ISSN : 2407-1730

VOL. 3 NO.2, Juli - Desember 2017

INFORMANIKA

JURNAL MANAJAMEN INFORMATIKA

POLITEKNIK ANIKA

www.politekanika.ac.id

E-Mail : polika_anika@yahoo.co.id

KEBIJAKAN EDITORIAL

Jurnal Informanika merupakan jurnal yang berisi tentang hasil penelitian, gagasan konseptual, kajian dan aplikasi teori, tinjauan pustaka, atau referensi buku baru dalam bidang Manajemen Informatika. Terbit pertama kali pada bulan Januari 2015 dan terbit dua kali setahun yaitu untuk periode Januari – Juni dan periode Juli – Desember, dengan **ISSN: 2407-1730**

Jurnal Informanika menerima tulisan dalam bentuk hasil penelitian, catatan penelitian, artikel ulas balik, atau ulasan dengan topik bidang komputer dalam bahasa Indonesia maupun bahasa Inggris. Tulisan yang dikirimkan ke Jurnal Informanika adalah jurnal yang tidak sedang dikirimkan ke jurnal atau terbitan lain dan belum pernah dimuat dan dipublikasikan dalam jurnal lain. Tulisan yang dimuat adalah tulisan yang memenuhi persyaratan baku publikasi jurnal, metodologi riset yang digunakan, dan signifikansi kontribusi artikel terhadap perkembangan profesi dan keilmuan di bidang Manajemen Informatika.

Editor bertanggungjawab untuk memberikan telah konstruktif dan jika dipandang perlu, menyampaikan hasil evaluasi kepada penulis artikel. Tanggung jawab redaksi terbatas pada hasil *editing*, sedangkan isi keseluruhan naskah merupakan tanggung jawab penulis.

Jurnal yang telah terbit, penulis akan mendapat dua cetak jurnal dimana tulisan tersebut dimuat dan naskah beserta *softcopy* menjadi milik editor. Artikel yang tidak dimuat tidak akan dikembalikan. Artikel dikirim ke editor Jurnal Informanika dengan alamat:

Editor Jurnal INFORMANIKA
Politeknik Anika Palembang
Jalan Jend. Sudirman No. 3010 B Palembang
Telp. (0711) 311625
Website : www.politeknikanika.ac.id
Email: polika_anika@yahoo.co.id

ISSN: 2407-1730

INFORMANIKA

Vol. 3 No. 2, Juli-Desember 2017

JURNAL KOMPUTER

Alamat Redaksi
Jln. Jend. Sudirman No. 3010 B Palembang
Telp. (0711) 311625
Website : www.politeknikanika.ac.id
E-mail : polika_anika@yahoo.co.id

Terbit Perdana Januari 2015

Frekuensi Terbit
Enam bulan sekali

ISSN: 2407-1730

INFORMANIKA

Vol. 3 No. 1, Juli-Desember 2017

JURNAL KOMPUTER

Daftar Isi

PRIVAT CLOUD STORAGE SERVER RENDAH ENERGI MENGGUNAKAN RASPBERRY PI SEBAGAI MEDIA PENYIMPANAN ONLINE PRIBADI
M. Agus Syamsul Arifin 1-5

PEMANFAATAN *VIRTUAL PRIVATE SERVER* DALAM MENUNJANG SISTEM *HIGH AVAILABILITY*
Chairul Mukmin 6-17

EVALUASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN *DMZ FORTIGAGE-200B*
Kurniati 18-29

TATA KELOLA TEKNOLOGI INFORMASI DENGAN COBIT 5
Tri Oktarina 30-38

SISTEM INFORMASI ADMINISTRASI PENSIUN DAN MUTASI PADA BADAN KEPEGAWAIAN NEGARA KANTOR REGIONAL VII PALEMBANG BERBASIS WEB
Nurul Adha Oktarini Saputri 39-50

APLIKASI PENCARIAN DATA DOSEN PEMBIMBING PADA FAKULTAS ILMU KOMPUTER UNIVERSITAS BINA DARMA BERBASIS WEB
M. Soekarno Putra 51-58

SISTEM INFORMASI KELURAHAN ALANG-ALANG LEBAR KECAMATAN ALANG-ALANG LEBAR PALEMBANG BERBASIS WEB
Edi Supratman 59-64

SISTEM INFORMASI TRANSKRIP NILAI DAN PRASYARAT MATAKULIAH BERBASIS WEB MENGGUNAKAN METODE FUSION
Rahayu Amalia 65-74

ANALISIS TEKNOLOGI INFORMASI PADA PERGURUAN TINGGI AMIK BINA SRIWIJAYA PALEMBANG MENGGUNAKAN METODE SWOT
Nurul Huda 75-80

RANCANG BANGUN MEDIA KOMUNIKASI VOIP JARINGAN KOMPUTER PADA DINAS KEPENDUDUKAN CATATAN SIPIL MUSI BANYUASIN
Zaid Romegar Mair..... 81-91

SISTEM INFORMASI RESERVASI HOTEL 929 BERBASIS WEB MOBILE DI KOTA LUBUKLINGGAU
Davit Irawan 92-102

EVALUASI PENGUKURAN KINERJA SISTEM INFORMASI PT.PERKEBUNAN NUSANTARA VII (PERSERO) DENGAN METODE MALCOLM BALDRIGE CRITERIA
Dewi Oktafiani 103-110

(STUDI KASUS PT BUKIT ASAM (PERSERO) TBK)

Kurniati, M.Kom
Dosen Universitas Bina Darma Palembang

Abstrak : *Satuan kerja Teknologi Informasi yang merupakan jantungnya informasi di PT Bukit Asam (Persero) Tbk Tanjung Enim. Statistik tingkat eksploitasi keamanan terhadap banyak server dan jaringan makin hari makin meningkat. Untuk mengatasinya PT Bukit Asam (Persero) Tbk menerapkan DMZ FortiGate-200B yang mana merupakan produk dari Fortinet yang merupakan perusahaan penyedia insfrastruktur pengamanan komputer dan jaringan. Perangkat keamanan ini merupakan bentuk penyederhanaan Perangkat keamanan ini merupakan bentuk penyederhanaan dari beberapa komponen penting dalam sistem keamanan jaringan yaitu firewall, VPN, IPS, Web Filtering dan Aplication Control. Semakin kompleksnya jaringan heterogeneous, memicu kebutuhan untuk dapat mengintegrasikan semua peralatan dan standart tersebut dalam satu control management yang terpusat. Sehingga dapat memperkaya sistem pengamanan jaringan komputer dalam meningkatkan pelayanan pengelolaan transaksi data dan informasi maka, terjadi pembatasan aktivitas pengiriman data pada jaringan internet dan dapat meminimalisir atau mencegah terjadinya serangan virus dan cybercrime.*

Kata kunci*: FortiGate-200B, Firewall, Virus*

1. PENDAHULUAN

Keamanan pada suatu jaringan komputer sangat penting untuk menjaga keaslian dan keamanan data serta menjamin ketersediaan layanan bagi penggunanya. Teknologi informasi yang semakin maju dan berkembang memiliki banyak keuntungan dalam kehidupan manusia, namun di balik itu terdapat juga aspek negatifnya. Terutama ancaman serangan dunia maya seperti *SQL injection* dan *BOTNET-CNC*.

PT Bukit Asam (Persero) Tbk Tanjung Enim adalah perusahaan yang bergerak dalam bidang pertambangan. Keamanan data aset perusahaan sangat penting untuk dijaga kerahasiaanya. Oleh karena itu untuk mengatasi masalah sistem kemananan jaringan komputer, perusahaan ini menerapkan *DMZ (Demiliterized Zone) Fortigate-200B* yang merupakan bentuk penyederhanaan dari beberapa komponen penting dalam sistem keamanan jaringan. Namun, dalam hal penerapannya, PT Bukit Asam (Persero) Tbk hanya *features firewall* dan *UTM* saja yang digunakan. Padahal, tidak hanya kedua *feature* sistem perangkat ini *suport* karena

perangkat ini dapat mengintegrasikan semua peralatan dan *standart* tersebut dalam satu *control management* yang terpusat. Jadi setiap *feature* dapat digunakan untuk meningkatkan sistem keamanan jaringan yang ada pada PT Bukit Asam (Persero) Tbk Tanjung Enim.

Melihat kondisi di atas maka penulis tertarik untuk melakukan analisa sistem keamanan *DMZ FortiGate-200B* pada PT Bukit Asam (Persero) Tbk yang hanya menerapkan beberapa *feature* tertentu yaitu *firewall* dan *UTM* selama dua tahun ini. Dengan demikian, ditinjau dari bagaimana perangkat *DMZ FortiGate-200B* ini mengatasi *insident* yang terjadi pada sistem keamanan PT Bukit Asam (Persero) Tbk maka, efektif atau tidaknya penerapan sistem keamanan ini guna mendukung keamanan jaringan komputer dalam meningkatkan pelayanan pengelolaan transaksi data dan informasi pada PT Bukit Asam (Persero) Tbk.

Dari latar belakang di atas untuk lebih mengarahkan masalah yang ada, serta tidak terlalu menyimpang dari permasalahan yang akan dilakukan dalam penelitian ini, maka dalam penelitian ini rumusan masalahnya hanya lebih diarahkan kepada "Bagaimana menganalisis Sistem Keamanan Jaringan Komputer pada PT Bukit Asam (Persero) Tbk Tanjung Enim?". Dengan menekankan pada sistem keamanan jaringan komputer menggunakan *FortiGate-200B* pada PT Bukit Asam (Persero) Tbk Tanjung Enim khususnya *feature Firewall* dan *UTM* serta penetrasi sistem keamanan PT Bukit Asam (Persero) Tbk Tanjung Enim. Tujuan dari penelitian ini adalah untuk mengetahui mengapa PT Bukit Asam (Persero) Tbk tidak menggunakan *feature* yang ada dalam *FortiGate-200B* secara menyeluruh dan efektif atau tidaknya penggunaan perangkat ini, jika dilihat dari bagaimana *FortiGate-200B* mengatasi *insident* yang terjadi pada sistem keamanan PT Bukit Asam (Persero) Tbk Tanjung Enim. Sehingga akan diperolah manfaat melakukan penelitian ini adalah:

1. Penulis dapat mengetahui mengapa PT Bukit Asam (Persero) Tbk Tanjung Enim tidak menerapkan *feature FortiGate-200B* secara menyeluruh yaitu hanya *fiture firewall* dan *UTM*.
2. Penulis dapat mengetahui efektif atau tidaknya penerapan *DMZ FortiGate-200B* terhadap sistem keamanan jaringan PT Bukit Asam (Persero) Tbk.
3. Penulis dapat mengetahui bagaimana *FortiGate-200B* mengatasi *insident* yang terjadi pada sistem keamanan PT Bukit Asam (Persero) Tbk.
4. Diharapkan dapat membantu memberikan saran dalam mengoptimalkan sistem keamanan yang telah berjalan di PT Bukit Asam (Persero) Tbk, dengan memberi perbandingan dengan versi terbaru saat ini.
5. Menambah wawasan berfikir serta meningkatkan pengetahuan penulis dibidang jaringan dan bagaimana meminimalisir dan mengamankan jaringan tersebut dari ancaman *cybercrime*.

2. METODOLOGI 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 *Diagnosing, Action Planning, Action Taking, Evaluating* dan *Learning*.

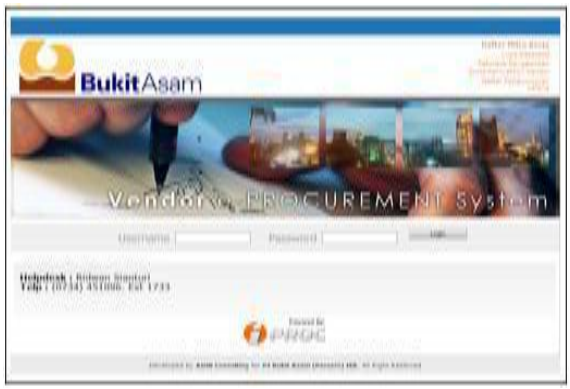
Sedangkan, metode analisis sistem keamanan jaringan penulis menggunakan metode *stress test*. Metode *stress test* menurut Riadi (2011), adalah metode yang didesain untuk melawan system dalam keadaan yang tidak normal, dilakukan dengan cara mengakses beberapa alamat *web* yang telah di *filter* oleh mikrotik sebagai analisis proses untuk menentukan alur lalulintas yang melewati proses pem*filter*an menggunakan *firewall, desain* untuk mendapatkan cara yang paling efektif dan efisien mengimplementasikan *router*, implementasi serta pengujian.

3. HASIL

3.1. Melakukan Diagnosa (*Diagnosing*)

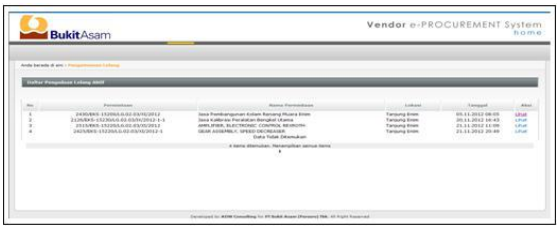
Jaringan komputer pada PT Bukit Asam (Persero) Tbk Tanjung Enim sangat besar peranannya, dalam berkomunikasi antar unit perusahaan yang tersebar di beberapa wialayah yang ada di Indonesia. Dalam hal transaksi yaitu penyediaaan barang berupa batubara dan jasa yang disebut *e-Procuremen*, perusahaan ini melakukannya dengan sistem *online* karena lebih efektif dan efisien. Sistem *e-Procurement* PT. Bukit Asam (Persero) Tbk adalah perangkat lunak aplikasi yang bertujuan memfasilitasi Penyedia Barang dan Jasa dan PT. Bukit Asam (Persero) Tbk agar dapat melakukan transaksi pengadaan barang dan jasa melalui media

internet, termasuk registrasi *online* untuk menjadi Penyedia Barang dan Jasa. Di bawah ini adalah gambar *e-procurement* PT Bukit Asam (Persero) Tbk:



Sumber: PT Bunkit Asam Tanjung Enim

Gambar 3.1 Layar Utama *e-Procurement* PT Bukit Asam (Persero) Tbk

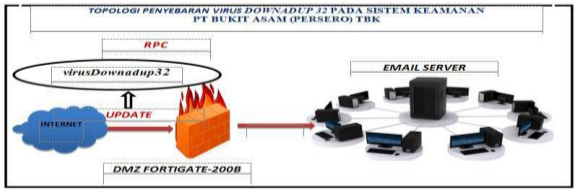


Sumber: PT Bunkit Asam Tanjung Enim

Gambar 3.2 Daftar Pengumuman Lelang *Vendor e-Procurement*

Padahal dengan menggunakan sistem ini ancaman sangat besar. Sehingga penerapan sebuah sistem keamanan yang handal sangatlah penting guna menjaga data perusahaan. Penerapan *firewall* sangat dibutuhkan untuk menciptakan area aman yang biasa disebut *DMZ (Demiliterized Zone)* untuk mem*filter* paket data yang masuk ke jaringan.

Selain itu, pada tahun 2009, PT Bukit Asam (Persero) Tbk pernah mengalami *insident* yang menyebabkan kevakuman akibat *threat Downadup32* yang biasanya *virus* ini menyerang pada akhir tahun dengan melakukan *lock* pada *password email admin* dan *user*,



Sumber: PT Bunkit Asam Tanjung Enim

Gambar 3.3 Penyebaran *Virus Downadup32*

Dari gambar di atas, serangan *virus Downadup32* yang menyerang akhir tahun ini melakukan serangan *spam* 1000/detik ketika melakukan *update* sistem. *Virus* ini menyerang *account user* yang menyebabkan *password user* dan termasuk *password admin* sehingga, terjadi *lock password* yang mengakibatkan tidak bisanya *login* dan sistem *email* mati total. Meskipun, telah menggunakan *firewall* sebagai *fortal*, tetap saja *virus* tersebut dapat lolos dikarenakan *virus* tersebut menyusup dan tertanam pada *protocol Remote Procedure Call (RPC)* yang pada *firewall* di *settting allow*.

Untuk mengatasi semua kendala yang ada saat ini, PT Bukit Asam (Persero) Tbk Tanjung Enim menerapkan perangkat sistem keamanan jaringan *FortiGate-200B* pada *feature firewall* dan *UTM* saja dari beberapa *feature* keamanan jaringan yang tersedia pada perangkat tersebut. Untuk mengetahui kebenaran itu semua pentingnya melakukan uji penetrasi, karena dengan melakukan uji penetrasi penulis dapat melakukan penilaian keamanan jaringan untuk menemukan kerentanan potensial dan untuk mengeksploitasi mereka segera. Sehingga, akan dapat mengambil tindakan selanjutnya untuk memperbaiki celah tersebut dengan perencanaan yang tepat.

3.2. Melakukan Rencana Tindakan (*Action Planning*)

Pada tahapan ini penulis melakukan rencana tindakan yang akan dilakukan pada perangkat sistem keamanan jaringan *FortiGate-200B* pada PT Bukit Asam (Persero) Tbk Tanjung Enim, yang akan dilakukan dalam rencana tindakan ini adalah:

1. Penulis akan menjelaskan bagaimana konfigurasi *FortiGate-200B* khususnya pada *feature firewall* dan *UTM*.
2. Serta melakukan pengujian terhadap sistem tersebut pada jaringan PTBA.
3. Dengan melakukan rencana tindakan ini penulis akan mendapatkan hasil yang didapat berupa *report* dari sistem tersebut dan kemudian *report* itu dilanjutkan dengan evaluasi.

3.2.1. Action Planning FortiGate-200B

Melakukan rencana tindakan yang akan dilakukan pada perangkat sistem keamanan jaringan *FortiGate-200B* pada PT Bukit Asam (Persero) Tbk Tanjung Enim, terbagi atas dua *feature* sebagai berikut:

3.2.1.1. *Feature Firewall FortiGate-200B*

Pada PT Bukit Asam (Persero) Tbk Tanjung Enim dalam penerapan *feature firewall*, fasilitas yang digunakan adalah fasilitas *Policy*. Fasilitas ini berfungsi untuk menambahkan

kebijakan *firewall* untuk mengontrol koneksi dan lalu lintas antara antarmuka *FortiGate*, zona, dan *VLAN subinterfaces*. Adapun prosedur dalam melakukan konfigurasi *Policy* diantaranya adalah *add, delete, edit, re-order, disable,* dan *enable* sebuah *firewall policy*.

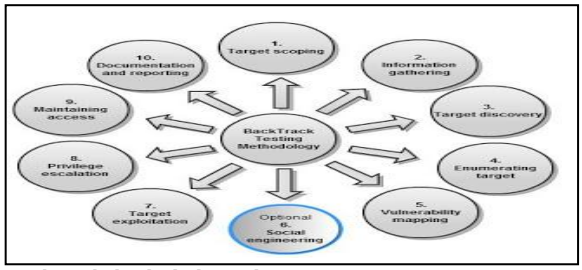
3.2.1.2. *Feature UTM FortiGate-200B*

Pada PT Bukit Asam (Persero) Tbk Tanjung Enim dalam penerapan *feature UTM*, fasilitas yang digunakan adalah fasilitas IPS. Fasilitas ini sangat penting dalam suatu jaringan sebagai cara untuk mencegah dan meminimalisir adanya ancaman serangan *cybercrime*. Untuk hasil terbaik dalam mengkonfigurasi scanning IPS, ikuti prosedur di bawah ini:

1. Membuat *sensor IPS*,
2. Buat *filter* dan menimpa di *sensor IPS*. Filter dan menimpa menentukan tanda tangan mesin *IPS* akan mencari di lalu lintas jaringan,
3. Pilih profil perlindungan atau membuat yang baru,
4. Dalam profil perlindungan, memungkinkan *Sensor IPS* dan pilih *sensor IPS*,
5. Pilih kebijakan *firewall* atau membuat yang baru,
6. Dalam kebijakan *firewall*, pilih kotak centang Perlindungan Profil dan pilih perlindungan *profile*.

3.2.2. *Action Planning* Penetrasi

Dalam melakukan penetrasi, di sini penulis menggunakan *OS BackTrack* dengan tahapan-tahapan seperti gambar 2.4,



Sumber: Shakeel Ali dan Tedi Hermanto

Gambar3. 4. *BackTrack Testing Methodology*

Pada gambar di atas terlihat ada sepuluh tahapan dalam melakukan penetrasi berdasarkan Ali dan Heriyanto, 2011 yaitu dalam melakukan penetrasi langkah pertama seorang tester melakukan target *scoping*, dalam hal ini targetnya adalah PT Bukit Asam (Persero) Tbk Tanjung Enim yang bergerak di bidang pertambangan. Langkah selanjutnya adalah penulis menggunakan *tools dnsenum* yang ada pada *OS BackTrack* guna mencari informasi gathering, mencari target *discovery* dengan melakukan *ping* pada target dengan memanfaatkan informasi yang telah di dapat pada tahap kedua, melakukan *enumerating* target dengan *Nmap* dan *Zenmap* untuk mengetahui *port* berapa yang *open* dan *filtered*, melakukan *vulnerability mapping*, melakukan *spcial engineering*, melakukan target *eksploitation*, melakukan *privilage escalation*, melakukan *maintaining access*, kemudian di akhiri dengan melakukan *dokumentation* dan *reporting*.

3.2.3. *Report* dari *FortiGate-200B*

Report merupakan kumpulan data yang di dapat dari status sistem berdasarkan *log* dan *DLP archive*, yang akan dilakukan pada tahap ini yaitu melakukan evaluasi terhadap hasil yang didapat.

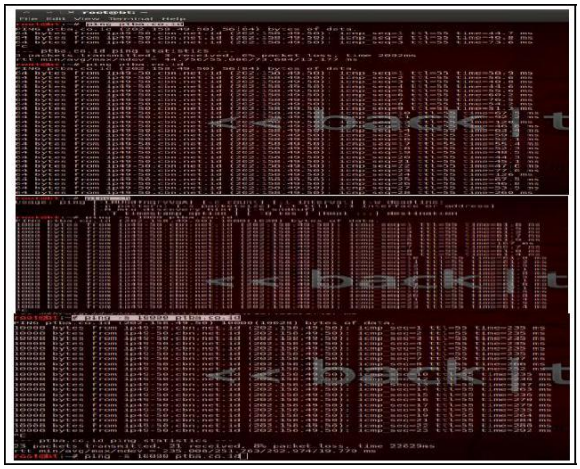
R*eport* ini nantinya berisi tentang aktivitas dari *FortiGate-200B* pada setiap bulannya. Namun, dalam hal ini penulis hanya mengambil *report* guna mengetahui perbandingan dari kinerja *FortiGate-200B*.

Sumber: PT Bunkit Asam Tanjung Enim

Gambar 3.5. Status *Report FortiGate-200B*

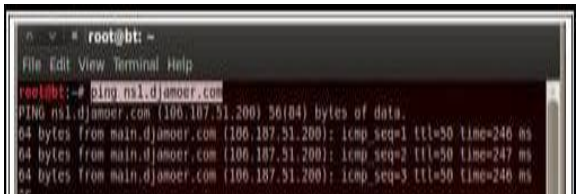
3.3.2.3. *Target Discovery*

Untuk mengetahui *Target Discovery* PT Bukit Asam (Persero) Tbk, penulis melakukan *ping* pada *IP Host's Address* dan *IP Name's Server*.



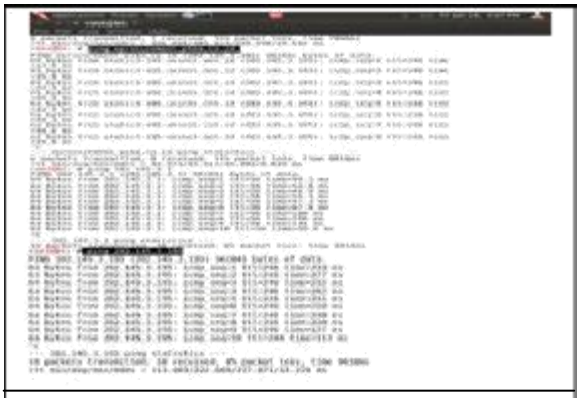
Sumber: PT Bunkit Asam Tanjung Enim

Gambar 3.6. *Output Ping* pada *situs ptba.co.id*



Sumber: PT Bunkit Asam Tanjung Enim

Gambar 3.7. *Output Ping* ns1.djamoer.com



Sumber: PT Bunkit Asam Tanjung Enim

Gambar3.8. *Output Ping eprocurement. ptba.co.id*

Dengan melakukan *ping* pada target, maka penulis pengirimkan paket *ICMP* dalam jumlah besar yang tergolong sebagai serangan *DOS Attack (Denial of Service).*

3.3.2.4. *Enumerating Target*

Untuk mengetahui *Enumerating Target* PT Bukit Asam (Persero) Tbk, penulis melakukan *Nmap* dan *Zenmap* pada *IP Host's Address* dan *IP Name's Server* mereka dengan menjalankan perintah seperti gambar di bawah ini:

Sumber: PT Bunkit Asam Tanjung Enim

Gambar 3.9 *Output nmap* ptba.co.id

Dengan melakukan *scan* terhadap target menggunakan *Nmap*, kita dapat mencari celah dengan mengetahui *port* yang terbuka, *enumerating system detail*, dan versi layanan yang ter-*install* pada PT Bukit Asam (Persero) Tbk Tanjung Enim. Pada gambar di atas menunjukkan *port* yang terbuka diantaranya adalah *port* 80 yang merupakan *service http*. Sedangkan *port 25, port 135, port 139,* dan *port 445* menerangkan adanya *filtered*. Terdapat tiga macam tipe serangan yang digunakan dalam *hacking nmap*, yaitu:

1. *SYN SCAN*, ini adalah tipe serangan yang paling mudah dan banyak digunakan. *Syn Scan* akan menampilkan hasil serangan lebih cepat, namun kelemahanya hasil yang ditampilkan tidak spesifik (umum).
2. *FIN SCAN*, metode serangan ini lebih akaurat dibanding *SYN SCAN*. *Fin Scan* akan menampilkan jenis- jenis paket yang ter*filter* dan kelemahan *firewall*. Dengan meggunakan metode serangan ini, penyerang dapat mengetahui kelemahan sistem yang akan diserang sebelum melakukan serang lebih lanjut.
3. *ACK SCAN*, *port* yang terfilter atau tidak akan ditampilkan disini. Tipe serangan ini adalah yang paling spesifik dan menampilkan hasil yang sangat akurat. Bagi anda yang terbiasa menggunakan *nmap*, maka tipe serangan ketiga ini yang sering digunakanmeskipun sedikit rumit.

Sumber: PT Bukut Asam Tanjung Enim

Gambar 3.10 *Output* Zenmap pada *host address ptba.co.id* pada *ip target*

Sumber: PT Bukut Asam Tanjung Enim

Gambar 3.12 *Output Zenmap* pada *Name Server* ptba.co.id ns1.djamoer.com

Sumber: Sumber: PT Bukut Asam Tanjung Enim

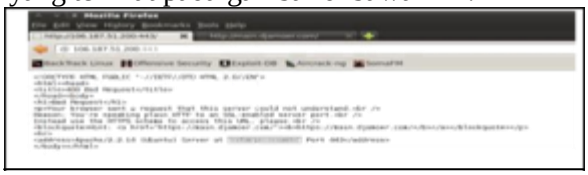
Gambar 3.11 *Output Zenmap* pada *Name Server* ptba.co.id ns1.djamoer.com

Sumber: PT Bukut Asam Tanjung Enim

Gambar 3.13 *Scan Port Zenmap* pada *Eprocurement*.ptba.co.

Dari gambar di atas hasil *scan* oleh *Zenmap* yang menunjukan port apa saja yang terbuka pada jaringan PT Bukit Asam (Persero) Tbk, setiap *port* yang *state*nya *open* maka, akan berdampak pada pertahanan sistem keamanan jaringan PT Bukit Asam (Persero) Tbk dari serangan penyusup yang memasuki sistem tanpa otorisasi ataupun seorang *user* yang sah tetapi menyalahgunakan *privilege* sumber daya sistem.

Dengan menggunakan *Nmap* dan *Zenmap*, kita akan mengetahui *port* mana yang terkondisi *unclosed*. Sedangkan *port* yang terfilter (*Filtered*) dikarenakan *firewall* dalam jaringan masih aktif. Dengan adanya *mapping* maka, akan menimbulkan beberapa ancaman kejahatan yang diantaranya adalah terjadinya pembajakan situs *web*, *probing* dan *port scanning*, *virus*, *Denial of Service (DoS)* dan *Distributed DoS (DDos) attack*, kejahatan yang berhubungan dengan nama *domain*, *hacking*, dan penyerangan situs atau *e-mail* melalui *virus* (*spamming)*. Masih adanya kelemahan pada sistem keamanan jaringan PT. Bukit Asam (Persero) Tbk ditemukan juga celah ketika, penulis mencoba masuk melalui *web base* dengan *ip 106.187.51.200* pada *port* 443 dan 8080 seperti yang terlihat pada gambar di bawah ini:



Sumber: PT Bukit Asam Tanjung Enim

Gambar 3.14. Tampilan *ip* 106.187.51.200 pada *port* 443

Pada kedua gambar di atas, maka terlihat bahwa PT Bukit Asam (Persero) Tbk menggunakan *Apache/2.2.24 Ubuntu Server at main.djamoer.com*. Informasi ini yang menjadi celah sistem keamanan jaringan PT Bukit Asam (Persero) Tbk karena, dapat di manfaatkan penyusup untuk mengetahui halaman *login admin*,

Sumber: PT Bukut Asam Tanjung Enim

Gambar 3.16 Halaman *login Admin* di *ISP Config*

Jika hal di atas telah di peroleh penyusup maka, kemungkinan besar penyusup untuk masuk dengan melakukan beberapa teknik serangan salah satunya adalah *Password Attacks* dengan cara menebak (*Guessing*), *Brute Force*, *Cracking* dan *Sniffing* untuk mengetahui *username* dan *password login admin*.

3.3.3. Hasil *Report DMZ FortiGate-200B* PT Bukit Asam

3.3.3.1. *FortiGate-200B* September 2012

Sumber: PT Bukit Asam Tanjung Enim

Gambar 3.17 *Status System Log and Archive*

Sumber: PT Bukit Asam Tanjung Enim

Gambar 3.15 Tampilan *Statistic FortiGate-200B* Bulan September *port* 8080

Gambar di atas merupakan tampilan dari *System> Status* pada bulan September, yang di dalamnya terdapat *System Information*, *License Information*, *Unit Operation*, *CLI Console*, *System Recorces*, *Alert Message Console*, *Log And Archive Statistic* dan *Top Sessions* .

Sumber: PT Bukit Asam Tanjunga Enim

Gambar 3.18 Layar Menu *Firewall* pada *Global View Policy* Bulan September

Gambar di atas merupakan tampilan *report* dari *Firewall>Policy* pada bulan September pada *Global View*, yang di dalamnnya memperlihatkan *port* berapa saja yang berjalan pada sistem.

3.3.3.2. *FortiGate-200B* Oktober 2012

Sumber: PT Bukit Asam Tanjunga Enim

Gambar 3.19 *Status System Log and Archive Statistic FortiGate-200B* Bulan Oktober

Gambar di atas merupakan tampilan dari *System> Status* pada bulan Oktober, yang di dalamnya terdapat beberapa *report* seperti pada bulan September di atas yaitu *System Information, License Information, Unit Operation, CLI Console, System Recorces, Alert Message Console, Log And Archive Statistic* dan *Top Sessions* .

Sumber: PT Bukit Asam Tanjunga Enim

Gambar 3.20. Layar Menu *Firewall* pada *Global View Policy* Bulan Oktober

Gambar di atas merupakan tampilan *report* dari *Firewall>Policy* pada bulan Oktober pada *Global View*, yang di dalamnnya memperlihatkan *port* berapa saja yang berjalan pada sistem sama seperti *report* bulan September.

3.4. Pembahasan dan Evaluasi*(Evaluating)*

Setelah masa tahap *action taking* dianggap cukup, kemudian peneliti melakukan evaluasi tentang hasil yang didapat hasil dari analisis yang telah dilakukan tadi, dalam tahap ini dilihat efektif

atau tidaknya penerapan *FortiGate-200B* pada PT Bukit Asam (Persero) Tbk Tanjung Enim, dilihat dari bagaimana *FortiGate-200B* dalam mengatasi *serangan* yang terjadi pada sistem keamanan jaringan PT Bukit Asam (Persero) Tbk Tanjung Enim yang dapat dilihat dari hasil *report* pada *system* tersebut.

3.4.1. *DMZ FortiGate-200B*

Perangkat keamanan ini telah diterapkan PT. Bukit Asam (Persero) Tbk Tanjung Enim, lebih kurang dua tahun terakhir ini. Dalam sisi keahandalan dan kinerja sistem, perangkat ini sudah sangat baik dibandingkan dengan perangkat yang digunakan sebelumnya karena, semua *feature* untuk sistem keamanan jaringan dapat diterapkan dalam satu perangkat ini.

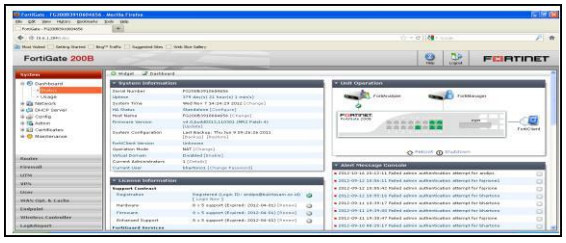
Namun, PT. Bukit Asam (Persero) Tbk hanya menerapkan dua *feature* saja yaitu *firewall* dan *UTM* sesuai kebutuhan perusahaan. Dari hasil sub bab di atas, dapat kita lihat pada *feature firewall* dan *UTM*. Pada fasilitas *policy feature firewall* menentukan kebijakan-kebijakan apa saja yang dapat berjalan pada sistem. Sehingga, sebagai *filter firewall* dapat mengatur masuknya paket data yang tidak diinginkan dari luar untuk meminimalisir ancanam dari ancaman penyusup. Begitupun dengan *feature UTM* pada fasilitas *IPS*, mengurangi ancaman dari luar dan mencegah terjadinya kasus yang sama seperti adanya *threat Downadup 32* yang biasanya *virus* ini menyerang pada akhir tahun dengan melakukan *lock* pada *password email admin* dan *user*.

Dalam penggunaan perangkat sistem keamanan jaringan *FortiGate-200B* ini seorang administrator harus melakukan *login* terlebih dahulu, seperti pada gambar di bawah ini yang merukan layar menu *login*:

Sumber: PT Bukit Asam Tanjunga Enim

Gambar 3.21 Layar *login DMZ FortiGate-200B*

Layar *login* ini akan tampil ketika akan menjalankan *DMZ FortiGate-200B*. Setelah *administrator* mengarahkan ke *link https://*192.168.1.99. *User Name* dan *Password* dapat berupa huruf besar, kecil atau campuran keduannya. Jika setelah melakukan *login password* maja akan tampil layar menu utama setelah pengguna mengisi *user name* dan *password* dengan benar pada layar *login*. layar menu utama gunakan untuk menjalankan satu persatu aplikasi sesuai dengan penggunaannya.
Pada layar menu utama dapat dilihat komponen-komponen apa saja yang bisa dijalankan pada *DMZ FortiGate-200B*. Hal ini dapat dilihat pada gambar 3.22,



Sumber :PT Bukit Asam Tanjung Enim

Gambar 3.22 Layar Menu Utama *DMZ Fortigate-200B*

Dari gambar di atas ada beberapa *feature* sistem keamanan yang dapat diterapkan sebagai pertahan jaringan terhadap ancaman *cybercrime*.

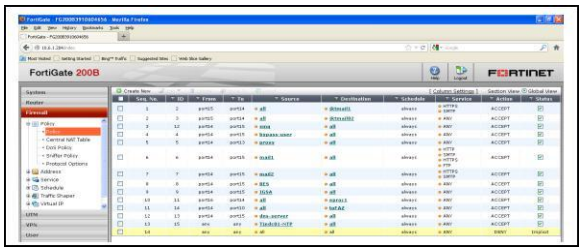
3.4.1.1. *Feature Firewall* pada *FortiGate-200B*

Dari hasil di atas berkenaan dengan *feature firewall* pada *FortiGate-200B* setelah melakukukan *setting Policy* pada layar menu *Firewall>Policy* maka, akan tampil seperti gambar di bawah ini:

Sumber :PT Bukit Asam Tanjung Enim

Gambar 3.23 Hasil *Feature Firewall* pada *Section View FortiGate-200B*

Dari gambar di atas pada layar *section view* tetrdapat beberapa *ID* yang merupakan hasil *settting policy* sebelumnya. Pada *port1>FIOS (3)port* yang sedang berjalan adalah *port 8*, *port 12* dan *port 14*.



Sumber :PT Bukit Asam Tanjung Enim

Gambar 3.24 Hasil *Setting Feature Firewall* pada *Global View FortiGate-200B*

Pada gambar di atas untuk tampilan layar *Global View* terlihat jelas *port* berapa saja yang sedang berjalan pada sistem dan *service* yang ada di dalamnya.

3.4.1.2. *Feature UTM* pada *FortiGate-200B*

Dari hasil di atas berkenaan dengan *feature UTM* pada *FortiGate-200B* setelah melakukukan *setting IPS* pada layar menu *UTM>Intrusion Protection>IPS* akan tampil seperti gambar 3.39 pada sub bab hasil. Pada layar *UTM* tersebut *protocol* yang berjalan diantaranya *BACK ORIFACE*, *DCE RPC*, *DHCP*, *DNP3*, *DNS*, *FTP*, *H323*, *HTTP*, *Instant Massaging*, *IMAP*, *LDAP*, *MSSQL*, *NetBIOS*, *NNTP*, *Peer-to-Peer*, *POP3*, *Protocol (L3/4) Analyser*, *RADIUS*, *RDT*, *SuN RPC*, dan *RTCP*. Seperti pada tabel di bawah ini:

Tabel 3.1 *Protocol Decoder*

NO	*PROTOKOL*	*PORT*
1	*BACK ORIFACE*	*AUTO*
2	*DCE RPC*	*AUTO*
3	*DHCP*	*AUTO*
4	*DNP3*	*AUTO*
5	*DNS*	*53*
6	*FTP*	*AUTO*
7	*H323*	*1720*
8	*HTTP*	*AUTO*
9	*Instant Massaging*	*AUTO*
10	*IMAP*	*AUTO*
11	*LDAP*	*389*
12	*MSSQL*	*1433*
13	*NetBIOS*	*139,445*
14	*NNTP*	*AUTO*
15	*Peer –to Peer*	*AUTO*
16	*POP3*	*AUTO*
17	*PROTOCOL (L3/4) ANALYSER*	*AUTO*
18	*RADIUS*	*812,1813*
19	*RDT*	*AUTO*
20	*SuNRPC*	*11, 32771*
21	*RTCP*	*AUTO*

Sumber: PT Bukit Asam Tanjung Enim

3.4.2. Penetrasi

Pada sub ini yang akan dijelaskan yaitu mengevaluasi dari hasil pengujian pada *FortiGate-200B* pada Jaringan PTBA. Pada penetrasi di jaringan komputer adalah kunci untuk keberhasilan dalam perlindungan pada jaringan komputer. Pengujian penetrasi memungkinkan perusahaan atau individu dengan beberapa komputer pada jaringan yang sama untuk melindungi komputer mereka dan untuk mencegah bahaya dari luar yang mempengaruhi sistem mereka. Dengan pengujian penetrasi jaringan seluruh komputer dapat dilindungi dan efektif untuk mencegah *hacking* dalam

penyebaran virus. Dengan melakukan pengujian ini pastinya mendapatkan celah yang didapat. Apabila celah tersebut dimanfaatkan untuk kejahatan, maka besar kemungkinan jaringan perusahaan tersebut bisa terganggu bahkan terjadi kevakuman terhadap jaringan komputer khususnya PTBA. Kemudian pada penetrasi pada *FortiGate-200B* kebijakan yang diterapkan juga harus sesuai dengan kebutuhan melihat dengan banyak serangan terutama virus, otomatis kebijakan yang diterapkan, baik dalam pemasangan anti virus maupun *update* secara berkala pada suatu sistem dengan sistem yang baru, agar kinerja dalam melindungi jaringan dapat bekerja dengan baik dan dapat mencegah dari hal-hal yang dapat merusak jaringan komputer.

Dari hasil penetrasi di atas, penulis dapat mengetahui *port* berapa saja yang *open* dan *filtered* dengan menggunakan *tool nmap* dengan target *IP 109.74.202.116* dan *IP 202.145.3.195* sebagai langkah awal untuk mencari celah dalam melakukan penetrasi pada sistem keamanan jaringan PT. Bukit Asam (Persero) Tbk Tanjung Enim. Setelah penulis melakukan *nmap* pada *IP 109.74.202.116*.

Tabel 3.2 Tabel *Scanning Port* pada *IP 106.74.202.116*

NO	PORT	PROTOKOL	PORT
1	21	OPEN	FTP
2	22	OPEN	SSH
3	53	FILTERED	SMTP
4	80	OPEN	DOMAIN
5	53	OPEN	HTTP
6	80	OPEN	POP3
7	110	OPEN	IMAP
8	143	OPEN	HTTPS
9	443	OPEN	IAMPS
10	995	OPEN	POP3S
11	3306	OPEN	MYSQL
12	8081	OPEN	BLACKICE-ICECAP

Sumber: PT Bukit Asam (Persero) Tbk Tanjung Enim

Dari tabel di atas menunjukan pada *IP 109.74.202.116* hanya *port 53* dengan *service smtp* yang *filtered*, sedangkan *port* lain *open* dan itu merupakan celah pada target, karena rentan dari serangan penyusup.

Tabel 3.3 Tabel *Scanning Port* pada *IP 202.145.3.195*

NO	PORT	SERVICE	PORT
1	13	OPEN	DAYTIME
2	21	OPEN	FTP
3	23	OPEN	TELNET
4	25	FILTERED	SMTP
5	37	OPEN	TIME
6	80	OPEN	HTTP
7	11	OPEN	RPCBIND
8	199	OPEN	SMUX
9	427	OPEN	SVRLOC
10	443	OPEN	HTTPS
11	445	FILTERED	MICROSOFT-DS
12	512	OPEN	EXEC
13	513	Open	Login
14	514	Open	Shell
15	1334	Open	Writesrv
16	2121	Open	ccproxy-ftp
17	2222	Open	EtherNet/ip-1
18	2809	Open	Corbaloc
19	5988	Open	wbeb-http
20	5989	Open	wbeb-https
21	6000	Open	x11
22	6112	Open	Dtspc
23	7777	Open	Cbt
24	8088	Open	radan-http
NO	**PORT**	**PROTOKOL**	**PORT**
25	9080	Open	Glrpc

26	9090	*Open*	*zeus-admin*
27	9100	*Open*	*Jetdirect*
28	32768	*Open*	*filenet-tms*
29	32769	*Open*	*filnet-rpc*
30	32771	*Open*	*sometimes-rpc5*
31	32775	*Open*	*sometimes-rpc13*
32	32776	*Open*	*sometimes-rpc15*

Sumber: PT Bukit Asam Tanjung Enim

Dari tabel di atas sama halnya dengan tabel 3.4 pada *IP 109.74.202.116* menunjukkan hanya *port 25* dengan *service smtp* yang *filtered* dan*port 445* dengan *service-ds,* sedangkan *port* lain *open* dan itu merupakan celah pada target, karena rentan dari serangan penyusup.

3.4.3. Hasil *Report FortiGate-200B*

Hasil *report* merupakan kumpulan data yang di dapat dari *status system* berdasarkan *log* dan *DLP archive*, melakukan evaluasi terhadap hasil yang di dapat dengan melakukan perbandinganpada bulan Septemberdan Oktober 2012,

Tabel 3.4. *DLP Archive FortiGate-200B* Bulan September 2012

NO	*LOG - - Avarage 2 MB (10685 messages)*		
1	*TRAFFICK*	*TrafficAllowed*	*4015860*
		Traffic Violated	*0*
2	*AV*	*Viruses Caught*	*0*
3	*IPS*	*Attacks Detected*	*0*
4	*EMAIL*	*Spams Detected*	*0*
5	*WEB*	*URLs Blocked*	*0*
6		*Data*	*0*
7	*DLP APLICATION CONTROL*	*LossDetected APLICATION CONTROL MASSAGES*	*0*
8	*EVEN*	*Event*	*1619*
9	*TOTAL*	*Total*	*665MB*

Tabel 3.5. *DLP Archive FortiGate-200B* Bulan Oktober 2012

NO	*LOG - - Avarage 2 MB (10685 messages)*		
1	*TRAFFICK*	*TrafficAllowed*	*403407*
		Traffic Violated	*0*
2	*AV*	*Viruses Caught*	*0*
3	*IPS*	*Attacks Detected*	*0*
4	*EMAIL*	*Spams Detected*	*0*
5	*WEB*	*URLs Blocked*	*0*
6		*Data*	*0*
7	*DLP APLICATION CONTROL*	*LossDetected APLICATION CONTROL MASSAGES*	*0*
8	*EVEN*	*Event*	*1698*
9	*TOTAL*	*Total*	*736MB*

Sumber: PT Bukit Asam Tanjung Enim

Dari data tabel di atas maka dapat kita lihat perbadingan hasil *report status* pada *System Log and Archive Statistic FortiGate-200B* yang mana setiap bulannya terjadi peningkatan akses pada *http, https* dan *e-mail*. Semakin meningkatnya akses tersebut maka, semakin meningkatnya *threat* pada sistem keamanan jaringan komputer yang ada pada PT Bukit Asam (Persero) Tbk.

Pada hasil *report, Attack detection* pada *IPS* adalah 0. Dengan demikian, dipastikan bahwa *DMZ FortiGate-200B* ini berjalan dengan baik untuk menjaga keamanan jaringan perusahaan tersebut dibandingkan dengan menggunakan *Firewall CiscoPIX*. Hal ini terlihat dengan tidak adanya lagi terjadi kevakuman akibat serangan *virus Downadup 32*.Dari hasil pembahasan di atas, penerapan

feature firewall pada *FortiGate-200B* dalam menjaga sistem keamanan jaringan PT. Bukit Asam (Persero) Tbk sudah baik.

Hal ini terlihat dari hasil *report* yang menunjukkan bahwa pada bulan September dan bulan Oktober untuk *trafic violated* hasilnya adalah sama yaitu bernilai 0. Oleh karena itu, dapat disimpulkan bahwa cara kerja dari sistem stabil dilihat dari tidak adanya *traffic violated* yang terdeteksi oleh sistem. Walaupun demikian, masih adanya kemungkinan terjadinya ancaman oleh penyusup dengan melihat perbandingan hasil *report* pada bulan September dan bulan Oktober yang menunjukkan pada *DLP Archive* jumlah dari *http,* dan *https* semakin meningkat. Dan hal ini lah yang dapat dimanfaatkan oleh penyusup karena *port* yang menunjukkan *service http* dan *https* adalah *open*. Begitupun pada *service Email* meskipun *filtered* masih ada kemungkinan ancaman dari penyusup karena, bnyak tekhik yang bisa dilakukan oleh penyusup dengan *tutorial* yang lebih praktis salah satunya, dengan menggunakan *OS BackTrack 4* dan *BackTrack 5*.

4. SIMPULAN

Berdasarkan pembahasan pada bab sebelumnya mengenai analisa dan evaluasi sistem keamanan jaringan komputer menggunakan *DMZ FortiGate-200B* PT Bukit Asam (Persero) Tbk, maka kesimpulan yang dapat diambil diantaranya:

1. Penerapan *feature firewall* dan *UTM* pada *FortiGate-200B* dalam menjaga sistem keamanan jaringan PT. Bukit Asam (Persero) Tbk sudah baik. Hal ini terlihat dari hasil *report* yang menunjukkan bahwa pada bulan September dan bulan Oktober untuk *trafic violated, antivirus* dan *IPS* hasilnya adalah sama yaitu bernilai 0. Cara kerja sistem stabil, dilihat dari tidak adanya *traffic violated* yang terdeteksi oleh sistem. Meskipun dalam penerapan *feature firewall* pada *FortiGate-200B* sudah baik. Namun, PT. Bukit Asam (Persero) Tbk harus tetap waspada dengan kemungkinan ancaman yang akan datang karena, semakin meningkatnya perkembangan teknologi terutama dari sisi sistem keamanan jaringan. Maka, seorang administrator jaringan harus lebih peka terhadap munculnya versi baru dan melakukan *update licency* secara berkala guna meningkatkan sistem keamanan jaringan perusahaan. Selain itu, pemilihan suatu produk IT, survei sangat penting guna mengetahui kelebihan dan kekurangan dari suatu produk yang akan diterapkan sesui kebutuhan perusahaan.
2. Dilihat dari perangkat sistem keamanan yang digunakan saat ini, PT. Bukit Asam (Persero) Tbk Tanjung Enim sudah baik karena, sistem keamanan yang diterapkan sudah berlapis yang terdiri dari perangkat *FortiGate-200B* dan sistem keamanan *ISA* sebagai *firewall* dan *Symantec Enpoint Protection* sebagai *antivirus*. Namun, setelah penulis melakukan penetrasi terhadap sistem keamanan pada PT. Bukit Asam Tanjung Enim masih terdapat celah yang dapat digunakan penyusup untuk masuk kedalam jaringan. Sehingga, akan berdampak buruk pada data dan informasi yang sifatnya *privat* jatuhketangan penyusup yang tidak memiliki otorisasi atau seorang *user* yang sah tetapi menyalahkan *privilege* sumber daya sistem. Dari hasil penetrasi ditemukan beberapa celah. Oleh karena itu, untuk menambah kinerja sistem keamanan jaringan yang sudah ada saat ini. PT Bukit Asam (Persero) Tbk Tanjung Enim, harus malakukan penambahan *feature* sistem keamanan lainnya yang ada pada perangkat *FortiGate-200B* tersebut selain *feature firewall* dan *UTM*.

DAFTAR RUJUKAN

Ali dan Heriyanto. (2011). *BackTrack 4: Assuring security by Penetration Testing*. Birmingham-Mumbai: *Packet Publishing Ltd.* (Diakses dari http: // www.packtpub.com/ sites/default/ files/3944OS- Chapter -2-Penetration-Testing- Methodology.pdf, 27 Desember 2012).

Fortinet Inc. (2004). FortiGate-200 Administration Guide. (Diakses dari http:// docs. fortinet.com/ fgt /archives / 2.8MR7/ 01- 28007- 0004- 20041203 FortiGate-200 Administration Guide. pdf, 5 November 2012)

Fortinet Inc. (2009). FortiGate®-200B. Jakarta: Fortinet Inc. (Diakases dari http: //www. tbpgroup.com/ fortinet/ FGT200B_ DS. pdf, 5 November 2012).

Fortinet Inc. (2012). FortiGate®-200B/200B-POE. Jakarta: Fortinet Inc. (Diakses dari http://www.fortinet.com/ sites/ default/files/productdatasheets/FortiGate -200B-POE.pdf, 5

November 2012).

Fortinet Inc. (2009). FortiGate® UTM User Guide. (Diakses dari http: //docs. fortinet.com/ fgt/ techdocs /fortigate-utm.pdf, 2 Desember 2012).

Pescatore, John. (2012). *Magic Quadrant for Unified Threat Management.* (Diakses darihttp://www.gartner.com/technology/reprints.o?id=119PNY6P&ct=120315&st =sg, 22 November 2012).

Riadi, Imam. (2011). Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik. (Diakses darihttp://www.http://undana.ac.id/jsmallfib_top/JURNAL/ICT/ICT%202011/08-JUSI-Vol-1 No-1-_Optimalisasi-KeamananJaringan-Menggunakan-Pemfilteran-Aplikasi-Berbasis-Mikrotik.pdf, 5 November 2012).

Sugiyono.(1999).*MetodePenelitianBisnis*.Ban-dung: ALFABETA.