SATIN – Sains dan Teknologi Informasi

journal homepage : http://jurnal.Universitas-amik-riau.ac.id

Keamanan Jaringan Menggunakan IDS/IPS Strataguard sebagai Layanan Kemanan Jaringan Terpusat

Joko Dwi Susanto
Teknik Komputer Universitas AMIKOM Yogyakarta
jokodwisantoso509@hotmail.com

Sidiq Wahyu Surya Wijaya
Teknik Informatika Universitas AMIKOM Yogyakarta
sidiqw@amikom.ac.id

Abstrak

Jaringan komputer memerlukan pengelolaan yang baik agar ketersediaanya selalu tinggi. Tugas administrator jaringan memiliki banyak permasalahan, diantaranya yang berkaitan dengan keamanan jaringan komputer. Intrusion Detection Sistem (IDS) adalah sistem komputer yang berusaha melakukan deteksi penyusupan. IDS serta memberitahu saat mendeteksi sesuatu yang dianggap mencurigakan. IDS tidak melakukan pencegahan terjadinya penyusupan. Pengamatan untuk melakukan pemberitahuan itu bergantung pada bagaimana baik melakukan konfigurasi IDS. Penelitian ini ditujukan untuk mengurangi kerentanan jaringan di lingkungan Universitas AMIKOM Yogyakarta. Adapun metode penerapan penelitian ini akan ditempatkan pada layanan Network-Based dan Host-Based, sehingga pola keamanan jaringan menjadi terpadu dan mudah dipantau. Penggunaan IDS/IPS Strataguard ini menghasilkan beberapa temuan dan rekomendasi. Jaringan komputer Universitas Amikom dikembangkan dengan sistem jaringan yang bersifat tradisional. Distribusi IP Public ke setiap PC Router menjadikan keamanan jaringan intranet menjadi rentan dan vulnerable. Solusi bagi instansi ini adalah dengan membangun IDS / IPS StrataGuard, sehingga bisa dilakukan pencegahan pada saat intruder melakukan penetrasi.

Kata Kunci : Host, Network, IDS, IPS, Jaringan Komputer, Keamanan Jaringan.

1. Pendahuluan

Jaringan komputer terus mengalami perkembangan, baik dari skalabilitas, jumlah simpul dan teknologi yang digunakan. Hal ini memerlukan pengelolaan jaringan yang baik agar ketersediaan jaringan selalu tinggi [1]. Tugas pengelolaan jaringan yang dilakukan administrator jaringan memiliki banyak permasalahan, diantaranya yang berkaitan dengan keamanan jaringan komputer. Seiring bertambahnya pengguna di dalam sebuah jaringan maka tingkat keamanan jaringan juga menjadi krusial. Intrusion Detection Sistem (IDS) merupakan salah satu pilihan untuk meningkatkan keamanan jaringan dalam sebuah jaringan baik dalam bentuk intranet maupun internet.

Intrusion Detection Sistem (IDS) atau Sistem Deteksi Penyusupan adalah sistem komputer yang berusaha melakukan deteksi penyusupan [2]. IDS akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap mencurigakan atau tindakan ilegal. IDS tidak melakukan pencegahan terjadinya penyusupan. Proses pengamatan yang berlangsung memunculkan pemberitahuan yang bergantung pada konfigurasi IDS.

Selain itu, juga terdapat penelitian lain mengenai keamanan jaringan computer tentang Intrusion Detection System (IDS). Penelitian ini membahas IDS sebagai sistem yang memberikan keamanan untuk suatu jaringan. Hal ini dilakuakn dengan Elimination of False Positives atau dapat juga disebut kesalahan positif [3]. Hal ini juga menunjukkan algoritma suatu program yang menyatakan suatu gejala atau alarm yang sebetulnya tidak ada. Hal ini juga disebut juga dengan false alarm karenakemungkinanbanyak false positive, dengan demikian menghasilkan suatu istilah

FUD (fear, uncertainty, and doubt) pada keamanan jaringan. Pengguna dapat memahami bahwa IDS yang bagus memiliki kapabilitas untuk mengeliminasi false positive.

Penelitian keamanan jaringan juga dapat dilakukan pada kelas bilingual di suatu instansi tertentu. Tema penelitian ini masih mengenai IDS (Intrusion Detection System) dan IPS (Instrusion Prevention System) [4]. Sebagai manajemen keamanan informasi dan pengamanan Jaringan“, IDS yang membahas masalah pada switch yaitu proses pendeteksian terhadap paket data yang datang menjadi tidak berfungsi, salah satu cara yang mudah untuk mengatasi masalah seperti ini, cara tersebut adalah dengan melakukan spoofing MAC address terhadap host – host yang akan diamati.

Intrusion Detection System (IDS) sangat dibutuhkan seorang administrator untuk menjaga keamanan. Keahlian seorang administrator sistem diyakini penting untuk penggunaan yang efektif dari sistem deteksi intrusi (IDS) [5]. Peneltian ini membahas dua hipotesis mengenai kemampuan sistem administrator 'untuk menyaring alarm yang diproduksi oleh IDS dengan membandingkan kinerja IDS untuk kinerja administrator sistem menggunakan IDS. Metodologi yang dibangun dalam 5 jaringan komputer yang diserang selama 4 hari. Percobaan diindikasikan antara output dari administrator menggunakan IDS dan output dari IDS sendiri. Proses analisis administrator juga diselidiki melalui wawancara. Temuan menunjukkan bahwa administrator sistem menganalisis output dari IDS yang secara signifikan meningkatkan porsi alarm sesuai dengan serangan, tanpa mengurangi kemungkinan bahwa serangan terdeteksi. Selain itu, analisis terbuat dari jenis keahlian yang digunakan ketika output dari IDS diproses oleh administrator. Berdasarkan wawancara dengan administrator sistem, telah menyarankan bahwa sistem administrator yang kompeten penting dalam rangka mencapai solusi IDS efektif.

Intrusion Detection Systems (IDS) telah menjadi kebutuhan dalam sistem keamanan komputer karena peningkatan akses tidak sah dan serangan [6]. Intrusion Detection adalah komponen utama dalam sistem keamanan komputer yang dapat diklasifikasikan berbasis Host Intrusion Detection System (HIDS), yang melindungi sebuah host tertentu atau sistem Network-based Intrusion detection sistem(NIDS), yang melindungi jaringan dari host dan sistem. Penelitian ini membahas serangan probe atau serangan pengintai, yang mencoba untuk mengumpulkan informasi yang relevan yang mungkin dalam jaringan. Serangan penyelidikan jaringan memiliki dua jenis: serangan Host Sweep and Port Scan. Serangan Host Sweep menentukan host yang ada di jaringan, sementara serangan port scan menentukan layanan yang tersedia yang ada di jaringan. Penelitian ini juga menggunakan sistem cerdas untuk memaksimalkan tingkat pengenalan serangan jaringan dengan menanamkan perilaku temporal serangan menjadi struktur jaringan saraf TDNN. Sistem yang diusulkan terdiri dari 5 modul yaitu paket mesin capture, preprocessor, pengenalan pola, klasifikasi, dan monitoring, dan modul peringatan. Sistem ini menggunakan prinsip komponen jaringan saraf untuk identifikasi serangan dan modul untuk mengklasifikasikan serangan host atau port scan. Hasil penelitian telah diuji dalam lingkungan yang nyata di mana mampu mendeteksi semua serangan. Selain itu, sistem diuji dan dibandingkan dengan Snort menggunakan DARPA dataset.

Deteksi anomali serangan jaringan telah menjadi prioritas tinggi karena kebutuhan untuk menjamin keamanan, privasi, dan kehandalan [7]. Penelitian ini bertujuan untuk menggambarkan kedua pendekatan imunologi cerdas dan sistem pemantauan tradisional untuk deteksi anomali. Pendekatan artificial immune sistem(AIS) yang berbeda dan mengusulkan bagaimana menggabungkan ide-ide yang berbeda untuk memecahkan masalah dari domain keamanan jaringan. Sistem deteksi anomali yang berlaku ide-ide dibangun dan diuji di lingkungan real time, untuk menguji pro dan kontra dari AIS dan mengklarifikasi penerapannya. Ruang lingkup penelitian ini mencoba untuk mengeksplorasi prinsip dalam kekebalan jaringan yang fokus pada dorganisasi, kemampuan belajar adaptif, dan umpan balik kekebalan sistem. Sistem kekebalan sistem alami memiliki mekanisme cerdas sendiri untuk mendeteksi benda asing dan melawan mereka dan tanpa itu, seorang individu tidak bisa hidup, bahkan hanya untuk beberapa hari. Penyerang jaringan berkembang jenis baru dari serangan semula. Serangan menjadi lebih kompleks, parah dan sulit untuk dideteksi. Hal ini menyebabkan meningkatnya kebutuhan untuk sistem pertahanan jaringan, terutama dengan kemampuan untuk pendekatan menghadapi sifat dinamis dari terus berubah ancaman jaringan. KDD CUP'99 dataset yang digunakan sebagai data training untuk mengevaluasi hibrida diusulkan prinsip kekebalan deteksi anomali buatan. Biaya rata-rata model yang diusulkan adalah 0.1195 di mana bahwa penambangan dari KDD99 dataset memiliki hasil perhitungan 0.233. Orisinalitas nilai ini adalah asli untuk memperkenalkan penyelidikan pada proses biologis vaksinasi. Sebuah modul khusus dibangun untuk melakukan proses ini dan memeriksa penggunaan dan bagaimana hal itu dapat dirumuskan dalam kehidupan buatan.

2. Metode Penelitian

Tahapan untukmelakukan penelitian ini yang nantinya untuk mendapatkan solusi yang ttepat, yaitu, mendefinisikan masalah, studi kelayakan, analisis kebutuhan, merancang konsep, merancang isi, menulis

naskah, memproduksi sistem, tes pemakai, menggunakan sistem dan memelihara sistem. Teknik pengumpulan data dalam penelitian akan menggunakan teknik sebagai berikut :

1. Observasi atau pengamatan

Pengumpulan data penelitian ini akan dilakukan melalui pengamatan langsung terhadap obyek analisis untuk menggali aspek-aspek yang relevan dan penting sebagai dasar analisis dan interpretasi yang akan dilakukan.

2. Wawancara

Wawancara dimaksudkan untuk memperoleh data kualitatif serta beberapa keterangan atau informasi dari informan.

3. Dokumentasi

Penggunaan dokumen dalam penelitian ini adalah dokumen resmi dari jurusan tentang arsip ataupun dokumen, mencakup surat-surat, data-data, catatan, foto-foto kegiatan, dan lainnya yang relevan.

Metode penelitian yang dilakukan adalah metode kuantitatif dengan menerapkan perancangan sistem melalui tahap-tahap siklus hidup pengembangan sistem (System Development Life Cycle). Penelitian ini dilakukan di Universitas AMIKOM Yogyakarta, pada bagian Kerumahtanggaan, Jalan Ring Road Utara, Condong Catur, Depok, Sleman. Penelitian ini mengikuti kerangka kerja Siklus Hidup Pengembangan Sistem, yaitu :

Tahap I: Survei ruang lingkup dan kelayakan proyek Ruang lingkup penelitian ini adalah kartu pasien yang digunakan di Universitas AMIKOM.

Tahap II: Analisis sistem yang ada kegiatan yang dilakukan pada tahap ini adalah menganalisis sistem yang sedang berjalan, sehingga diketahui kekurangan dan peluang perbaikan yang mungkin dilakukan.

Tahap III: Pendefinisian kebutuhan user. Pada tahap ini dilakukan pendefinisian kebutuhan. Sistem yang dibutuhkan dalam pengembangan hardware dan software.

Tahap IV: Memilih solusi yang layak Pada tahap ini dilakukan pemilihan dari berbagai alternatif NIDS, HIPS, NIPS, HIDS yang memungkinkan sampai dengan alternative database yang akan digunakan.

Tahap V: Perancangan sistem. Pada tahap perancangan sistem, langkah-langkah yang dilakukan adalah mendesain sistem secara keseluruhan.

Tahap VI: Pengadaan hardware. Pada tahap ini dilakukan pembelian Server, yang digunakan sebagai alat uji.

Tahap VII: Pembangunan sistem baru. Pembangunan sistem baru dilakukan sesuai dengan perancangan sistem. Pembangunan sistem baru ini berupa pembuatan IDS/IPS. Pengembangan sistem menggunakan metode SDLC (Software Development Life Cycle) yang terdiri dari Analsis sistem, Perancangan, Implementasi dan pengujian sistem. Sistem ini akan di integrasi dengan teknologi IDS/IPS.

Tahap VIII: Penerapan sistem baru. Penerapan atau implementasi sistem baru dilakukan secara total pada saat sistem baru dan infrastruktur hardware sudah siap untuk diimplementasikan. Termasuk di dalam tahap ini adalah simulasi.

Dalam mencari beberapa sumber data yang bisa di gunakan untuk menjadi acuan, dalam penelitian disini menggunakan Metode Observasi, Metode Interview dan Metode Analisis Data.

1. Metode Observasi

Metode observasi yang di terapkan adalah monitoring seluruh aktifitas jaringan pada Universitas AMIKOM Yogyakarta. Dimana untuk mendapatkan beberapa sampel data yang bisa di gunakan sebagai penguat penelitian. Dalam penelitian ini menggunakan beberapa tools antara lain :

a. Wireshark

Digunakan untuk menyadap semua informasi layanan data yang terkoneksi di jaringan wifi dan lan kampus.

b. Digiblast

Tools yang berfungsi untuk penetrasi ke dalam jaringan wifi dan lan kampus.

c. Softperfect Network Scanner

Tools scanning jaringan yang di gunakan untuk melihat macaddres user yang terkoneksi di jaringan, perolehan IP dalam jaringan dan juga data yang di share pada client.

d. Colasoft Capsa

Digunakan untuk melihat protokol – protokol jaringan.

e. IDS Sax2

Digunakan untuk melihat protokol – protokol jaringan dan percentase ancaman yang ada dalam suatu jaringan yang berfungsi untuk lookup jaringan wireles dan Lokal Area Network (LAN) di Universitas AMIKOM Yogyakarta. Sebagian data di peroleh dari IC (INNOVATION CENTER),dimana data ini nantinya akan di bandingkan dengan data yang di dapatkan di lapangan. Adapun data yang di dapatkan adalah sebagai berikut:

2. Metode Interview

Metode Interview yang digunakan adalah langsung bertanya pada sumber – sumber yang ada. Dimana di dapatkan beberapa permasalahan yang terdapat pada jaringan Universitas AMIKOM Yogyakarta di anatara lain adalah sebagai berikut:

a. Hak akses kontrol jaringan yang bisa di akses oleh siapa saja yang berada di lingkungan Universitas AMIKOM Yogyakarta hal ini merupakan tugas pokok dari seorang administrator jaringan.
b. Pembagian IP pada jaringan wireless yang semakin membengkak tanpa pernah ada yang mengauditnya. Hal ini terjadi karena pada saat user registrasi tidak dilakukan filtering dan hanya menerima registrasi dari user saja, akan tetapi tidak memberikan batasan usia masa studi mahasiswa

yang masih aktif dan yang sudah lulus pada masa registrasi koneksi internet pada jaringan Universitas AMIKOM Yogyakarta.

c. Enkripsi pada jaringan wireless amikom yang masih bisa di dekripsi dengan mudah sehingga user dari luar mampu untuk menjebolnya. Enkripsi yang ada pada wifi di amikom masih menggunakan 32Bit dapaun jenis – jenis enkripsi yang didapatkan adalah sebagai berikut :

WEP (Wired Equivalent Privacy) merupakan standart keamanan dan enkripsi pertama yang digunakan pada wireless, WEP (Wired Equivalent Privacy) adalah suatu metoda pengamanan jaringan nirkabel, disebut juga dengan Shared Key Authentication. Shared Key Authentication adalah metoda otentikasi yang membutuhkan penggunaan WEP. Enkripsi WEP menggunakan kunci yang dimasukkan (oleh administrator) ke client maupun access point. Kunci ini harus cocok dari yang diberikan akses point ke client, dengan yang dimasukkan client untuk authentikasi menuju access point, dan WEP mempunyai standar 802.11b. Proses Shared Key Authentication:

1. Client meminta asosiasi ke access point, langkah ini sama seperti Open System Authentication.
2. Access point mengirimkan text challenge ke client secara transparan.
3. Client akan memberikan respon dengan mengenkripsi text challenge dengan menggunakan kunci WEP dan mengirimkan kembali ke access point.
4. Access point memberi respon atas tanggapan client, akses point akan melakukan decrypt terhadap respon enkripsi dari client untuk melakukan verifikasi bahwa text challenge dienkripsi dengan menggunakan WEP key yang sesuai. Pada proses ini, access point akan menentukan apakah client sudah memberikan kunci WEP yang sesuai. Apabila kunci WEP yang diberikan oleh client sudah benar, maka access point akan merespon positif dan langsung meng-authentikasi client. Namun bila kunci WEP yang dimasukkan client adalah salah, maka access point akan merespon negatif dan client tidak akan diberi authentikasi. Dengan demikian, client tidak akan terauthentikasi dan tidak terasosiasi.

Menurut Arief Hamdani Gunawan, Komunikasi Data via IEEE 802.11, Shared Key Authentication kelihatannya lebih aman dari dari pada Open System Authentication, namun pada kenyataannya tidak. Shared Key malah membuka pintu bagi penyusup atau cracker. Penting untuk dimengerti dua jalan yang digunakan oleh WEP. WEP bisa digunakan untuk memverifikasi identitas client selama proses shared key dari authentikasi, tapi juga bisa digunakan untuk men-dekripsi data yang dikirimkan oleh client melalui access point. WEP memiliki berbagai kelemahan antara lain :

a) Masalah kunci yang lemah, algoritma RC4 yang digunakan dapat dipecahkan..
b) WEP menggunakan kunci yang bersifat statis.
c) Masalah initialization vector (IV) WEP.
d) Masalah integritas pesan Cyclic Redundancy Check (CRC-32).

WEP terdiri dari dua tingkatan, yakni kunci 64 bit, dan 128 bit. Sebenarnya kunci rahasia pada kunci WEP 64 bit hanya 40 bit, sedang 24bit merupakan Inisialisasi Vektor (IV). Demikian juga pada kunci WEP 128 bit, kunci rahasia terdiri dari 104bit.

Serangan-serangan pada kelemahan WEP antara lain :

a) Serangan terhadap kelemahan inisialisasi vektor (IV), sering disebut FMS attack. FMS singkatan dari nama ketiga penemu kelemahan IV yakni Fluhrer, Mantin, dan Shamir. Serangan ini dilakukan dengan cara mengumpulkan IV yang lemah sebanyak-banyaknya. Semakin banyak IV lemah yang diperoleh, semakin cepat ditemukan kunci yang digunakan.
b) Mendapatkan IV yang unik melalui packet data yang diperoleh untuk diolah untuk proses cracking kunci WEP dengan lebih cepat. Cara ini disebut chopping attack, pertama kali ditemukan oleh h1kari. Teknik ini hanya membutuhkan IV yang unik sehingga mengurangi kebutuhan IV yang lemah dalam melakukan cracking WEP.
c) Kedua serangan diatas membutuhkan waktu dan packet yang cukup, untuk mempersingkat waktu, para hacker biasanya melakukan traffic injection. Traffic Injection yang sering dilakukan adalah dengan cara mengumpulkan packet ARP kemudian mengirimkan kembali ke access point. Hal ini mengakibatkan pengumpulan initial vektor lebih mudah dan cepat. Berbeda dengan serangan pertama dan kedua, untuk serangan traffic injection,diperlukan spesifikasi alat dan aplikasi tertentu yang mulai jarang ditemui di toko-toko, mulai dari chipset, versi firmware, dan versi driver serta tidak jarang harus melakukan patching terhadap driver dan aplikasinya.

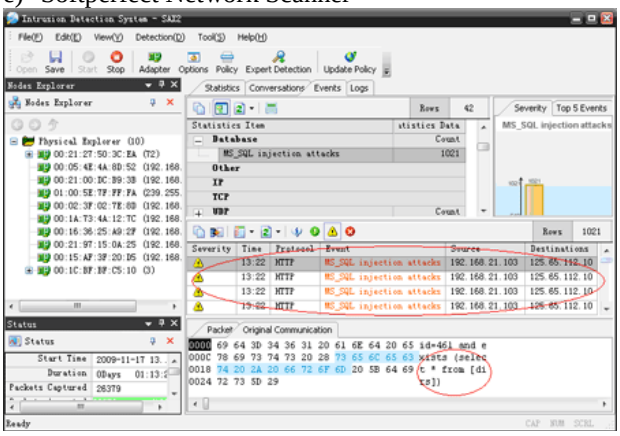
Di dalam metode ini memberikan sample dari analisis yang di lakukan pada jaringan Universitas AMIKOM menggunakan Intrusion Detection System - Sax2 adapun sample log data yang di kumpulkan sebagai pembanding dari log data yang di berikan oleh IC (INNOVATION CENTER) Universitas “AMIKOM“ dengan data di lapangan.

Peristiwa yang dipilih dalam Gambar 2 menunjukkan penyerang IP 192.168.21.103, korban IP 125.65.112.10. Dan pesan asli adalah "* pilih dari [dirs]", berarti menanyakan apakah ada datasheet bernama "dirs" dalam database saat ini, dalam tampilan

Komunikasi Asli. Penyerang akan mengulangi operasi untuk mendapatkan datasheet yang diharapkan.

Untuk mendapatkan data yang akurat maka perlu melakukan beberapa sample penetrasi dalam infrastruktur jaringan amikom dengan menggunakan tools sebagai berikut :

a) Intrusion Detection System – Sax2
b) Digiblast Ddos
c) Wireshark
d) Colasoft
e) Softperfect Network Scanner



Gambar 1. Alarm IDS Sax2 Pada Serangan Injeksi Ms_Sql Sifatnya Real-Time

Adapun hasil dari capture data dan log data dari lapangan dan IC (INNOVATION CENTER) ditunjukkan pada Tabel 1.

Tabel 1. Pengujian Jaringan Wifi dan LAN

Tanggal	Jam	Lokasi	SSID	Jenis Serangan
11 - 09 - 2010	13:20	Pengajaran Lama	Gejayan Selat 2 dan 3	SYN ACK ATTACK
IDS Sax2				BruteForce
Colasoft				Thresold
Wireshark				Floodder
11 - 09 - 2010	16:00	LAN Pengajaran Lama	-	Malware Decoder
Colasoft				
IDS Sax2				
02 – 02 - 2010	10:15	MSV Studio	-	Malware Decoder
IDS Sax2				
Wireshark				
03 - 08 - 2010	14:00	Wifi	Selat 2 dan 3	SYN ACK ATTACK
IDS Sax2				BruteForce
Colasoft				Thresold
Wireshark				Floodder
Digiblast				Ddos
11 - 10 - 2010	18:00	Wifi	Unit III	Trojan
IDS Sax2				Malware
Colasoft				SYN ACK ATTACK
12 - 03 - 2010	09:00	Wifi	Unit III	BruteForce
IDS Sax2				Thresold
Colasoft				Floodder
Wireshark				Ddos
Digiblast				Trojan
				Malware
				SYN ACK ATTACK
02 - 12 - 2010	10:00	Pengajaran Baru	Pengajaran Baru	Floodder
IDS Sax2				Ddos
Colasoft				Trojan
Wireshark				Malware
Digiblast				SYN ACK ATTACK
				Duplicated MAC
12 - 12 - 2010	12:20	Basemant Unit II	Basemant Unit II	Ddos
IDS Sax2				SSH Tunneling
Colasoft				SYN ACK ATTACK
Wireshark				Duplicated MAC

Analisis sistem dapat didefinisikan sebagai penguraian dari suatu komponen informasi yang utuh kedalam bagian-bagian kompnennya, dengan maksud untuk mengidentifikasikan dan mengevaluasi permasalahan-permaasalahan, kesimpulan-kesimpulan, hambatan-hambatan yang terjadi, serta kebutuhan-kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan-perbaikannya.

Tinjauan kasus yang telah diidentifikasi berdasarkan bukti dari MasterPlan yang di berikan oleh pihak IC (Innovation Center) adalahdiuraikan pada penjelasan berikut ini.

Jaringan Komputer Universitas AMIKOM Yogyakarta dikembangkan dengan sistem jaringan yang bersifat tradisional yakni memanfaatkan PC router sebagai pembagi broadcast domain ke setiap unit kerja atau group pengguna jaringan di setiap gedung Universitas AMIKOM Yogyakarta Yogyakarta. Hal ini menyebabkan setiap penambahan unit kerja atau group tertentu maka akan membutuhkan sebuah PC router atau minimal sebuah kartu jaringan agar mampu membentuk jaringan (subnetwork) yang baru sehingga manajemen jaringan dan maintenance lebih kompleks dan cenderung kesulitan untuk menerapkan standart policy pada setiap jaringan.

Pada beberapa subnet (jaringan) atau kelompok user (group), terdapat jaringan yang hanya dimanage menggunakan ip aliases melalui interface pc router, hal ini membuat performance jaringan tidak bekerja dengan optimal. Penggunaan lebih dari satu subnet pada jaringan yang memiliki broadcast domain yang sama mengakibatkan broadcast yang lebih besar, disamping terdapat permasalahan keamanan karena administrator tidak dapat mengontrol komunikasi kedua jaringan yang masih berada pada broadcast domain yang sama. Pembagian subnet jaringan yang hanya memanfaatkan IP aliases justru akan mengurangi kinerja atau performa jaringan komputer itu sendiri.

Distribusi Internet Protokol Public (IP Public) ke setiap PC Router yang dimaksudkan untuk membagi koneksi internet ke setiap unit/lab menjadikan sistem keamanan jaringan intranetUniversitas AMIKOM Yogyakarta menjadi rentan dan vulnerable. Hal ini karena IP Public yang digunakan oleh setiap PC router otomatis terpublikasi di Internet yang harusnya menjadi jaringan yang tidak dapat dipercaya (untrust network). Dengan kondisi sekarang, maka setiap pengguna internet dimungkinkan untuk melakukan penyerangan ke jaringan Intranet Universitas AMIKOM Yogyakarta, padahal jaringan intranet menjadi jaringan yang aman dari jaringan di luar Jaringan Kampus Universitas AMIKOM Yogyakarta (termasuk Internet).

Penggunaan IP Private dan IP Public di setiap PC router di unit-unit/laboratorium, menyebabkan routing jaringan internal dan jaringan public (internet) menjadi satu (digabung), hal ini membuat manajemen dan monitoring komunikasi data antar jaringan intranet atau antar unit/lab sulit dilakukan, karena adanya pemanfaatan fungsi masquarade (NAT) atau penyembunyian identitasinternet protokolpengguna jaringan. Selain itu komunikasi antar ip public dan ip private sudah tidak sesuai aturan RFC, dimana IP Private seharusnya tidak dapat di routingkan melalui IP Public (non-routabel)

Pemberian alamat Internet Protokol pada beberapa unit kerja tidak seragam atau berada pada kelas IP yang berbeda, selain mengakibatkan kesulitan menjamin skalabilitas dan kemampuan untuk dapat diakses dari mana saja, juga membuat administrasi jaringan semakin rumit.

Saat ini server-server intranet pada kampus Universitas AMIKOM Yogyakarta dipasangkan IP public yang menyebabkan kemungkinan terpublikasikan atau dapat diaksesnya informasi server internal tersebut dari Internet.

Koneksi dari setiap client ke internet masih bersifat koneksi langsung (direct connection), tanpa ada filtering, proses caching atau otentikasi melalui proxy server. Hal ini selain akan mengakibatkan kesulitan dalam melakukan monitoring ataupun audit penggunaan jaringan komputer di Universitas AMIKOM Yogyakarta Yogyakarta, juga mengakibatkan bandwidth terpakai banyak yang terbuang percuma atau tidak optimal pemanfaatannya.

Pemasangan Wireless Access Point untuk mendistribusikan koneksi internet di lingkungan luar gedung kampus Universitas AMIKOM Yogyakarta sebaiknya dipertimbangkan kembali. Jaringan wireless merupakan jaringan yang memiliki tingkat vulnerable yang sangat tinggi, diperlukan monitoring yang terus-menerus dan pemanfaatan teknologi keamanan jaringan wireless berlapis untuk menjamin pengguna benar benar memiliki otorisasi menggunakan akses tersebut.

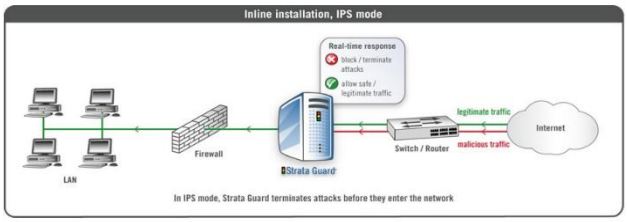
Saat ini, beberapa jaringan wireless (AP) digunakan sebagai bridge yang terhubung secara langsung ke pengguna pada jaringan kabel tanpa ada proteksi (filtering), hal ini akan sangat mengganggu trafik yang terjadi pada kedua jaringan tersebut karena masih menggunakan broadcast domain yang sama. Sebaiknya broadcast domain untuk jaringan wireless dipisahkan dengan broadcastdomain jaringan kabel (wired network).

Pendistribusian koneksi jaringan kabel UTP melalui switch secara bertingkat (koneksi dari switch yang satu ke switch yang lain karena harus menjangkau lebih dari 100 meter) perlu mendapatkan perhatian atau pengukuran kembali. Karena jika sudah melalui beberapa switch, signal koneksi jaringan akan melemah dan mengakibatkan akses yang lambat atau bahkan terputus.

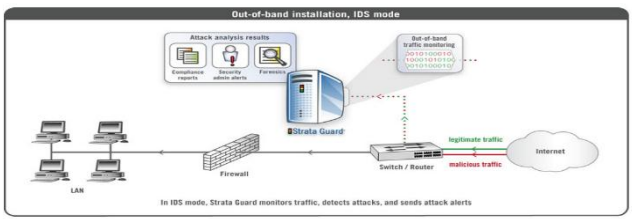
Penggunaan kanal frekwensi dalam pemasangan Access Point atau HotSpot umumnya belum melakukan site-survey terlebih dahulu, sehingga jangkauan atau pemanfaatan hotspot kurang maksimal, akibat terjadi interference antar wireless yang satu dengan yang lainnya. Penempatan Wireless Access point sebaiknya mengukuti kaidah frekwensi yang bersifat re-usable dan dapat dialokasikan pada lokasi yang berdekatan seperti aturan penggunan kanal 1, kanal 6 dan kanal 11 di lokasi yang berdekatan.

Kondisi saat ini, monitoring traffic hanya dilakukan di backbone internet saja, hal ini dapat menyulitkan penelusuran jika terdapat anomali traffik seperti malware yang menginfeksi sebuah komputer client. Monitoring traffic hingga ke level pengguna sebaiknya dapat dilakukan agar jika terjadi suatu anomali atau gangguan trafik pada jaringan, dapat langsung ditelusuri penyebab dan permasalahannya.

Skema IDS / IPS StrataGuard Yang Di Usulkan Untuk Jaringan Universitas AMIKOM Yogyakarta. Adapun Skema IDS/IPS StrataGuard Bisa di lihat pada Gambar 2.



Gambar 2. Inline Deployment



Gambar 3. Out-Of-Band Deployment

Perangkat lunak juga merupakan perangkat yang sangat penting dalam proses pembuatan system, karena perangkat lunak berisikan program yang perintahnya digunakan untuk menjalankan sistemkomputer.Adapun software yang digunakan dalam proses pembangunan keamanan jaringan StratGuard IDS/IPS.

Sistem operasi StratGuard IDS/IPS merupakan Flatform Sistem Operasi yang digunakan dalam pembuatan sistemkeamanan jaringan yang berbasis GNU Linux.Saat ini sistem operasi Windows sudah dikembangkan, tetapi ada software yang dijalankan tidak selancar linux dan sistem kemanan di windows tidak sebaik di linux. Sistem operasi ini akan digunakan untuk kebutuhan Client yang sifatnya User Friendly

a) Intrusion Detection System – Sax2

Merupakan tools monitoring jaringan ini dapat mendeteksi arah broadcast dari user dan akan memblok secara otomatis.

b) Digiblast Ddos

Sebagai tools untuk menflood jaringan amikom, hal ini di gunakan untuk elihat kinerja dari StrataGuard.

Wireshark

Software untuk paket sniffing atau software pengintai di dalam jaringan.

c) Colasoft

Merupakan tools monitoring jaringan ini dapat mendeteksi arah broadcast dari user dan akan memblok secara otomatis dan lebih lengkap dari IDS – Sax2.

d) Softperfect Network Scanner

Software untuk melihat filesharing yang di lakukan oleh end – user di dalam jaringan wifi maupun lan.

Analisis kebutuhan sistem merupakan proses identifikasi dan evaluasi permasalahan-permasalahan yang ada, sehingga dapat dibangun sebuah sistem yang sesuai dengan yang diharapkan. Sistem Deteksi IDS/IPS StratGuard Pada Jaringan Komputer ini dibuat untuk kebutuhan sebagai berikut :

a) Mampu mengidentifikasi adanya usaha-usaha penyusupan pada suatu jaringan komputer.
b) Mampu mengirimkan peringatan jika ada usaha-usaha penyusupan pada suatu jaringan komputer.
c) Mampu meminimalkan kerugian akibat kehilangan data atau informasi penting akibat adanya penyusupan yang berniat jahat.

Setelah melihat akan kebutuhan di atas, maka masukan yang diperlukan untuk memenuhi kebutuhan sistem adalah aktivitas penyusup yang terekam dalam log file, yaitu semua kejadian terutama lalu lintas data yang terjadi pada komputer server, yang kemudian akan digunakan sebagai data untuk analisis penentuan ada tidaknya usaha penyusupan.Tahapan ini berfungsi untuk mengetahui keluaran apa saja yang akan dihasilkan dari sistem yang dibangun. Adapun spesifikasi keluaran dalam bentuk peringatan adanya usaha penyusupan pada sistem jaringan komputer.Data-data penyusup (jika ada penyusup), yaitu: user name, host name dan IP address.Adapun profile dari pengguna perangkat lunak ini adalah :

a) Administrator

Sistem deteksi penyusup ini digunakan oleh administrator jaringan komputer sebagai sarana utama untuk mendeteksi adanya penyusup.

b) Operator

Operator adalah staff yang diberi wewenang/hak oleh administrator untuk menggantikan tugas dan tanggung jawab administrator jika diperlukan.

Sistem deteksi penyusup menggunakan teknologi IDS/IPS StrataGuard untuk memonitoring segala bentuk aktifitas dan laju data dalam suatu jaringan,dengan tujuan utama meningkatkan keamanan jaringan komputer dari serangan penyusup. Pada sistem ini komputer server akan menggunakan sistem operasi server (pada penelitian ini menggunakan IDS/IPS StrataGuard). Untuk itu administrator disyaratkan mempunyai pengetahuan yang memadai mengenai jaringan komputer, setidaknya memiliki kemampuan:

a) Administrator

Memiliki pengetahuan jaringan komputer.Memiliki pengetahuan tentang keamanan jaringan komputer dan karakteristik penyusup pada jaringan komputer.Dapat melakukan tindakan yang diperlukan untuk menangkal kegiatan lebih jauh dari penyusup yang telah teridentifikasi oleh sistem.Dapat mengoperasikan MultiPlatform.

b) Operator

Memiliki pengetahuan jaringan komputer.Memiliki pengetahuan tentang keamanan jaringan komputer dan penyusup pada jaringan komputer.Dapat mengoperasikan Platform tertentu.Strategi Program

Sesuai dengan tujuan penelitian ini yaitu mengidentifikasi adanya usaha penyusupan yang berusaha masuk ke sistemjaringan, membuat pintu belakang untuk masuk kembali ke sistem, dan menghilangkan jejak pada sistem operasi IDS/IPS StrataGuard dengan cara remote login, install backdoor, dan menghapus log file, dengan menganalisa log file sesuai dengan aturan pada penelitian ini.

Perancangan sistem keamanan jaringan StratGuard IDS/IPS ini merupakan filterisasi suatu pelewatan data melalui jaringan computer baik intranet maupun internet. Hasil identifikasi sistem dikirimkan berupa alert.

3. Hasil dan Pembahasan

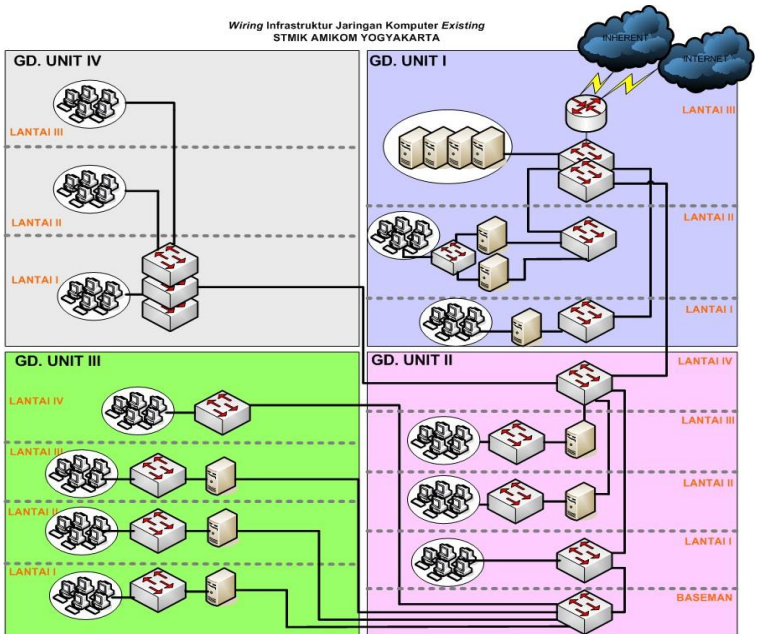
Pembangunan sistem keamanan jaringan IDS/IPS StrataGuard dilakukan menggunakan prosedur operasi dan pengujian yang mengacu pada desain perancangan. Pada bab ini membahas infrastruktur jaringan Universitas AMIKOM dan beberapa prosedur yang dilakukan. Kendala yang di hadapi dalam penelitian ini antara lain sebagai berikut:

a. Tidak memungkinkanya mengakses ke server Universitas AMIKOM dengan pertimbangan untuk keamanan data, sehingga penelitian tidak bisa di implementasikan secara nyata.
b. Sulitnya mendapatkan log real activity network di Universitas AMIKOM, yang tidak memungkinkanya melakukan auditing IP. Hal ini berhubungan dengan sistem IDS untuk melihat real time request IP.
c. Banyaknya SSID yang seragam dan cluster jaringan yang tidak sesuai dengan blueprint rancangan jaringan Universitas AMIKOM.
d. Lamanya pemberian data dari pihak instansi, sehingga penelitian menjadi tertunda.

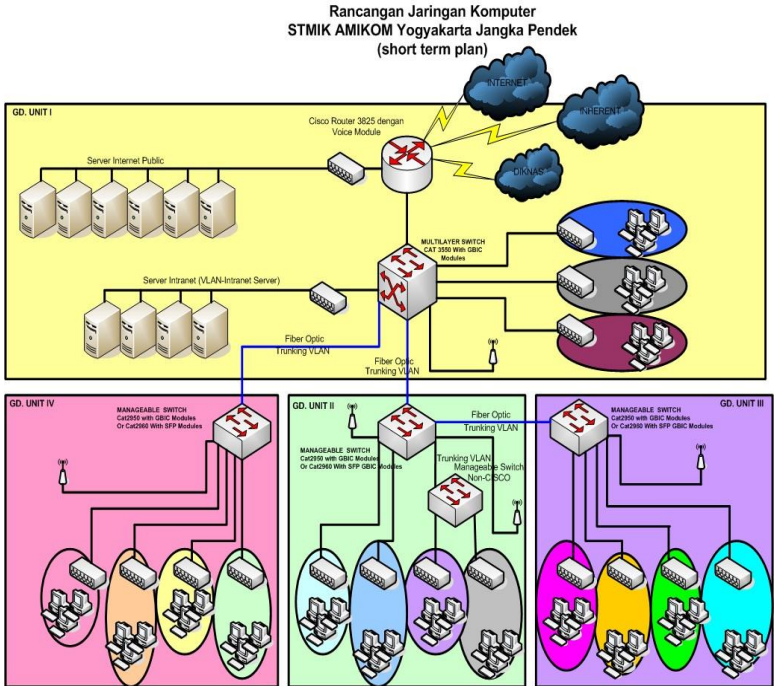
Penelitian hanya dapat dilakukan pada hostbased jaringan Universitas AMIKOM, sehingga menghasilkan rancangan keamanan jaringan yang ditawarkan pada Universitas AMIKOM. Adapun log data yang di ambil di lapangan berasal dari pengumpulan beberapa SSID Wifi di lingkup kampus Universitas AMIKOM. Hasil dari log data di cantumkan di lampiran.

Berdasarkan master plan jaringan yang diberikan pihak yang menungi jaringan maka tujuan langkah ini dapat dilakukan dengan mempelajari secara terinci, mengenai opesi sistem yang ada. Pembelajaran sistem ini diperlukan data yang diperoleh dengan cara melakukan penelitian secara terinci. Adapun sistem yang sedang berjalan ataupun baru rencana ini didapatkan dari IC (Innovation Center) ditunjunkkan pada Gambar 4 ddan 5.

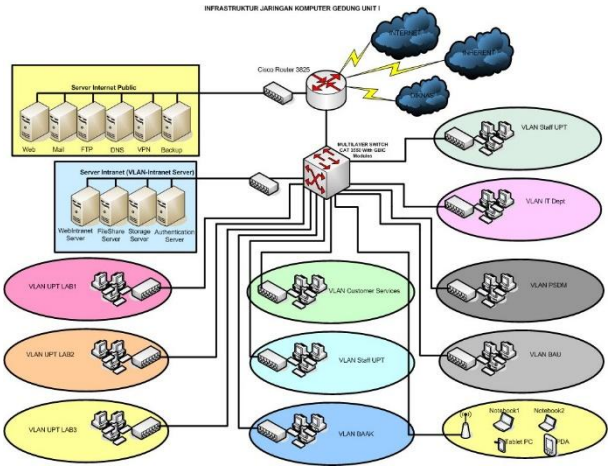
Pada Gedung Unit I terdapat NOC (Network Operating Center) yang terletak di lantai 3. Pada gedung ini dirancang beberapa VLAN sesuai fungsi dan unit kerja masing masing pengguna seperti VLAN Staff UPT, VLAN IT Dept, VLAN PSDM, VLAN BAU, VLAN Customer Services, VLAN BAAK dan beberapa VLAN UPT LAB. Pada gedung ini merupakan lokasi beroperasinya Server Public dan Server Intranet. Server Public yang terdiri dari Web Server, Mail Server, Proxy Server, VPN Server, FTP Server dan DNS Server merupakan server-server yang dapat diakses dari Intranet dan Internet. Sedang server-server yang berada di VLAN Intranet serta dikhususkan untuk keperluan Intranet sehingga hanya dapat diakses dari area local Kampus Universitas AMIKOM saja.



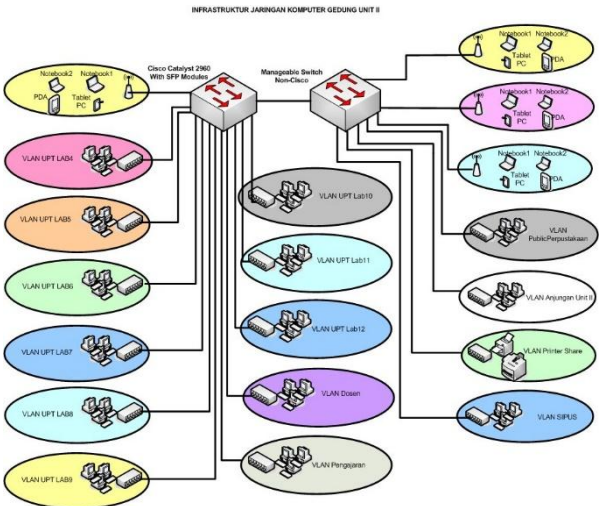
Gambar 4. Skema Jaringan Komputer Universitas AMIKOM



Gambar 5. Skema Infrastruktur Jaringan Komputer Universitas AMIKOM Jangka Pendek



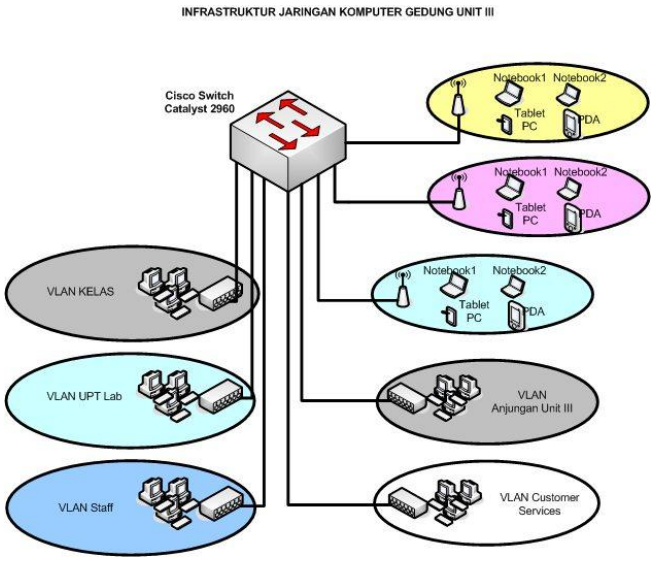
Gambar 6. Skema Rancangan untuk Gedung Unit I



Gambar 7. Skema Rancangan untuk Gedung Unit II

Pada Gedung Unit II terdapat lebih banyak VLAN, karena pada gedung ini selain areanya lebih luas, juga aktifitas lebih padat. Dirancang 8 buah Laboratorium yang memiliki VLAN masing masing. Pada gedung ini juga terdapat unit kampus seperti Perpustakaan dan Ruang Dosen serta Pengelola. Di Perpustakaan dirancang terdiri dari beberapa VLAN yakni, VLAN Anjungan Unit II, VLAN SIPUS dan VLAN Public Perpustakaan. Untuk Dosen Tetap yang berada di Ruang Dosen dan Dosen Tamu di Pengajaran masing masing memiliki VLAN tersendiri. Untuk mahasiswa yang mobile, disediakan beberapa Hotspot dengan jaringan VLAN tersendiri. Jaringan Komputer Gedung Unit III terdiri dari beberapa VLAN, seperti Customer services, VLAN Kelas , VLAN Anjungan Unit III dan beberapa VLAN Hostpot.

Pada perencanaan dan implementasi skema jaringan diatas, maka diperlukan prancangan ulang alamat logikal atau IP Addressing seluruh jaringan yang ada. Pemilihan pengalamatan jaringan (IP addressing) harus benar-benar dipertimbangkan secara baik, agar disesuaikan kebutuhan sekarang dan mendatang. Jadi, tidak perlu ada perubahan yang signifikan lagi. Pada Tabel 2 ditunjukkan rencana pengalamatan Internet Protokol pada jaringan Intranet berbasis VLAN.



Gambar 8. Skema Rancangan untuk Gedung Unit III

Tabel 2. Alokasi IP Address Intranet Universitas AMIKOM

No	Nama VLAN	No VLAN	IP Network	IP Gateway
1	BAAK	11	172.16.11.0/24	172.16.11.254
2	BAU	12	172.16.12.0/24	172.16.12.254
3	CustomerService	13	172.16.13.0/24	172.16.13.254
4	IT Dept	14	172.16.14.0/24	172.16.14.254
5	PSDM	15	172.16.15.0/24	172.16.15.254
6	CNAP	16	172.16.16.0/24	172.16.16.254
7	Dosen(r.dosen)	17	172.16.17.0/24	172.16.17.254
8	Pengajaran	18	172.16.18.0/24	172.16.18.254
9	PengelolaEksekutif	19	172.16.19.0/24	172.16.19.254
10	SIPUS	20	172.16.20.0/24	172.16.20.254
11	PublicPerpustakaan	21	172.16.21.0/24	172.16.21.254
12	AnjunganUnit3	22	172.16.22.0/24	172.16.22.254
13	AnjunganUnit2	23	172.16.23.0/24	172.16.23.254
14	Server Intranet	24	172.16.24.0/24	172.16.24.254
1	Print Server	25	172.16.25.0/2	172.16.25.25

No	Nama VLAN	No VLAN	IP Network	IP Gateway
5			6	4
16	StaffUPT	26	172.16.26.0/24	172.16.26.254
17	UPT Lab1	101	172.16.101.0/24	172.16.101.254
18	UPT Lab2	102	172.16.102.0/24	172.16.102.254
19	UPT Lab3	103	172.16.103.0/24	172.16.103.254
20	UPT Lab4	104	172.16.104.0/24	172.16.104.254
21	UPT Lab5	105	172.16.105.0/24	172.16.105.254
22	UPT Lab6	106	172.16.106.0/24	172.16.106.254
23	UPT Lab7	107	172.16.107.0/24	172.16.107.254
24	UPT Lab8	108	172.16.108.0/24	172.16.108.254
25	UPT Lab9	109	172.16.109.0/24	172.16.109.254
26	UPT Lab10	110	172.16.110.0/24	172.16.110.254
27	UPT Lab11	111	172.16.111.0/24	172.16.111.254
28	UPT Lab12	112	172.16.112.0/24	172.16.112.254
29	Wifi 1	201	172.16.201.0/24	172.16.201.254
30	Wifi 2	202	172.16.202.0/24	172.16.202.254
31	Wifi 3	203	172.16.203.0/24	172.16.203.254
32	Wifi 4	204	172.16.204.0/24	172.16.204.254
33	Wifi 5	205	172.16.205.0/24	172.16.205.254
34	Wifi 6	206	172.16.206.0/24	172.16.206.254
35	Wifi 7	207	172.16.207.0/24	172.16.207.254
36	Wifi 8	208	172.16.208.0/24	172.16.208.254
37	Wifi 9	209	172.16.209.0/24	172.16.209.254
38	Wifi 10	210	172.16.210.0/24	172.16.210.254
39	Wifi 11	211	172.16.211.0/24	172.16.211.254
40	Wifi 12	212	172.16.212.0/24	172.16.212.254

Berdasarkan hasil penelitian ini makadihasilkan analisis masterplan jaringan di Universitas AMIKOM Yogyakarta yang tidak sesuai dengan konsepkeamanan jaringan. Adapun langkah ini dilakukan berdasarkan data yang diperoleh dari hasil penelitia. Analsisi masalah bertujuan untuk menemukan jawaban penyebab sebenarnya dari masalah yang timbul. Pengujian yang dilakukan adalah pada jaringan wifi di lingkungan kampus Universitas AMIKOM Yogyakarta. Adapun lebih detilnya ditunjukkan pada tabel 3.

Tabel 3. Pengujian Jaringan Wifi dan Lan Universitas AMIKOM Yogyakarta

Tanggal	Jam	Lokasi	SSID	Jenis Serangan
11 - 09 - 2010	13:20	Pengajaran Lama	Gejayan	SYN ACK ATTACK
			Selat 2 dan 3	BruteForce
				Thresold
				Floodder
11 - 09 - 2010	16:00	LAN Pengajaran Lama	-	Malware Decoder
02 – 02 - 2010	10:15	MSV Studio	-	Malware Decoder
03 - 08 - 2010	14:00	Wifi	Selat 2 dan 3	SYN ACK ATTACK
				BruteForce
				Thresold
				Floodder
				Ddos
11 - 10 - 2010	18:00	Wifi	Unit III	Trojan
				Malware
				SYN ACK ATTACK
12 - 03 - 2010	09:00	Wifi	Unit III	BruteForce
				Thresold
				Floodder
				Ddos
				Trojan
				Malware
				SYN ACK ATTACK
02 - 12 - 2010	10:00	Pengajaran Baru	Pengajaran Baru	Floodder
				Ddos
				Trojan
				Malware
				SYN ACK ATTACK
				Duplicated MAC
12 - 12 - 2010	12:20	Basemant Unit II	Basemant Unit II	Ddos
				SSH Tunneling

Tanggal	Jam	Lokasi	SSID	Jenis Serangan
				SYN ACK ATTACK
				Duplicated MAC

Untuk itu penulis menawarkan jenis portal OpenSource yang difungsikan sebagai pengganti frewall. Implementasi dan prosedur operasi pada jaringan IDS/IPS StrataGuard sistem akan dilakukan sesuai dengan langkah-langkah diatas. Pada pengujian sistem akan dilakukan beberapa pengujian agar sistem bisa diketahui dapat berjalan dengan normal serta dapat dianalisis keamanan dalam sistemkeamanan jaringan menggunakan IDS/IPS StrataGuard tersebut.

Instalasi server ada dua hal yang harus dipersiapkan yaitu pada sisi hardware dan software. Pada sisi hardware dilakukan dengan mempersiapkan PC server dengan ditunjukkan pada Tabel 4.

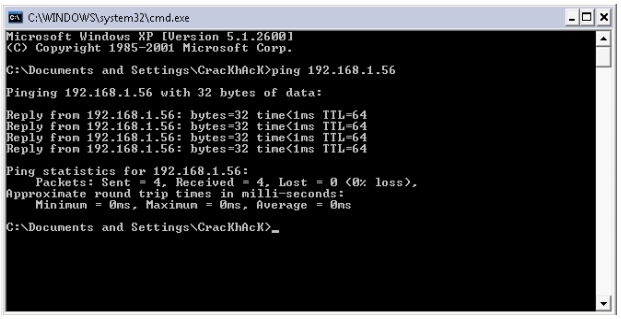
Tabel 4. StratGuard Rekomendasi Sistem

Item	Minimum	Rekomendasi
Server – A dedicated server for product installation with the following minimum sistemrequirements:		
Processor	Single Core (2.8 GHz)	Quad Core, 2.33 GHz minimum Eight Core for Multi-Gig Speeds
RAM	2 GB	4 GB
Disk space	36 GB	160 GB to 250 GB
Server-class network interfaces: Strata Guard standard mode – 2 ea. Strata Guard gateway mode – 3 ea.	10/100/1000 serverquality (Intel)	10/100/1000 serverquality (Intel)
CD R/W ROM drive: • CD W drive to create an install CD • CD R drive to use for first-time installation • DVD	Yes	Yes
An Internet connection that allows outbound SSL communications	Yes	Yes
High-availability (HA) bypass card [optional])	Not available	Optional
Workstation – Windows workstation running Internet Explorer 6.0 or 7.0 with 128-bit encryption and Microsoft Java Virtual Machine plug-in.	Yes	Yes
License – A subscription license key	Yes	Yes

Tujuan pengujian koneksi adalah perangkat komunikasi dalam jaringan komputer berjalan dengan baik dengan cara mengirimkan paket menuju komputer lain kemudian dikirimkan kembali dalam jangka waktu yang telah ditentukan oleh komputer.

a) Semua komputer baik dari client atau server melakukan pengujian terhadap interface network dapat melewatkan paket TCP/ IP berjalan dengan baik dengan menjalankan perintah di command prompt ‘ping 127.0.0.1’. (Ping 127.0.0.1 adalah alamat localhost)
b) Pengujian dari sisi server dengan menjalankan perintah ping menuju ke semua client.

Ketika menjalankan perintah ping di command prompt jika dilayar akan muncul seperti pada Gambar 10. Pada Gambar 10 Menunjukkan bahwa koneksi pada jaringan berjalan dengan normal sehingga data bisa dikirimkan dan diterima.

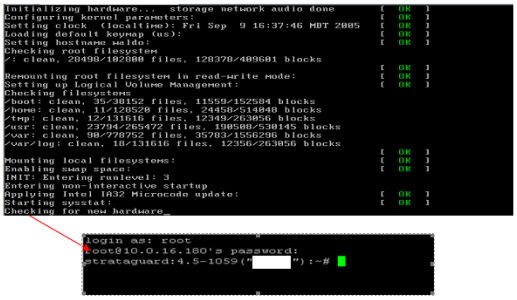


Gambar 9. Pengujian Ping Sudah Berjalan Dengan Bafik

Tujuan perancangan pengujian server adalah mengetahui PC server dapat bekerja dengan baik untuk melayani segala bentuk serangan atau intruder yang di lakukan pada sisi client baik lan mau wireless. Mekanisme Pengujian Server adalah sebagai berikut:

a) Komputer server booting secara normal sampai proses berakhir ditandai dengan munculnya halaman login user pada layar monitor.
b) Komputer Server dapat dikonfigurasi melalui remote web base sampai` ke tahap halaman login user.
c) Komputer Server dapat menambahkan serta aturan untuk sekuriti jaringan dan os yang akan kita pilih.
d) Komputer Server dapat menjalankan gateway dan firewall mode serta dapat berjalan di single node atau multiple node.

Pada layar komputer akan muncul tampilan awal login seperti pada Gambar 11 Menunjukkan proses booting pada komputer server berjalan dengan normal dan siap untuk dilakukan konfigurasi.

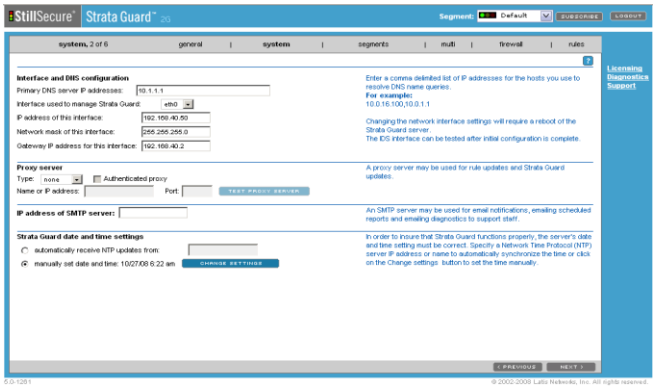


Gambar 10. Tampilan Login StrataGuard

Komputer server akan dikonfigurasi melalui remote web base sehingga pada tampilan web browser akan muncul seperti pada Gambar 11 sebagai tampilan user mode kemudian dapat melakukan login sehingga menjadi user privilege seperti pada Gambar 12. Komputer server dapat menambahkan gateway dan firewall mode baru dengan login sebagai privilege user pada web base. OpenVPN dapat dijalankan dengan mengetahui status ketika diaktifkan seperti pada Gambar 13. OpenVPN dapat dijalankan dengan mengetahui status ketika diaktifkan seperti pada Gambar 14. Pada Gambar 14 OpenVPN dijalankan secara manual dengan cara men-start di perintah console /etc/init.d/openvpn start. Jika status yang ditampilkan OK maka OpenVPN dapat berjalan sebagai server VPN dengan baik. Ketika server VPN telah aktif kemudian dijalankan perintah ifconfig pada konsole maka akan muncul interface virtual baru seperti berikut :

```
tun0 Link encap:
UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr:10.10.10.1 P-t-P:10.10.10.2 Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

Gambar 11. Tampilan Awal Login



Gambar 12. Tampilan Ketika Sudah Login Sebagai User Privilege

Gambar 13. Menjalankan Openvpn

Tabel 5. Tabel Pengujian Sisi Server

No.	Nama Pengujian	Indikator Pengujian	Manfaat Pengujian	Status Pengujian
1	Komputer *Server* Booting dengan normal	Muncul halaman *login* pada layar monitor	Mengetahui server berjalan dengan baik	Muncul halaman *login*
2	Komputer *Server* dapat dikonfigurasi melalui *remote web base*	Muncul tampilan pada *web browser* halaman *Stratguard Mode*	Mempermudah konfigurasi strataguard	Muncul halaman *stratguard user mode*

No.	Nama Pengujian	Indikator Pengujian	Manfaat Pengujian	Status Pengujian
3	Komputer *Server* dapat menambahkan serta *teregister extension* dari vlan dan backbone *client* ketika dikonfigurasi melalui *remote web base*	Pada *konsole* ketik *strataguard –r,* kemudian ketik *sip show peers*	Mempermudah manajemen user IDS/IPS Stratguard	Muncul status dari Stratguard
4	Komputer *Server* dapat menjalankan *OpenVPN Server*	Pada *konsole* mengetikkan perintah */etc/init.d/openvpn start* , kemudian *ifconfig*	Paket data yang berlebihan akan di amankan	Muncul *interface* dan *IP address virtual* untuk koneksi VPN,Vlan dan kbone

4. Simpulan

Berikut ini terdapat beberapa kesimpulan dari capaian penelitian ini. Beberapa kesimpulan tersebut adalah jaringan komputer Universitas Amikom dikembangkan dengan sistem jaringan yang bersifat tradisional yakni memanfaatkan PC router sebagai pembagi broadcast domain ke setiap unit kerja atau group pengguna jaringan di setiap gedung. Hal ini menyebabkan setiap penambahan unit kerja atau group tertentu maka akan membutuhkan sebuah PC router atau minimal sebuah kartu jaringan agar mampu membentuk jaringan (subnetwork) yang baru sehingga manajemen jaringan dan maintenance lebih kompleks dan cenderung kesulitan untuk menerapkan standart policy pada setiap jaringan.

Pada beberapa subnet (jaringan) atau kelompok user (group), terdapat jaringan yang hanya dimanage menggunakan ip aliases melalui interface pc router, hal ini membuat performance jaringan tidak bekerja dengan optimal. Penggunaan lebih dari satu subnet pada jaringan yang memiliki broadcast domain yang sama mengakibatkan broadcast yang lebih besar, disamping terdapat permasalahan keamanan karena administrator tidak dapat mengontrol komunikasi kedua jaringan yang masih berada pada broadcast domain yang sama. Pembagian subnet jaringan yang hanya memanfaatkan IP aliases justru akan mengurangi kinerja atau performa jaringan komputer itu sendiri.

Distribusi Internet Protokol Public (IP Public) ke setiap PC Router yang dimaksudkan untuk membagi koneksi internet ke setiap unit/lab menjadikan sistem keamanan jaringan intranet Universitas Amikom menjadi rentan dan vulnerable. Hal ini karena IP Public yang digunakan oleh setiap PC router otomatis terpublikasi di Internet yang harusnya menjadi jaringan yang tidak dapat dipercaya (untrust network). Dengan kondisi sekarang, maka setiap pengguna internet dimungkinkan untuk melakukan penyerangan ke jaringan Intranet Universitas Amikom, padahal jaringan intranet menjadi jaringan yang aman dari jaringan di luar Jaringan Kampus Universitas Amikom (termasuk Internet). Solusi bagi jaringan Universitas AMIKOM adalah dengan membangun IDS / IPS StrataGuard, sehingga bisa dilakukan pencegahan pada saat intruder melakukan penetrasi. Cara merancang IDS / IPS di Universitas AMIKOM adalah dengan meletakkan IDS / IPS StrataGuard pada HostBase. IDS / IPS StratGuard mampu berjalan disemua platform sistem operasi. IDS/IPS StrataGuard mampu menggantikan peranan firewall dan proxy.

Pada penelitian ini ada beberapa saran untuk peningkatan penelitian selanjutnya. Saran-saran tersebut adalah sebagai berikut. Pentingnya di lakukan audit IP dan distribusi bandwith pada jaringan Universitas AMIKOM Yogyakarta. Pentingnya pembatasan akses keluar dan masuk pada jaringan wifi Universitas AMIKOM Yogyakarta. Pemberian quota pada user yang masih aktif saja, dalam artian masih berstatuskan mahasiswa aktif. Lebih di tegaskan kembali untuk job description administrator jaringan pada Universitas AMIKOM Yogyakarta.

5. Referensi

Andalep, S.S. dan Basu, K.A. (1994), Technical Complexity and Consumer Knowledge as Moderators of Service Quality Evaluation in Automobile Service Industry, Journal of Retailing, Vol.70, No.4:367-381.

Anonymous, Maximum Linux Security: A Hacker's Guide to Protecting Your Linux Server and Workstation, Sams Publishing, 2000.

Sommestad, T, dan Hunstad, A, 2013, Intrusion Detection and Tthe Role of The System Administrator, Journal of Information Management & Computer Security. 2013, Vol. 21 Issue 1, p30-40. 11p.

Al-Jarrah,O, dan Arafat, A, 2015, Network Intrusion Detection System Using Neural Network Classification of Attack Behavior, Journal of Advances in Information Technology. Feb2015, Vol. 6 Issue 1, p1-8. 8p.

Sobh, T, S, 2013, Anomaly detection based on hybrid artificial immune principles, Journal of Information Management & Computer Security. 2013, Vol. 21 Issue 4, p288-314. 27p.