Perancangan dan Implementasi Intrusion Detection System pada Jaringan Nirkabel BINUS University

Abraham Nethanel Setiawan Junior, Agus Harianto, Alexander

***Abstract*— Intrusion Detection System (IDS) membantu pengguna dalam memonitor dan menganalisa gangguan pada keamanan jaringan. Tujuan penelitian ini adalah merancang IDS menggunakan Snort dengan tampilan antarmuka berbasiskan *web* dan implementasi sistem untuk memantau aktifitas para pengguna HotSpot BINUS University. Penelitian ini berisi analisa gangguan pada jaringan nirkabel BINUS, usulan solusi keamanan pada jaringan, proses dan cara kerja sistem IDS yang dibuat dengan basis *web*, serta evaluasi penerapan sistem IDS pada jaringan.**

***Index*—intrusion detection system, nirkabel BINUS, *web*, solusi keamanan jaringan.**

I. PENDAHULUAN

Penerapan jaringan nirkabel selain memberikan kemudahan dalam berkomunikasi atau transaksi data, ternyata terdapat pula beberapa kelemahan pada segi kemanannya. Jaringan nirkabel tidak memiliki jalur pertahanan yang jelas, sehingga setiap komputer pengguna harus siap terhadap gangguan ataupun serangan yang mungkin terjadi.

Keamanan jaringan bergantung pada kecepatan pengatur jaringan dalam menindaklanjuti sistem saat terjadi gangguan. Penerapan IDS diusulkan sebagai salah satu solusi yang dapat digunakan untuk membantu pengatur jaringan dalam memantau kondisi jaringan dan menganalisa paket-paket berbahaya yang terdapat dalam jaringan tersebut.

IDS diterapkan karena sistem ini mampu mendeteksi paket-paket berbahaya pada jaringan dan langsung memberikan peringatan kepada pengatur jaringan tentang kondisi jaringannya saat itu.

Pada dasarnya IDS terbagi menjadi dua jenis yaitu *rule based* dan *adaptive system*. Sistem *rule based* mendeteksi suatu serangan berdasarkan aturan-aturan yang sudah didefinisikan pada kumpulan data aturan, sedangkan sistem *adaptive* dapat mengenali jenis serangan baru dengan cara membandingkan kondisi saat ini dengan kondisi normal suatu sistem.

Sudah terdapat banyak software IDS seperti Snort yang merupakan open source IDS yang juga digunakan dalam penelitian ini. Namun belum terdapat sistem antar muka yang membantu para pengguna dalam mengatur sistem sehingga penerapan IDS ini masih sulit dilakukan. Oleh karena itu diusulkan untuk membuat sebuah sistem IDS lengkap dengan tampilan antarmuka berbasiskan web dengan beberapa fitur tambahan yang diharapkan dapat membantu administrator dalam memonitor kondisi jaringannya serta meningkatkan mutu keamanan jaringan tersebut..

Naskah diterima pada tanggal 15 Maret 2009. Jurnal ini merupakan bagian dari penelitian skripsi jurusan Teknik Informatika, BINUS University Jakarta.

Abraham N. S. Jr., Agus H., Alexander merupakan mahasiswa program Sarjana 1 jurusan Teknik Informatika – Jaringan Komputer, BINUS University Jakarta.

Abraham N. S. Jr., Agus H., Alexander mengucapkan terimakasih kepada Bpk. Johan Muliadi Kerta atas bimbingannya selama penelitian skripsi ini.

Abraham N. S. Jr., Agus H., Alexander mengucapkan terimakasih kepada para staf dari BINUS University IT Directorate dalam menyediakan setiap keperluan terkait penelitian skripsi ini.

II. Referensi Literatur

A. *Jaringan Komputer*

Jaringan komputer adalah dua atau lebih komputer yang saling terhubung melalui kabel atau dengan koneksi nirkabel sehingga mereka dapat saling bertukar informasi [1].

Komputer – komputer tersebut saling terhubung dengan Network Interface Card (NIC) di tiap komputer dengan menggunakan media kabel ataupun nirkabel tergantung dari jenis NIC yang digunakan.

Menurut jangkauannya, jaringan komputer dibagi menjadi 3 yaitu :

1. Local Area Network (LAN)
   LAN merupakan jaringan komputer yang saling terhubung ke suatu komputer server dengan menggunakan topologi tertentu, biasanya digunakan dalam kawasan satu gedung atau kawasan yang jaraknya tidak lebih dari 1 Km [2].

2. Metropolitan Area Network (MAN)
   MAN merupakan jaringan komputer yang saling terkoneksi dalam satu kawasan kota yang jaraknya bisa lebih dari 1 Km [2].

3. Wide Area Network (WAN)
   WAN merupakan jaringan komputer yang menghubungkan banyak LAN ke dalam suatu jaringan terpadu. Antara satu jaringan dengan jaringan lain dapat berjarak ribuan kilometer atau terpisahkan oleh letak geografi dengan menggunakan metode komunikasi tertentu [2].

B. *Arsitektur Jaringan*

Standar yang paling populer untuk menggambarkan arsitektur jaringan adalah model referensi Open System Interconnect (OSI) yang dikembangkan oleh International Organization for Standarization (ISO) pada tahun 1977 dan diperkenalkan pada tahun 1984. Pada model referensi OSI terdapat 7 buah lapisan yang setiap lapis-nya mengilustrasikan fungsi – fungsi jaringan. Pembagian fungsi – fungsi jaringan ini antara lain:

1. Lapisan ke-7 – Application
   Lapisan yang paling dekat dengan pengguna dan memiliki fungsi untuk menyediakan sebuah layanan jaringan kepada pengguna aplikasi, berisi protokol – protokol yang umum digunakan oleh pengguna. Lapisan ini berbeda dengan lapisan lainnya yang dapat menyediakan layanan kepada lapisan lain.

   Contoh : Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP) dan File Transfer Protocol (FTP) [3].

2. Lapisan ke-6 – Presentation
   Lapisan ini menentukan format data yang dipindahkan di antara aplikasi dan mengelola informasi yang disediakan oleh lapisan Application supaya informasi yang dikirimkan dapat dibaca oleh lapisan Application pada sistem lain. Lapisan ini menyediakan layanan berupa transformasi format data, enkripsi dan kompresi [3].

3. Lapisan ke-5 – Session
   Lapisan ini berfungsi untuk menyelenggarakan, mengatur dan memutuskan sesi komunikasi. Lapisan Session menyediakan layanan kepada lapisan Presentation dan juga mensinkronisasi dialog di antara dua computer lapisan Presentation dan mengatur pertukaran data [3].

4. Lapisan ke-4 – Transport
   Lapisan ini berfungsi sebagai pemecah informasi menjadi paket – paket data yang akan dikirim dan menyusun kembali paket – paket data menjadi sebuah informasi yang dapat diterima. Dua protokol umum pada lapisan ini adalah Transfer Control Protocol (TCP) yang berorientasi koneksi dan User Datagram Protocol (UDP) yang tidak berorientasi koneksi [3].

5. Lapisan ke-3 – Network
   Lapisan ini menyediakan transfer informasi di antara ujung sistem melewati beberapa jaringan komunikasi berurutan. Lapisan ini melakukan pemilihan jalur terbaik dalam komunikasi jaringan yang terpisah secara geografis [3].

6. Lapisan ke-2 – Data Link
   Lapisan ini berfungsi mengubah paket – paket data menjadi bentuk *frame*, menghasilkan alamat fisik, pesan – pesan kesalahan, pemesanan pengiriman data. Lapisan Data Link mengupayakan agar lapisan Physical dapat bekerja dengan baik dengan menyediakan layanan untuk mengaktifkan, mempertahankan dan menonaktifkan hubungan [3].

7. Lapisan ke-1 – Physical
   Lapisan ini bertugas menangani transmisi data dalam bentuk *bit* melalui jalur komunikasi. Lapisan ini menjamin transmisi data berjalan dengan baik dengan cara mengatur karakteristik tinggi tegangan, periode perubahan tegangan, lebar jalur komunikasi, jarak maksimum komunikasi dan koneksi [3].

C. Jaringan LAN Nirkabel (WLAN)

WLAN menggunakan dua macam teknik modulasi, yaitu Orthogonal Frequency Division Multiplexing (OFDM) dan Direct Sequence Spread Spectrum (DSSS). OFDM akan menyebabkan kecepatan pengiriman data lebih tinggi dibandingkan dengan DSSS, tetapi DSSS lebih sederhana daripada OFDM sehingga akan lebih murah dalam implementasinya. Standar yang lazim digunakan untuk WLAN adalah 802.11 yang ditetapkan oleh IEEE pada akhir tahun 1990. Standar 802.11 kemudian terbagi lagi menjadi beberapa jenis, yakni :

• 802.11a

Menggunakan teknik modulasi OFDM dan berjalan pada frekuensi 5 GHz dengan kecepatan pengiriman data mencapai 54 Mbps. Kecepatan pengiriman data lebih tinggi sehingga potensi terjadinya gangguan dari perangkat nirkabel lainnya lebih kecil karena frekuensi ini jarang digunakan. Ada beberapa kelemahan antara lain membutuhkan biaya yang lebih besar, jarak jangkauan lebih pendek karena frekuensi tinggi dan juga dapat menyebabkan sinyal mudah diserap oleh benda penghalang seperti tembok.

• 802.11b

Menggunakan teknik modulasi DSSS dan berjalan pada frekuensi 2,4 GHz dengan kecepatan pengiriman data mencapai 11 Mbps. Kelebihan dari standar ini adalah biaya implementasi lebih kecil dan jarak jangkau lebih luas. Kelemahannya adalah kecepatan pengiriman data lebih lambat dan rentan terhadap gangguan karena frekuensi 2,4 GHz banyak digunakan oleh perangkat lainnya.

• 802.11g

Menggunakan teknik modulasi OFDM dan DSSS sehingga memiliki karakteristik dari kedua standar di atas. Standar ini bekerja pada frekuensi 2,4 GHz dengan kecepatan pengiriman data mencapai 54 Mbps tergantung dari jenis modulasi yang digunakan. Kecepatan pengiriman data tinggi (menyamai standar 802.11a), jarak jangkauan cukup luas dan lebih tahan terhadap penyerapan oleh material tertentu karena bekerja pada frekuensi 2,4 GHz, namun rentan terhadap gangguan dari perangkat nirkabel lainnya.

D. Keamanan Jaringan

Masalah keamanan menjadi salah satu perhatian pada jaringan nirkabel karena resiko keamanan semakin bertambah seiring semakin populernya jaringan nirkabel.

Berikut beberapa ancaman yang umum ditemui pada jaringan nirkabel:

• MAC Spoofing

Penyerang berusaha mendapatkan koneksi ke dalam jaringan dengan mengambil alamat NIC dari suatu perangkat komputer pada jaringan tersebut [4].

• ARP Spoofing

Penyerang menangkap penyebaran paket ARP dari *access point* dan kemudian mengirimkan balasan ARP fiktif sehingga informasi perangkat dari penyerang akan terpetakan ke dalam tabel ARP

untuk kemudian mendapatkan hak akses kedalam jaringan [4].

• Man in the Middle Attack

Metode serangan ini biasanya didahului dengan ARP spoofing kemudian penyerang menempatkan perangkat yang dimilikinya sebagai sebuah komputer fiktif yang akan terlihat resmi dari sisi *access point* [5].

• Denial of Service

Metode serangan dengan mengirimkan paket data dalam jumlah yang sangat besar terhadap jaringan yang menjadi targetnya secara terus-menerus. Hal ini dapat mengganggu lalu-lintas data bahkan kerusakan sistem jaringan [5].

Pada jaringan nirkabel semua data dilewatkan dalam suatu medium gelombang radio (udara), bukan dalam medium yang lebih aman seperti kabel pada jaringan kabel. Hal ini berarti aliran data pada jaringan nirkabel dapat dengan mudah disadap oleh orang – orang yang tidak berhak. Untuk itulah dibuat media keamanan berupa enkripsi data pada jaringan nirkabel, antara lain :

• Wired Equivalent Privacy (WEP)

Teknik enkripsi WEP menggunakan kunci yang disebar antara *access point* dengan kliennya dalam satu jaringan supaya masing – masing dapat melakukan proses enkripsi dan dekripsi, karena kedua proses tersebut hanya mungkin dilakukan jika memiliki kunci yang sama. Kunci yang digunakan pada WEP standar adalah 64 *bit*, 40 *bit* untuk kunci dan 24 *bit* sisanya untuk initialization vector (IV) yang dikirimkan berupa teks untuk proses otentikasi.

Enkripsi ini diketahui terdapat kelemahan yaitu IV yang pendek, sehingga memungkinkan terjadinya pengulangan IV yang digunakan untuk setiap jumlah *frame* yang dikirimkan, tergantung pada luas jaringan dan jumlah pengguna yang terhubung dan membuat penyerang bisa dengan mudah menerka IV dan menembus enkripsi WEP. Namun WEP masih tetap menjadi pilihan untuk keamanan minimal yang biasa digunakan pada jaringan nirkabel rumahan [5].

• Wi – Fi Protected Access (WPA)

WPA dibuat sebagai tindak lanjut atas kelemahan WEP dengan menggunakan algoritma enkripsi baru menggunakan kunci yang dinamis dan berubah secara periodik. Teknik enkripsi yang digunakan WPA bisa dibagi menjadi dua jenis, yaitu Temporal Key Integrity Protocol (TKIP) yang menggunakan algoritma RC4 yang dibuat sebagai pengganti WEP dengan menggunakan kunci sepanjang 128 *bit* dan berubah untuk setiap *frame* yang akan dikirimkan serta Advanced Encryption Standard (AES) yang menggunakan algoritma Rine Dale yang sangat kuat namun membutuhkan sumber daya yang lebih besar dan digunakan pada WPA2.

WPA digolongkan menjadi dua jenis, yaitu WPA Personal menggunakan Pre-Shared Key (PSK) dan WPA Enterprise. Penggunaan PSK ditujukan pada jaringan yang berada di lingkungan rumah atau kantor kecil dimana tidak ada penggunaan server otentikasi yang kompleks. WPA enterprise kebanyakan digunakan pada jaringan perusahaan yang menggunakan server otentikasi sendiri seperti Remote Authentication Dial-In User Service (RADIUS). Extensible Aunthentication Protocol (EAP) digunakan pada jenis WPA ini yang hanya mengizinkan pemakaian sebuah jalur untuk mengirimkan paket – paket EAP dari klien ke server otentikasi. EAP akan menutup semua jalur lalu lintas data lainnya yg menuju server sampai terbukti bahwa pengguna adalah pemakai yang sah [5].

E. Mikrotik HotSpot

Penggunaan mikrotik HotSpot memungkinkan untuk mengatur ketetapan pengaksesan terhadap jaringan publik untuk pengguna yang menggunakan jaringan kabel maupun nirkabel, dengan fitur – fitur sebagai berikut:

1. Menggunakan server DHCP untuk memberikan alamat IP sementara kepada klien untuk proses otentikasi.
2. Otentikasi klien menggunakan penyimpanan data lokal atau server RADIUS.
3. Pemberian IP tetap setelah proses otentikasi berhasil.

Jalur keluaran dari mikrotik HotSpot harus memiliki minimal dua buah antar muka jaringan, yaitu antar muka HotSpot yang digunakan untuk terhubung ke klien dan antar muka LAN/ WAN yang digunakan untuk mengakses sumber daya jaringan seperti server RADIUS. Untuk antar muka HotSpot harus memiliki dua alamat IP, satu sebagai jalur keluaran untuk alamat sementara sebelum otentikasi dan satu lagi sebagai jalur keluaran untuk alamat IP tetap setelah proses otentikasi [6].

Untuk proses otentikasi pertama kali komputer klien akan menerima alamat IP sementara dari server DHCP, yaitu mikrotik HotSpot. Pada saat pengguna melakukan penelusuran *web*, maka akan secara otomatis dialihkan ke halaman pengesahan yang akan meminta nama pengguna dan kata sandi. Mikrotik HotSpot bisa melakukan otentikasi dengan mengacu kepada penyimpanan data lokal maupun server RADIUS [6].

Setelah proses otentikasi berhasil maka mikrotik HotSpot akan memberikan alamat IP lain yang tetap. Untuk permintaan DHCP berikutnya, alamat IP yang baru akan diberikan kepada klien. Waktu yang dibutuhkan untuk mengubah alamat IP klien tergantung dari waktu yang ditentukan di pengaturan HotSpot, biasanya sekitar 14 detik. Setelah proses perubahan alamat IP selesai, halaman *web* akan langsung dialihkan ke alamat tujuan yang sebenarnya atau halaman status jika pengguna belum memasukkan alamat tujuan [6].

F. Intrusion Detection System (IDS)

IDS adalah sebuah aplikasi perangkat lunak atau perangkat keras yang bekerja secara otomatis untuk memonitor kejadian pada jaringan komputer dan menganalisis masalah keamanan jaringan [4]. Terdapat 2 jenis IDS, yaitu:

1. Network-based IDS (NIDS)
   NIDS akan melakukan pemantauan terhadap seluruh bagian pada jaringan dengan mengumpulkan paket-paket data yang terdapat pada jaringan tersebut serta melakukan analisa dan menentukan apakah paket-paket tersebut merupakan paket normal atau paket serangan [4].
2. Host-based IDS (HIDS)
   HIDS hanya melakukan pemantauan pada perangkat komputer tertentu dalam jaringan. HIDS biasanya akan memantau kejadian seperti kesalahan *login* berkali – kali dan melakukan pengecekan pada file [4].

Hal yang perlu diperhatikan pada implementasi IDS adalah perihal *false positive* dan *false negative*. *False positive* adalah peringatan serangan yang dihasilkan oleh IDS akan sebuah paket normal pada sistem yang dimonitor. *False negative* adalah sebuah serangan yang benar – benar terjadi namun terlewatkan oleh IDS sehingga IDS tidak akan menghasilkan peringatan apapun atas serangan tersebut. IDS dapat melewatkan serangan karena serangan tersebut tidak dikenali oleh IDS atau karena penyerang berhasil menggunakan sebuah metode serangan yang dapat menghindari IDS [7].

Beberapa pendekatan yang sering digunakan untuk mengenali serangan, antara lain:

1. Rule Based Detection

Analisis dilakukan terhadap aktivitas sistem, mencari kejadian yang cocok dengan pola perilaku yang dikenali sebagai serangan [8].
Ada empat tahap proses analisis pada system deteksi ini:

• *Preprocessing*

Mengumpulkan data tentang pola dari serangan dan meletakkannya pada skema klasifikasi. Kemudian suatu model akan dibangun dan dimasukkan ke dalam bentuk format yang umum seperti nama pola serangan, nomor identitas pola serangan dan penjelasan pola serangan [8].

• *Analysis*

Data dan formatnya akan dibandingkan dengan pola serangan yang sudah dikenali [8].

• *Response*

Jika ada yang cocok dengan pola serangan, mesin analisis akan mengirimkan peringatan ke server [8].

• *Refinement*

Perbaikan dari analisis pencocokan pola yang diturunkan untuk memperbarui pola serangan. Banyak IDS mengizinkan pembaharuan pola serangan secara manual sehingga tidak mudah untuk diserang dengan menggunakan pola serangan terbaru [8].

2. Adaptive Detection System

Sistem deteksi Adaptive mengidentifikasi perilaku tidak normal yang terjadi pada suatu komputer atau jaringan. Adaptive detektor menyusun profil – profil yang merepresentasikan kebiasaan pengguna normal suatu computer atau koneksi jaringan dari data historis selama periode operasi normal. Sistem ini bukan hanya mendefinisikan aktivitas yang tidak diperbolehkan namun juga aktivitas apa saja yang diperbolehkan. Kelebihan dari metode ini terletak pada kemampuannya dalam mengumpulkan data mengenai perilaku sistem baik secara statistik (kuantitatif) maupun secara karakteristik (kualitatif) [8]. Sistem deteksi Adaptive dapat dibagi menjadi tiga kategori utama, yakni :

• *Behavioral analysis*, mencari anomali dari perilaku sistem.

• *Traffic - pattern analysis*, mencari pola – pola tertentu dari lalu lintas jaringan.

• *Protocol analysis*, mencari pelanggaran atau penyalahgunaan protokol jaringan. Analisis ini memiliki kelebihan untuk mengidentifikasi serangan yang belum dikenali.

G. Snort

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisa paket yang melintasi jaringan secara langsung dan melakukan pencatatan ke dalam penyimpanan data serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan [4]. Snort merupakan sebuah produk terbuka yang dikembangkan oleh Marty Roesch dan tersedia gratis di www.snort.org. Snort bisa digunakan pada sistem operasi Linux, Windows, BSD, Solaris dan sistem operasi lainnya. Snort merupakan IDS berbasis jaringan yang menggunakan metode deteksi rule based, menganalisis paket data apakah sesuai dengan jenis serangan yang sudah diketahui olehnya. Snort digunakan karena memiliki beberapa kelebihan berikut : [7]

• Mudah dalam konfigurasi dan penambahan aturan-aturan

• Gratis

• Dapat berjalan pada sistem operasi yang berbeda – beda

• Pembaharuan pola serangan secara berkala

Snort memanfaatkan perangkat tcpdump untuk mengambil dan menganalisa paket data terhadap sekumpulan jenis serangan yang sudah terdefinisi. Snort dapat berjalan dalam tiga mode antara lain: [4]

• Paket Sniffer, melihat paket yang lewat di jaringan.

• Paket Logger, mencatat semua paket yang lewat di jaringan untuk dianalisis.

• NIDS, mendeteksi serangan yang dilakukan melalui jaringan komputer dengan konfigurasi dari berbagai

aturan yang akan membedakan sebuah paket normal dengan paket serangan.

Snort terdiri dari komponen – komponen yang mempunyai tugas dan fungsinya sendiri – sendiri yaitu:

• Packet capture library

Packet capture library adalah sebuah perangkat lunak yang terpisah yang mengambil paket data dari NIC. Paket – paket data itu adalah paket data Lapisan Data Link (OSI model) yang biasanya disebut *frame* yang masih belum diproses. Pada sistem Linux dan UNIX, Snort menggunakan libpcap, sedangkan pada sistem Windows, Snort menggunakan winpcap [7].

• Packet decoder

Packet decoder mengambil frame lapisan 2 (Data Link) yang dikirimkan oleh packet capture library dan kemudian memecahnya. Pertama – tama komponen ini membaca kode sandi terhadap *frame* lapisan 2, kemudian paket lapisan 3 (protokol IP), lalu kemudian paket lapisan 4 (paket TCP atau UDP). Setelah proses selesai dilakukan, Snort mempunyai semua informasi masing – masing protokol untuk pemrosesan lebih lanjut [7].

• Preprocessor

Preprocessor pada Snort memiliki beberapa fitur tambahan yang dapat dimatikan atau dinyalakan. Preprocessor bekerja pada paket yang sudah dibaca kode sandinya dan kemudian melakukan transformasi pada data itu supaya lebih mudah untuk diproses oleh Snort [7].

• Detection engine

Komponen ini mengambil informasi dari packet decoder dan preprocessor yang kemudian memproses data itu pada lapisan Transport dan Application, membandingkan data yang terkandung dalam paket dengan aturan-aturan yang juga merupakan fitur tambahan dari komponen ini [7].

• Output

Ketika preprocessor terpancing karena adanya data yang cocok dengan definisi jenis serangan, Snort kemudian menghasilkan peringatan dan kemudian melakukan pencatatan. Snort mendukung beberapa macam keluaran, seperti keluaran dalam format teks atau biner. Pencatatan juga bisa dilakukan ke dalam penyimpanan data ataupun syslog [7].

III. ANALISIS

A. Analisa Kuesioner

Kuesioner dibagikan untuk mendapatkan data – data mengenai permasalahan seputar HotSpot BINUS yang akan digunakan sebagai dasar pengembangan. Kuesioner ini terdiri dari 7 pertanyaan yang diedarkan secara langsung dengan jumlah responden sebanyak 35 orang Binusian (pegawai atau pun mahasiswa Bina Nusantara). Jawaban dari responden telah dihitung dengan persentase sebagai berikut:

1. Berapa lama setiap kali Anda *online* menggunakan HotSpot BINUS University?

TABEL I
PERSENTASE JAWABAN KUESIONER NO. 1

Pilihan	Responden	Persentase
Kurang dari 1 jam	11	31.43 %
1 – 2 jam	17	48.57 %
Lebih dari 2 jam	7	20 %
Total	35	100 %

2. Apakah yang Anda lakukan ketika sedang *online*?

TABEL 2
PERSENTASE JAWABAN KUESIONER NO. 2

Pilihan	Jawaban	Persentase
Browsing	32	46.38 %
Chatting	18	26.08 %
Video streaming	2	2.9 %
Download	13	18.84 %
Game online	2	2.9 %
Lain-lain	2	2.9 %
Total	69	100 %

3. Situs – situs seperti apa sajakah yang Anda kunjungi saat *browsing internet*?

TABEL 3
PERSENTASE JAWABAN KUESIONER NO. 3

Pilihan	Jawaban	Persentase
Situs Komunitas (seperti : Facebook, Friendster, hi5, dll.)	26	38.24 %
Email	22	32.35 %
Situs Forum (seperti : Kaskus, dll)	13	19.12 %
Situs-situs lainnya	7	10.29 %
Total	68	100 %

4. Apakah Anda kesulitan untuk terkoneksi dengan jaringan HotSpot BINUS University? (Jika ya lanjut ke pertanyaan berikut)

TABEL 4
PERSENTASE JAWABAN KUESIONER NO. 4

Pilihan	Jawaban	Persentase
Ya	26	74.29 %
Tidak	9	25.71 %
Total	35	100 %

5. Apa saja kesulitan yang anda alami pada saat terkoneksi
dengan jaringan HotSpot BINUS University?

TABEL 5
PERSENTASE JAWABAN KUESIONER NO. 5

Pilihan	Jawaban	Persentase
Kesulitan untuk *login*	7	23.33 %
Kecepatan koneksi internet tidak stabil	21	70 %
Lain-lain	2	6.67 %
Total	30	100 %

6. Apakah Anda pernah mendapatkan paket berbahaya seperti
virus, spyware / trojan ketika menggunakan HotSpot BINUS University?

TABEL 6
PERSENTASE JAWABAN KUESIONER NO. 6

Pilihan	Responden	Persentase
Ya	6	17.14 %
Tidak	22	62.86 %
Tidak Tahu	7	20 %
Total	35	100 %

7. Apakah komputer / laptop Anda memiliki perangkat keamanan untuk mengatasi paket berbahaya yang masuk?

TABEL 7
PERSENTASE JAWABAN KUESIONER NO. 7

Pilihan	Responden	Persentase
Ya	28	80 %
Tidak	7	20 %
Total	35	100 %

8. Apakah komputer Anda sudah cukup terproteksi dengan adanya perangkat kemanan tersebut?

TABEL 8
PERSENTASE JAWABAN KUESIONER NO. 8

Pilihan	Responden	Persentase
Ya	14	40 %
Tidak	6	17.14 %
Tidak Tahu	15	42.86 %
Total	35	100 %

B. Analisa Permasalahan

Berdasarkan hasil kuesioner dan pengamatan yang dilakukan, dapat disimpulkan beberapa kelemahan pada sistem jaringan HotSpot BINUS, antara lain:

a) HotSpot belum dapat dikatakan aman untuk para pengguna.
b) Kecepatan koneksi internet tidak stabil pada saat terhubung ke jaringan HotSpot, yang dapat disebabkan oleh paket – paket serangan yang menyebar pada jaringan.
c) Aktivitas responden banyak mengundang ancaman terhadap jaringan.
d) Belum ada sebuah sistem keamanan yang dapat digunakan untuk memonitor lalu lintas jaringan.
e) Pengatur jaringan tidak bisa melakukan analisis terhadap jaringannya sendiri karena tidak ada sebuah sistem yang dapat menyediakan informasi untuk dianalisis.

C. Usulan Solusi

Dari permasalahan yang ditemukan, diusulkan suatu sistem keamanan IDS (menggunakan Snort) sebagai sistem peringatan jika terdapat aktivitas – aktivitas ilegal yang terjadi dalam jaringan HotSpot BINUS. Karena Snort tidak memiliki tampilan antar muka yang memadai, maka diusulkan untuk membuat suatu sistem IDS dengan antar muka berbasiskan *web*. Beberapa fitur yang ditawarkan sebagai solusi dari permasalahan di atas antara lain:

a. Fasilitas pemantauan lalu lintas jaringan dengan menampilkan jumlah paket yang masuk untuk empat jenis protokol yang umum yaitu TCP, UDP, ICMP dan ARP.

b. Menampilkan jumlah paket yang masuk untuk tiap jalur khusus untuk paket TCP dan UDP.

c. Menampilkan paket – paket yang dianggap berbahaya sesuai dengan aturan-aturan yang sudah terdefinisikan, lengkap dengan rincian mengenai paket tersebut.

d. Fasilitas untuk mengirimkan peringatan melalui *email* kepada pengatur jaringan saat terdeteksi paket serangan.

e. Fasilitas untuk menambahkan, mengaktifkan, menonaktifkan, atau menghapus aturan baru.

f. Fasilitas laporan, *export*, dan *archive* informasi mengenai keadaan jaringan dalam kurun waktu tertentu.

IV. PERANCANGAN

A. Perancangan Aplikasi

Berdasarkan hasil analisa, maka dibuat sebuah aplikasi yang dinamakan Management and Analysis for Intrusion Detection (MAID). Aplikasi sistem IDS berbasis *web* ini dikembangkan dengan menggunakan PHP dan Snort dan terdapat beberapa komponen yang dirancang, antara lain:

a. Pemantauan Jaringan

Fitur ini menampilkan informasi jumlah paket yang melalui jaringan dalam empat jenis protokol yaitu TCP, UDP, ICMP dan ARP. Data akan ditampilkan dalam bentuk diagram pie dengan atribut persentase jumlah paket dari tiap protokol. Dapat pula diketahui total

paket tiap port dan dibuat pula dalam bentuk grafik garis sebagai hostoris jaringan tiap bulan.

b. Intrusion Detection

Fitur ini mendeteksi aktivitas – aktivitas ilegal yang terjadi dalam jaringan. Fitur ini menampilkan informasi mengenai kejadian – kejadian yang sesuai dengan aturan-aturan yang sudah didefinisikan. Informasi yang ditampilkan antara lain perangkat yang menerima paket, jenis kejadian, waktu kejadian, alamat IP asal dan tujuan, serta jalur asal dan tujuan. Sistem ini kemudian mengirimkan *email* peringatan kepada pengatur jaringan setiap mendeteksi suatu kejadian.

c. Perubahan Status Aturan

Terdapat dua hak akses pada sistem ini yaitu administrator dan super administrator. Administrator dan super administrator dapat menambahkan aturan-aturan baru sesuai dengan kepentingan jaringannya, namun hanya super administrator yang dapat melakukan perubahan status pada aturan tersebut yaitu mengaktifkan, menonaktifkan, serta menghapus aturan.

d. Laporan dan Archive/Export

Fitur laporan menampilkan informasi detail semua kejadian yang terjadi. Fitur export dan archive menyimpan dokumentasi laporan ke dalam bentuk berkas Microsoft Excel (.xls). Fitur export dapat digunakan oleh administrator maupun super administrator untuk menyimpan berkas pada komputer klien dan tidak menghapus data dari sistem penyimpanan, sedangkan fitur archive hanya dapat digunakan oleh super administrator untuk menyimpan data di komputer server dan akan dihapus dari sistem penyimpanan.

e. Pengaturan Aplikasi

Fitur ini hanya dapat diakses oleh super administrator karena fitur ini dapat melakukan perubahan alamat *email*, perubahan perangkat yang digunakan untuk mendeteksi paket, pengaturan terhadap aplikasi – aplikasi yang berjalan, dan pengaturan terhadap seluruh pengatur jaringan dengan hak akses administrator.

B. Spesifikasi Perangkat Keras dan Perangkat Lunakl

- Spesifikasi Perangkat Keras

Agar sistem IDS dapat berjalan dengan semestinya, komputer yang digunakan sebagai server IDS harus memiliki spesifikasi minimum sebagai berikut:

1. *Processor* 2 GHz

2. *Motherboard* dengan *slot* PCI

3. 512 MB RAM

4. *Harddisk* 40 GB

5. 2 buah NIC

- Spesifikasi Perangkat Lunak

Sistem IDS ini membutuhkan beberapa perangkat lunak pendukung untuk dapat berjalan, antara lain:

1.Sistem operasi Windows XP / Vista / Linux

2.XAMPP versi 1.6.7 atau lebih tinggi

3.Java Development Kit versi 6 atau lebih tinggi

(http://java.sun.com/javase/downloads/index_jdk5.jsp)

4.WinPcap versi 4.0 atau lebih tinggi

(http://www.winpcap.org/install/default.htm)

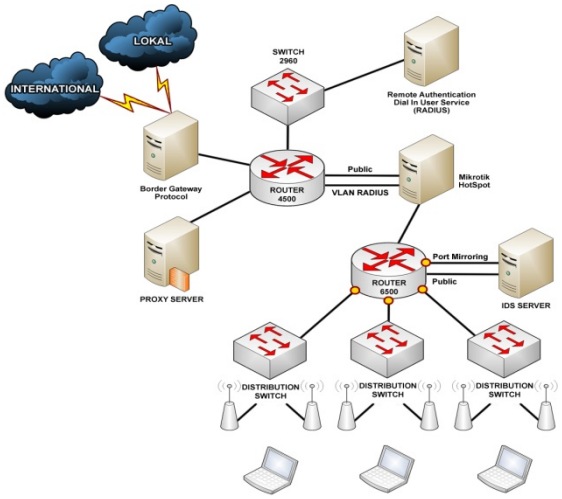
5.Jpcap versi 0.7

6.MySQL Connector/ J versi 5.1.6

7.Snort versi 2.8.2.1 (http://www.snort.org/dl/binaries/win32/)

V. IMPLEMENTASI

IDS akan ditempatkan pada jaringan nirkabel BINUS untuk megamati aktivitas para pengguna HotSpot, seperti pada Gambar 1 berikut ini.



Gambar 1. Topologi Jaringan Nirkabel BINUS University

Semua paket dari atau menuju klien akan melalui Mikrotik HotSpot, sehingga untuk dapat mengamati lalu-lintas paket tersebut sistem IDS ditempatkan pada *interface public mirroring* Mikrotik HotSpot pada Router 6500. Semua paket yang masuk maupun keluar jaringan melalui *interface public* Mikrotik HotSpot akan dicerminkan ke IDS untuk kemudian dianalisis.

VI. EVALUASI

Hasil pengamatan dari implementasi selama 6 hari, dapat dikatakan bahwa sistem MAID mampu memonitor secara terus-menerus lalu-lintas data pada jaringan nirkabel BINUS University dan dapat mendeteksi paket-paket serangan sesuai dengan aturan-aturan yang sedang aktif, kemudian memberikan peringatan kepada pengatur jaringan melalui *email.*

Secara teknis sistem MAID berjalan dengan persentase penggunaan *processor* antara 50% sampai dengan 70% dilihat dari grafik pemakaian CPU, seperti yang ditampilkan pada Gambar 2.

Gambar 2. CPU Usage History

Pemakaian RAM pada sistem ini masih menyisakan cukup banyak memori seperti yang ditunjukkan pada Gambar 3.

Gambar 3. Physical Memory / RAM Usage

Pengamatan dilakukan pula terhadap terhadap beberapa direktori yang berisikan berkas pencatatan total paket, jalur, kejadian dan system penyimpanan data MySQL untuk mengetahui rata-rata pemakaian ruang pada *harddisk* tiap harinya agar pengatur jaringan dapat mengetahui seberapa besar *harddisk* yang diperlukan untuk menampung data selama beberapa waktu kedepan. Berikut pencatatan total paket per-hari dan pertambahan ukuran pada direktori Snort/traffic (sebagai direktori pencatatan berkas total paket) seperti yang ditampilkan pada Tabel 9.

TABEL 9
TOTAL PAKET DAN UKURAN DIREKTORI TRAFFIC

Tanggal	Paket				Total Paket	Ukuran Folder Traffic *(bytes)*	Pertambahan *(bytes)*
	TCP	UDP	ICMP	ARP			
12/01/09	36,939,700	2,189,897	258,760	892,200	40,821,465	4,096	4,096
13/01/09	24,979,798	1,375,020	132,378	624,745	27,554,002	8,192	4,096
14/01/09	23,789,875	1,195,180	108,953	447,814	25,945,997	12,288	4,096
15/01/09	18,692,911	2,492,463	70,530	456,725	22,069,836	16,384	4,096
16/01/09	21,711,824	1,159,837	68,371	581,197	23,855,141	20,480	4,096
17/01/09	31,800,210	1,648,432	121,320	627,033	34,631,450	24,576	4,096

Dari data Tabel 9 dapat disimpulkan bahwa pertambahan ukuran pada direktori traffic ini cukup konstan yakni 4,096 *bytes* (4KB) tiap harinya.

Berikut pertambahan ukuran direktori port (sebagai direktori pencatatan berkas jalur setiap paket) seperti yang ditampilkan pada Tabel 10.

TABEL 10
UKURAN DIREKTORI PORT (TCP/UDP)

Tanggal	Ukuran Folder *(bytes)*		Ukuran Folder Port (TCP/UDP) *(bytes)*	Pertambahan *(bytes)*
	TCP	UDP		
12/01/09	77,657,753	32,148,710	109,806,463	109,806,463
13/01/09	130,172,391	52,334,645	182,507,036	72,700,573
14/01/09	180,185,473	69,880,445	250,065,918	67,558,882
15/01/09	219,483,287	106,470,965	325,954,252	75,888,334
16/01/09	265,127,716	123,497,913	388,625,629	62,671,377
17/01/09	331,980,800	147,697,664	479,678,464	91,052,835

Dari Tabel 10 dapat disimpulkan bahwa rata-rata pertambahan ukuran pada direktori port tiap harinya sekitar 79,946,411 *bytes* (80MB).

Berikut pertambahan ukuran direktori log (sebagai direktori pencatatan berkas kejadian) seperti yang ditampilkan pada Tabel 11.

TABEL 11

UKURAN DIREKTORI LOG

Tanggal	Total Event	Ukuran Folder Log *(bytes)*	Pertambahan *(bytes)*
12/01/09	486	649,773	649,773
13/01/09	1,563	2,739,474	2,089,701
14/01/09	898	3,940,083	1,200,609
15/01/09	1,380	5,785,116	1,845,033
16/01/09	1,632	7,967,069	2,181,953
17/01/09	542	8,691,712	724,643

Dari Tabel 11 dapat disimpulkan bahwa rata-rata pertambahan ukuran pada direktori log tiap harinya sekitar 1,448,619 *bytes* (1,5MB).

Berikut pertambahan ukuran direktori XAMPP (sebagai direktori sstem penyimpanan data kejadian) *seperti yang ditampilkan pada Tabel 12.*

TABEL 12

SIZE DIREKTORI XAMPP

Tanggal	Total Event	Total Ukuran Folder XAMPP *(bytes)*	Pertambahan *(bytes)*
11/01/09	0	280,460,997	0
12/01/09	486	281,752,299	1,291,302
13/01/09	1,563	285,905,190	4,152,891
14/01/09	898	288,291,176	2,385,986
15/01/09	1,380	291,957,836	3,666,660
16/01/09	1,632	296,294,060	4,336,224
17/01/09	542	297,734,154	1,440,094

Dari Tabel 12 dapat disimpulkan bahwa rata-rata pertambahan size pada folder XAMPP tiap harinya sekitar 2,467,594 *bytes* (2,5MB).

Berdasarkan hasil pengamatan dan pencatatan tabel data diatas, dapat diketahui bahwa rata-rata ukuran *harddisk* yang akan terpakai tiap harinya sekitar 83,866,720 *bytes* atau kurang lebih 84MB. Dari rata-rata ini, dapat ditarik kesimpulan bahwa dengan menggunakan *harddisk* sebesar 40 GB dapat menampung jumlah kenaikan data tiap harinya kurang lebih selama 400 hari atau sekitar 1 tahun. Dalam hal ini pengatur jaringan harus terus melakukan pemantauan agar tidak terjadi gangguan pada sistem akibat kekurangan ruang kosong pada *harddisk.*

Sistem MAID ditempatkan di salah satu bagian pada jaringan untuk memantau aktifitas para pengguna HotSpot BINUS. Sistem ini melakukan penangkapan data paket dari para pengguna HotSpot untuk kemudian dianalisa apakah paket tersebut memiliki kriteria berbahaya atau tidak. Paket yang ditangkap sistem ini adalah paket bayangan bukan paket aslinya sehingga dapat dikatakan bahwa sistem ini tidak memperlambat transaksi data dari dan menuju pengguna HotSpot dan juga tidak menyebabkan gangguan pada kinerja jaringan lainnya.

Secara non-teknis, proses instalasi dan konfigurasi pada sistem MAID pertama kali dapat dikatakan cukup rumit sehingga akan sedikit menyulitkan pengguna dalam melakukannya. Sistem MAID dibuat berbasiskan *web* dengan antarmuka dan navigasi yang baik, sehingga mempermudah pengguna dalam melakukan pengaturan dan pengontrolan sistem dimanapun dan kapanpun.

VII. SIMPULAN DAN SARAN

A. Simpulan

Berdasarkan hasil evaluasi implementasi sistem MAID pada jaringan nirkabel BINUS University, maka dapat ditarik beberapa kesimpulan sebagai berikut:

1. Sistem MAID dapat mengamati lalu-lintas paket data dengan memberikan informasi total paket tiap protokol pada jaringan nirkabel BINUS University dengan cepat dan akurat.

2. Sistem MAID mampu memberikan informasi total paket yang lewat melalui tiap jalur (TCP dan UDP), sehingga memudahkan pengatur jaringan untuk mengetahui jalur-jalur mana saja yang lalu-lintas paketnya terlalu tinggi dari keadaan normal dan yang berkemungkinan mengganggu kinerja keseluruhan sistem pada jaringan ataupun ancaman lainnya.

3. Sistem MAID mampu menangkap dan menampilkan informasi setiap paket yang dianggap sebagai serangan atau berbahaya sesuai dengan aturan-aturan yang sedang aktif.

4. Sistem MAID melakukan pengiriman *email* kepada pengatur jaringan ber-hak akses super administrator maupun administrator sebagai peringatan akan setiap paket serangan yang terdeteksi.

5. Sistem MAID memungkinkan pengatur jaringan untuk menentukan kriteria aturan baru yang ingin dibuat sesuai dengan kebutuhannya, serta dapat dengan mudah mengaktifkan, menonaktifkan serta menghapus aturan-aturan dari sistem penyimpanan data.

6. Sistem MAID memberikan fasilitas laporan, *export*, dan *archive* yang dapat digunakan sebagai dokumentasi dari informasi kejadian yang terjadi pada jaringan dalam kurun waktu tertentu.

7. Sistem MAID dibuat berbasiskan *web* sehingga pengguna dapat dengan mudah mengontrol sistem ini.

8. Sistem MAID dapat berjalan selama 24 jam penuh pada jaringan tanpa mengganggu kinerja sistem lain dan juga aktivitas para pengguna HotSpot BINUS karena sistem IDS ini hanya mengambil paket bayangan yang dikirim maupun diterima oleh para pengguna HotSpot untuk kemudian dianalisis.

B. Saran

Berdasarkan hasil evaluasi sistem MAID yang telah diimplementasi, maka penulis memberikan saran untuk meningkatkan sistem keamanan jaringan nirkabel BINUS University untuk menjadi lebih optimal.

Saran-saran yang dapat disampaikan antara lain:

1. Dibutuhkan pengatur jaringan untuk selalu memantau kondisi jaringan melalui sistem MAID ini karena kondisi dan kinerja jaringan ditentukan pula oleh seberapa cepatnya pengatur jaringan dalam merespon setiap gangguan yang terjadi.

2. Proses instalasi dan pengaturan pertama kali pada sistem MAID sedikit menyulitkan pengguna, maka disarankan untuk kedepannya sistem IDS ini dibuat dalam bentuk kotak hitam atau perangkat keras.

3. Sistem MAID saat ini menggunakan metode deteksi rule based yaitu mengenali paket serangan dari pola serangan yang telah didefinisikan. Untuk pengembangannya, sistem MAID sebaiknya dilengkapi dengan metode deteksi lebih lanjut dimana sistem dapat mengenali pola serangan baru tanpa harus membandingkannya dengan pola aturan tercatat.

4. Pemberitahuan akan suatu kejadian pada MAID saat ini dikirimkan melalui *email*, untuk pengembangan sebaiknya dapat dikirimkan juga melalui Short Message Service (SMS).

5. Sistem MAID yang berjalan saat ini mencatat total paket yang melewati jaringan nirkabel BINUS University tiap harinya serta mencatat pula total paket di tiap jalur. Untuk pengembangan, sebaiknya sistem IDS ini juga dapat mencatat rincian setiap paket yang melalui jaringan untuk kemudian dianalisis lebih lanjut, dengan catatan memperhitungkan penggunaan memori pada *processor* maupun RAM serta kapasitas *harddisk* untuk sistem penyimpanan data.

6. MAID merupakan sistem pendeteksi gangguan pada jaringan. Untuk kedepan, sebaiknya sistem ini dikembangkan menjadi model Intrusion Prevention System yang bukan hanya mendeteksi tetapi juga dapat melakukan pencegahan terhadap paket-paket berbahaya yang mencoba masuk untuk merusak dan mengganggu kinerja sistem pada jaringan.

REFERENCES

[1] Lowe (2005, p10)

[2] Setiawan, Deris. 2003. Mengenal Infrastruktur Jaringan Komputer. *Sman13-mdn.* [Online] November 15, 2003. [Cited: September 10, 2008.] http://sman13-mdn.sch.id/download.php?id=14.

[3] Stallings, William. *Data and Computer Communications, 6th edition.* New Jersey : Prentice Hall, 2000.

[4] Ariyus, Dony. *Intrusion Detection System.* Yogyakarta : Penerbit Andi 2007.

[5] Geier, Jim. *Wireless Network First-Step.* Yogyakarta : Penerbit Andi 2005.

[6] Mikrotik. 1999-2003. HotSpot Gateway. *Mikrotik.* [Online] January 25, 2003. [Cited: September 10, 2008.] http://www.mikrotik.com/documentation//manual_2.6/IP/Hotspot.html.

[7] Scott, Wolfe, dan Hayes (2004, p9)

[8] Endorf, Schultz, dan Mellander (2004, p8)