PENGAMANAN KOMPUTER JARINGAN *LAN* KAMPUS A UNIVERSITAS BINA DARMA BERDASARKAN *LOG ROUTER*

Irwansyah
Dosen Universitas Bina Darma
Jalan Jenderal Ahmad Yani No.12 Palembang

Pos-el: irwansyah@mail.binadarma.ac.id

Abstract: *Bina Darma University is an institution that has intranet and internet networks are large. Computer networks are composed by a network that spread to several campuses. Each building will have space and laboratories. The number of intranet users who want to access the Internet will have an impact on network security, by increasing the number of deliveries virus, trojan or spam will be entered at the time of accessing the Internet network. In such conditions it is in this study make use of log router as a mechanism that is used to analyze network security at the University of Bina Darma. The scope of the discussion covers Laboratory Campus A. Based on the results of research and analysis, it can be concluded that there is still a lack of a PC to update the Operating System on a campus lab, or can be said to be very weak.*

Keywords: *Internet Network, Log Router, Virus, Operating System*

Abstrak: *Universitas Bina Darma merupakan institusi yang memiliki jaringan intranet dan internet yang cukup besar. Jaringan komputer tersebut tersusun oleh jaringan jaringan komputer yang tersebar kebeberapa kampus atau gedung dan masing–masing gedung memiliki ruang serta laboratorium–laboratorium. Banyaknya pengguna jaringan intranet yang ingin melakukan koneksi internet ini akan berdampak pada kemanan jaringan, yaitu dengan bertambah banyaknya pengiriman virus, trojan atau spam yang akan masuk pada saat pengaksesan pada jaringan internet. Dengan kondisi yang demikian maka pada penelitian ini memanfaatkan penggunaan log router sebagai mekanisme yang digunakan untuk menganalisa keamanan jaringan pada Universitas Bina Darma. Adapun lingkup pembahasan meliputi Laboratorium Kampus A Universitas Bina Darma. Berdasarkan hasil penelitian dan analisa, dapat ditarik kesimpulan bahwa masih kurangnya PC yang melakukan update Operating System pada laboratorium kampus A, atau dapat dikatakan sangat lemah.*

Kata kunci: *Jaringan Internet, Log Router, Virus, Operating System*

1. PENDAHULUAN

Perkembangan teknologi *internet* tidak hanya membawa dampak positif saja, melainkan juga berdampak negatif. Adapun dampak negatif tersebut mulai dari pengiriman virus, pengiriman *spam* atau jenis kejahatan lainnya pada saat user mengakses situs-situs pada *internet*. Sehingga institusi atau lembaga lainnya yang terhubung dalam suatu jaringan *internet* akan sangat rentan dengan keamanan jaringan. Hal ini mengingat bahwa produktivitas suatu institusi ataupun lembaga akan sangat bergantung pada kinerja jaringan didalamnya.

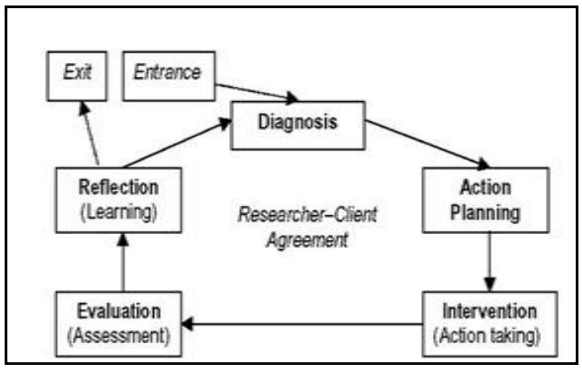
Universitas Bina Darma merupakan institusi yang memiliki jaringan *intranet* dan *internet* yang cukup besar. Jaringan komputer tersebut tersusun oleh jaringan jaringan komputer yang tersebar kebeberapa kampus atau gedung dan masing-masing gedung memiliki ruang serta laboratorium-laboratorium. Jaringan *Internet* pada Universitas Bina Darma dengan lebar jalur akses data (*bandwidth*) sebesar 10 Mbps dengan ISP (*Internet Service Provider*) Telkom. Banyaknya pengguna jaringan *intranet* yang ingin melakukan koneksi *internet* ini akan berdampak pada kemanan jaringan, yaitu dengan bertambah banyaknya pengiriman *virus, trojan* atau *spam* yang akan masuk pada saat pengaksesan pada jaringan internet. *Trojan, spam* dan *virus* biasanya disusupkan ke dalam suatu file atau program. *Virus* adalah program yang dapat menduplikasikan diri dan menyebar tanpa intervensi manusia setelah program tersebut dijalankan. Virus juga mempunyai kemungkinan untuk menduplikasikan diri namun biasanya memerlukan intervensi dari user komputer untuk menyebar ke program atau

sistem yang lain, dan ini dapat menyebabkan kerusakan atau kehilangan data yang serius.

Dengan kondisi yang demikian maka pada penelitian ini memanfaatkan penggunaan log router sebagai mekanisme yang digunakan untuk menganalisa keamanan jaringan pada Universitas Bina Darma. Mekanisme analisa *log files* merupakan catatan aktivitas yang terjadi pada router dalam suatu jaringan (J. Han & M. Kamber, 2006:16). *Router log files* menyediakan secara terperinci mengenai *file request* terhadap *web server* dan respon server terhadap *request* tersebut. *Log files* tersebut berisi waktu akses berdasarkan format waktu Unix, *source IP, url, server response, action,* operasi, *username, server IP, hierarchy, mime type*.

2. METODOLOGI PENELITIAN

Metode yang digunakan dalam peneltian ini menggunakan metode penelitian tindakan atau *action research.* Berikut tahapan penelitian tindakan (*action research*) yang dapat ditempuh yaitu (Davison, Martinsons & Kock (2004) lihat gambar 1 berikut:



Gambar1. Siklus *action research*

1) Melakukan diagnosa (*diagnosing*); Melakukan identifikasi masalah-masalah pokok yang ada guna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan., untuk pengembangan pada tahap ini peneliti mengidentifikasi kebutuhan *stakeholder* dengan cara mengadakan wawancara mendalam kepada stakeholder yang terkait langsung maupun yang tidak langsung.
2) Membuat rencana tindakan (*action planning*); Peneliti dan partisipan bersama-sama memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada.
3) Melakukan tindakan (*action taking*); Peneliti dan partisipan bersama-sama mengimplementasikan rencana tindakan dengan harapan dapat menyelesaikan masalah. Selanjutnya setelah model dibuat berdasarkan sketsa, dilanjutkan dengan mengadakan ujicoba.
4) Melakukan evaluasi (*evaluating*); Setelah masa implementasi (*action taking*) dianggap cukup kemudian peneliti bersama partisipan melaksanakan evaluasi hasil dari implementasi dalam tahap ini dilihat bagaimana pegguna yang ditandai dengan berbagai aktivitas-aktivitas.
5) Pembelajaran (*learning*); Tahap ini merupakan bagian akhir siklus yang telah dilalui dengan melaksanakan review tahap-pertahap yang telah berakhir kemudian penelitian ini dapat berakhir.

2.1 Analisis

Analisis adalah kegiatan berfikir untuk menguraikan suatu keseluruhan menjadi komponen sehingga dapat mengenal tanda-tanda komponen, hubungannya satu sama lain dan fungsi masing-masing dalam satu keseluruhan terpadu (Komaruddin, 2001:53). Analisis adalah penguraian suatu pokok atas berbagai bagiannya dan penelaahan bagian itu sendiri serta hubungan antar bagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan (Kamus Besar Bahasa Indonesia, 2002:43).

Analisis adalah mengelompokkan, membuat suatu urutan, memanipulasi, serta menyingkatkan data sehingga mudah dibaca (Nazir, 2003:358). Analisis data merupakan salah satu rangkaian dalam kegiatan penelitian. Sehingga kegiatan menganalisis data berkaitan dengan rangkaian kegiatan sebelumnya mulai dari jenis penelitian yang telah dipilih, rumusan masalah dan tujuan penelitian, jenis data, jumlah variabel, serta asumsi-asumsi teoritis yang melandasi kegiatan-kegiatan penelitian. Dengan demikian, dalam melakukan analisis data perlu memperhatikan rangkaian tahap sebelumnya sebagai rujukan agar penelitian yang dilaksanakan bertalian atau berhubungan dengan tahap-tahap penelitian yang lain.

2.2 *Internet*

Internet merupakan kepanjangan dari *Interconnection Networking*. Menurut Jill. H. Ellsworth dan Matthew. V. Ellsworth, (2002: 10): *"Internet is : large interconnected network of network computer linking people and computer all over the world, via phone line, satellites and other telecommunication systems".*

Pengertiannya adalah *internet* adalah jaringan besar yang saling berhubungan dari jaringan-jaringan komputer yang menghubungkan orang-orang dan komputer di seluruh dunia, melalui telepon, satelit dan sistem-sistem komunikasi yang lain. *Internet* dibentuk oleh jutaan komputer yang terhubung bersama dari seluruh dunia, memberi jalan bagi informasi untuk dapat dikirim dan dinikmati bersama. Untuk dapat bertukar informasi, digunakan protokol standar yaitu *Transmision Control Protocol* dan *Internet Protocol* yang lebih dikenal sebagai *TCP/IP*.

2.3 TCP/IP dan Subnet

2.3.1 *TCP/IP*

TCP/IP bukanlah sebuah protokol tunggal tetapi satu kesatuan protokol dan *utility*. Setiap protokol dalam kesatuan ini memiliki aturan yang spesifik. Protokol ini dikembangkan oleh *Advanced Research Project Agency* (ARPA) untuk Departemen Pertahanan Amerika Serikat pada tahun 1969. (Rafiudin, 2004:17).

Seperti yang disebutkan di atas, bahwa nilai *IP* adalah nilai biner 32 bit. Nilai tersebut terbagi menjadi empat bagian nomor 8 *bit* yang disebut *oktet*. Contoh alamat IP 202.149.240.66.

Dengan menggunakan contoh di atas, semua komputer memiliki bagian nilai yang sama: 202.149.24. xxx. Ini adalah network ID. Nomor pada xxx adalah *node ID*-nya.Setiap alamat *TCP/IP* jatuh pada satu kelas alamat. Kelas mewakili sebuah grup alamat yang segera

dapat dikenali komponen *software* sebagai bagian dari sebuah jaringan fisik.

Tabel 1. *IP Address*

Kelas	Jangkauan *Oktet* Pertama	Jumlah Jaringan	Jumlah *Host*
A	1 – 126	126	16.777.216
B	128 – 191	16.384	16.536
C	192 – 223	2.097.152	256

2.3.2 *Subnet Mask*

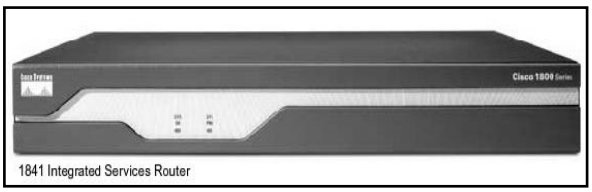
Setiap komputer di sebuah jaringan biasanya ingin mengirim data langsung ke komputer lainnya. Komputer pengirim harus memastikan bahwa si penerima berada di jaringan yang sama atau di luar itu. Subnet mask digunakan oleh protokol *stack* TCP/IP untuk menentukan bahwa *host* yang akan dicoba dikomunikasikan berada di jaringan lokal yang sama atau berada di jaringan *remote*. Ini adalah bagian yang sangat penting dalam konfigurasi TCP/IP. Tabel 2.3. berikut adalah klasifikasi dari *subnet mask*.

Tabel 2. *Subnet Mask*

Kelas	*Subnet Mask*
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

2.4 Cisco Router

Cisco *Router* berfungsi untuk meneruskan paket data dari suatu *LAN* ke *LAN* lainnya yang biasanya saling berjauhan. Untuk itu *cisco router* menggunakan *table* dan *protocol routing* yang berfungsi untuk mengatur lalu lintas data. Paket data yang tiba di *router* diperiksa dan diteruskan ke alamat yang dituju. Agar paket data yang diterima dapat sampai ke tujuannya dengan cepat, *router* harus memproses data tersebut dengan sangat cepat (Wijaya, 2002 : 61).



Gambar 2. Cisco Router 1841 (www.cisco.com)

Router merupakan *device network layer* yang menggunakan satu atau lebih system metrik untuk menentukan *path-path* optimal guna mem-*forward traffic* suatu *network*. *Router* akan menghantarkan paket – paket dari suatu *network* ke *network* lainnya berbasiskan *network layer information* (Rafiudin, 2004 : 01).

2.5 *Logging*

Logging merupakan salah satu bagian yang kritis terutama menyangkut *isu-isu security* dan pertahanan. Sistem yang senantiasa mencatat *log-log* untuk setiap sesi yang terjadi, dapat membantu menemukan titik-titik permasalahan seandainya ditengarai adanya *error-error* dan ketidaklaziman. (Rafiudin, 2004:224).

Cisco IOS dapat dikategorikan berdasarkan *severity level*. Sebagaimana digambarkan dalam tabel dibawah ini, nomor *severity level* paling rendah merupakan pesan-pesan yang lebih kritis dibanding yang lainnya.

Tabel 3. *Cisco Log Message Severity Levels*

Level	Nama Level	Deskripsi	Contoh
0	Emergencies	Router tidak dapat digunakan	*IOS could not load*
1	Alerts	aksi	*Temperature*

		penanganan segera	*too high*
2	Critical	Kondisi kritis	*Unable to allocate*
3	Errors	Kondisi error	*Invalid memory size*
4	Warnings	Kondisi peringatan	*Crypto operation failed*
5	Notifications	Normal tetapi event penting	*Interface changed state, up to down, or down to up*
6	Informational	Pesan informasi	*Packet denied by an access list on an interface*
7	Debugging	Pesan debug	*Appears only when debugging is enabled*

2.6 Keamanan Jaringan

Network Security pada awalnya konsep ini menjelaskan lebih banyak mengenai keterjaminan (*security*) dari sebuah sistem jaringan komputer yang terhubung ke Internet terhadap ancaman dan gangguan yang ditujukan kepada sistem tersebut. Network Security hanyalah menjelaskan kemungkinan-kemungkinan yang akan timbul dari konektivitas jaringan komputer lokal kita dengan *wide-area network*.

Secara umum, terdapat 3 (tiga) kata kunci dalam konsep *Network Security* ini, yaitu: resiko/ tingkat bahaya, ancaman, dan kerapuhan sistem (*vulnerability*).

Dalam hal ini, resiko berarti berapa besar kemungkinan keberhasilan para penyusup dalam rangka memperoleh akses ke dalam jaringan komputer lokal yang dimiliki melalui konektivitas jaringan local ke *wide-area network*. Secara umum, akses-akses yang diinginkan adalah: 1) *Read Access*: mampu mengetahui keseluruhan sistem jaringan informasi; 2) *Write Access*: mampu melakukan proses menulis ataupun menghancurkan data yang terdapat di sistem tersebut; 3) *Denial of Service*: menutup penggunaan utilitas-utilitas jaringan normal dengan cara menghabiskan jatah *CPU, bandwidth* maupun *memory*.

2.7 *Data Mining*

Data mining adalah kombinasi secara logis antara pengetahuan data, dan analisa statistik yang dikembangkan dalam pengetahuan bisnis atau suatu proses yang menggunakan teknik statistik, matematika, kecerdasan buatan, tiruan dan *machine-learning* untuk mengekstraksi dan mengidentifikasi informasi yang bermanfaat bagi pengetahuan yang terkait dari berbagai database besar (J.Han & M. Kamber, 2006:112).

Data mining meliputi tugas-tugas yang dikenal sebagai ekstraksi pengetahuan, arkeologi data, eksplorasi dalam pemrosesan pola data dan memanen informasi. Semua aktifitas ini dilakukan secara otomatis dan mengizinkan adanya penemuan cepat bahkan oleh non programmer.

2.8 MySQL

MySQL adalah merupakan perangkat lunak untuk sistem manajemen database (*Database Management System*). Karena sifatnya yang *open source* dalam memiliki kemampuan menampung kapasitas yang sangat besar, maka *MySQL* menjadi database yang

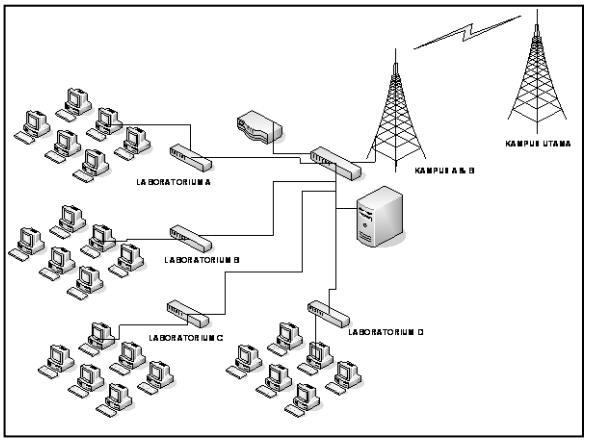
sangat populer di kalangan programer web. (Sukarno, 2006:3).

MySQL adalah suatu database popular dengan pengembangan *web developer*. Kecepatan dan ukuran yang kecil membuatnya ideal untuk website. Ditambah lagi dengan fakta bahwa *MySQL* adalah *open source* yang artinya gratis (Sinarmata, 2006:29).

2.9 Tahap Penelitian

2.9.1 Melakukan Diagnosa *(Diagnosing)*

Langkah selanjutnya pada penelitian ini adalah mendiagnosa jaringan *LAN* di Laboratorium Universitas Bina Darma yaitu dilakukan dengan mengenal dan mempelajari sistem *log* yang terdapat pada *router* yang digunakan sebagai keamanan jaringan, hal ini dikarenakan untuk mengetahui apakah semua user yang mengakses pada jaringan di laboratorium terfilter pada perangkat jaringan yang digunakan khususnya *router*. Adapun skema jaringan dapat dilihat pada gambar 2 berikut:



Gambar 3. Skema Jaringan Kampus A dan B

2.9.2 Membuat Rencana Tindakan (*Action Planning*)

Pada tahap ini peneliti terlebih dahulu mempelajari dan memahami bersama-sama dengan *network Administrator*, dan Kepala Laboratorium sebagai admin jaringan mengenai pokok permasalahan yang ada pada jaringan *LAN* di Laboratorium yang ada di Universitas Bina Darma.

Rencana tindakan yang akan dilakukan dalam tahap ini meliputi: 1) Menentukan kembali penerapan *access control* lalu lintas data dalam jaringan dengan cara membuat *buffer log router*; 2) Membuat pengolahan data dengan menggunakan database *MySQL*; 3) Implementasi monitoring yang dilakukan dari tanggal 07 mei s/d 12 mei 2012 pada skema jaringan *LAN* di masing-masing Laboratorium kampus A dan B melalui *log router*.

Pada rancangan basis data ini akan dirancang 2 buah tabel yang akan digunakan untuk mempermudah akses *query* data yang dihasilkan dari *log buffer router*.

Tabel 4. File *Log Update* Sistem Operasi

No.	Field	Type	Size	Description
1.	Jam_Akses	Date/ Time	12	Waktu akses
2.	Tgl_Akses	Date/ Time	12	Tanggal akses
3.	Ip_Address	Varchar	15	IP Adress
4.	URL_OS	Varchar	25	Url system operasi

Tabel 5. File *Log Update Anti Virus*

No.	Field	Type	Size	Description
1.	Jam_Akses	Date/ Time	12	Waktu akses
2.	Tgl_Akses	Date/ Time	12	Tanggal akses
3.	Ip_Address	Varchar	15	IP Adress

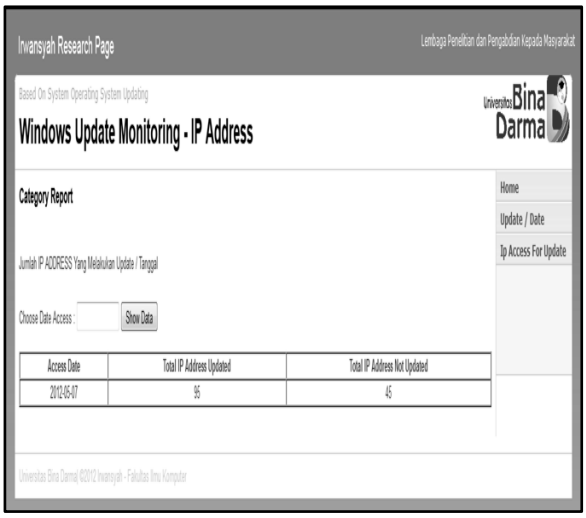
4.	URL_AnVir	Varchar	25	URL Anti Virus

2.9.3 Melakukan Tindakan (*Action Taking*)

Pada tahap ini yaitu mengimplementasi rencana tindakan dengan dimulai dari membaca secara keseluruhan data *file log* yang kemudian secara satu persatu data tersebut dimasukkan ke dalam database MYSQL. Analisa selanjutnya adalah memfilterisasi data dengan memilah jumlah *record* yang tidak diperlukan. Proses filterisasi yang pertama yaitu memilah ip address yang aktif dari Laboratorium A, B, C dan D. Jumlah *ip address* dari ke empat laboratorium tersebut adalah 150 *ip address* dimana masing – masing ip hanya digunakan oleh satu user. Monitoring untuk *ip address* dilakukan dalam satu minggu atau 6 hari kerja. Contoh *ip address* yang terakses pada *log router*.

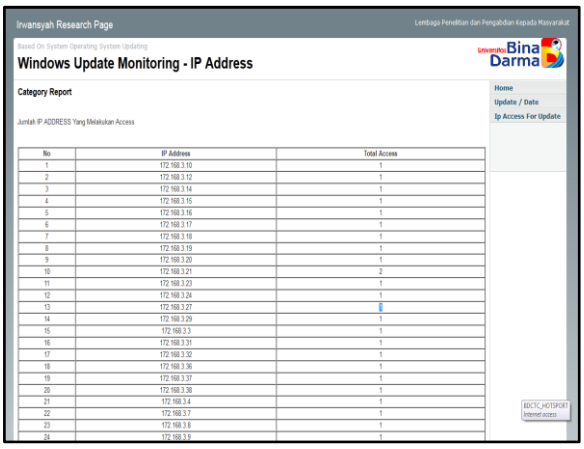
```
2012 May 07 08:10:02: %SEC-6-IPACCESSLOGP:
list 101 permitted tcp 172.168.3.10(1019)
GET http:// update.microsoft.com/window …..

2012 May 07 08:10:02: %SEC-6-IPACCESSLOGP:
list 101 permitted tcp 172.168.3.16(1019)
GET http:// update.microsoft.com/window …..

2012 May 07 08:10:02: %SEC-6-IPACCESSLOGP:
list 101 permitted tcp 172.168.5.22(1019)
GET http://www.google.co.id/..... ……..…..

2012 May 07 08:10:02: %SEC-6-IPACCESSLOGP:
list 101 permitted tcp 172.168.3.3(1019)  GET
http:// update.microsoft.com/window …..

2012 May 07 08:10:03: %SEC-6-IPACCESSLOGP:
list 101 permitted tcp 172.168.6.34(1019)
GET http:// update.microsoft.com/window …..
```

Langkah selanjutnya dari data diatas dimasukan kedalam database *MySQL* yang akan mempermudah akses *query* data yang diinginkan. Disini data yang akan di-*query* kan yaitu *ip address*, *update url operating system* dan *update url* antivirus.



Gambar 4. Tampilan program *Query* pada Database *MySQL*

Dari gambar 4 seluruh *ip address* yang di-*record* pada *log buffer router* dimasukan pada program *Query*, kemudian dari program tersebut akan diproses pencarian dari masing-masing ip yang aktif, serta *ip address* yang *update windows* ataupun *update anti virus*.



Gambar 5. Hasil *Query IP Address Windows Update*

Dari hasil penggunaan program diatas didapatkan total *record* pada *log router* selama 1

minggu dari tanggal 7 mei sampai 12 mei berjumlah 4377 record.

Tabel 6. Monitoring *log URL Operating System*

No.	Jam Akses	Tgl Akses	Ip Address	URL OS
1	8:10:02	5/7/2012	172.168.3.10	http://update.microsoft.com/window
2	8:10:02	5/7/2012	172.168.3.16	http://update.microsoft.com/window
3	8:10:02	5/7/2012	172.168.5.22	
4	8:10:02	5/7/2012	172.168.3.3	http://update.microsoft.com/window
5	8:10:03	5/7/2012	172.168.6.34	http://update.microsoft.com/window
6	8:10:03	5/7/2012	172.168.3.19	http://update.microsoft.com/window
7	8:10:04	5/7/2012	172.168.6.20	http://update.microsoft.com/window
8	8:10:04	5/7/2012	172.168.5.18	
9	8:10:04	5/7/2012	172.168.6.8	http://update.microsoft.com/window
10	8:10:05	5/7/2012	172.168.6.16	http://update.microsoft.com/window
…				

Untuk tabel 6 diatas terlihat *url update* untuk *microsoft windows*, karena semua laboratorium yang dimonitor menggunakan system operasi *windows xp*.

Tabel 7. Monitoring *log URL Update Anti Virus*

No.	Jam Akses	Tgl Akses	*Ip Address*	*URL Update Anti Virus*
1	10:09:34	5/7/2012	172.168.4.10	http://....avgate.net
2	10:09:50	5/7/2012	172.168.3.25	http:// …..eset.com….
3	10:15:11	5/7/2012	172.168.6.15	http://……..grisoft..../.....
4	10:15:18	5/7/2012	172.168.4.19	http://....avgate.net
5	10:23:03	5/7/2012	172.168.6.3	http://……..grisoft..../.....
6	10:34:10	5/7/2012	172.168.3.11	http:// …..eset.com….
7	10:55:22	5/7/2012	172.168.4.21	http://....avgate.net
8	10:55:32	5/7/2012	172.168.6.4	http://……..grisoft..../.....
…				

Untuk tabel 7 yaitu monitoring *log url update Antivirus* terdapat beberapa *ip address* yang aktif meng-*update* alamat *url* pada masing-masing provider yang berbeda. Dari jumlah total record sebanyak 4377 tesebut, peneliti mendapatkan hasil proses *query* terhadap *ip address* yang melakukan *update operating system windows* sebanyak 35 ip dari 145 ip aktif, dan untuk *update anti virus* dapat dilihat pada tabel 8 di bawah ini :

Tabel 8. Jumlah IP yang *Update* Anti Virus

No.	Jenis Anti Virus	Jumlah IP yang *update*
1.	NOD32	54
2.	AVG	23
3.	Antivir	27

Dari jumlah ip yang aktif sebanyak 154 didapat tiga jenis anti virus yang di *update* oleh masing – masing user. Untuk anti virus NOD32 sebanyak 54 ip yang *update*. Anti Virus AVG sebanyak 23 ip dan 27 ip yang *update* anti virus Antivir.

3. HASIL

3.1 Hasil Evaluasi (*evaluating*)

Pada tahap ini melaksanakan evaluasi hasil dari implementasi monitoring file log yang telah diproses yang dibantu dengan menggunakan *tools MySQL* yang digunakan untuk menampung keseluruhan data *file log* serta PHP yang digunakan untuk menampilkan hasil *query* yang dilakukan terhadap *database file log* dalam melakukan filterisasi. Dari keseluruhan data *file log*, tersimpan 4.377 *record* data. Dimana data tersebut merupakan data yang merekam aktifitas setiap kali mengakses suatu

url, jadi pada hari yang sama dan *user* yang sama dapat melakukan akses *url* lebih dari satu kali, hal ini menyebabkan banyaknya *record* yang tersimpan pada database. Untuk itu dilakukan filterisasi IP aktif yang digunakan untuk mengetahui berapa jumlah IP yang aktif. Dengan melakukan *database filtering* maka dapat diketahui bahwa dari 4.377 *record* didapatkan 145 ip aktif.

3.2 Pembahasan

Pada tahap proses filterisasi URL, peneliti akan membahas dua jenis filterisasi yang dilakukan yaitu filterisasi untuk *update system* operasi dan *update* anti virus.

3.2.1 Proses Hasil Filterisasi URL *update Operating System Windows*

Hasil proses filter untuk URL *update OS windows* yang dilakukan dengan menggunakan database *MySQL* dihasilkan 145 IP yang aktif dan didapatkan 35 IP yang melakukan *update OS*. Jika dihitung dalam prosentase menggunakan rumus berikut:

$$\frac{jumla\ h\ IP\ Update\ \ Operating\ \ System\ \ Windows}{Jumla\ h\ IP\ Aktif} x\ 100\% \ldots(1)$$

Berdasarkan rumus di atas didapatkan:

$$\frac{35}{145} x\ 100\% = 24{,}13\% \ldots(2)$$

Hasil dari rumus 1 didapatkan 24,13% jumlah ip yang melakukan *update Operating System Windows.* Dari hasil tersebut dapat dikatakan bahwa hampir semua laboratorium komputer kampus A *Operating System Windows* tidak melakukan *update*. Hal ini akan berdampak pada serangan dari *virus, trojan* ataupun *spam* yang akan merusak *Operating System Windows.*

3.2.2 Proses Hasil Filterisasi URL *update* Anti Virus

URL *update* antivirus yang difilter terdiri dari beberapa jenis URL antivirus yang biasa digunakan. Pada penelitian ini didapatkan 3 jenis Antivirus NOD32, AVG dan Antivir.

Dari 3 jenis antivirus tersebut dapat melakukan *update* secara automatis atau *update* yang dilakukan secara langsung pada saat terhubung dengan *internet*, serta *update* yang dilakukan dengan cara manual atau *update* yang dilakukan oleh *user*. Pada penelitian ini hanya menggunakan data yang didapat dari hasil filterisasi URL *update antivirus* yang dilakukan secara automatis. Hal ini dikarenakan *update* yang dilakukan secara manual dapat dilakukan dengan mengakses *url* yang menyediakan *patch update antivirus* tersebut, seperti yang kita ketahui bahwa yang menyediakan *patch update antivirus* untuk salah satu jenis *antivirus* seperti halnya *antivirus* AVG tidak hanya satu URL, kini banyak URL yang menyediakan *patch update antivirus* tersebut.

Pada tabel 8 jumlah ip yang *update* antivirus sebanyak 104 ip dari ketiga antivirus yang digunakan masing-masing user. Jika dihitung berdasarkan prosentase dengan rumus 2 maka didapat :

$$\frac{Jumla\ h\ IP\ update\ \ antivirus}{Jumla\ h\ IP\ aktif} x100\% \ldots (3)$$

Berdasarkan rumus 2 didapatkan:

$$\frac{104}{145} x\ 100\% = 71{,}72\% \ldots(4)$$

Hasil dari rumus 2 didapatkan 71,72% jumlah *ip* yang melakukan *update antivirus.* Dari hasil tersebut dapat dikatakan bahwa hampir semua PC laboratorium komputer pada kampus A melakukan *update* antivirus. Tetapi hal ini belum dapat dikatakan aman atau *secure,* karena sebaiknya hasil yang diharapkan berdasarkan rumus 2 diatas 90%, dari hasil itu tentunya sangat baik bagi keamanan dari serangan *virus* atau *trojan* dan *spam* pada laboratorium komputer kampus A.

4. SIMPULAN

Berdasarkan hasil penelitian dan analisa, dapat ditarik kesimpulan: 1) bahwa masih kurangnya PC yang melakukan *update Operating System* pada laboratorium kampus A, atau dapat dikatakan sangat lemah. Hal ini terbukti dengan adanya hasil perhitungan jumlah *user* (dalam hal ini perhitungan melalui IP) yang meng*update Operating System* sebanyak 24,13% dari jumlah IP yang aktif yang menggunakan *Operating System Windows* yaitu 145 IP aktif.; 2) Begitu juga terrlihat dari hasil perhitungan jumlah *user* yang malakukan *update* antivirus secara *automatic* (yaitu pada keadaan dimana komputer baru diaktifkan) sebesar 71,72% dari jumlah IP yang aktif yang menggunakan *Operating System* Windows. Hasil perhitungan yang didapatkan nilainya masih di bawah 90% dimana peneliti mengasumsikan bahwa 90% merupakan prosentase yang menjadi batasan suatu jaringan dapat dikatakan *secure*; 3) Dari hasil penelitian ini juga, peneliti menemukan beberapa permasalahan pada peng*update*-an yang terjadi pada semua laboratorium kampus A. Dimana peng*update*-an terjadi secara berulang – ulang, baik pada proses peng*update*-an *Operating System Windows* maupun *antivirus*. Hal ini terjadi dikarenakan semua PC pada laboratorium kampus A di *install software deep preeze*. *Software* ini berfungsi mengunci hardisk atau mengembalikan ke kondisi semula walaupun kita merubah dan menghapus setelah computer di *restart*.

Adapun saran dari peneliti setelah melihat hasil di atas maka dapat diketahui bahwa keamanan jaringan yang terdiri dari *informasi update windows* dan *antivirus* tersebut kurang *secure*, bahkan rentan terhadap serangan dari luar. Untuk itu, dengan adanya analisis ini keamanan jaringan dapat ditingkatkan dengan memberikan peringatan kepada *user* yang terhubung dalam satu jaringan tersebut bahwa komputer yang digunakan beresiko terhadap masalah kemanan komputer dan jaringan.

Sebaiknya penggunaan *software deep preeze* dihilangkan karena *windows* dan antivirus tidak akan dapat meng-*update* secara otomatis. Untuk keseragaman penggunaan Sistem operasi yang digunakan pada laboratorium hendaknya dibuatkan prosedur atau semacam SOP *(Standar Operation Procedure)* pada masing-masing laboratorium.

Adapun saran untuk pengembangan penelitian ini diharapkan, analisis ini akan lebih mewakili keadaan yang lebih baik dengan data yang lebih banyak dan penambahan parameter yang lebih banyak lagi misalnya url untuk *update* antivirus, jenis system operasi dan lain-lain.

DAFTAR RUJUKAN

Davison, R. M., Martinsons, M. G., Kock N. 2004. *Journal: Information Systems Journal: Principles of Canonical Action Research.*

Ellsworth, Jill H., Ellsworth, M atthew V. 2002. *Marketing on the internet*. Grasindo. Jakarta.

J. Han and M. Kamber. 2006. *Data Mining: Concepts and Techniques*. Morgan Kaufmann Publishers. Massachusetts.

Kamus Besar Bahasa Indonesia.2002. hal. 43.

Nazir, Moh. 2003. *Metodologi Penelitian.* Ghalia Indonesia. Jakarta.

Rafiudin, Rahmat. 2004. *Mengupas Tuntas Cisco Router*. PT Elex Media Komputindo. Jakarta.

Wijaya, Hendra. 2002. *Cisco Router*. PT. Gramedia. Jakarta.