koneksi *SMTP*, selanjutnya yaitu konfigurasi fitur yang ada pada *Symantec Message Gateway* 9.5.

* + - 1. ***Konfigurasi Feature Pada Symantec Messaging Gateway 9.5***

*Symantec Message Gateway*9.5 mencakup beberapa fitur untuk memberikan perlindungan serta fitur penyaringan dan membuatnya lebih mudah untuk mengontrol data. Sehingga *administratur* dapat dengan mudah membangun kebijakan yang efektif dalam menegakkan suatu kepatuhan terhadap peraturan untuk melindungi terhadap hilangnya data-data penting. Pada fitur menu *Symantec Message Gateway 9.5* terdapat menu yang dapat digunakan.Konfigurasi pada fitur *Symantec Message Gateway 9.5* ini sangat penting, kerena dengan dilakukan *konfigurasi* agar kinerja dari *Symantec Message Gateway 9.5* ini dapat bekerja dengan baik dalam menagamankan surat elektronik yang keluar maupun masuk.Berikut adalah carakonfigurasi fitur penting pada *Symantec Messaging Gateway 9.5;*

Konfigurasi*Customer-specifik Spam submission* yaitu mengikuti kepatuhan dalam melakukan pendaftaran perangkat *customer*, di mana dalam mendaftarkan perangkat ini kita akan mendapatkan aturan langsung dari *Symantec.* Pilih menu *"Spam"* menu dari atas halaman kemudian di bawah menu *"Settings"* dari menu di bagian kiri, pilih *" Submission Settings "* seperti yang Anda lihat pada gambar 5.10,

Gambar 5.10.*Submission Settings*

Pada gambar “*Customer-specifik Spam submission”* terdapat *coloumns “EnableCustomer-specifik Spam submission”* untuk memungkinkan menggunakan fitur ini. Selanjutnya pada “*Configuration”*akan mendapatkan *ID* dari *Symantec* setelah melakukan *register*. Kemudian pilih *“Register for a New Submitter ID Now”,*

Pada saat melakukan *register,* akan tampil *Pop Up*, yaitu perintah untuk *Privacy Policy*, agar *costumer* menyetujui dalam mengaktifkan fitur *Symantec Messaging Gateway 9.5 ini,*

Gambar 5.11. *Spesifik Spam Submission*

Pada *pop up* perintah *Privacy Policy*pilih*“ I agree to teterm of this privacy policy”,* kemudian pilih*“EnableCustomer-specifik Spam submission”,*

* + 1. Pada proses mendaftarkan perangkat ini ke *Symantec* akan memakan waktu,

Gambar 5.12. *Submitter ID Registration*

Pada gambar di atas adalah proses masa *registrasi ID Costumer,*

Gambar 5.13. *Registration Completed*

Setelah proses masa *registrasi,* terlihat pada gambar bahwa *Costumer* berhasil dalam melakukan *registrasi* dalam mengaktifkan fitur ini,

* + 1. Berikut adalah tampilan *Customer-specifik Spam submission* yang telah terdaftar,

Gambar 5.14. *Submission Setting*

Pada gambar di atas terdapatperintah untuk melakukan kebijakan keamanan yang terdapat di bawah *Customer-specifik Spam submission.administratur*selanjutnya melakukan *Customer-specifik Spam policy.* Maka yang dilakukan *Administratur* yaitu membuat suatu kebijakan dengan memilih *“Click here to configure”,*

* + 1. Pada*Customer-specifik Spam submission setting* di sini *Admin* dapat mengatur siapa yang dapat mengirimkan pesan. Ada dua cara untuk mengidentifikasi. Dengan pengaturan *default, administratur* dan pengguna yang terdaftar dapat mengirimkan pesan dan pilihan kedua adalah untuk memblokir pengguna terdaftar untuk mengirimkan pesan seperti pada gambar 5.15. Dengan cara Anda juga dapat mengimpor daftar Anda untuk mengizinkan atau memblokir mengirimkan pesan,

Gambar 5.15. *Subbmitters List*

* + 1. Sekarang, kita harus memilih kebijakan untuk mengaktifkan *"Submissions Customer*" sebelum mengirimkan pesan apapun. Untuk melakukannya, pilih menu *"Spam"* dari menu atas maka Anda akan melihat 4 kebijakan dimulai dengan "*Customer Spesifik Spam"tag*. Anda dapat memodifikasi subjek, menghapus, karantina atau menyampaikan pesan secara normal,

Gambar 5.16. *Customer Spesifik Spam*

* + 1. Untuk mengaktifkan salah satu kebijakan, pilihsaja dan memilih kelompok kebijakan di bawah ini untuk menerapkannya ke grup berikut,

Gambar 5.17. *Setting Email Spam Policy*

* + 1. Selanjutnya setelah melakukan pemilihan salah satu kebijakan, pilih tombol *save*. Setelah memilih*save* akan tampil kebijakan yang sudah diterapkan tadi pada gambar 5.18,

Gambar 5.18. Tampilan *Email Spam Policy*

**5.1.3.Pengujian**

Tujuan pengujianpada jaringan komputermerupakan kunci keberhasilan dalam perlindungan pada jaringan komputer.

* + - 1. **Pengujian Pengiriman Pesan Melalui *Symantec Message Gateway 9.5.***

Pada *Symantec Message Gateway9.5* ini terdapat 3 cara dalam melakukan penyampaian pesan dari *Symantec Message Gateway.* Yaitu di mana pesan yang disimpan dalam *spam* karantina,sehingga dengan melakukan pengujian ini kita dapat melihat hasil penyaringansurat elektronikitu sendiri.

Dilakukan dengan cara meng*upload* pesan dengan secara manual. Yaitu dengan cara memilih menu *“Spam”* kemudian pilih *“Submission”* di menu bagian kiri. Setelah itu *“send message”,*

Gambar 5.19*Subbmit A Message*

Pada gambar di atas untuk meng*upload* sebuah *file*, pada *submission content* tinggal masukkan data dengan cara *“Browse”.* Atau bisa dengan mengetikkan pada “*Paste a Message”*. Kemudian kirim pesan tersebut,

Pada pilihan kedua dapat menggunakan pada menu *“Content”* pilih *“Incident management”,* setelah itu pilih *“Quarantine Incidents”,*

Gambar 5.20. *Quarantine Incidents*

Pada gambar *“Quarantine Incidents”* merupakan kejadian yang dikarantina, untuk menyerahkan pesan tersebut kepada *Symantec* dengan mengklik tombol *“This is Spam”* atau *“This is Not Spam”.* Di *“Quarantine Incidents”*di sana terdapat *columns* yang diisi dari status, kepada siapa pesan itu dikirimkan kemudian kebijakan yang ditentukan,

Selanjutnya pada pilihan pengiriman terakhir yaitu adalah mengirimkan dari karantina *spam* yang dapat akses melalui menu *Spam Message Quarantine,*

Gambar 5.21. *Spam Message Quarantine*

Pada gambar di atas terdapat pilihan *Delete, Delete All, Relasse, This is Spam, This is Not Spam* dan *Show Filter*. Kemudian *“to”* untuk siapa pesan tersebut, *subjek* nama pesan yang akan dikirim,

Pada saat kita memilih pesan tersebut dengan memilih *“This is Spam”* maka akan muncul konfirmasi sebelum mengirimkan pesan yang dapat dilihat pada gambar 5.22,

Gambar 5.22. *Submit as Spam*

Pada saat kita memilih “*Submit as Spam”.* Maka setelah itu kita dapat melihat bahwa pesan berhasil disampaikan,

Gambar 5.23. *Message Successfully*

Langkah terakhir untuk melihat status kiriman. Pada menu pilih*"Status*kemudian pilih “*Submissions*” pada menu dibagian kiri, setelah itu pilih “*Detail Submission",*

Gambar 5.24. *Status*

Pada gambar di atas merupakan status kiriman yang dapat dilihat pada komputer *administratur.* Pada status di *dashboard* merupakan gambaran dalam bentuk grafik jumlah serangan yang berhasil disaring oleh *Symantec Message gateway,* pada hasil serangan yang didapat,akan dibahas pada pembahasan *subreport,*

Kemudian pada status di “*Submission”* merupakan pilihan untuk melihat rincian penyaringan secara rinci dalam melihat kiriman.*Administratur* dapat memantau jumlah pesan, waktu pengiriman pesan, siapa dan kepada siapa pesan tersebut disampaikan,

Gambar 5.25. Tampilan *Filter*

Kemudian pada *Submission detail*, merupakan untuk melihat ringkasan dan sejarah tentang apa yang terjadi pada pengiriman setelah kita kirimkan,

Gambar 5.26. *Submission Details*

Pada gambar di atas merupakan rincian pesan yang dapat dilihat oleh *administratur.*Pada *“Submission Detail”* yang mengrimkan pesan.Yang memiliki *ID* ini hanya untuk karyawan PTBA saja.

* + - 1. **Pengujian Terhadap Jaringan PT. Bukit Asam (Persero) Tbk**

Untuk mengetahui apakah kemanan jaringan telah bekerja dengan baik atau tidak dalam mengamankan sistem keamanan jaringan PT Bukit Asam (Persero) Tbk Tanjung Enim, sehingga dapat mengetahui efektif atau tidaknya penerapan perangkat tersebut dengan melakukan penetrasi terhadap *server,* melalui beberapa trik pentrasi untuk menguji adakah celah pada sistem keamanan PT Bukit Asam (Persero) Tbk Tanjung Enim. Tahapan untuk melakukan pengujian adalah sebagai berikut;

*TargetScoping,*

Sebelum memulai penilaian keamanan teknis,yang terpenting adalah untuk mengamati dan memahami ruang lingkup yang diberikan dari lingkungan jaringan target. Hal ini juga penting untuk mengetahui bahwa ruang lingkup dapat didefinisikan untuk entitas tunggal atau *set* entitas yang diberikan kepada auditor. Apa yang harus diuji, bagaimana harus diuji, kondisi apa harus diterapkan selama proses pengujian, apa yang akan membatasi pelaksanaan proses pengujian, berapa lama waktu yang dibutuhkan untuk menyelesaikan tes, dan apa tujuan bisnis yang akan dicapai, yang semua kemungkinan garis yang harus diputuskan di bawah target *scoping.*Untuk memimpin sebuah pengujian penetrasi sukses, auditor harus menyadari teknologi yang sedang dinilai, fungsi dasar, dan interaksi dengan lingkungan jaringan.Di bawah ini merupakan alamat *web* PT Bukit Asam (Persero) Tbk, melalui *web* ini kita dapat menganalisis celah dari sistem keamanan jaringan yang ada pada perusahaan ini.

Sumber: bukitasam.co.id

Gambar 5.27. *Web* PT Bukit Asam (Persero) Tbk

* + - 1. *DNS Information,*

Untuk mengetahui *DNS Information* ada beberapa *tool* yang dapat dilakukan. Namun, penulis hanya menggunakan *tooldnswalk* dan *dnsenum*. Dengan menjalankan perintah ./*dnswalk ptba.co.id* dan ./*dnsenum.pl ptba.co.id* maka, dapat kita lihat *DNS Information* pada terminal *OS BackTrack* 5 seperti gambar di bawah ini:

Sumber: *BackTrack 5*

Gambar 5.28. *Output* pada Perintah *dnswalk*

Pada Gambar 5.28 merupakan tampilan perintah *dnswalk.* Di sana terdapat *dns* bernama *ns1.djamoer.com. DNS (Domain Name Service)* merupakan layanan di internet untuk jaringan yang menggunakan *TCP/IP.* Layanan ini digunakan untuk mengidentifikasi sebuah komputer dengan nama bukan dengan menggunakan alamat *IP address*. Singkatnya *DNS* melakukan konversi dari nama ke angka. *DNS* dilakukan secara *desentralisasi*, dimana setiap daerah atau tingkat organisasi memiliki *domain* sendiri.Masing-masing memberikan servis *DNS* untuk *domain* yang dikelola.

Sumber: *BackTrack 5*

Gambar 5.29. *Output* pada Perintah *dnsenum*

Sumber: *BackTrack 5*

Gambar 5.30. *Output*pada Perintah*dnsenum*

Pada gambar di atas merupakan tampilan dari perintah *dnsenum*. Kita ketikkan perintah *./dnsenum.pl ptba.co.id* maka akan tampilan seperti gambar di atas. Di sana dapat kita ketahui nama *host* pada ptba, *IP address* yang digunakan, kemudian *name server* serta *mail server* ptba. Dari hasil gambar di atas maka, dapat terlihat celah yang bisa dimanfaatkan untuk menorobos sistem keamanan jaringan PT Bukit Asam (Persero) Tbk, yang mana dalam melakukan penetrasi penulis memanfaatkan *IP* yang tertera pada gambar tersebut yaitu *IP Host’s Address* dan *Name’s Server*.

* + - 1. *Enumerating Target,*

Untuk mengetahui *Enumerating Target* PT Bukit Asam (Persero) Tbk, penulis melakukan *Nmap* dan *Zenmap* pada *IP Host’s Address* dan *IPName’s Server* mereka dengan menjalankan perintah seperti gambar5.31,

Sumber: *BackTrack 5*

Gambar 5.31.*Output nmap* ptba.*co.id*

Pada gambar 5.31 merupakan cara melakukan *Enumerating Target* PT Bukit Asam (Persero) Tbk dengan menggunakan perintah *nmap ptba.co.id* pada layar terminal. Pada saat di *enter* maka akan tampil dimana *port* mana saja yang terbuka pada ptba. Pada *port* inilah kita menemukan celah pada target yang dapat dimanfaatkan.

Sumber: *BackTrack 5*

Gambar 5.32. *Output Zenmap* pada *host addressptba.co.id* pada *ip* target

202.158.49.50

Sumber: *BackTrack 5*

Gambar 5.33. *Output Zenmap* pada *host addressptba.co.id*dan *name server*

*ns1.djamoer.com* pada *ip* target 106.187.51.200

Pada gambar 5.33 merupakan tampilan teknik ke 2 menggunakan *zenmap* pada *host server ptba.co.id* dan *name server ns1.djamoer.com* pada *ip* target 106.187.51.200. Di sana juga terdapat lebih rinci *port – port* yang terbuka yang dapat dimanfaatkan untuk mencari celah pada *port* yang terbuka tadi. Yang akan kita coba untuk mencari celah yaitu pada *port* 21 yaitu *FTP (File Transfer Protocol), port* 443 *SSL*, dan *port* 8080.

Sumber: *BackTrack 5*

Gambar 5.34. *Output* [*ftp.bukitasam.co.id*](ftp://ftp.bukitasam.co.id)

Pada gambar 5.34 kita mencoba melakukan *browser* pada *port* 21 yaitu *FTP (File Transfer Protocol)* yang merupakan *Protokol* standar untuk kegiatan lalu lintas *file (upload* maupun *download)* antara dua komputer yang terhubung dengan jaringan internet. Pada saat melakukan *browsing* pada [*ftp.bukitasam.co.id*](ftp://ftp.bukitasam.co.id) tidak bisa dilakukan, *ftp* bukitasam ptba hanya bisa diakses pada jaringan internal saja.

Sumber: *BackTrack 5*

Gambar 5.35. Tampilan *ip* 106.187.51.200 pada *port*443

Sumber: *BackTrack 5*

Gambar 5.36. Tampilan *ip* 106.187.51.200 pada *port*8080

Kemudian kita mencoba lagi membuka pada *port* 8080 pada *ip* 106.187.51.200 yang merupakan *dns* dari ptba.Pada gambar 5.36 terdapat *name server main.djamoer.com* yang hanya diakses pada *https*.

Sumber: *BackTrack 5*

Gambar 5.37. Halaman *login Admin* di *ISPConfig* pada alamat

[*https://main.djamoer.com*](https://main.djamoer.com) pada *port* 8080

*ISP (Internet service provider)* adalah penyedia layanan internet*.* Sebagian besar *ISP* mempunyai jaringan *server (mail, berita, Web), router,* modem yang dihubungkan dengan koneksi *“backbone”* internet yang permanen dan berkecepatan tinggi. Pelanggan *ISP* dapat mendapatkan koneksi internetdengan modem dan telepon. Untuk mengakses internet pelanggan *ISP* harus melakukan *dial* ke jaringan dengan menekan nomor telepon tertentu milik *ISP*.Pada gambar di atas kita berhasil menembus dan mencari celah dari keamanan jaringan ptba. Apabila celah ini dimanfaatkan oleh orang yang tidak bertanggung jawab, maka besar kemungkinan jaringan ptba akan*crash.*

* + - 1. Melakukan Serangan *Spam*,

Untukmelakukan serangan ini,kita masukkan alamat situs [*www.anonymailler.net*](http://www.anonymailler.net)*.* Alamat ini berisi tentang bagaimana cara kita melakukan serangan *spam* dengan mudah kepada target yang kita inginkan. Berikut adalah tampilan *form* yang akan diisi sebelum mengirimkan pesan tersebut kepada target.

Gambar 5.38. Isi *Form*

Pada gambar 5.38 kita bisa lihat terdapat *form* yang harus diisi. Pada “*FromName”* diisikan nama tampilan pesan yang kita inginkan, pada *From Name* kita isi dengan “Dari *Spam*”. Selanjutnya pada *From Name* yaitu isi dengan alamat surat elektronik yang kita kehendaki supaya tidak diketahui dari mana asal surat elektronik yang kita kirimkan. Kemudian *To Email* yaitu tujuan surat elektronikyang akan kita serang. Pada *subject* isikan dengan judul surat elektronikkita. Sebagai contoh di atas kita isi dengan Penetrasi *Spamming.*Setelah mengisi *form* tersebut kemudian masukkan kode, selanjutnya pilih *Submit.*

Gambar 5.39. Gagal Mengirim Pesan

Pada gambar 5.39 merupakan tampilan konfirmasi pengiriman pesan yang gagal, tidak dapat melakukan serangan terhadap *mail server* milik ptba pada saat akan mencoba mengirimkan. Karena *mail server* milik ptba merupakan *mail server* yang dapat diakses pada jaringan internal saja.

Selanjutnya penulis mencoba melakukan serangan *spam* kepada alamat target yang lain.

Gambar 5.40. Isi *Form*

Pada gambar 5.40 penulis mencoba melakukan serangan *spam* terhadap alamat target yang lain. Setelah mengisi *form* tersebut kemudian masukkan kode, selanjutnya pilih *Submit.*

Gambar 5.41. Masukkan Kode

Gambar 5.42 Pesan berhasil dikirimkan

Gambar 5.43. Tampilan *email* target yang dikirim *spam*

Pada gambar 5.43 merupakan tampilan surat elektronik target yang telah kita kirim serangan berupa *spam*. Pada menu surat elektronikterdapat menu sampah, di sana dapat kita lihat serangan yang kita kirimkan tadi masuk dalam menu sampah dengan nama penetrasi *spam.*

* + - 1. Melakukan Serangan *Dos* Terhadap *Mail Server* PT. Bukit Asam (Persero) Tbk

Untuk melakukan serangan ini, penulis memakai operasi sistem *Backtrack 5,* menggunakan terminal dengan mengetikkan perintah *ping mail.ptba.co.id* dan *ping –s 10000 mail.ptba.co.id* pada gambar 5.44*.*

Gambar 5.44. Melakukan *ping* pada situs *mail.ptba.co.id*

Pada gambar di atas merupakan cara untuk *ping* pada situs *mail.ptba.co.id*penulis melakukan *ping* pada *IP Host’s Address* dan *IPName’s Server* mereka dengan menjalankan perintah *ping mail.ptba.co.id.* di sana terdapat ip target 74.125.31.121. Selanjutnya terdapat pengiriman paket sebanyak 64 *bytes* kepada *tb-in-f121.le100.net* pada *ip* 74.125.31.121 dengan waktu tempuh penerimaan paket 109 *ms.* Berikut adalah cara melakukan serangan *Dos* dengan pengiriman sebanyak 10000 paket.

Gambar 5.45. Melakukan *ping –s 10000*pada situs *mail.ptba.co.id*

Pada gambar di atas merupakan cara untuk *ping –s 10000* pada situs *mail.ptba.co.id*penulis melakukan *ping* pada *IP Host’s Address* dan *IPName’s Server* mereka dengan menjalankan perintah *ping –s 10000 mail.ptba.co.id.* di sana terdapat *ip* target 74.125.31.121. pada saat kita mengetikkan perintah di atas tadi dengan memasukkan *–s* 10000 yaitu perintah untuk melakukan serangan *Dos(Denial of Service)* atau bentuk penyerangan dengan membanjiri *(flood)* jaringan dengan data yang sangat besar atau dengan sengaja menghabiskan sumber daya yang memang terbatas, seperti *pending network connection.*Selanjutnya pada gambar di atas terdapat pengiriman paket sebanyak 10008 *bytes* kepada *tb-in-f121.le100.net* ttl=55 dengan waktu tempuh penerimaan paket 235*ms* dan seterusnya bisa sampai 292 *ms.* Dengan melakukan serangan ini, apabila seseorang ingin mengakses situs *mail.ptba.co.id* akan merasa lama saat melakukan *browsing*.

* + - 1. Melakukan Serangan *Phising* Terhadap *WebMail Server* PT. Bukit Asam (Persero) Tbk.

Untuk melakukan serangan ini, penulis memakai operasi sistem *Backtrack 5,* menggunakan *tools* yang ada dalam *Backtrak 5* ini yaitu *Social Enginnering Tools*yang dapat dilihat pada gambar 5.46,

Gambar 5.46. Menggunakan *Social Enginnering Tools*

untuk melakukan *phising.*

Pada gambar di atas merupakan tampilan di terminal pada saat kita membuka *Social Enginnering Tools*pada *Backtrack 5.* Pada tampilan di atas terdapat 3 pilhan untuk melakukan serangan, terdapat yaitu *Automatic, Manual* dan *Continue using SET (NO UPDATES ANYMORE!).*Untuk melakukan serangan *phising* ini pada *web mail server ptba*, langkah pertama yang kita pilih adalahnomor 2. *Manual* yaitu melakukan serangan dengan teknik “*manual”*. Kemudian tekan *enter* untuk melakukan perintah selanjutnya.

Gambar 5.47. *Press (return) to continue to use SET*.

Gambar 5.4. *Press (return) to continue to use SET*.

Gambar 5.48. *Social-Engineering Attacks*

Pada gambar di atas, kita disuruh untuk memilih menu untuk melakukan serangan. Untuk melakukan serangan *phising* ini kita pilih menu nomor 1 yaitu *Social-Engineering Attacks.* Selanjutnya tekan *enter* untuk melanjutkan perintah selanjutnya.

Gambar 5.49. *Website Attack Vectors*

SelanjutnyaPada gambar di atas, terdapat banyak pilhan menu jenis serangan yang akan dipilih ada 11 menu. Untuk melakukan serangan *phising*terhadap *website.* kita pilih menu nomor 2 yaitu *Website Attack Vektors* yaitu kita akan melakukan serangan pada sebuah *website.* Selanjutnya tekan *enter* untuk melanjutkan perintah selanjutnya.

Gambar 5.50. *Credential Harvester Attack Method*

SelanjutnyaPada gambar di atas, perintah yang kita pilih yaitu menu nomor 3 yaitu *Credential Harvester Attack Method* Selanjutnya tekan *enter* untuk melanjutkan perintah selanjutnya.

Gambar 5.51. *Site Cloner*

Perintah selanjutnya pada gambar di atas merupakan perintah di mana kita akan memilih menu nomor 2 yaitu *Site Cloner* yaitu di sini kita akan melakukan menggandakan suatu *website* atau dengan kata lain penipuan terhadap halaman *website* yang bukan alamat situs yang sebenarnya. Pada saat kita memilih perintah nomor 2. Perintah selanjutnya yaitu memasukkan alamat *IP* kita untuk mengalihkan situs target supaya masuk melewati ke *IP* kita dulu. Untuk melakukan pencarian *IP* kita, di sini perintah yang digunakan yaitu menggunakan terminal dengan menggetikkan *ifconfig.* Setelah itu tekan *enter.*

Gambar 5.52. Mengetahui *IP* Kita

Pada gambar di atas merupakan tampilan di terminal dengan menggetikan perintah *ifconfig*. Kemudian di sana akan tampil alamat *IP Address* 192.168.77.196. pada alamat *IP* inilah yang kita masukkan untuk mengelabuhi alamat *website*yang akan kita *Cloner*. Selanjutnya kembali pada perintah selanjutnya untuk melakukan serangan *phising.*

Gambar 5.53Masukkan *IP* Kita

Gambar 5.54Masukkan Alamat *Website* Target yang akan di *cloner*

Pada perintah di atas kita disuruh untuk memasukkan alamat *IP*. Dan pada perintah selanjutnya kita masukkan alamat *website* target kita. Kemudian tekan *enter.*Langkah selanjutnya adalah pada saat membuka di *browser* dengan mengetikkan alamat 192.168.77.196. Maka tampilan *browser* yang akan tampil yaitu alamat situs *mail.ptba.co.id.*

Gambar 5.55. Melakukan *Browser* Pada *IP*192.168.77.196

Pada gambar di atas, saat melakukan *browser*. Tampilan *browser* tidak bisa menampilkan halaman *website mail.ptba.co.id.* karena untuk *mail server* ptba ini hanya bisa diakses untuk jaringan internal saja.

Dan berikut contoh gambar yang berhasil melakukan serangan *phising* terhadap *websiteptba.co.id*. Pada saat membuka di *browser* dengan mengetikkan alamat 192.168.77.196. Maka tampilan *browser* yang akan tampil yaitu alamat situs *ptba.co.id.*

Gambar 5.56. Melakukan *Browser* Pada *IP*192.168.77.196

Gambar di atas adalah pada saat melakukan *browser* pada alamat IP 192.168.77.196. tampilan yang keluar yaitu tampilan halaman *web ptba.co.id*. pada saat sebuah *admin* atau karyawan lain ingin *login* pada *website* ini tetapi dengan catatan dengan mengtikkan alamat *ip* kita, otomatis nama *user* dan *password* akan tersimpan dalam *tools social engineering tools* tadi. Berikut adalah tampilan *record user* dan *password* pada saat *login.*

Gambar 5.57. *Record Username dan Password*

* + 1. **Hasil *Report***

Berikut adalah hasil pengamatan yang dilakukan dalam analisis kemanan jaringan menggunakan *email gateway* sebagai penyaringan pesan pada PT Bukit Asam (Persero) Tbk yang dilakukan selama 24 jam dari Rabu, 21 November 2012 jam 09.00 AM sampai Kamis, 22 November 2012 jam 09.00 AM.

Sumber :Admin PT Bukit Asam (Persero) Tbk

Gambar 5.58*Report* dari tanggal 21 sampai 22 Novemver 2012

* 1. **Pembahasan dan Evaluasi**

Setelah masa tahap *action taking* dianggap cukup, kemudian peneliti melakukan evaluasi tentang hasil yang didapat hasil dari analisis yang telah dilakukan tadi, dalam tahap ini dilihat efektif atau tidaknya penerapan *email gateway*pada PT Bukit Asam (Persero) Tbk Tanjung Enim, dilihat dari bagaimana*email gateway*dalammengatasi seranganyang terjadi pada sistem keamanan jaringan pada surat elektronik PT Bukit Asam (Persero) Tbk Tanjung Enim yang dapat dilihat dari *report* pada sistem tersebut.

* + 1. **Cara Kerja *Symantec Message Gateway 9.5***

Pada sub ini yang akan dijelaskan yaitu mengevaluasicara kerja anti*spam* yang digunakan PTBA selama kurang lebih hampir 3 tahun menggunakan jasa produk dari perusahaan *Symantec* yaitu *Symantec Message Gateway* versi 9.5**.** Dalam mengamankan jaringan terutama pada surat elektronik ptba menggunakan *Symantec Message Gateway 9.5* sebagai perlindungan terhadap lalu lintas surat elektronik pada jaringan. Prinsip kerja dari *Symantec Message Gateway*ini dapat dilihat pada gambar 5.1 yang merupakan cara kerja *Symantec Message Gateway*dalam mengamankan surat elektronik. SMG ini bekerja pada saat sebuah *user* mengrimkan surat elektronik, kemudian masuk menuju ke gerbang *Symantec Message Gateway*, di dalam *SMG* ini, pesan tersebut di proses untuk di*encription* apakah kunci yang dibawa pesan tersebut sesuai, maka pesan tersebut aman untuk di kirimkan kepada yang dituju. Fungsi dari *Symantec Message Gateway*ini dapat meminimalisir terhadap serangan pada jaringan dan jenis surat yang tidak diinginkan dan di dalamnya terdapat anti*spam real time*, serta membatasi koneksi yang tidak diinginkan,melakukan penyaringan surat elektronik untuk menghapus konten yang tidak diinginkan, dan pencegahan kehilangan data.

* + 1. **Konfigurasi*Symantec Message Gateway 9.5***

Pada sub ini yang akan dijelaskan yaitu mengevaluasidari Konfigurasi *Symantec Message Gateway 9.5.* Dengan melakukan konfigurasisistem ini seorang *admin* dapat mengatur koneksi serta kebijakan keamanan yang dibuat sesuai dengan kepentingan yang digunakan guna untuk melindungi sumber daya perusahaan yang mereka kelola. Konfigurasi pada *Symantec Messaging Gateway 9.5* yang dilakukan yaitumengatur koneksi pada *SMTP (Simple Mail Transfer Protokol).*Pada hasil yang didapat pada konfigurasi koneksi *SMTP* ini yaitu *SMTP(Simple Mail Transfer Protokol)* merupakan *protokol* yang digunakan sebagai pengelola dan pengatur lalu lintas keluar masuk pesanpada jaringan. Fungsi utama dari *SMTP* adalah menyampaikan pesan dari komputer pengirim ke komputer penerima, baik dalam jaringan yang sama*LAN* atau *WAN* maupun ke komputer penerima dalam suatu jaringan yang berbeda. Kemudian pada konfigurasi fitur *Symantec Messaging Gateway 9.5* mencakup beberapa fitur untuk memberikan perlindungan serta fitur penyaringan dan membuatnya lebih mudah untuk mengontrol data. Sehingga *administratur* dapat dengan mudah membangun kebijakan yang efektif dalam menegakkan suatu kepatuhan terhadap peraturan untuk melindungi terhadap hilangnya data-data penting. Pada fitur menu *Symantec Message Gateway 9.5* terdapat menu yang dapat digunakan. Terdapat 8 menu yaitu *status, report, protocol, reputation, spam, malware, content* dan *administration*.Konfigurasipada fitur *Symantec Message Gateway 9.5* ini sangat penting, kerena dengan dilakukan konfigurasi agar kinerja dari *Symantec Message Gateway 9.5* ini dapat bekerja dengan baik dalam menagamankan surat elektronikyang keluar maupun masuk pada jaringan komputer.

* + 1. **Pengujian**

Pada sub ini akan dijelaskan yaitu mengevaluasidari hasil pengujian pada *Symantec Message Gateway* dan padaJaringanPTBA*.* Dengan melakukan pengujian ini pastinya mendapatkan celah celah yang didapat.Apabila celah tersebut dimanfaatkan untuk kejahatan, maka besar kemungkinan jaringan perusahaan tersebut bisa terganggu bahkan terjadi kevakuman terhadap jaringan komputer khususnya PTBA. Kemudian pada penetrasi pada *Symantec Message Gateway* kebijakan yang diterapkan juga harus sesuai dengan kebutuhan melihat dengan banyak serangan terutama virus, otomatis kebijakan yang diterapkan, baik dalam pemasangan anti virus maupun *update* secara berkala pada suatu sistem dengan sistem yang baru, agar kinerja dalam melindungi jaringan dapat bekerja dengan baik dan dapat mencegah dari hal-hal yang dapat merusak jaringan komputer.

* + 1. ***Report* Dari Penyaringan Surat Elektronik**

Pada sub ini merupakan penjelasan tentang *report* yang berisi jenis-jenis serangan yang terdapat pada surat elektronikyang berhasil disaring*.* Pada *report* ini nanti akan tampil jenis serangan yang didapat. Dari serangan inilah yang dapat merusak sistem keamanan jaringan apabila serangan tersebut berhasil menembus ke dalam sistem tersebut.

Pada penelitian ini terdapat dua tabel yang masing masing berisi tentang hasil *report* dari sistem penyaringan terhadap surat elektronik*.*pada tabel 5.1 berisi tentang *message summary* yaitu jenis pesan dan jumlah surat elektronik yang di *capture* selama 24 jam. Kemudian pada tabel 5.2 berisi tentang jenis serangan yang tertangkap atau *spam* dan *unwanted mail summary (Inbound dan Outbound)*.

Tabel 5.1 *Message Type*

|  |  |  |
| --- | --- | --- |
| **No.** | ***Message Type*** | **Jumlah** |
| 1.  2. | *Message With a Single Threat*  *Message With Multiple Threat* | 1.723  8 |
| **Total *Threat message*** | | **1.731** |
| 3. | *Message Without Spam Threat* | 9.753 |
| **Total *Message*** | | **11.484** |

Pada tabel 5.1 merupakan hasil *report* yang menjelaskan tentang jenis-jenis surat elektronik dan jumlah surat elektronik yang masuk. Untuk jumlah surat elektronikyang masuk terhitung selama 24 jam dari 21 November 2012 jam 09.00 AM sampai 22 November 2012 jam 09.00 AM berjumlah 11.484 *message*. Kemudian pada tabel di atas terdapat jenis-jenis pesan yang di dalamnya terdapat banyak ancaman dan sedikit ancaman.Pada *Message with a single threat* berjumlah 1.723 *message* dan pesan yang di dalamnya memiliki banyak serangan jumlahnya hanya sedikit terdapat 8 *message* yang berhasil disaring.Kemudian dengan jumlah 9.753 message merupakan hasil penyaringan dengan pesan yang aman tidak ada ancaman terdapat *spam.*

Tabel 5.2 *Threat Type*

|  |  |  |
| --- | --- | --- |
| **No** | ***Threat Type*** | **Jumlah** |
| 1.  2.  3.  4.  5.  6.  7. | *Spam*  *Suspect Spam*  *Bounce Attack*  *Sennder Authentication Failure*  *Marketing Mail*  *Newsletter*  *Susplicious URL* | 823  5  -  -  -  340  571 |
| **Total *Spam Threat*** | | **1.739** |

Pada tabel 5.2 merupakan *report* yang menjelaskan tentang jenis-jenis serangan yang terdapat pada surat elektronik yang berhasil disaring*.* Terdapat banyak jenis serangan yang didapat diantaranya *Spam, Suspect Spam, Bounce Spam, sender Authentication Failure, Marketing Mail, Newsletter* dan *Susplicious URL.*

Jumlah serangan *spam* yang masuk terhitung selama 24 jam dari 21 November 2012 jam 09.00 AM sampai 22 November 2012 jam 09.00 AM berjumlah 1.739 surat elektronik. Di sini *report* penyaringan terdapat 823 dari 11.484 surat elektronik yang di dalamnya terdapat serangan *spam.* Untuk jenis ancaman *suspect spam* yaitu pesan yang diidentifikasi dan dicurigai adanya *spam.Suspect spam* hanya terdapat 5 *message. suspect spam* yang disaring*.* Kemudian pada jenis serangan *bounce attacks, sender authentication failure* dan *marketing mail* tidak terdapat pada surat elektronik*,* sehingga hasil penyaringan untuk jenis serangan ini tidak terdeteksi adanya jenis serangan tersebut.Kemudian serangan *newsletter* berjumlah 340 *message* yang terdapat serangan ini. Pada jenis *suspicious URL* yang merupakan alamat *URL* yang dicurigai di mana di dalamnya terdapat pesan yang terdapat *spam* dan *malware*. Untuk jenis serangan ini berhasil disaring sebanyak 571 surat elektronik*.*

* + - 1. **Solusi**

Melihat *report* di atas, banyak terdapat serangan pada surat elektronik*.*Dalam 1 hari saja sudah terdapat banyak ancaman yang masuk dan berhasil disaringdari berbagai bentuk jenis ancaman. Apabila jenis serangan tersebut berhasil menembus dinding pertahanan jaringan terutama pada surat elektroniktanpa adanya *email gateway* dan *antispam*, dampak yang didapat akan menggangu bahkan merusak jalannya bisnis perusahaan menjadi kacau bahkan dan vakum terutama pada jaringan di PT Bukit Asam (Persero) Tbk. Berikut solusi yang penulis berikan;

* + - * 1. **Solusi pada cara kerja *Symantec Message Gateway 9.5,***

Solusi yang dapat diberikan pada cara kerja *Symantec Message Gateway*ini yaitumelihat dari *report* yang didapat masih terdapat banyak jenis serangan yang masih terdeteksi yang berhasil disaring, maka solusi yang dapat diberikan yaitu perusahaan wajib melakukan pembayaran lisensi.Lisensi di sini merupakan pembayaran pada jasa yang digunakan dalam melindungi jaringan pada PTBA.Apabila terjadi keterlambatan pembayaran pada lisensi ini, maka sistem tersebut dengan otomatis tidak berfungsi dengan sendirinya sehingga dampak yang di dapat bisa saja jaringan menjadi *crash* bahkan menjadi rusak yang mengakibatkan kevakuman terhadap sistem pada PTBA.

* + - * 1. **Solusi pada konfigurasi*Symantec Message Gateway 9.5,***

Pada konfigurasi yang telah ditetapkan pada PT Bukit Asam (Persero) Tbk Tanjung Enim masih belum cukup sempurna dalam mengamankan jaringan terutama pada surat elektronik*,* melihat dari *report,* dapat dijelaskan masih banyak jumlah pesan yang masih terdapat banyak ancaman di dalamnya. Maka solusi yang diberikan pada konfigurasi ini yaitu seorang *administratur* harus lebih memperhatikan kebijakan yang ditentukan dalam mengamankan jaringan. Semakin kuat kebijakan keamanan jaringan yang di buat maka semakin susah serangan yang masuk pada jaringan terutama pada surat elektronik.

* + - * 1. **Solusi pada pengujian Jaringan PTBA,**

Pada pengujian di *mail server* di sini tidak dapat dilakukan karena *mail server* milik PTBA di sini hanya menggunakan jaringan internalyang hanya bisa diakses oleh pegawai PTBA saja.Kemudian solusi yang dapat diberikan pada jaringan PTBAmelihat dari hasil pengujian yang dilakukan yaitu masih terdapat celah celah yang dapat dimanfaatkan seorang *hacker* dalam melakukan serangan.Solusinya seorang *administratur* harus lebih aktif dalam memonitoring jaringan guna untuk mendeteksi gangguan pada jaringan serta membuat kebijakan yang kuat dalam melindungi jaringan.Misalnya menutup dan membuka *port* yang dibutuhkan saja.Kemudian solusi untuk menghindari dari ancaman tersebut adalah seorang *administratur* wajib melakukan *backup* data secara teratur, dan di sini membutuhkan *space* penyimpanan yang cukup besar supaya data – data penting yang di *backup* cukup untuk menyimpan data yang besar.Sehingga apabila terjadi *crash* pada jaringan baik itu dari *human error* maupun dari sistem itu sendiri data – data penting dapat di selamatkan.

Kemudian tidak hanya pada *backup* saja, pada *update* suatu sistem juga sangat dibutuhkan, melihat dari serangan yang semakin lama semakin banyak, maka *update* sistem dengan kemampuan dari sistem itu sendiri perlu ditingkatkan untuk menghindari dari ancaman dari serangan yang baru.

**BAB VI**

**KESIMPULAN DAN SARAN**

* 1. **Kesimpulan**

Berdasarkan pembahasan pada bab sebelumnya mengenai analisa keamanan jaringan menggunakan *email gateway* sebagai penyaringan surat elektronik pada Satuan Kerja Teknologi Informasi PT Bukit Asam (Persero) Tbk, maka kesimpulan yang dapat diambil diantaranya;

Melihat dari cara kerja*Symantec Message Gateway*dalam mengamankan jaringan terutama pada surat elektronikkita dapat mengetahui cara kerja yang dari sistem tersebut. Di mana di di dalam SMG terdapat anti*spam real time*, serta membatasi koneksi yang tidak diinginkan, melakukan penyaringan pesan untuk menghapus konten yang tidak diinginkan sehingga data perusahaan dapat terjaga,

Dengan melakukan konfigurasisistem ini seorang *admin* dapat mengatur koneksi serta kebijakan keamanan yang dibuat sesuai dengan kepentingan yang digunakan guna untuk melindungi sumber daya perusahaan yang mereka kelola, dan

Dengan melakukan pengujian ini pastinya mendapatkan celah celah yang didapat. Apabila celah tersebut dimanfaatkan untuk kejahatan, maka besar kemungkinan jaringan perusahaan tersebut bisa terganggu bahkan terjadi kevakuman terhadap jaringan komputer khususnya PTBA.

­

* 1. **Saran**

Dari penjelasan serta pengumpulan data-data dan pengalaman yang penulis dapatkan saat melakukan penelitian, ada beberapa saran yang dapat berguna bagi pembaca antara lain;

1. Untuk memastikan lisensi suatu produk yang digunakan harus lebih diperhatikan, apabila terjadi keterlambatan dalam pembayaran lisensi Maka sistem keamanan menjadi tidak akftif dan hal-hal yang tidak diinginkan akan mengancam keamanan jaringan perusahaan. Sehingga kerusakan pada sistem maupun data – data penting perusahaan dapat terjadi, bahkan jaringan perusahaan bisa menjadi vakum,
2. Pada konfigurasi ini yaitu seorang *administratur* harus lebih memperhatikan kebijakan yang ditentukan dalam mengamankan jaringan. Semakin kuat kebijakan keamanan jaringan yang di buat maka semakin susah serangan yang masuk pada jaringan terutama pada surat elektronik, dan
3. Melakukan *update* sebuah produk yang digunakan sangat penting dilakukan guna untuk mengoptimalkan kerja dari sistem tersebut. Serta melakukan *backup* data merupakan peran penting dalam mengamankan data-data penting. *backup* data wajib guna untuk menghindari dari kehilangan data apabila terjadi serangan atau terjadi *crash* pada sistem komputer.