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, elektronik bahkan sudah surat meniadi komunikasi utama di kantor atau antara pelanggan dan nasabahnya. Pada PT Bukit Asam (Persero) Tbk, fasilitas surat elektronik yaitu berfungsi sebagai penggerak roda 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 antispam. 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 antispam 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,

- Dapat mencegah ancaman dari hal-hal yang membahayakan jaringan,
- Membuat analisa terhadap sistem yang diterapkan di perusahaan.

1.1.2. Manfaat Penelitian

Manfaat yang bisa didapatkan dari penelitian ini adalah;

- 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.
- 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 РТ 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;

- Penulis akan menjelaskan bagaimana cara kerja dari *email gateway* yaitu Symantec Message Gateway 9.5 yang digunakan oleh PTBA dalam mengamankan surat elektronik perusahaan,
- Kemudian bagaimana konfigurasi sistem yang digunakan,
- 3. Serta melakukan pengujian terhadap sistem tersebut pada jaringan PTBA,

 Dengan melakukan rencana tindakan ini penulis akan mendapatkan hasil yang didapat berupa *report* dari sistem tersebut dan kemudian report 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 diencription. 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 diencryption, 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 diencryption 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,

9	Symantec Mes	saging Gateway	
	Select language:	English	*
	User name:		
	Password:		
		(Login)	
		Need help logging in?	
	Copyright @ 1998-2012 Sys	mantec Corporation. All rights reserved.	

Gambar 4. Login 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

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

Settings
Alerts
Control Center
Directory Integration Logs
Reports SNMP
UPS

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,

ge certificates for your system. The TL cure Web management; Domain keys a	S certificate is used by MTAs in each Scar are used for DomainKeys Identified Mail (I	nner appliance; the Contro DKIM) signing of outbound	I Center uses the HTTPS cert mail.
tificates			
TLS & HTTPS Certificates	Certificate Authority	Domain Keys	
Add Edit Delete View	Import Export		
TLS & HTTPS Certificates		Status	Expiration
No certificates specified			

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,

Host Configuration		
Reconfigure a Scanner or Control (Center host.	
		1
AddEdit	Delete Enable	Disable
Hostname	Description	Enabled
SPC-DEMO-SMGv2	Local Host	✓
SPC-DEMO-SMGv2	Local Host	✓

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,

Inbound	Outbound	Authentication		
Inbound Mail Settin	gs			
Inbound mail IP addres Ethernet 1: (10.101.1	s: Port: 4.113) • 25			
Accept TLS encr	yption RC-Self	fSignedTLS 🔹		
-	nt costificato			

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;

 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,

					Construction of the local division of the lo		and the second second	Concerning.	
Spiers	Customer	opecific Span	submission	1. T					
ferent	Providen and Customer	specific Spam	Submission 1	idealan altrig					
Probe Accounts Guar settings Goan Settings Dender Authentication Rabinissian Settings	Enable E En To utility	Costomer spec die Costorer-sp roles created ho	die Span Feat ofs Span Sdra n your span o.b	ures nam (* nadore you hud	also create and app	dy a span pole	with the condition Th	e message in	culturer-specific spani.
Submit Hesseges Guarant lan -	- Cont Visual Visual	nfiguration tomer specific natiobtain a Sub ad from your sub	Suber System Provid nitter ID from Sy ference specifica	itters Lok Ionieng Inarited Before yo By to your envelo	u can mårat messag mert.	pee. The ID war	ke with your Systemeter	Managing (Latamay to apply spars rules
		brotter ID:				1940	a is currently rep Subre	ther 3D respon	recent to this Control Center
Symantec.						Engiler fo	a figure (Subscription (S) for		an Entring Substitution (D)
	- 546	nstaation Aggres	siveness						
	Set the apprendications of customer-specific span adversion rules.								
		Conservative - Or Appreciate - Ever	dy messages with y submission get:	nultiple nultress s nult	onsi get rules				
	and the second second								

Gambar 12. Submission Settings

 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,

Symantec Messagi	ng Gateway Status Reports Proto	cols Reputation Spain Malware Can	tent Administration
ipam	Customer-specific Spam submissions		
olicies	Provision and configure customer-specific span submission a	antinus.	
Email		1990 (* 40)	
ettings	Customer-specific spam submission Settings		
Probe Accounts Quarantine Settings Scan Settings Sender Authentication Submission Settings	 Enable Customer-specific Spain Submission III To ublice rules created from your spain submissions y 	New Submitter ID Registration in Progress	ge is customer-specific s
ubmissions -	Configuration Subvitters List	Please wait, This could take several minutes. Please do not close your browser or turn off your computer unbil the process has been completed.	
Submit Hessages	Customer-specific System Provisioning		
Juarantice	You must obtain a Submitter ID from Symantec be created from your submissions specifically to your	1.1	ng Gateway to apply sp
	Submitter ID:	There is currently no Submitter I	D registered to this Control
Symantec.		Register for a New Submitter ID New	Enter an Elisting Subm
	Submission Appressiveness Set the appressiveness of custome-specific span @ Conservative - Only messages with multiple so @ Appressive - Every submission gets a rule	automosion nales. Jonessons get nales	
	Customer-specific Spam Data Retention		

Gambar 14. Submitter ID Registration

Pada gambar di atas adalah proses masa registrasi ID Costumer,

Symantec Messagi	ng Gateway	Status	Reports	Protocols	Reputation	Sparm	Malmare	Control	Administration
Ggam	Customer-1	specific Span	n submissions .						
Policies -	Provision and	configure custore	er-specific span suf	omission settar					
Ersail	Customer	specific Span	n Submission Se	times					
Settings									
Probe Accounts Quararitime Settings Scan Sattings Sender Authentication Submission Settings	1 the	able Customer-spin	oofic Span Subrissi on your span subris	kon (B) Re Assions y	gistration Comp	pleted			e is customer-specific spani.
Submissions -	C.0	inliguration	Submitt	ters List	Submitter ID is specific span	n submission i	ccessfully. Custor settings have bee	n l	
Submit Messages	Cust	tomer-specific	System Provision	ning		societanity -	Lergu.	-	
Quarantine	Your	nust obtain a Sub	mitter ID from Syna	intec be					g Galeway to apply spam n
Email Spam	creat	ied (non your sub)	missions specifically	so your				ON.	
	Su	bmitter ID:							912540
Symantec.						Register for	a New Submitter ID	Novil 5	Enter an Existing Submitter
	Suba	mission Aggress he aggressivenes Conservative - O Aggressive - Eve	silveness is of customer-speci Xily messages with n ity submission gets *	fic spam subme ruftiple submer a rufe	ssion rules. Rone get rules				

Gambar 15. Registration Completed

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

Symantec Mer	saging Gateway	Status	Reports	Protocols	Reputation	Sparn	Malware	Content	Lopged in as: Administration
spam	Customer-	specific Spam	submission	\$					
olicies Email ettings Probe Accounts	Custome Group. C Provision and Customer	rr-specific Span lick here to conf configure custome -specific Spam	Policies are r Interes r-specific span : Submission :	not enabled. Cur submission setting Settings	s.	ules are not r	etrieved until a p	solicy is enabl	rd and assigned to a poli
Quarantine Settings Scan Settings Sender Authentication Submission Settings	Enable V En	Customer-spec	i fic Spam Feal ofic Span Subm	ission ®	t also maala and an	nhu a sman nois	suith the condition	The marrane i	national startific man
Submit Messages Exarantine Email Spam	Co	infiguration tomer-specific S must obtain a Subm ted from your subm	Subn System Provis uiter ID from Sy uisions specifica	vitters List Ioning Huaritec before yo ily to your enviror	u can submit messa went.	ges. This ID wor	ils with your Syman	thec Messaging (lateway to apply span rules
Symantec.	Su	ømitter ID:							91254040
						Register fo	r a New Submitter I	En Now	ter an Existing Submitter ID
	Sector	mission Aggress the aggressiveness Conservative - Ori Aggressive - Every	elveness of customer-sp ly messages wit y submission get	ecific span submis h multiple submissi s a rule	sion rules. ons get rules				

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,

	Distomer-snerific Sham Submission Settions
Probe Accounts Quarantine Settings Scan Settings Sender Authentication Submission Settings	Tradic Contrare specific Specific Datasets
Submissions	To date rues character rue your span submasces you must also character and apply a span pacy with the conduction the bessage a customer specific span.
Submit Messages	Configuration Submitters List
Quarantine	
Email Spam	Blowd: Only absention on drived additions on this bit is on obtait messages. Blowd: Speen shows of one to an outlet for messages that are additisted from even additional in the lat. Education Additionals: Housely, all mult addresses: Additional additionals: Additional additionals: Additional additionals:
	Import enal addresses:
	Dekto Al Export Entries per page (25 = Displays (0 = of 0 = 1 + 1 + 2)
	Submitter Imail Address 💌
	There are no Submitter Enal Addresses.

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,

	Customer-specific Span: Modily subject line with "Customer-specific Span."	-	Inbound only	0
6	Customer-specific Span: Delete message	a.	Inbound only	0
2	Outone-specific Span: Our aritire message	-	Inbound only	0
1	Customer-specific Span: Deliver normally	-	Inbound only	0



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

-oncies ~	Configure an email spam policy and apply it to selected policy groups. Specify filtering conditions and corresponding actions to					
Email	take on spam or unwanted mail.					
Settings	Email Spam Policy					
Probe Accounts	Policy name:					
Quarantine Settings	Customer-specific Spam: Quarantine message					
Scan Settings Sender Authentication	Candhiana					
Submission Settings	Conditions					
	Inbound messages					
Submissions	If the following condition is met:					
Submit Messages	If a message is customer-specific spam v					
Quarantine ^	Actions					
Email Snam	Specify actions to take on messages that trigger this policy.					
	Add Edt Delete					
Symantec.	Actions					
	Hold message in Spam Quarantine					
	Apply to the following policy groups					
	V Policy Groups					
	[☑] Default					
	Save Cancel					

Gambar 19. Setting Email Spam Policy

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

Oustoner-specific Span: Modily subject line with "Oustomer-specific Span"	-	Irbound only	0
🗍 Gustomer-specific Soom: Delete message	-	Inbound only	0
7 Ostone-specific Span: Quarantine message	1	Inbound only	1
🛛 Customer sanche Saam. Deiver normaliv	-	Inbound only	0

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. Dilakukan dengan cara mengupload pesan dengan secara manual. Yaitu dengan cara memilih menu "Spam" kemudian pilih "Submission" di menu bagian kiri. Setelah itu "send message",

	Submit & Messane
opani Delicies	Julimit A Pressuge
Email	Select a message type and paste or upload a message below. Then press the 'Submit Message' button to submit it to Symanities for rule creation.
Settings	Message Submission Form
Probe Accounts Quarantine Settings Scan Settings Sender Authentication Submission Settings	Message Type Faite Negation - Hood Span Table Positive - Hood state Table Positive - Hood state
Submissions Submit Messages	Subinission Centent Uplind a Message Browne.
Quarantine	Padre a Message
Email Spam	
Symantec.	

Gambar 21. Subbmit A Message

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

	COLUCITICA	donutio	10015				
DLP	Conned	t					No Disclair
Incid	ent Man	ageme	nt	-			Disclaimer
Fold	ler Over		Migro				
INFO	ORMATIC		Inbour				
Info	rmationa	al Incid	ents			Migros	
Cre	dit Card	Folde	er			Restrict	
OLIA	RANTIN	E FOLD	ERS				Outbound
Qua	rantine I	nciden	ts				Delete Ex
						(m)	
	-				_		
Quarantine Incid	ents						
Quarantine Incid Search Filters	lents	vinessaes. In any field, wa	unavuse an adtesis (*) In nerfor	n a uidrard swirth.			
Quarantine Incide Search Filters Use filters to search Status:	ents h the Incident Management for sidelin All	ed messages. In any field, you • Severity:	u may use an asterisk (*) to perfor All	n a wildkard search. • Message state:	Al		
Quarantine Incid Search Filters Use filters to seard Status: To:	ents h the Incident Management for sidein All	sd messages. In any field, you • Sevenky: Franc	u nay use an asterisk (*) to perfor All	n e wiktand search. • Message state: Subject:	Al		•
Quarantine Incid Search Filters Use filters to search Status: To: Policy name:	ents h the Indient Management for sidelin All All Policies	ed messages. In any field, you • Severity: • From: • Time range:	u nay use an astersk (*) to perfor All Past hour	n e wildrand seerch. • Message state: Subject: •	All		-
Quarantine Incid Search Filters Use filters to seard Status: To: Polcy name:	ents All All Policies	ed nessages. In any field, you Seventy: From: Time range:	any use an astersk (*) to perfor All Pest hour	n e vikkord search. V Message state: Subject: V	All	ay	Gar
Quarantine Incid Search Filters Use filters to seard Status: To: Poky name: Hide Filters	ents All All Policies Ethnis per page 500 - 0	ed nessages. In any field, you Severity: Pross Time range: splay: 0 - of 0	anay use an asterisk (*) to perfor All Past hour	n a vilikard search. • Message state: • •	Al	8y	- Ger
Quarantine Incid Search Filters Use filters to seard Status: To: Policy tane: Hole Filters Hole Filters	ents http://www.internet.for.iddin Al Al Al Al Al Al Policies Entries.per.page(500 D TTF-0) D	ed messages. In any field, you seenity: Franc Time range: splay: (- of 0 () inhate: Comma (,) -	a nay use an asterisk (*) to perfor all Pest hour Export Inodent Hetery	n a wikkard search. • Message state: • Sobject:	All	87	Ger
Quarantine Incid Search Filters Use filters to seard Satus: To: Poky name: Hole Filters Inciding (Unicode (UT Delete Del	ents the holder Khangerer for skills Al Al Policies Doins per page 100 - D Tri-0 - D ier. Al Approve	ed messages. In any field, you severity: Prove Time range: piley: 0 - jel 0 Reject Comma (,)	All Past hour Export incident Hitlery This Span	n a vidóard search. • Messaga state: • Sabject: • The is NOT Span	All Disp	ay)	Clev Forwed Incolor

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,

Su	bmit as Spam		*
₫	Are you sure you w SPAM to Symantec	ant to submit selecte Security Response?	d message(s) as
		Cancel	Submit as Snam

Gambar 24. Submit as Spam

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

down.		Spam Messag	e Quarantine				
olicies		Message(s) s	accessfully subm	itted to Symani			
Email	1	Delete Delete Al Release This is Span			This is NOT Span	Show Filters	
iettings		Entries per page: 100 • Display: 1-100 • of 114,258					
Probe Accounts		8	To		From	5	iubject
Quarantine Settings				kristal	hotel	YENE SEZON FEYATLAR	
				and the lot of the lot			
Symantec Mess	aging Gateway	Ratus In	o () ports Protocols	Republican	Span Malware Cantent	Administration	
Symantec Mess	aging Gateway Spam M	Status Au	9 () parts Protocols	Reputation	Spon Malware Carterk	Adransfordian	
Symantec Mess Span Polices	aging Gateway Span N	Status Ro Status Ro Inscape Quarantine	9 (b) parts Protocols Polose	Republican The super	Spann Makawe Castere Noskoli Span Star	Advance allow	-
Symantec Mess Span Polices Enel	aging Gateway Span N Ethespe	Ratus Ro Rescape Quarantine E Detes Al	Ports Protocols Rokaze	Republikan The slipes	Spon Makare Cateret	Administration	-
Span Span Nokes Ettel ettaps	aging Gateway Span N Deer pr	Status A Escage Quarantine Detec Al poper 101 + Deple To	9 0 parts Protocols Rebase	Republican Nossipan (20) () () ()	Spann Makare Califord	Admostration offers	Submission State

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",

	Symantec	Messagin	g Gateway	-	atus
Status System Deskt Hosts Schodu SHIP Messag Submis Submis Submis	o ard led Tasks is Audit Louis outputs lione l		Dashboa	rd	atus
Status	Satméssions				
System + Del/board Hotts Loos	Find submissions using custom search other is - Mitter - Schwarzen hann	to activity			
Sydem - Dehtsand Hoth Lop Scheduled Teeks	Find submissions using custom search othere. Filter Submission type: Submitter type:	No restriction • All •			
System - Deaboard Hote Lops Schebuled Tesks System -	Find submissions using custom search otheria. - Filter Submission type: Submission type: Time range: Submit:	No restriction - all - Fast hour - motivas	adobiis (raa-isaaidia)		
System - Dailheard Hota Lop Schebdel Taiks Syttit - Nemege Auft Logi	Find submasters using sature search others. - Hitter Submaster hope: Submitter hope: Su	No redrition - All - Fast hour - natibes - natibes -	substring (case-mansatri-e) -		
System - Davihoseri Hots Schebdel Tasks Setti Message Qorues	Find schmasters untig statum sound unterval - Mare Schmasters Types Schmatter Types Schmatter	Na rudridun - Al - Pat hour - nathes - nathes - nathes -	substring (case-insensibles) substring (case-insensibles) substring (case-insensibles)		
System - Deuthosard Hots Lop Schebdel Teeks State Nessage Qorues Schemistens	Find submeans using cutten search others. - Hiter Submitten tope: Submitten tope: Submitten tope: Submitten tope: Submitten medi subdem: True or Submitten and subdem: True or Submitten and subdem:	No restriction - Al - Path hour - matches - matches - matches - matches -	substras (case-instablee) - edistras (case-instablee) - substras (case-instablee) - substras (case-instablee) -		
System - Desitioneri Houta Logo Logo Soft Setterbiod Tasks System Hensione Courses Softensiones Softensiones Detail	Fiel submore sing submore in the sub- Field automore site submore sub	la notidas al entre estados Instituies entre estados natiles entre estados natiles entre estados natiles estados estados natiles estados estados estados estados natiles estados estados estados estados estados natiles estados estados estados estados estados estados estados natiles estados estados natiles estados estados natiles estados estados natiles estados estad	silating (san-manifes) silating (san-manifes) silating (san-manifes) silating (san-manifes) silating (san-manifes) silating (san-manifes)	es Display Fillend	
System - Davitsered hvots Lackbool Taxis SHE	Pref submisses sing submisses (integration see), china Filter Salantian Age: Salantian A	la mototon al e hatibue natibae natibae natibae natibae natibae natibae	sáðring (sam-innstaline) haðring (sam-innstaline) sáðring (sam-innstaline) sáðring (sam-innstaline) Gær Re	es Dada Mend	
System - Desthered instit up totebole Tests	Pet adverse ung auton seef, others. PER Satistics hope Salable hipe The engs, Salable Hours Select mill address Hours Select mill address Hours Select mill address Thor of ce mill address Boort Clor There	la reductos al Partour - natora - natora - natora - natora - natora -	sårting (son-konstitue) sårting (son-konstitue) sårting (son-konstitue) sårting (son-konstitue) sårting (son-konstitue) Sødpet	es Daday Filtered Daday Filtered Salantiter	- Courd of
System - Conferent - moto - Conferent - moto - Logo - Software - S	Productions unique to the set of	le mobilito al fattor nation nation nation nation nation nation nation nation nation nation nation nation nation	sådning (sam-kanstänn)	es Daday Rend Daday Zen Salauter	- e cour o Trace Ma

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,

nia subresens using cusion search circana.					1	This list is generated at 0	(5:43:40 PM on Septembe	r 25, 2012
Filter Submission type:	Non	estriction						
Submitter type:	Al							
Time range:	Past	hour	,					
Subject:	mate	hes		substring (case-insensitive)	•			
Submitter email address:	mat	hes	,	substring (case-insensitive)	•			
From: or Sender: email address:	mate	hes		substring (case-insensitive)	•			
To: or Cc: email address:	mate	hes		substring (case-insensitive)	•			
					Clear Filters	Display Filter	ed	
Export CSV						Display:	8 • 901•	d 1()[
ne 🕶	To/Cc	Fn	om	Subject		Submitter	Туре	Valid
andres from the total of the second sec				and strong than apply			Moral Scan	Mar

Gambar 27. Tampilan Filter

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

		This view is generated at (5:44:28 PM on September 25,
🛙 Message Data		
Submission ID:	06000011505061be63d5d24010076c0b50000000093	740554242563
Submission type:	Missed Span	
Submitter type:	Adhin	
Time received:	Tuesday, Sep 25, 2012 05:23:31 PM EEST	
Submitter email address:		
Sender email address:		
To/Cc email addresses:		
Subject:	YON SECONFORMLARIN CHAIL	
Caught by good rules at submission time? Caught by contomer, marilic rules at submission time?	ND No.	
valid	Ver	
Message history:	Details	
Message data options:	A Vew raw message data	
	Annotate this message	
	Resubrit this message as Mixdentified as Spani	
∃Message Data		
Submission ID:	06000011505061be63d3d24010076c0b500000	00000937a0554242563
Submission type:	Missed Spam	
Submitter type:	Admin	
Transist	T C AT ANALY AN AL BUTT	
have received.	TUE908Y, SEp.25, 2012/05/23:31 PM EEST	
Submitter email address:	1089089, 580.25, 2012/15/28:31 PM 6651	
submitter email address: Sender email address:	1089089, 969 25, 2012 18:23:31 PM CEST	
inne recovers: Submitter email address: Sender email address: To/Cc email addresses:	108984, 580.65, 2012 (IS-23: 54 PRIEES)	
subarter enail address: Sender enail address: To/Cc email addresse: Sender de Salarder	196999, 369, 26, 202, 2012, 23, 31, PM (22, 31, PM (22	
sum receives: Sobmitter email address: Societ e mail address: To/Cc email addresses: Sobject: Sobject:	YEM SEZON FYNALARHI Cotals	
sinterecoverse Submittere enval address: To/Cc enval address: To/Cc enval addresses: Subject: Cought by chol rules at submission time? Cought by chol rules at submission time?	Heldery, Sep. Co., OLICIAL CO. IN CASH	
Intercenent Submitter ennal address: To, T.C. email address: To, T.C. email addresses: Subject Cought by global rules at submission time? Cought by customer-specific rules at submission time?	HBROW, MD CS, ULL (MCLS) YBM SECON FILMLARIE (MCLS) No No	
min recover. Sender ennal address: Sender ennal address: Subject: Subject: Caught by clubal rules at submission time? Caught by clubal rules at submission time? Wald: Distances Recover.	INSTRUCTION OF THE OWNER OWNE OWNER OWNER OWNE	
min roomen Solutire end address: Souder end address: To (Ce end) addresses: Solyto: Cought ty gold and less at submission time? Cought ty cold and less at submission time? Cought sy cold and less at submission time? Nake B Pessage history:	INFORME AND A DECEMBENT OF A DECEMBENTAL OF A DECEMBENTAL OF A DECEMBENT OF A DECEMBENTAL OF A DECEMBENT OF A DECEMBENTAL OF A DECEMBENTA	
nine recovers Soudor enail address: Soudor enail address: Solghert: Caught by goldan niles at submission time? Caught by contame-specific rules at submission time? Kald: Message history:	Internet, yes on plant sources in the second	Dea .
nine recovers Sender enail address: Sender enail address: To (E. email addresse: E shalpet: Caught by cloads index at submission time? Caught by cload mer specific rules at submission time? Wald: El Message listory:	Inderson, yes da, data features i Inder 2020 Film Lucitis information Inder 2020 Film Lucitis Inder Inder Inder Specify Specify 2021 Strict States Information Inder	Duta Succión admission
nine recover. Sonder en all address: Sonder en all address: To (C en må addresse: Solyhot: Canglet by gibbal rules at submission time? Canglet by gibbal rules at submission time? Canglet by construer-specific rules at submission time? Waldet	164 5204 F141,46 H (beta) 164 5204 F141,46 H (beta) 16 16 16 16 16 16 16 16 16 16	Dela Successful submission Biodytela signature ess credited
min recover Sender ennal address: Sender ennal address: E subject: Cought by subject inter? Cought by costome-specific rules at rubmission time? Kuble № Hessage lastory:	104 22011 F1A1LAHI (briefs 104 22011 F1A1LAHI (briefs 106 22011 F1A1LAHI (briefs 106 106 106 106 106 106 106 106	bala Sunstri sahasan Sudyka sahasan Sudyka sahar wa cealad
min roomen Solartise email address: Souder email address: To (C. email addresse: Solaris: Canght by solar helps at solarission time? Canght by solar helps at solarission time? Wald: ≥ Hessage history:	Intel Intel Intel <td>Buta Succedul administra Bodhishi ngadura wa creded Ingliciji gadura wa creded Techal againt customengedir culas</td>	Buta Succedul administra Bodhishi ngadura wa creded Ingliciji gadura wa creded Techal againt customengedir culas
nine recover. Soudor enail address: Soudor enail address: Solghett: Solghett: Caught by goldar nikes at submission time? Caught by contoner-specific rules at submission time? Wald: Pressage history:	Intelligence Intelligence	Buta Sunströf abnision Bolthän ägnäter was created Brythöjä spature vas created Tarkho gänä dyösän synsä väisi Tarkho gänä dyösän sisi
min rooms Sender enail address: Sender enail address: Sender Subject: Cought by color and a solumission time? Cought by color and a solumission time? Yaid: Pressage history:	164/82/, 166 20, 2011 (164/04) 164/82/2011 (164/04) 166 160 160 160 160 160 160 160	Deta Sunstrik sherition Boğhtah signalur wa created Hotal qujeta ustrane-genific ules Tentel qujeta ustrane-genific ules Tentel quieta global ules Honage untrabulated bolah het bullotti. Deng preseted

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*



Gambar 33. Output nmap ptba.co.id

anmand: mmap -T4	-A v 202 158 49 50
Training I	
NAGA SOVINS	Aming Carpon Ports / Hester Supprogram Roads
5 HUST D (149-50.ctm.m	(map 14 % 1 502 130 45.0)
	Starting Mmap 6.01 (http://mmap.org) at 2013-01-17 15:21 MIT
	Bit Script Pre-scanning
	Conting Q2.158.49.5 [4 ports]
	Initiating Parallel DBS resolution of 1 host, at 15:21
	Completed Parallel DMS resolution of 1 host, at 15:21, 0.05s elapsed Initiating SYM Stealth Scan at 15:21
	Scaning 1949-50.cbn.met.16 (202.135.49.50) [1009 ports] Discovered come port No/tcp or 202.135.49.50
	Completed SYM Stealth Scan at 15:21, 5:40s elapsed (1000 total ports) Initiation territor scan at 15:21
	Scanning 1 service on 1949-38.cbn.net.14 (202.154.48.50) Committed Service scan 21 19-22. A 195 allocated 1) service on 1 host1
	Initiating 05 detection (try #1) against 1949-30.cbm.met.id (202.158.49.50)
	Initiating Traceroote at 15:22
	Completed FaceFolder at 19122, 1.000 stoppen Initialing Parallel Disc resolution of 13 hosts, at 15:22
	completed Parallel DBS resolution of 13 hosts, at 15:22, 0.22% elapsed MSE: Script scaming 202.150.40.50.
	Initiating MSE at 15:22 Completed NHE at 15:22, 2.65s stapsed
	<pre>Mmap scan repurt for ip49-50.cbm.met.id (202.130.49.50) Host is up (0.045s latency).</pre>
-	Not state SERVICE VERSION
Characteriza 1	Ent/top filtered ontp
n ipsy so con ne	00/tcp open http Apache httpd 2.2.14 ([Ubuntu]) I http-methods: No Allow or Public header in OPTIONS response (status code 302)
	http-title: PT Bukit Asam Tbk.
	1 Requested resource was http://ptba.co.id/en/home 135/tcp filtered warpc
	139/tcp filtered netboos-ssn
	Parise types energing unpose terminal firesall MAP
	Running (JUST GUESSING): Linux 2.6.X(2.4.X (87%), IGEL Linux 2.6.X (87%), IPFire Linux 2.6.X (85%)
	Description of guessies; Linux 26.32 (BPA), Jobs 001 thin client (Linux 26) (BPA), Linux 26.52 (BPA), Lin
	IPFire firewall 2.11 (Linux 2.6) (85%), Linux 2.6.36 (85%), Linux 2.6.18 (85%), Linux 2.6.31 - 2.6.32 (85%), Linux 2.6.34 (85%) In every 66 matches for best (test conditions non-ideal).
	Uplime puess; 34.078 days (since fri Dec 14 13:30:09 2012)
	Hetwerk Distance: 13 hops TPP Semane Prediction: Difficulturabil (Seed Jurki)
	IP ID Sequence Generation: All zeros
	TRACEADUTE (using sert 587/tcs)
	HOP RTT ADDRESS
	1 00 m5 102.400.77.1 2 3.12 m 132.160.11
	3 33.25 ms 1.subnet110-137-128.speedy.telkom.net.id (110.137.128.1) d file d
	5 55.13 #5 118.99.43.249
	6 55.56 ms 102.submet118-98-57.astimet.telkom.met.id (118.98.57.102) 7 50 01 ms 118 98.55 241
_	0 56.73 as telkomet.openisp.met (218.100.27.29)
Eliter Meetre	9 49.57 ht g1g3-0-0.0pen1xp.met (218.100.27.129) 10 47.60 ht 218.100.36.36
Hite Hoss	Reveal for Contrait - webbes 110 Constrait a. Constrait - Transa Constrait -
B Index States or	Annualis M suscess tion 3.6.33 (PD). MD (D) this client (Lies 3.6) (PD). Lies 3.6.36 (PD). Lies 3.6.36 (PD). Lies 3.6.36 (PD).
Mark Accession	AND PERCENT OF DATABASE LINES 2.6.32 (074), DOL: OD CLINI CLINIS 2.6.0 (074), LINES 2.6.35 (074), LINES 2.6.30 (094), LINES 2.6.34 (094), LINES 2.
	No exact OS matches for host (test conditions non-ideal).
	Hetvork Distance: 13 hops
	IV sequence FreeLclass Dirically-201 (0000 1000)
	TRACERBITE (using sort SE7/tcs)
	HOP RIT ADDRESS
	1 0.3 m 192.100.1711
	3 33.25 ms 1.subset110-137-128.spredy.telkom.net.id (110.137.128.1) 4 45.50 ms 180.252 0.181
	5 55.13 ms 118.98.43.249
	n 55.50 m 102.500mt110.90-57.4511041.10(110.00.001.10(110.00.37.102) 7 55.01 m 110.90.15.241
	6 56.73 as telkomet.openiap.net (218.169.27.29) 9 49.57 as stan0-9 coreniap.net (218.169.27.19)
	10 47.00 m 218.100.36.36
	11 45.70 ms 210.210.181.177.cbm.met.id (210.210.161.177) 12 42.12 ms 210.210.181.138.cbm.met.id (210.210.161.130)
	13 43.02 m5 1p49-50.cbm.net.1d (202.158.49.50)
	MSE_Script Post-scanning.
	Read data files from: /usr/local/bis//share/map
	the set of the second becaused a react and there are second as which we have and the
_	Neap Song: 1 1P address (1 host up) scanned in 20.11 seconds

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 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

Thank you visitor anon Edit View History Dockmarks	ymizer I - Mozilla Firefox Innis, Mete			
tide 71.04" We can see you H	Nergitim E-M HI Palsu - "U	P Thank you visitor anonymiz		
d www.anonymatiot.netthanty			- • C 👌 📲 • 🔞 • Googe	۹ 🔶 ۱
lack Track Linux Mottensive Secu	ity DExploit DB & Aliciacking	Somaf H 🗾 Microsoft Windows		
		CorporateTrainingMaterials.com		
	Customizz	ble training materials to teach soft skills workshops.	AdChases (>	
	Sign In Ubername			
		a) 525		
		Elman		
	Sante	Thank you !		
	Rept to			
	Pargal plan (summint)	\$		
	Maiters			
	191 05 109,145	Your message has been sent		
	GE 37,485			
	11 20,537			
	4, 10, 202			
	AV 8,010			
	1,740,444			
	TO PLAS STREET			
	E2100 (525)			
	Strenge .			

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*.

 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,

File Edit View Terminal Help
root@bt:~# ping mail.ptba.co.id
PING ghs.l.google.com (74.125.31.121) 56(84) bytes of data.
64 bytes from tb-in-f121.le100.net (74.125.31.121): icmp_seq=1 ttl=47 time=109 m
64 bytes from tb-in-f121.1e100.net (74.125.31.121): icmp_seq=2 ttl=47 time=108 m
s 64 bytes from tb-in-f121,1e100.net (74,125,31,121); icmp seq=3 ttl=47 time=107 m
s
b4 bytes from tb-in-fi21.1e100.net (/4.125.31.121): 1cmp_seq=4 ttl=47 time=168 m
64 bytes from tb-in-f121.1e100.net (74.125.31.121): icmp_seq=5 ttl=47 time=135 m
5 64 bytes from tb-in-f121.le100.net (74.l25.31.l21): icmp seq=6 ttl=47 time=109 m
5
64 bytes from tb-in-f121.1e100.net (74.125.31.121): icmp_seq=7 ttl=47 time=109 m 5
64 bytes from tb-in-f121.1e100.net (74.125.31.121): icmp_seq=8 ttl=47 time=109 m
5 ~C
ghs.l.google.com ping statistics
9 packets transmitted, 8 received, 11% packet loss, time 8011ms
rtt min/avg/max/mdev = 107.991/119.721/168.245/20.223 ms
root@bt:-#

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 terdapat ip target 74.125.31.121. sana Selanjutnya terdapat pengiriman paket sebanyak 64 bytes kepada tb-inf121.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. 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*.









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.

A S Brownial	
File Edit View Terminal Help	
The Social-Engineer Toolkit is a product of TrustedSec.	
Visit: https://www.trustedsec.com	
Select from the menu:	
1) Spear-Phishing Attack Vectors	
2) Website Attack Vectors	
a) Infectious Hedia Generator	
5) Mass Mailer Attack	
6) Arduino-Based Attack Vector	
7) SMS Spoofing Attack Vector	
B) WIFELESS ACCESS POINT ATTACK VECTOR	
10) Powershell Attack Vectors	
 Third Party Modules 	
99) Return back to the main menu.	
<u>aet</u> = 2	
The Web Attack module is a unique way of utilizing multipl in order to compromise the intended victim.	e web-based attacks
The Java Applet Attack method will spoof a Java Certificate metasploit based payload. Uses a customized java applet cre worth to deliver the payload.	and deliver a ated by Thomas
The Metasploit Browser Exploit method will utilize select M browser exploits through an iframe and deliver a Metasploit	payload.
The Credential Harvester method will utilize web cloning of site that has a username and password field and harvest all information posted to the website.	a web- the
The TabNabbing method will wait for a user to move to a dif tab, then refresh the page to something different.	ferent

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.

root@bt:	-# ifconfig
eth1	Link encap:Ethernet HWaddr c8:9c:dc:3d:f2:a7 inet addr:192.168.77.106 Ecast:192.168.77.255 Mask:255.255.255.0 inet6 addr: fe80::ca9c:dcff:fe3d:f2a7/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:30510 errors:0 dropped:0 everruns:0 frame:0 TX packets:31876 errors:0 dropped:0 everruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:29778395 (29.7 MB) TX bytes:6797282 (6.7 MB) Interrupt:41 Base addres:9ex2000
10	Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING M'UI:L6436 Metric:1 RX packets:369 errors:0 dropped:0 overruns:0 frame:0 TX packets:369 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:?2111 (27.4 KB) TX bytes:?2111 (27.4 KB)

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.

Pile Edit View Terminal Help applications that it can utilize within the attack.
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.
1) Web Templates 2) Site Cloner 3) Custom Import
99) Return to Webattack Menu
<pre>intitueDatiacb=2 if updatiacb=2 if updatiacb=2</pre>
<pre>[*] Cloning the website: http://ptba.co.id [*] This could take a little bit</pre>
The nest way to use this stick is if usering and instanced for website in the are available. Instances and instances and instances are instances and instances and instances and instances and instances and instances and instances and instances and prime and instances and instances and instances and instances prime and instances and instances and instances and instances prime and instances and instances and instances and instances prime and instances and instances and instances and instances and instances prime and instances and instances and instances and instances and instances prime and instances and

Gambar 55. Masukkan IP Kita

a v 🛛 🛪 Terminal
File Edit View Terminal Help
 Greate or import a CodeSigning Certificate
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.
1) Web Templates 2) Site Cloner 3) Custom Import
99) Return to Webattack Menu
<pre>set:webattack>2 [-] Credential harvester will allow you to utilize the clone capabilities within SET</pre>
[-] to harvest credentials or parameters from a website as well as place them in second second se
<pre>to a teport to a teport t</pre>
[-] SET Supports both HTTP and HTTPS [-] Example: http://www.thisisafakesite.com set:webattack> Enter the url to clone:mail.ptba.co.id
<pre>[*] Cloning the website: http://mail.ptba.co.id [*] This could take a little bit</pre>

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.

File Edit View Terminal Help
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website. [*] Social-Engineer Toolkit Credential Harvester Attack [*] Credential Harvester is running on port 80 [*] Information will be displayed to you as it arrives below: 192.168.77.196 - [19/Jan/2013 12:59:23] "GET / HTTP/1.1" 200 - [*] WE GOT A HIT! Printing the output: PARAM: Lsd=AvoiJBMY PARAM: lsd=AvaiJBMY PARAM: legacy_return=1 PARAM: trynum=1 PARAM: trynum=1 PARAM: timezone=-420 PARAM: timezone=-
POSSIBLE USERNAME FIELD FOUND: <u>emailemaileptbarco.id</u> POSSIBLE DASSNORD FIELD FOUND: pass=1234567890 PANAM: default persistent=0 [*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

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 antispam real time, serta membatasi koneksi yang tidak diinginkan, melakukan penyaringan pesan untuk menghapus konten tidak diinginkan sehingga data vang perusahaan dapat terjaga,
- 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 <u>http://41809129</u>. <u>blog.unikom. ac.id/ email-adalah. 5ne</u>.
- Brankazilmu.(2011). Router Dan Gateway. Diakses 08 November 2012 dari <u>2.bp.</u> blogspot. com/-F0 N6 vx kA_FQ/TpV <u>6C1Z NXI /AAA AA AAAA CM /ft0</u> L6auuo68/s1600/Router+dan+Gateway. bmp.
- Eueung Mulyana dan Onno W, Purbo.(2010). *Paket Filtering*.Diakses 02 Oktober 2012 dari <u>http:// hadewi. wordpress. com</u> /packet - filtering/.
- Jagat.(2010). ESET Akuisisi Pengembang Antispam Energi Baru Bagi Teknologi Antivirus Masa Depan. Diakses 20 Oktober 2012 dari <u>http://www.jagat</u> review. com/2010/ 09/pr- eset- akuisisipengembang-antispam-energi-baru-bagiteknologi-antivirus-masa-depan.
- Komarudin.(2012). Pengertian Definisi Analisis. Diakses 08 November 2012 dari <u>http://</u> <u>mediain formasill. blogspot. com/2012</u> /04/ pengertian-definisi-analisis.html.
- Meta.(2011). *Phising Adalah*. Diakses 20 November 2012 dari <u>http:// supernewbie.</u> wordpress. com/ 2011/05/07/ phisingadalah/.
- Nasir, Moh,Ph.D.(2003). *Metode Penelitian*. Jakarta: Ghalia Indonesia.

- Novianihasianna.(2012). Network Security. Diakses 06 Oktober 2012 dari <u>blog.ub</u> <u>.ac.id/ novian ihasianna/2012/ 09/24/</u> <u>network- security/.</u>
- 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 <u>http://agussale.com/ keamanan-jaringan-komputer</u>.
- Sugiyono, Dr. Prof.(1999). Metode Penelitian Bisnis.Bandung:ALFABETA.
- Symantec.(2011). Symantec Message Gateway 9.5. Diakses 12 November 2012 dari <u>http://symantec.com/ Symantec Message</u> <u>Gateway9.5.</u>
- 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.