ANALISIS KEAMANAN JARINGAN MENGGUNAKAN *EMAIL GATEWAY* SEBAGAI *FILTERING EMAIL* PADA PT BUKIT ASAM TBK

Toni Triatmojo, Fatoni dan Suryayusra
Jalan Jenderal Ahmad Yani No.12 Palembang
Pos-el : theviceroyztoni@yahoo.co.id, toni@mail.binadarma.ac.id, suryayusra@mail.binadarma.ac.id.

Abstract : *Along with the growth of technology, electronic mail became a means of communication that are increasingly used. In developed countries, electronic mail has become the main communication even in the office or between customers and clients. With a very important function, then the user must really pay attention to the safety factor electronic mail, because e-mail is very vulnerable to such security gaps that exist on the network, there are many attacks on the network. One of the attacks which often happen that an attack spam. Basically, the security system is indispensable for securing electronic mail using an email gateway instance. Email gateway managing traffic data packets between networks in which there are restrictions or security mechanisms (filtering) packets - packets of data to help ensure the integrity of electronic mail before entering the network. Antispam policy adopted Delete, Ignore and Quarantine.*

Keywords: *email, internet, email gateway, spam*

Abstrak : *Seiring dengan pertumbuhan teknologi, surat elektronik menjadi sarana komunikasi yang semakin banyak digunakan. Di negara maju, surat elektronik bahkan sudah menjadi komunikasi utama di kantor atau antara pelanggan dan nasabahnya. Dengan fungsinya yang sangat penting tersebut, maka sebagai pengguna harus benar-benar memperhatikan faktor keamanan surat elektroniknya, karena surat elektronik sangat rentan terhadap celah keamanan seperti yang ada pada jaringan, terdapat banyak serangan terhadap jaringan. Salah satu serangan yang sering terjadi yaitu serangan spam. Pada dasarnya sistem keamanan sangat diperlukan untuk mengamankan surat elektronik misalnya dengan menggunakan email gateway.* Email *gateway mengatur lalu lintas paket data antar jaringan yang di dalamnya terdapat mekanisme pembatasan atau pengamanan (filtering) paket – paket data untuk membantu memastikan terhadap integritas surat elektronik sebelum masuk ke jaringan. Kebijakan antispam yang diterapkan Delete, Abaikan dan Karantina.*

Kata kunci*: email, internet, email gateway, spam*

1. PENDAHULUAN

Seiring dengan pertumbuhan teknologi, surat elektronik menjadi sarana komunikasi yang semakin banyak digunakan. Di negara maju, surat elektronik bahkan sudah menjadi komunikasi utama di kantor atau antara pelanggan dan nasabahnya. Pada PT Bukit Asam (Persero) Tbk, fasilitas surat elektronik yaitu berfungsi sebagai roda penggerak bisnis perusahaan.

Namun perlu diperhatikan mengenai keamanan 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 yang sering terjadi yaitu serangan *spam*.

Melihat dari kondisi di atas dalam mengamankan jaringan dibutuhkan *email gateway dan* anti*spam. Email Gateway* yang sudah diterapkan PT Bukit Asam (Persero) Tbk menggunakan *Symantec Message Gateway 9.5* yang 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 pesan untuk menghapus konten yang tidak diinginkan, dan pencegahan kehilangan data.

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

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 *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.

1.1. Tujuan dan Manfaat Penelitian

1.1.1. Tujuan Penelitian

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

1. Melindungi sumber daya sebuah perusahaan,
2. Dapat mencegah ancaman dari hal-hal yang membahayakan jaringan,
3. Membuat analisa terhadap sistem yang diterapkan di perusahaan.

1.1.2. Manfaat Penelitian

Manfaat yang bisa didapatkan dari penelitian ini adalah;

1. Meningkatkan efektifitas dari kinerja jaringan di PTBA,
2. Sebagai usaha dalam meningkatkan sistem keamanan jaringan komputer di PTBA.
3. Dapat mengetahui bentuk sistem keamanan yang digunakan.
4. Dengan menggunakan *email gateway* akan mempermudah *administratur* jaringan untuk memantau aliran data yang masuk dan keluar di suatu jaringan.

2. METODOLOGI PENELITIAN

2.1. 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 jam 07.30 sampai dengan 16.00 WIB.

2.2. 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. Adapun tahapan penelitian yang merupakan bagian dari *action research* ini, yaitu ;

1. Diagnosa,

   Penulis melakukan diagnosa terhadap sistem keamanan jaringan komputer pada *administratur* yang ada pada pusat informasi di satuan kerja Teknologi Informasi PTBA.
2. Melakukan Rencana Tindakan,

   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.
3. 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.
4. Evaluasi,

   Peneliti melakukan evaluasi hasil dari analisis yang telah dilakukan tadi, dalam tahap ini dilihat penerapan *email gateway* sebagai penyaringan surat elektronik apakah sudah berjalan dengan baik dalam mengamankan surat elektronik dengan melihat hasil *report* dari sistem tersebut dalam mengatasi serangan yang terjadi pada sistem keamanan jaringan PT Bukit Asam (Persero) Tbk Tanjung Enim.
5. Pembelajaran.

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

2.2.1. Metode Pengumpulan Data

Metode yang digunakan dalam proses pengumpulan data adalah sebagai berikut;

1. Observasi,

   Penulis mengadakan peninjauan langsung ke PTBA dengan mengamati, mencatat dan mengevaluasi jaringan yang ada di perusahaan tersebut.
2. Wawancara,

   Dalam hal ini penulis mengajukan pertanyaan-pertanyaan kepada yang bertugas sebagai *administratur* jaringan pada perusahaan tersebut.
3. 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 jurnal yang erat kaitannya dengan penulisan penelitian.

2.2.2. Metode Analisis Sistem Keamanan Jaringan

2.2.2.1. Metode Penetrasi

Metode Penetrasi adalah suatu metode yang dilakukan guna mengevaluasi keamanan dari sebuah sistem komputer atau jaringan.

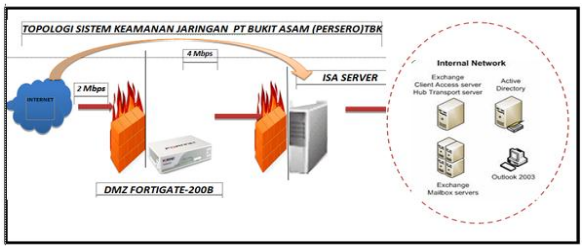
Tujuan pengujian penetrasi ini adalah untuk menemukan setiap dan semua titik kerentanan di dalam sistem jaringan komputer

dengan cara melakukan simulasi serangan dari luar maupun internal sistem atau jaringan. Pada dasarnya orang yang melakukan pengujian penetrasi sedang mencoba untuk kembali ke sistem. (Cymots, 2011)

3. HASIL

3.1. Melakukan Diagnosa

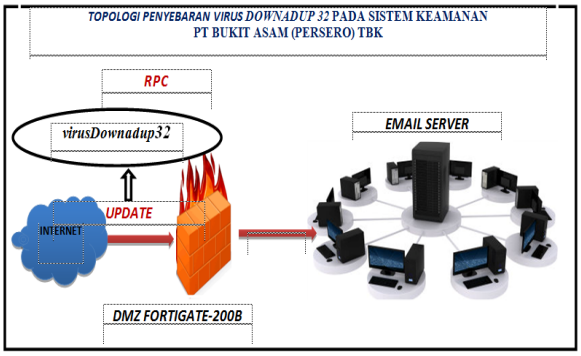
Penulis melakukan diagnosa terhadap sistem keamanan jaringan komputer pada surat elektronik di satuan kerja Teknologi Informasi PT Bukit Asam (Persero) Tbk Tanjung Enim. Untuk mengetahui gambaran sistem keamanan jaringan yang di PT Bukit Asam (Persero) Tbk Tanjung Enim dapat kita lihat dari gambar 4.1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



Sumber: PT Bukit Asam (Persero) Tbk Tanjung Enim

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

Pada gambar di atas dapat dilihat bahwa sistem keamanan jaringan yang ada di PT Bukit Asam (Persero) Tbk Tanjung Enim menggunakan *DMZ FortiGate-200B* dan *ISA Server* sebagai *firewall* guna menimimalisir penyusup untuk masuk ke jaringan PT Bukit Asam (Persero) Tbk Tanjung Enim. Kemudian dibelakang *firewall* merupakan jaringan *internal* yaitu *mail server* milik PT Bukit Asam (Persero) Tbk Tanjung Enim. Pada PT. Bukit Asam (Persero) Tbk, *Mail Server* yang digunakan yaitu *Exchange Server 2003*. 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 3.2,



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

Gambar 2. Penyebaran Virus *Downadup32*

Penggunaan surat elektronik bagi 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 elektronik masih menggunakan jaringan internet sebagai media penghantarnya dalam pengiriman. Maka surat elektronik juga 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. Anti *spam* yang digunakan PT Bukit Asam (Persero) Tbk adalah penggunaan *Symantec Messaging Gateway 9.5* yang dibuat

untuk melindungi sumber daya perusahaan yaitu keamanan pada surat elektronik. *Symantec Messaging Gateway 9.5* ini memiliki 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 pengguna yang menggunakan lisensi ini pada PT Bukit Asam (Persero) Tbk lebih kurang 800 *user*.

3.2. Membuat Rencana Tindakan

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 elektronik yang 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.

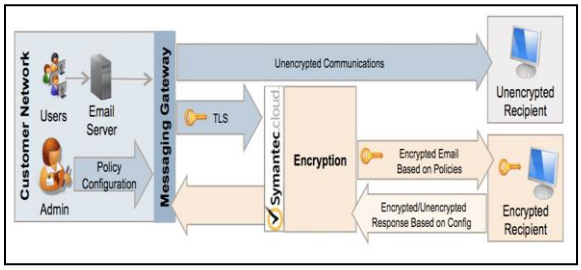
Yang akan dilakukan dalam rencana tindakan ini adalah;

1. Penulis akan menjelaskan bagaimana cara kerja dari *email gateway* yaitu *Symantec Message Gateway 9.5* yang digunakan oleh PTBA dalam mengamankan surat elektronik perusahaan,
2. Kemudian bagaimana konfigurasi sistem yang digunakan,
3. Serta melakukan pengujian terhadap sistem tersebut pada jaringan PTBA,
4. Dengan melakukan rencana tindakan ini penulis akan mendapatkan hasil yang didapat berupa *report* dari sistem tersebut dan kemudian r*eport* itu dilanjutkan dengan evaluasi.

3.3. Melakukan Tindakan

Peneliti menganalisis rencana dengan tindakan dengan mengumpulkan data-data yang dibutuhkan dalam penelitian. Dan melakukan analisis sistem keamanan jaringan komputer menggunakan *email gateway* dalam dalam hal peningkatan sistem keamanan jaringan terutaman pada kemanan surat elektronik PT Bukit Asam (Persero) Tbk Tanjung Enim.

3.3.1. Mengetahui Cara Kerja *Symantec Message Gateway 9.5*



Gambar 3. Cara Kerja *Symantec Message Gateway 9.5*

Pada gambar di atas dapat dijelaskan bagaimana *Symantec Message Gateway* 9.5 bekerja dengan menggunakan *Symantec Content Encryption*. 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).* Selanjutnya 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 di*encription*. Pada *Mail Infrastruktur* PT Bukit Asam (Persero) Tbk menggunakan *Symantec Content Encryption* dalam membantu 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. *Symantec Messaging Gateway* dengan *Symantec Content Encryption* dapat menghemat waktu dan sumber daya yang sebelumnya digunakan mencoba untuk memonitor lalu lintas surat elektronik dengan 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 terbaik bagi pelanggan yang tertarik dalam penawaran berbasis *cloud* dalam keamanan surat elektronik yang dikelola oleh *Symantec*. *Symantec Email Security.cloud* tidak memerlukan perangkat keras atau perangkat lunak.

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*

3.3.2. Konfigurasi *Symantec Messaging Gateway 9.5*

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

3.3.2.1. 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);*

1. Untuk memulai konfigurasi yaitu dengan melakukan *Login* ke *Web Symantec Message Gateway* 9.5,

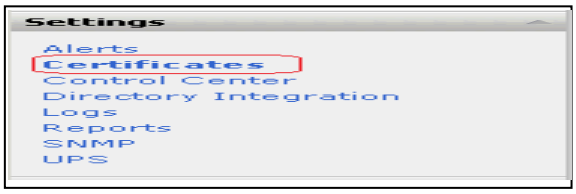
Gambar 4. L*ogin* ke *Web Symantec Message Gateway 9.5*

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.

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

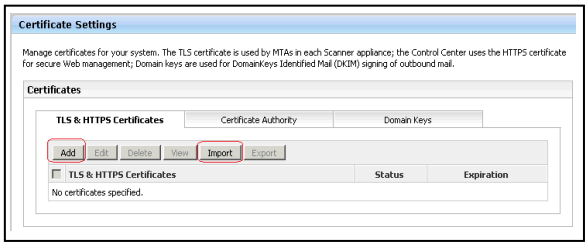
Gambar 5. *Administration*

3. pilih pada bawah *link Certificates* pada menu kiri bagian bawah, pilih *Settings header* di *sidebar*,



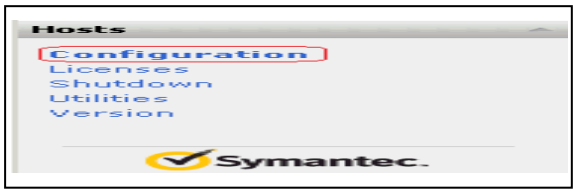
Gambar 6. *Setting*

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



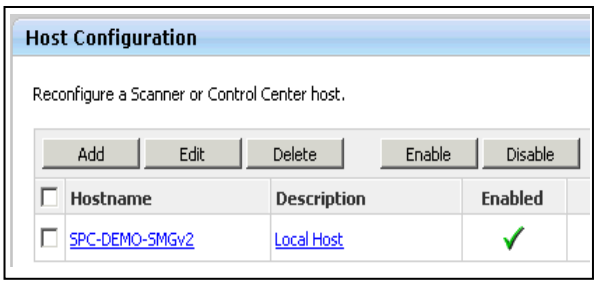
Gambar 7. *Certificate Settings*

5. Pilih pada *link Configuration* pada *header Host* di *sidebar* di menu bawah bagian kiri,



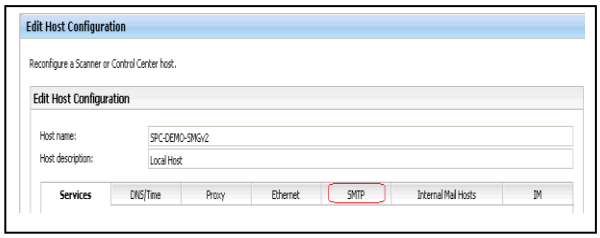
Gambar 8. *Hosts*

6. Pilih pada *Scanner* yang ingin dirubah,



Gambar 9. *Host Configuration*

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



Gambar 10. *Edit Host Configuration*

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

Gambar 11. *Inbound Mail Setting*

9. Kemudian pilih tombol *Save* di bagian bawah halaman untuk menyimpan konfigurasi tersebut.

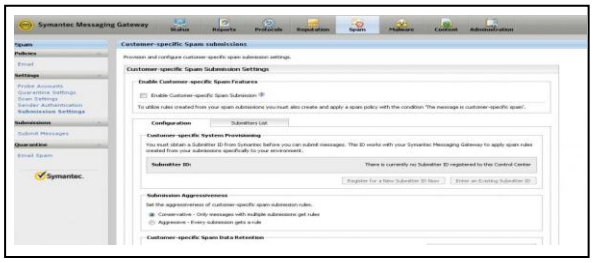
Setelah melakukan konfigurasi pada koneksi *SMTP*, selanjutnya yaitu konfigurasi fitur yang ada pada *Symantec Message Gateway* 9.5.

3.3.2.2. 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. Konfigurasi pada fitur

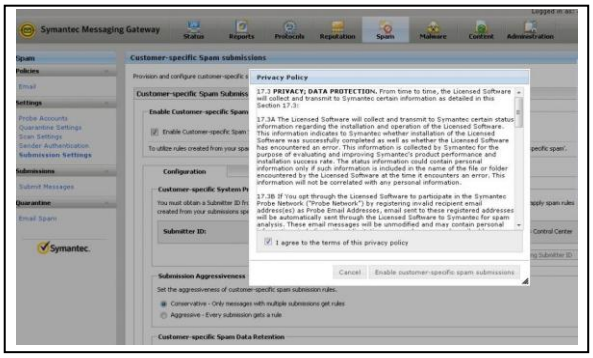
Symantec Message Gateway 9.5 ini sangat penting, kerena dengan dilakukan konfigurasi agar kinerja dari *Symantec Message Gateway 9.5* ini dapat bekerja dengan baik dalam mengamankan surat elektronik yang keluar maupun masuk. Berikut adalah cara konfigurasi fitur penting pada *Symantec Messaging Gateway 9.5;*

1. 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 12,



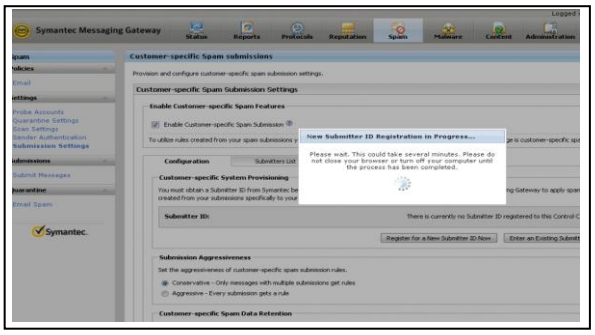
Gambar 12. *Submission Settings*

2. 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*,



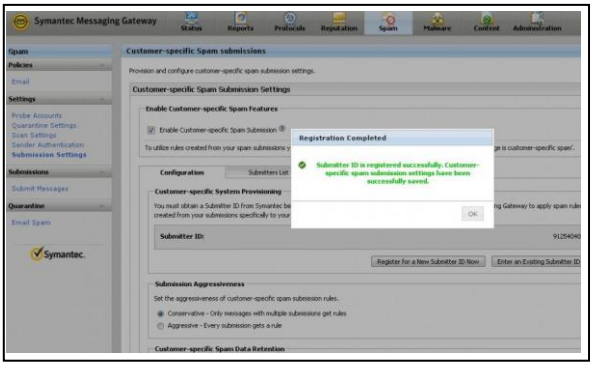
Gambar 13. *Spesifik Spam Submission*

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



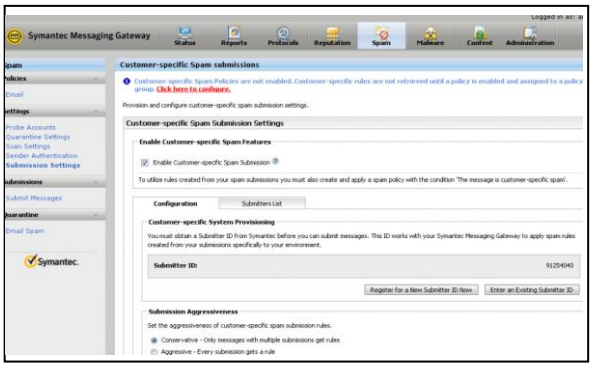
Gambar 14. *Submitter ID Registration*

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



Gambar 15. *Registration Completed*

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

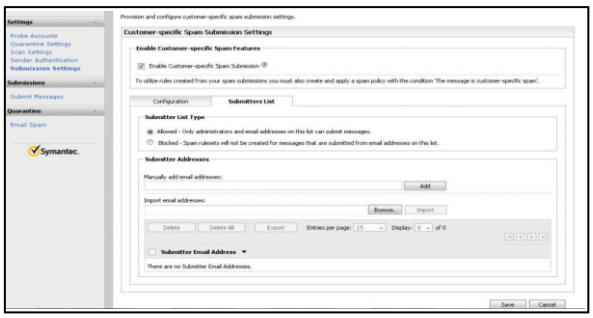


Gambar 16. *Submission Setting*

Pada gambar di atas terdapat perintah untuk melakukan kebijakan keamanan yang terdapat di bawah *Customer-specifik Spam submission. administratur* selanjutnya

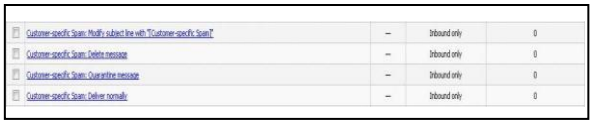
melakukan *Customer-specifik Spam policy*. Maka yang dilakukan *Administratur* yaitu membuat suatu kebijakan dengan memilih *"Click here to configure",*

5. 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 yang Anda lihat di bawah ini. Dengan cara Anda juga dapat mengimpor daftar Anda untuk mengizinkan atau memblokir mengirimkan pesan,



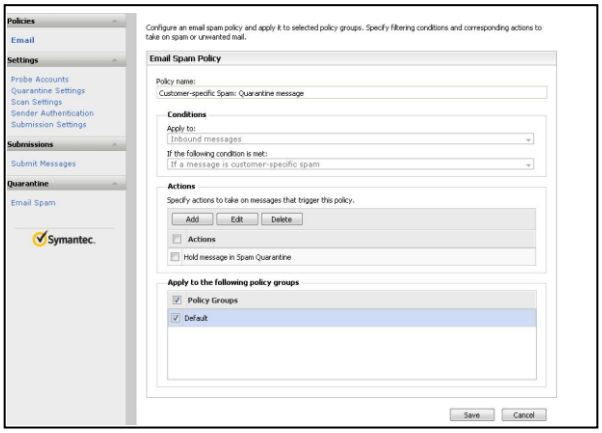
Gambar 17. *Subbmitters List*

6. Sekarang, kita harus memilih kebijakan untuk mengaktifkan *"Submissions Customer"* sebelum mengirimkan pesan apapun. Untuk melakukannya, klik 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 18. *Customer Spesifik Spam*

7. Untuk mengaktifkan salah satu kebijakan, pilih saja dan memilih kelompok kebijakan di bawah ini untuk menerapkannya ke grup berikut,



Gambar 19. *Setting Email Spam Policy*

8. Selanjutnya setelah melakukan pemilihan salah satu kebijakan, pilih tombol *save*. Setelah memilih *save* akan tampil kebijakan yang sudah diterapkan tadi pada gambar 20,

Gambar 20. Tampilan *Email Spam Policy*

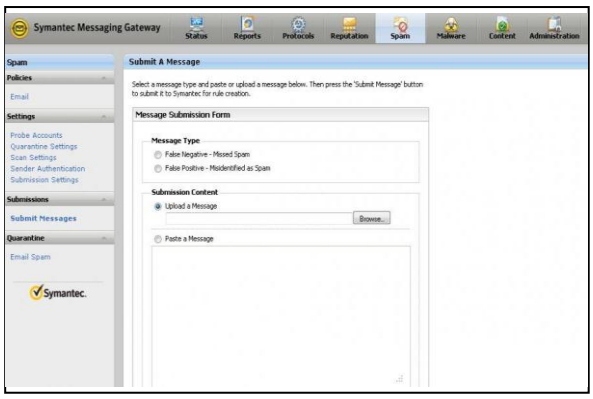
3.3.3. Pengujian

Tujuan pengujian pada jaringan komputer merupakan kunci keberhasilan dalam perlindungan pada jaringan komputer.

3.3.3.1. Pengujian Pengiriman Pesan Melalui *Symantec Message Gateway 9.5.*

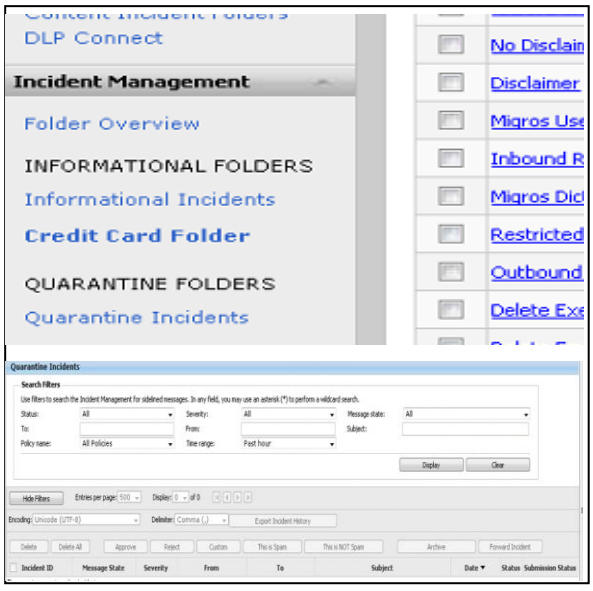
Pada *Symantec Message Gateway 9.5* ini terdapat 3 cara dalam melakukan penyampaian pesan dari *Symantec Message Gateway*. Yaitu di mana pesan yang disimpan dalam *spam* karantina, sehingga dengan melakukan pengujian ini kita dapat melihat hasil penyaringan surat elektronik itu sendiri.

1. 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 21. *Subbmit A Message*

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



Gambar 22. *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".*

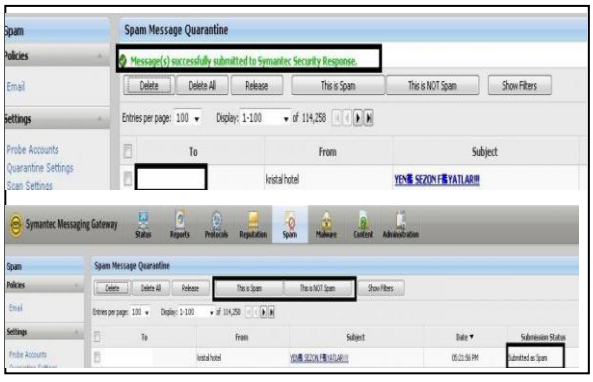
2. Selanjutnya pada pilihan pengiriman terakhir yaitu adalah mengirimkan dari karantina *spam* yang dapat akses melalui menu *Spam Message Quarantine,*

Gambar 23. *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,

Gambar 24. *Submit as Spam*

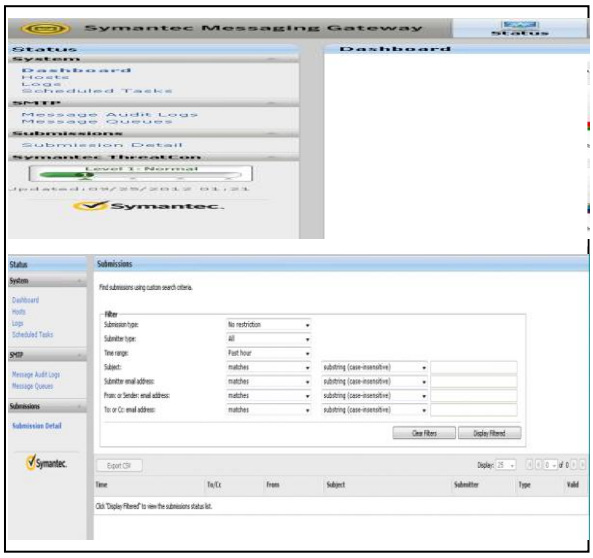
Pada saat kita memilih "*Submit as Spam".* Maka setelah itu kita dapat melihat bahwa pesan berhasil disampaikan,



Gambar 25. *Message Successfully*

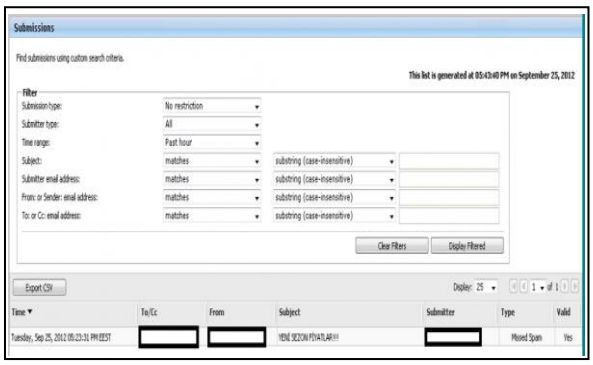
Langkah terakhir untuk melihat status kiriman. Pada menu pilih *"Status* kemudian

pilih "*Submissions*" pada menu dibagian kiri, setelah itu pilih "*Detail Submission*",



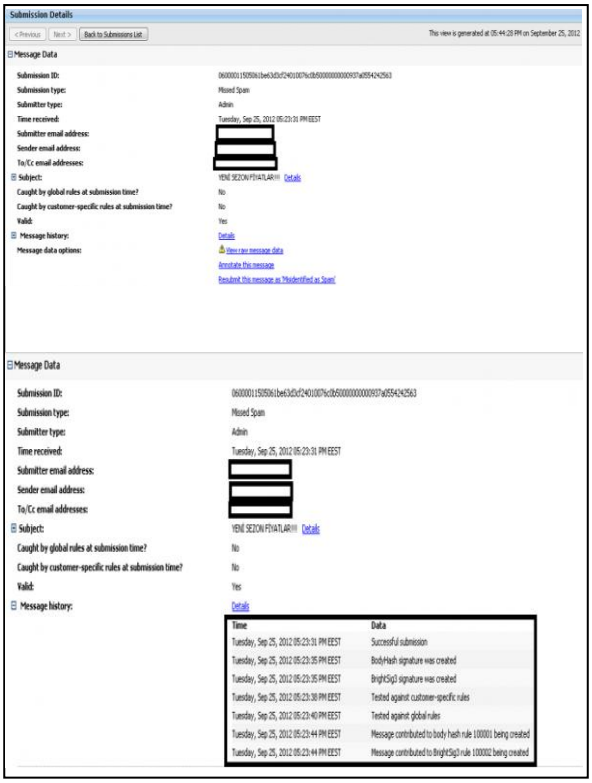
Gambar 26. *Status*

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 27. Tampilan *Filter*

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



Gambar 28. *Submission Details*

3.3.3.2. Pengujian Terhadap Jaringan PT. Bukit Asam (Persero) Tbk

Tahapan untuk melakukan pengujian adalah sebagai berikut;

1. *Target Scoping*,

   Sebelum memulai penilaian keamanan teknis, yang terpenting adalah untuk mengamati dan memahami ruang lingkup yang diberikan dari lingkungan jaringan target. 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 29. *Web* PT Bukit Asam (Persero) Tbk

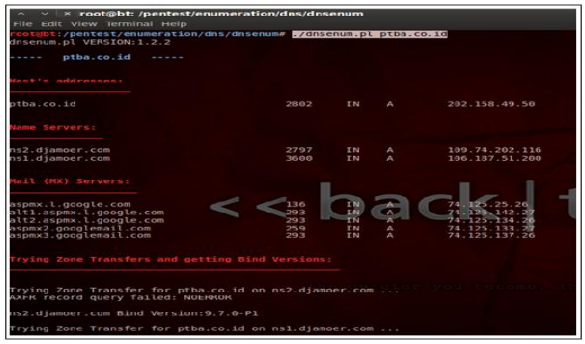
2. *DNS Information,*

   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 30,

Sumber: *BackTrack 5*

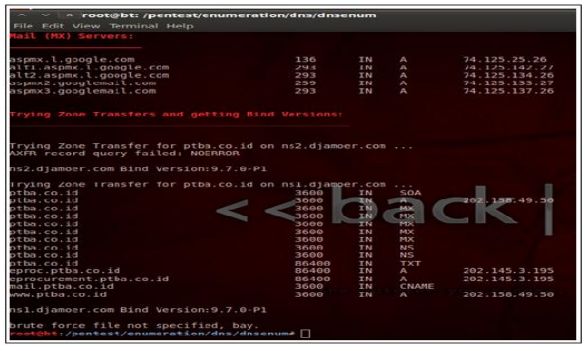
Gambar 30. *Output* pada Perintah *dnswalk*

Pada Gambar di atas merupakan tampilan perintah *dnswalk.* Di sana terdapat *dns* bernama *ns1.djamoer.com.*



Sumber: *BackTrack 5*

Gambar 31. *Output* pada Perintah *dnsenum*

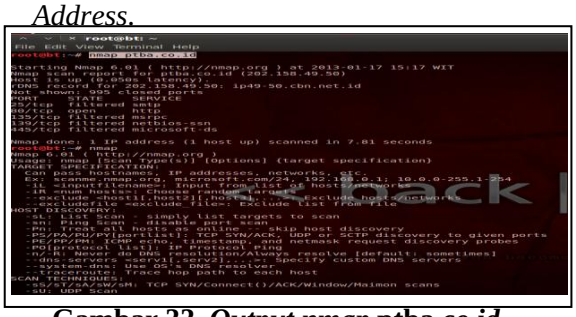


Gambar 32. *Output* pada Perintah *dnsenum*

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.

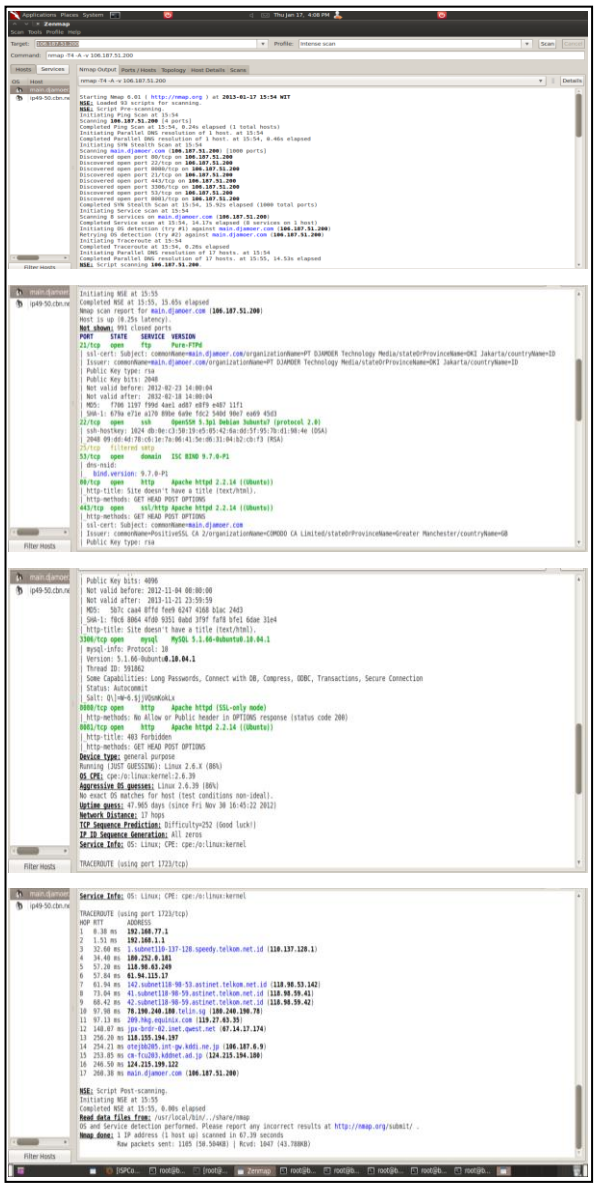
3. *Enumerating Target,*

   Untuk mengetahui *Enumerating Target* PT Bukit Asam (Persero) Tbk, penulis melakukan *Nmap* dan *Zenmap* pada *IP Host's Address.*

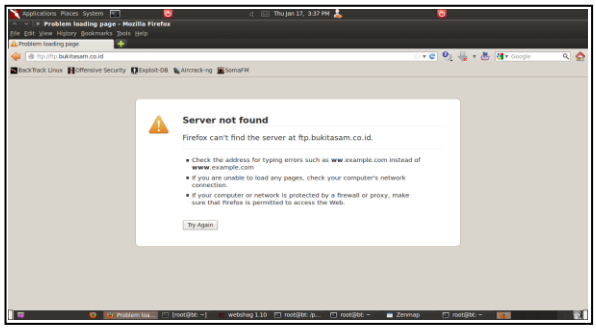


Gambar 33. *Output nmap* ptba.*co.id*

Gambar 34. *Output Zenmap*

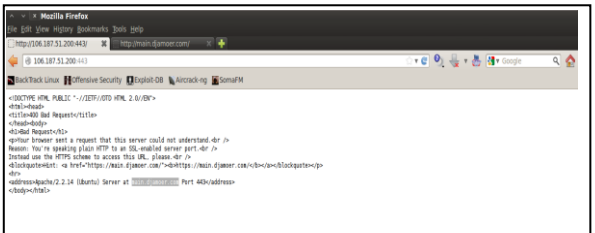


Gambar 35. *Output Zenmap* pada *host address ptba.co.id* dan *name server*



Gambar 36. *Output ftp.bukitasam.co.id*

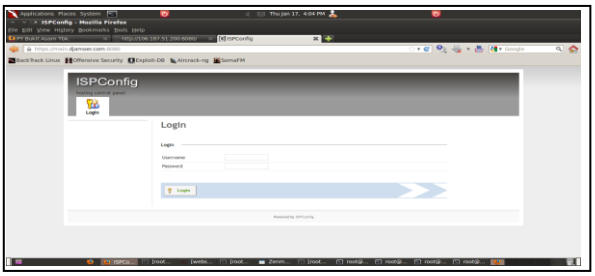
Pada gambar di atas kita mencoba melakukan *browser* pada *port* 21 yaitu *FTP (File Transfer Protocol)*. Pada saat melakukan *browsing* pada *ftp.bukitasam.co.id* tidak bisa dilakukan, *ftp* bukitasam ptba hanya bisa diakses pada jaringan internal saja.



Gambar 37. Tampilan *ip* 106.187.51.200 pada *port* 443

Gambar 38. Tampilan *ip* 106.187.51.200 pada *port* 8080

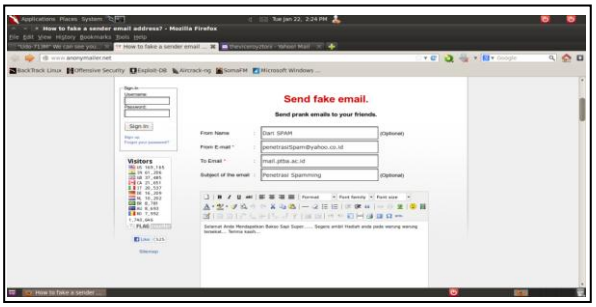
Kemudian kita mencoba lagi membuka pada *port* 8080 pada *ip* 106.187.51.200 yang merupakan *dns* dari ptba. Pada gambar di atas terdapat *name server main.djamoer.com* yang hanya diakses pada *https*.



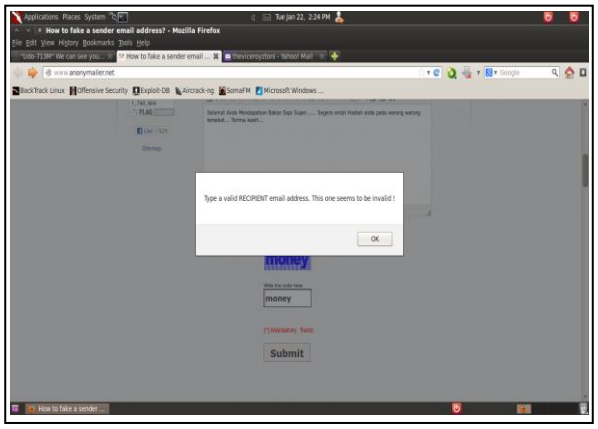
Gambar 39. Halaman *login Admin* di *ISPConfig*

4. Melakukan Serangan *Spam*,

   Untuk melakukan serangan ini, kita masukkan alamat situs *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.



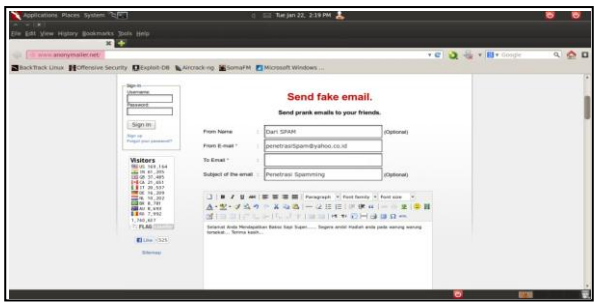
Gambar 40. Isi *Form*



Gambar 41. Gagal Mengirim Pesan

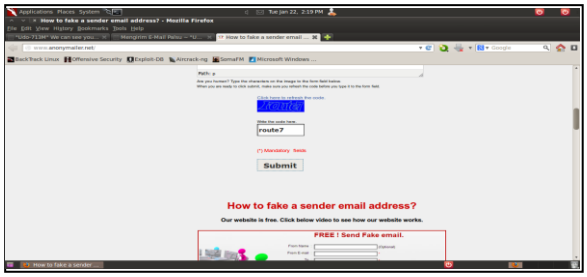
Pada gambar di atas merupakan tampilan konfirmasi pengiriman pesan yang gagal, tidak dapat melakukan serangan terhadap *mail server* milik ptba pada saat akan mencoba mengirimkan. Karena *mail server* milik ptba merupakan *mail server* yang dapat diakses pada jaringan internal saja.

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

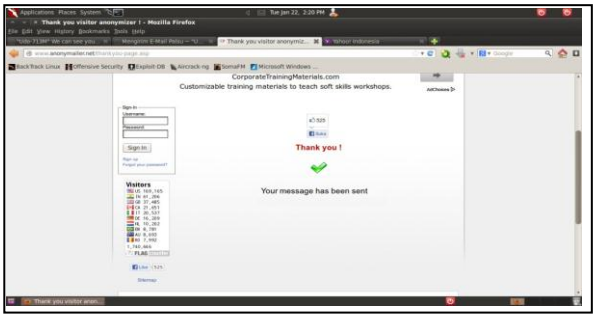


Gambar 42. Isi *Form*

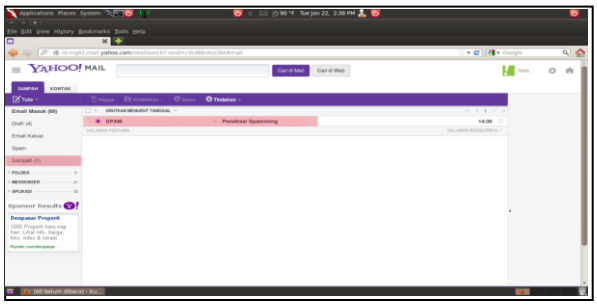
Pada gambar di atas penulis mencoba melakukan serangan *spam* terhadap alamat target yang lain. Setelah mengisi *form* tersebut kemudian masukkan kode, selanjutnya pilih *Submit.*



Gambar 43. Masukkan Kode



Gambar 44 Pesan berhasil dikirimkan



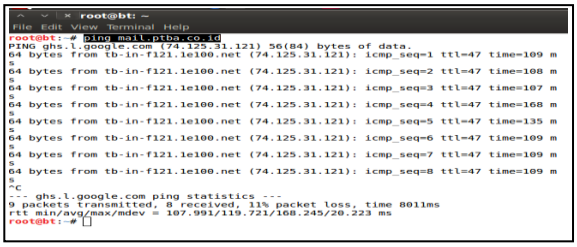
Gambar 45. Tampilan *email* target

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

5. Melakukan Serangan *Dos* Terhadap *Mail Server* PT. Bukit Asam (Persero) Tbk

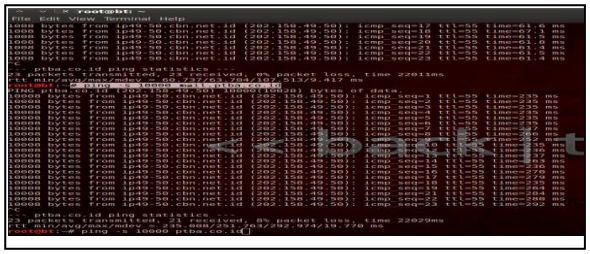
   Untuk melakukan serangan ini, penulis memakai operasi sistem *Backtrack 5,*

menggunakan terminal dengan mengetikkan perintah *ping mail.ptba.co.id* dan *ping –s 10000 mail.ptba.co.id* pada gambar 3.44,



Gambar 46. 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 *IP Name'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 47. Melakukan *ping –s 10000* pada situs *mail.ptba.co.id*

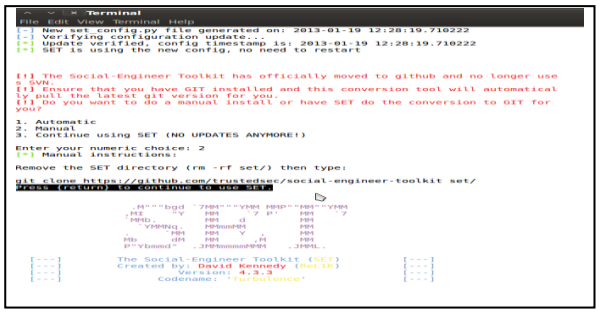
Pada gambar di atas merupakan cara untuk *ping –s 10000* pada situs *mail.ptba.co.id* penulis melakukan *ping* pada *IP Host's Address* dan *IP Name's Server* mereka dengan menjalankan perintah *ping –s 10000 mail.ptba.co.id.* Dengan melakukan serangan ini, apabila seseorang ingin mengakses situs *mail.ptba.co.id* akan merasa lama saat melakukan *browsing*.

6. Melakukan Serangan *Phising* Terhadap *Web Mail 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 48,

Gambar 48. *Social Enginnering Tools*

Pada gambar di atas merupakan tampilan di terminal pada saat kita membuka *Social Enginnering Tools* pada *Backtrack 5.*

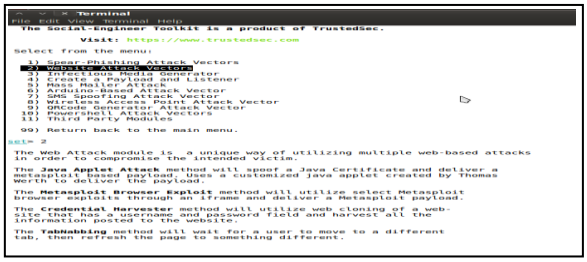


Gambar 49. *Press (return) to continue to use SET.*

Gambar 50. *Social-Engineering Attacks*

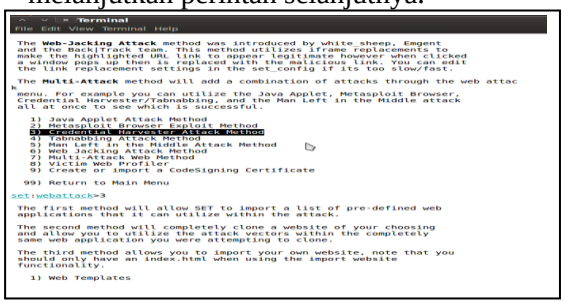
Pada gambar di atas, kita disuruh untuk memilih menu untuk melakukan serangan. Untuk melakukan serangan *phising* ini kita pilih menu nomor 1 yaitu *Social-Engineering*

Attacks. Selanjutnya tekan *enter* untuk melanjutkan perintah selanjutnya.



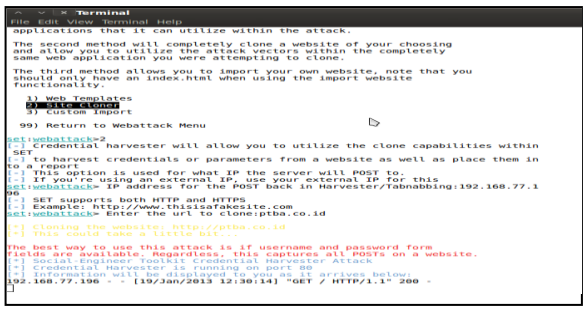
Gambar 51. *Website Attack Vectors*

Selanjutnya Pada 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.



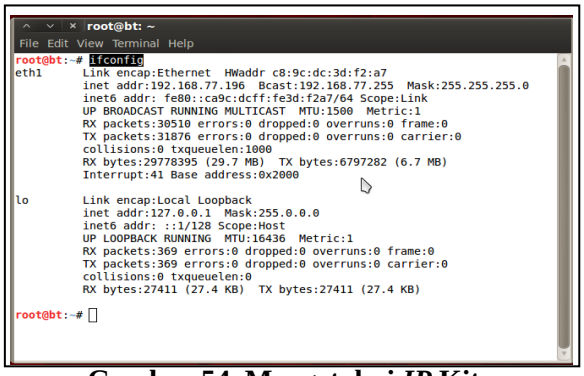
Gambar 52. *Credential Harvester Attack Method*

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



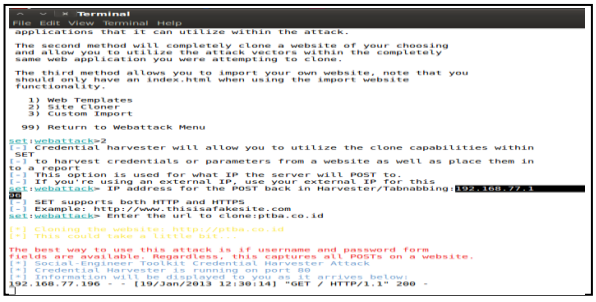
Gambar 53. *Site Cloner*

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.*

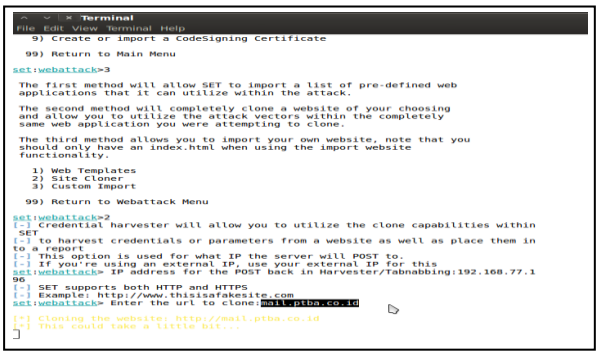


Gambar 54. Mengetahui *IP* Kita

Pada gambar di atas merupakan tampilan di terminal dengan menggetikan perintah *ifconfig*. Kemudian di sana akan tampil alamat *IP Address* 192.168.77.196.

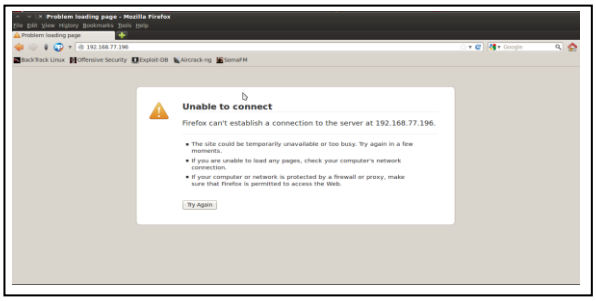


Gambar 55. Masukkan *IP* Kita



Gambar 56. Masukkan 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.*



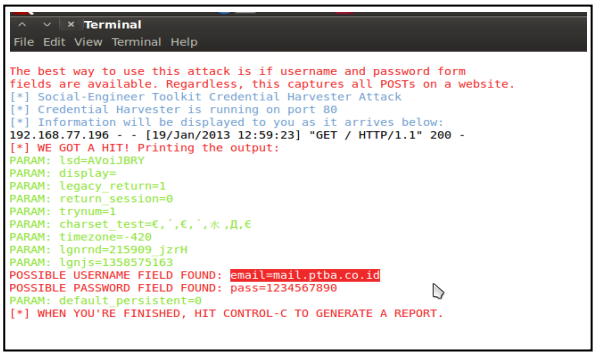
Gambar 57. Melakukan *Browser* Pada *IP* 192.168.77.196

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 pada gambar 58 yang berhasil melakukan serangan *phising* terhadap *website ptba.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 58. Melakukan *Browser* Pada *IP* 192.168.77.196

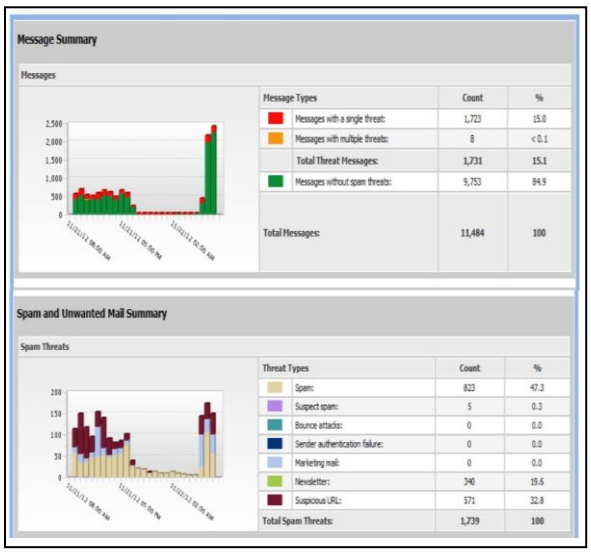
Gambar di atas adalah pada saat melakukan *browser* pada alamat IP 192.168.77.196. tampilan yang keluar yaitu tampilan halaman *web ptba.co.id*. pada saat sebuah *admin* atau karyawan lain ingin *login* pada *website* ini tetapi dengan catatan dengan mengtikkan alamat *ip* kita, otomatis nama *user*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



Gambar 59. *Record Username* dan *Password*

3.3.4. 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 60. *Report* dari tanggal 21 sampai 22 Novemver 2012

Pada gambar di atas merupakan penjelasan tentang *report* yang berisi jenis-jenis serangan yang terdapat pada surat elektronik yang berhasil disaring.

Pada penelitian ini terdapat dua tabel yang masing masing berisi tentang hasil *report* dari sistem penyaringan terhadap surat elektronik. pada tabel 3.1 berisi tentang *message summary* yaitu jenis pesan dan jumlah surat elektronik yang di *capture* selama 24 jam. Kemudian pada tabel 3.2 berisi tentang jenis serangan yang tertangkap atau *spam* dan *unwanted mail summary (Inbound dan Outbound).*

Tabel 1. *Message Type*

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

Pada tabel 1 merupakan *report* yang menjelaskan tentang jenis-jenis surat elektronik dan jumlah surat elektronik yang masuk. Untuk jumlah surat elektronik yang 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 2. *Threat Type*

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

Pada tabel 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.

4. SIMPULAN

Simpulan yang dapat diambil diantaranya;

1. Melihat dari cara kerja *Symantec Message Gateway* dalam mengamankan jaringan terutama pada surat elektronik kita 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,
2. Dengan melakukan konfigurasi sistem 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
3. 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.

DAFTAR RUJUKAN

Ardians.(2012). *Email Adalah.* Diakses 07 November 2012 dari http://41809129. blog.unikom. ac.id/ email-adalah. 5ne.

Brankazilmu.(2011). *Router Dan Gateway.* Diakses 08 November 2012 dari 2.bp. blogspot. com/-F0 N6 vx kA FQ/TpV 6C1Z NXI /AAA AA AAAA CM /ft0 L6auuo68/s1600/Router+dan+Gateway. bmp.

Eueung Mulyana dan Onno W, Purbo.(2010). *Paket Filtering.*Diakses 02 Oktober 2012 dari http:// hadewi. wordpress. com /packet - filtering/.

Jagat.(2010)**.** *ESET Akuisisi Pengembang Antispam Energi Baru Bagi Teknologi Antivirus Masa Depan.* Diakses 20 Oktober 2012 dari http://www.jagat review. com/2010/ 09/pr- eset- akuisisi-pengembang-antispam-energi-baru-bagi-teknologi-antivirus-masa-depan.

Komarudin.(2012). *Pengertian Definisi Analisis.* Diakses 08 November 2012 dari http:// mediain formasill. blogspot. com/2012 /04/ pengertian-definisi-analisis.html.

Meta.(2011). *Phising Adalah.* Diakses 20 November 2012 dari http:// supernewbie. wordpress. com/ 2011/05/07/ phising-adalah/.

Nasir, Moh,Ph.D.(2003). *Metode Penelitian*. Jakarta: Ghalia Indonesia.

Novianihasianna.(2012). *Network Security*. Diakses 06 Oktober 2012 dari blog.ub .ac.id/ novian ihasianna/2012/ 09/24/ network- security/.

Panjaitan.(2008). *Email Spam Filtering.* Diakses 10 November 2012 dari http:// panjitapen. wordpress. com/2008/01/27/email- spam-filtering.

Qbonk.(2011). *Keamanan Jaringan Komputer*. Diakses 2 Oktober 2012 dari http://agussale.com/ keamanan-jaringan-komputer.

Sugiyono, Dr. Prof.(1999). *Metode Penelitian Bisnis.Bandung*:ALFABETA.

Symantec.(2011). *Symantec Message Gateway 9.5*. Diakses 12 November 2012 dari http://symantec.com/ Symantec Message Gateway9.5.

Widagdo, Jason.(2011). *Dengan Jurnal Gateway Server*.

Zakaria, Teddy Marcus dan Oscar Wongso.(2011). *Dengan Jurnal Studi dan Implementasi Teknologi Flashdisk dan Email Gateway Dalam Penyewaan Alat Pada Perusahaan X*.