Implementasi Keamanan Jaringan LAN Berbasis ACLs dan VLAN

Febrian Wahyu Christanto[*1], Atmoko Nugroho[2], Whisnumurti Adhiwibowo[3]
Program Studi Teknik Informatika[1],[2],[3]
Universitas Semarang[1],[2],[3]
Jl. Arteri Soekarno-Hatta Tlogosari, Semarang, Jawa Tengah
e-mail: febrian.wahyu.christanto@usm.ac.id[*1], atmoko@usm.ac.id[2], whisnu@usm.ac.id[3]

***Abstrak*—Manajemen jaringan di era jaringan komputer modern adalah hal yang sangat penting karena setiap perangkat dapat berkoneksi dengan perangkat lain yang berada di seluruh dunia melalui kecanggihan teknologi *internet*. Tentu saja dengan kemajuan ini membutuhkan suatu sistem pemantauan jaringan komputer yang membantu *administrator* jaringan dalam mengelola *Local Area Network* (LAN). Permasalahan yang sering timbul adalah kesulitan untuk mengetahui status *open port* disaat terjadi *trouble* ataupun serangan di dalam jaringan karena jumlah *port* jaringan mencapai 65.536, sehingga membutuhkan waktu yang lebih lama untuk melakukan perbaikan jaringan. Selain itu kebutuhan akan suatu sistem terintegrasi dalam pemantauan proses serta statistik *port* dalam *Local Area Network* (LAN) menjadi landasan dalam penelitian ini sehingga dapat meminimalisasi penggunaan sistem yang terlalu banyak dalam pemantauan jaringan komputer. Hasil dari penelitian ini adalah suatu sistem baru hasil modifikasi dari Mandau Registry Tools and Information System dengan menambahkan layanan seperti informasi protokol, statistik *port*, dan informasi tentang *Domain Name System* (DNS) dan penambahan layanan *Access Control Lists* (ACLs) dengan Fail2Ban. Menggunakan tahapan perencanaan, analisis, desain, implementasi, dan pengujian sebagai metode pengembangan sistem, diharapkan penelitian ini dapat membantu pemantauan dan keamanan *Local Area Network* (LAN) yang lebih baik dengan kompleksitas informasi proses jaringan dan statistik *port* yang dihasilkan.**

Kata Kunci*—*Keamanan Jaringan Komputer, Statistik Port, Local Area Network, Mandau Registry Tools and Information System, Fail2Ban

I. PENDAHULUAN

Dunia teknologi modern saat ini sangat diperlukan untuk pertukaran informasi yang cepat, instan, dan akurat antara orang-orang di seluruh dunia. Dengan tuntutan teknologi yang semakin tinggi, maka dibutuhkan teknologi yang dapat membantu kerja manusia untuk diwujudkan dalam pertukaran informasi. *Internet* adalah teknologi yang paling cepat berkembang saat ini yang mendukung pertukaran informasi melalui jaringan komputer yang canggih, cepat, dan efisien ke wilayah yang sangat luas.

Dengan luasnya cakupan teknologi ini, maka sumber daya perangkat keras yang dibutuhkan juga harus canggih dan bagus. Masalahnya adalah biaya, karena tidak semua komputer dalam jaringan memiliki sumber daya yang canggih dan baik. Masalah ini diakomodasi dengan jaringan komputer *client-server*. Komputer *server* akan lebih baik dari komputer klien karena memiliki peran untuk menyediakan layanan ke komputer klien yang ada di jaringan komputer. *Administrator* berperan mengendalikan *server* dan bertanggung jawab untuk memantau jaringan agar sistem tetap berjalan baik, aman, dan sesuai dengan aturan yang ada. Beberapa kesulitan yang muncul adalah pada pemantauan sumber daya *server* jaringan komputer. Karena selain mengendalikan *server*, *administrator* juga ditugaskan untuk menjaga keamanan jaringan komputer dari serangan oleh pihak luar.

Saat ini banyak serangan jaringan komputer yang memanfaatkan *port* terbuka di jaringan komputer. Bahkan dikatakan hampir semua serangan yang terjadi pada jaringan komputer melalui *port* yang terbuka. Serangan seperti *Denial of Service* (DoS), *Back Door*, *Spoofing*, *Brute Force*, SQL *Injection*, *Port Scanning*, *Network Flooding*, hingga virus mengeksploitasi kerentanan *port* terbuka di jaringan komputer. *Port* dapat digambarkan sebagai jendela rumah, sehingga jumlah itu sangat banyak karena *port* di jaringan komputer bernilai 16 (enam belas) *bit*, sehingga jumlah total *port* dalam jaringan komputer adalah 65.536 buah [1]. Serangan melalui *port* biasanya merusak atau mencuri informasi dari *server* seperti *server email*, *server* data, *server web*, atau pencurian pengguna dan kata sandi sistem untuk tujuan tertentu [2]. Tentu saja permasalahan keamanan tersebut harus dapat diakomodasi oleh *administrator* agar stabilitas jaringan tetap berjalan dengan baik. Dengan tugas berat seorang *administrator* yang harus mengendalikan, memantau, dan mengamankan jaringan komputer dari serangan yang terjadi, dibutuhkan sistem pemantauan jaringan komputer untuk membantu *administrator* terutama dalam memantau *port* dan proses di *Local Area Network* (LAN).

Masalah tersebut dialami pula di Fakultas Teknologi Informasi dan Komunikasi (FTIK) Universitas Semarang. *Administrator* menemukan kesulitan dalam memantau *port* dan proses jika terjadi kerusakan dan serangan pada *Local Area Network* (LAN). Beberapa data serangan yang pernah terjadi dalam *Local Area Network* (LAN) Fakultas Teknologi Informasi dan Komunikasi (FTIK) Universitas Semarang antara rentang waktu 2017-2018 dengan memanfaatkan *port* jaringan yang terbuka terdapat di dalam Tabel 1 berikut.

TABLE I. DATA SERANGAN DI LAN FTIK UNIVERSITAS SEMARANG

Jenis Serangan	***Port* yang Digunakan**	**Permasalahan yang Ditimbulkan**
Sniffing user dan *password* jaringan *wifi internet*	53	Koneksi *internet* terutama untuk user "dosen" menjadi lebih lambat
Netcut	137	Drop koneksi *internet*
Bypass proxy	3128	Situs-situs yang dilarang dapat dibuka
Brute force telnet	23	Mencoba masuk ke *root* ftik.usm.ac.id, CPU *load server* meningkat
Brute force SSH	22	Mencoba masuk ke *root* ftik.usm.ac.id, CPU *load server* meningkat
DDOS	80	CPU *load server* meningkat, *traffic bandwidth* meningkat, ftik.usm.ac.id *down*
Virus	54320, 54321, 12345	XAMPP disembunyikan virus, muncul *pop-up* iklan di web ftik.usm.ac.id

Untuk menangani permasalahan yang terjadi pada Tabel 1, maka *administrator* menggunakan banyak perangkat lunak untuk memantau proses di dalam jaringan *Local Area Network* (LAN), tetapi sedikit perangkat lunak yang digunakan untuk memantau *port* jaringan. Selain itu juga dilakukan penutupan *port* yang terbuka melalui *router*. Tetapi perbaikan jaringan dengan cara tersebut membutuhkan waktu yang cukup lama.

Dari permasalahan yang dijabarkan, maka penelitian ini muncul untuk mengakomodasi permasalahan yang timbul di *Local Area Network* (LAN) Fakultas Teknologi Informasi dan Komunikasi (FTIK) Universitas Semarang. Penelitian ini membutuhkan pula beberapa penelitian terdahulu yang digunakan sebagai referensi dan acuan penelitian. Referensi ini berhubungan dengan pemantauan jaringan dan *port* yang merupakan inti dalam penelitian ini. Penelitian terdahulu terdapat pada Tabel 2 berikut.

TABLE II. PENELITIAN TERDAHULU

Judul	***Tools* yang Digunakan**	**Hasil Penelitian**
A Study of Internet Threats,Avoidance and Biometric Security Techniques-Comparison of Biometric Techniques [3]	-	Penggunaan teknik keamanan biometrik untuk keamanan jaringan komputer
Evaluation of Network Port Scanning Tools [4]	Nmap, SuperScan 4.0, Advanced Port Scanner, Advanced Administrative Tools, Angry IP Scanner, Atelier Web Security Port Scanner, Unicornscan	Survey tools pemantauan port jaringan bersama dengan kelebihannya
Port Scan-A Sequrity Concern [5]	CAIDA, UCSD Active Web Machines, Snort	Metodologi *port scanning* dalam analisa jaringan komputer untuk menemukan *port* paling aktif dalam jaringan
Analysing Port Scanning Tools and Security Techniques [6]	Atelier Web Security Port Scanner	Membahas tentang *tools* untuk *port scanning* dan cara mengantisipasi serangan DOS, Botnet, dan DDOS
An Insight in to Network Traffic Analysis using Packet Sniffer [7]	Wireshark	Menganalisa sebab koneksi hilang dan serangan menggunakan *packet sniffer* pada jaringan sehingga *administrator* dapat mengambil tindakan yang

Judul	*Tools* yang Digunakan	Hasil Penelitian
		tepat
Advanced Network Scanning [8]	Advanced IP Scanner, Wireless Network Watcher, Security Manager Plus	Menganalisa bagaimana penyerang masuk ke dalam jaringan dan menganalisa cara mendeteksi serangan dalam jaringan komputer

Dari penelitian terdahulu yang terdapat pada Tabel 2 membahas tentang jaringan, proses, dan pemantauan *port* menggunakan berbagai perangkat lunak. Dengan berbagai perangkat lunak yang digunakan tentunya akan menambah waktu *administrator* dalam melakukan pemantauan *port* dan jaringan komputer. Solusi yang ditawarkan dalam penelitian ini adalah integrasi sistem untuk mengakomodasi masalah yang dijelaskan sebelumnya. Dari hasil penelitian ini nantinya dapat digunakan untuk membantu pekerjaan *administrator* untuk mengelola *Local Area Network* (LAN). Kebutuhan tersebut dapat diakomodasi dengan menggunakan perangkat lunak *freeware open source* yang dapat dikonfigurasi sesuai dengan kebutuhan pengguna.

Mandau Registry Tools and Information System adalah perangkat lunak *open source* yang bersifat *freeware* sehingga dapat digunakan dalam jaringan komputer dalam sistem operasi berbasis Windows dengan menyediakan layanan konfigurasi untuk optimalisasi register dan proses pemantauan sistem operasi pada *server*. Hal ini dapat membantu *administrator* dalam mengontrol dan memantau kerja *server* khususnya di Fakultas Teknologi Informasi dan Komunikasi Universitas Semarang. Dengan *freeware* ini, kebutuhan mengoptimalkan register dan proses pemantauan sudah terpenuhi, tetapi kebutuhan untuk melihat informasi tentang *port* jaringan dengan status terbuka (*open port*) belum dapat diakomodasi, sehingga memerlukan perangkat lunak lain yang membantu *administrator* dalam pemantauan *Local Area Network* (LAN).

Dalam penelitian ini, peneliti akan mencoba untuk menambahkan konfigurasi baru ke Mandau Registry Tools and Information System dengan modifikasi layanan statistik jaringan yang berfokus pada pemantauan *port* jaringan komputer yang belum ada sebelumnya di dalam Mandau Registry Tools and Information System. Peneliti telah mengumpulkan informasi tentang data yang diperlukan untuk pemantauan *port* dari beberapa perangkat lunak yang telah digunakan dalam penelitian terdahulu pada Tabel 2 seperti NMAP, Advanced Port Scanner, dan Atelier Web Security Port Scanner untuk menambahkan konfigurasi baru di Mandau Registry Tools and Information System. Dengan modifikasi ini, maka hasil penelitian ini akan membangun suatu sistem baru yang terintegrasi dengan fitur yang lengkap, lebih efektif, dan efisien untuk membantu pekerjaan *administrator*. Selain itu akan dilakukan *Access Control Lists* (ACLs) terhadap alamat IP yang pernah melakukan serangan terhadap Local Area Network (LAN) di Fakultas Teknologi Informasi dan Komunikasi (FTIK) Universitas Semarang. Dengan menggunakan tahap perencanaan, analisis sistem, perancangan sistem, implementasi sistem, dan pengujian sebagai metode pengembangan sistem, diharapkan hasil dari penelitian ini akan memudahkan *administrator* dalam pemantauan *port* dan proses serta melakukan *Access Control Lists* (ACLs) pada *Local Area Network* (LAN) di Fakultas Teknologi Informasi dan Komunikasi (FTIK) Universitas Semarang melalui data statistik *port* jaringan komputer yang dihasilkan oleh sistem baru dalam penelitian ini sehingga *Local Area Network* (LAN) lebih aman daripada sebelumnya.

II. LANDASAN TEORI

A. *Pemantauan Jaringan Komputer*

Pemantauan lalu lintas jaringan adalah hal yang paling penting yang harus dilakukan oleh *administrator* jaringan. Dengan mendapatkan kondisi lalu lintas yang kompleks di dalam jaringan, banyak manfaat yang dapat diperoleh. Dengan pemantauan lalu lintas jaringan, hasilnya dapat digunakan untuk tujuan pemecahan masalah, tujuan pemeliharaan, tujuan penelitian, pemantauan keamanan jaringan, dan pemantauan virus yang masuk [9].

Apalagi ketika jaringan terhubung dengan *internet*, pemantauan lalu lintas jaringan harus dijalankan. Misalnya penggunaan lalu lintas *internet broadband* akan sangat berguna untuk memantau tren penggunaan koneksi *internet* dalam jaringan. Pemantauan lalu lintas jaringan adalah langkah pertama untuk mengetahui informasi lebih dalam tentang jaringan komputer yang ada [10].

Untuk melakukan pemantauan lalu lintas jaringan, langkah pertama yang harus diambil adalah menentukan titik pusat dimana aktivitas jaringan tersebut. Jika berbagi *internet* dalam jaringan, titik pusat jaringan ada terdapat pada komputer *server* yang memiliki tugas untuk membagi *bandwidth* layanan *internet*. Pada *server* ini, tempat yang paling tepat untuk memasang perangkat lunak pemantau jaringan. karena lalu lintas keluar masuk data pada titik *server* ini akan mewakili jumlah penggunaan *internet* pada *Local Area Network* (LAN).

B. *Statistik Jaringan Komputer*

Statistik jaringan digunakan untuk menampilkan data koneksi TCP yang aktif, *port* yang terdapat pada komputer, statistik *Ethernet*, tabel *routing* IP, statistik IPv4 (protokol IP, ICMP, TCP, dan UDP), dan statistik IPv6 (protokol IPv6, ICMPv6, TCP *over* IPv6, dan UDP *over* IPv6). Data statistik ini digunakan *administrator* dalam proses pemantauan jaringan komputer [11].

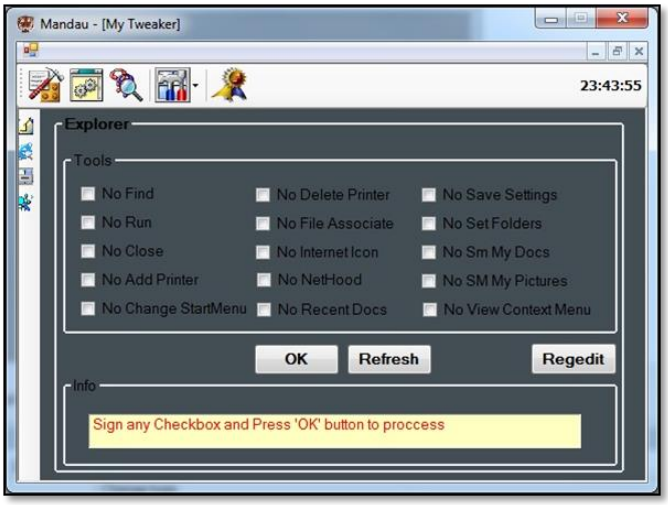
C. *Tracert (Traceroute)*

Menunjukkan rute yang dilewati paket untuk mencapai tujuannya. Hal ini dilakukan dengan mengirim pesan *Internet*

Control Message Protocol (ICMP) *Echo Request* ke tujuan dan nantinya akan menghasilkan nilai *Time to Live* yang semakin meningkat. Rute yang ditampilkan adalah daftar *interface router* (titik yang paling dekat dengan *host*) pada *Local Area Network* (LAN) antara komputer *host* dan komputer tujuan [12].

D. *Mandau Registry Tools and Information System*

Sistem ini adalah alat *freeware open source* berbasis Windows yang dapat dikelola sesuai dengan kebutuhan dalam jaringan komputer. Mandau Registry Tools and Information System berisi perangkat lunak untuk meningkatkan kinerja komputer, *task manager*, sistem informasi, dan statistik jaringan yang diperlukan *administrator* untuk memantau komputer *server* atau *Local Area Network* (LAN). Terdapat lebih dari 30 (tiga puluh) trik untuk memanipulasi register Windows yang tentu saja digunakan untuk meningkatkan kinerja komputer [13]. Tampilan Mandau Registry Tools and Information System ditunjukkan pada Gambar 1.



Gambar 1. Mandau Registry Tools and Information System

Tampilan pada Gambar 1 adalah halaman antar muka Mandau Registry Tools and Information System. Dalam perangkat lunak ini belum terdapat fitur untuk pemantauan proses dan statistik *port* dalam jaringan. Tetapi karena sifatnya yang *freeware open source*, sehingga perangkat lunak ini dapat dimodifikasi sesuai kebutuhan pengguna. Penelitian ini akan memodifikasi Mandau Registry Tools and Information System dengan penambahan fitur pemantauan proses dan statistik jaringan sehingga menjadi suatu perangkat lunak terintegrasi yang *powerful* untuk membantu permasalahan yang dialami *administrator* di Fakultas Teknologi Informasi dan Komunikasi (FTIK) Universitas Semarang.

III. METODOLOGI PENELITIAN

A. *Jenis Penelitian*

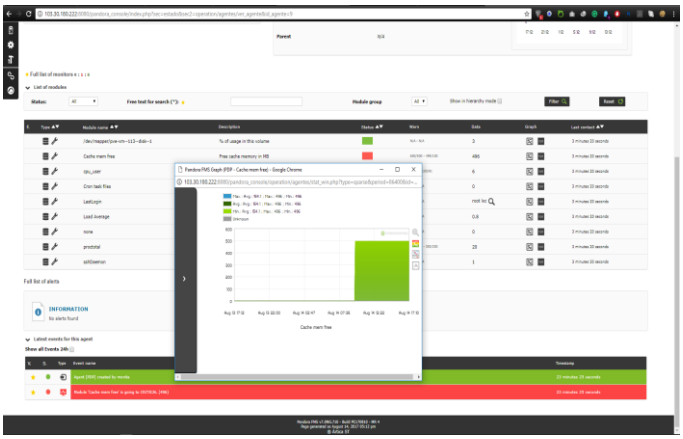
Penelitian ini termasuk jenis penelitian rekayasa, yang merupakan kegiatan perancangan non-rutin dengan kontribusi baru baik dalam proses maupun dalam bentuk produk [14]. Menggunakan rekayasa ulang yaitu perubahan dan reorganisasi komponen sistem yang dapat dilakukan pada desain atau implementasi pada tahap abstraksi sistem tanpa menghilangkan seluruh komponen lama dalam rangka mendapatkan metode, rumus, model, prototipe, produk, sistem, atau alat dengan tingkat kesempurnaan dan standar yang lebih tinggi.

Penelitian ini akan melakukan modifikasi terhadap Mandau Registry Tools and Information System dengan menambahkan sistem baru pada *freeware* ini dengan sistem pemantauan *port* jaringan komputer sehingga menjadi sistem yang lebih efektif dan *powerful* untuk membantu *administrator* sebagai manajer sumber daya *Local Area Network* (LAN) dan menjaga stabilitas jaringan komputer.

B. *Metode Pengumpulan Data*

Pengumpulan data dalam penelitian ini diawali dengan dokumentasi, pengumpulan data melalui literatur, dan pemahaman buku serta *internet* sebagai acuan untuk menentukan landasan teori. Peneliti mengumpulkan data literatur tentang pemantauan jaringan komputer, statistik jaringan komputer, dan *tools* pemantauan *port* pada jaringan komputer dari penelitian terdahulu yang pernah dilakukan yang terdapat dalam Tabel 2.

Sedangkan studi literatur lain yang dilakukan adalah mereferensi pula beberapa penelitian lain yang telah dilakukan tentang pemantauan (*monitoring*) jaringan komputer karena hal ini adalah merupakan *state of the art* dalam penelitian ini. Literatur yang dipelajari adalah tentang penelitian dengan memanfaatkan Nagios untuk memantau *server* [15], penelitian lain menggunakan sistem pemberitahuan menggunakan layanan *email* untuk mengirim pemberitahuan pemantauan *server* kepada *administrator* [16], dan penelitian tentang API's *channel* untuk mengirim pesan tentang pemantauan jaringan *cloud computing* [17]. Dari studi literatur didapatkan data mengenai lalu lintas (*traffic*) data normal di dalam jaringan komputer tanpa terjadi serangan jaringan. *Capture* dari *monitoring* lalu lintas data jaringan tersebut terdapat pada Gambar 2 berikut.



Gambar 2. *Capture* dari *Monitoring* Lalu Lintas Data Normal Tanpa Serangan [18]

Dari Gambar 2 tersebut dapat digunakan sebagai acuan bahwa jika terdapat serangan di dalam *Local Area Network* (LAN), maka lalu lintas data jaringan akan naik secara signifikan.

Metode pengumpulan data lain adalah dilakukan observasi dengan merekam langsung tentang hal-hal yang perlu diselidiki. Dalam penelitian ini, observasi dilakukan dengan survey dan wawancara dengan *administrator* Fakultas Teknologi Informasi dan Komunikasi (FTIK) Universitas Semarang. Dalam survey menghasilkan data topologi jaringan yang terdapat dalam Gambar 3 dan wawancara menghasilkan data terkait dengan kebutuhan sistem pemantauan dalam jaringan komputer untuk keamanan *Local Area Network* (LAN) karena sudah terdapat beberapa serangan yang terjadi dalam kurun waktu 2017-2018. Data serangan ini terdapat pada Tabel 1. Sehingga kebutuhan terbesar dari survey dan wawancara ini adalah sistem pemantauan dengan banyak fitur untuk pemantauan proses dan *port* jaringan yang terintegrasi dalam 1 (satu) perangkat lunak.

C. Metode Pengembangan Sistem

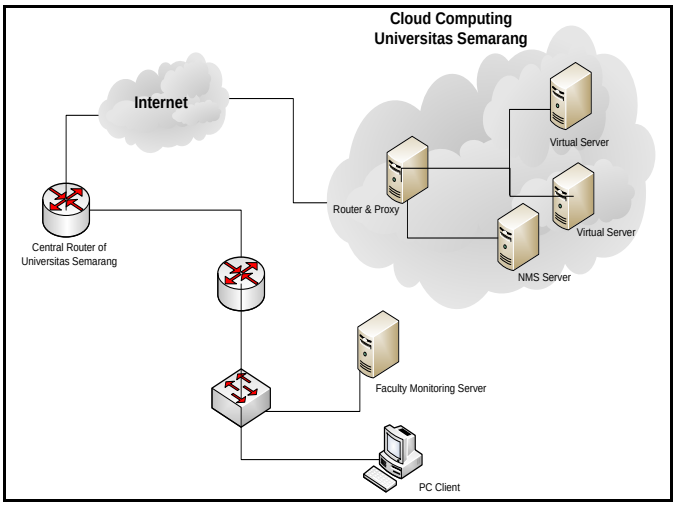
- Perencanaan

  Tahap ini berisi langkah-langkah untuk mengidentifikasi masalah, menentukan tujuan untuk pemecahan masalah, mengidentifikasi hambatan umum, dan mempelajari teknologi. Pada tahap ini peneliti melakukan survei dan wawancara kepada *administrator* jaringan komputer Universitas Semarang tentang masalah yang sering terjadi di jaringan komputer. Hal yang sering terjadi adalah sulitnya mendeteksi ketika ada kerusakan dan serangan pada jaringan komputer terutama tentang data status *port* yang terbuka di *Local Area Network* (LAN). Data yang diperoleh pada tahap ini adalah data statistik jaringan Universitas Semarang yang terdapat pada Gambar 2 dan data serangan jaringan pada Tabel 1.

- Analisa Sistem

  Tahapan ini berisi langkah-langkah dalam menganalisis data, menentukan kebutuhan informasi, dan menentukan kinerja sistem.

  Dari hasil tahap sebelumnya, terdapat masalah mengenai kendala *administrator* dalam memantau proses dan statistik *port* jaringan komputer saat terjadi beberapa gangguan yang terjadi. Dari masalah-masalah ini dapat dianalisis bahwa solusi dari masalah adalah sistem yang dapat memantau jaringan dan memberikan informasi rinci dengan banyak fitur yang terintegrasi dalam satu perangkat lunak. Modifikasi dari Mandau Registry Tools and Information System tentang pemantauan *port* jaringan akan menghasilkan sistem baru yang lebih efektif dan *powerful* sehingga menjadi solusi tepat dalam masalah yang terjadi di Fakultas Teknologi Informasi dan Komunikasi (FTIK) Universitas Semarang. Untuk merealisasikan sistem ini perlu diperhatikan terlebih dahulu topologi jaringan yang ada di Universitas Semarang sehingga sistem baru yang dihasilkan dalam penelitian ini dapat ditempatkan secara efektif. Hasil observasi ini ditunjukkan pada Gambar 3 berikut.



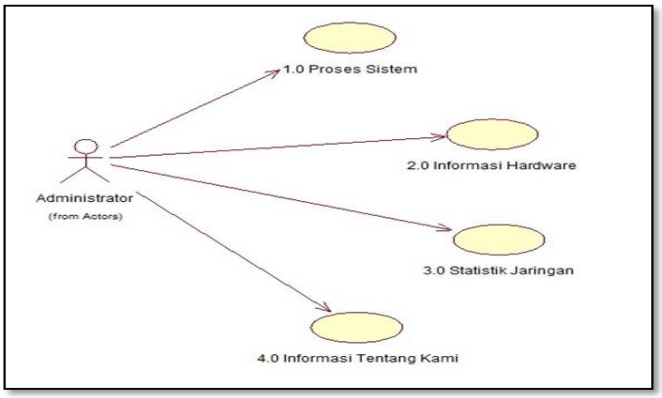
Gambar 3. Topologi Jaringan Universitas Semarang

Gambar 3 adalah hasil observasi topologi jaringan di Universitas Semarang. *Server* pusat Universitas Semarang berada dalam jaringan *cloud computing*, sedangkan setiap fakultas memiliki *dedicated server* sendiri untuk kebutuhan internal fakultas. Sistem baru yang dihasilkan dari penelitian ini akan ditempatkan pada komputer *server* setiap fakultas di Universitas Semarang yang nantinya akan dioperasikan oleh *administrator*.

- Desain Sistem

  Tahap selanjutnya adalah desain yang merupakan langkah-langkah untuk menyiapkan detail sistem. Kemudian mengidentifikasi alternatif konfigurasi untuk sistem yang dibangun diikuti dengan evaluasi konfigurasi dan akhirnya memilih konfigurasi terbaik.

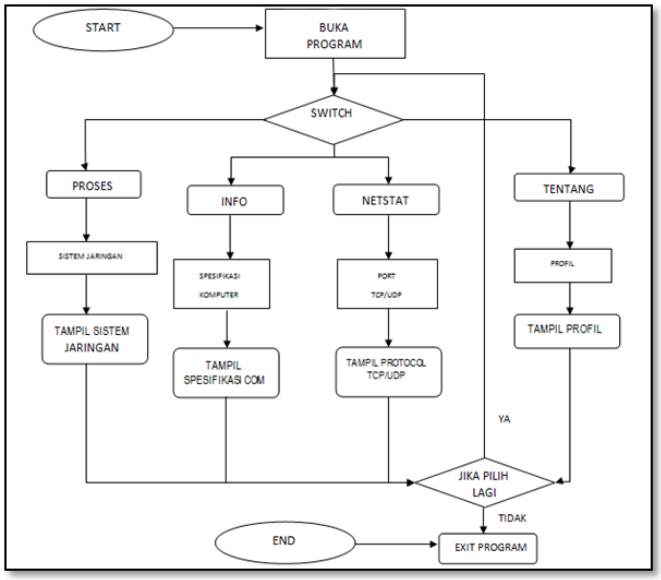
  Pada tahap ini, beberapa desain dilakukan untuk membangun sistem baru yang dalam hal ini menggunakan diagram *use case* dan desain aliran data dengan *flowchart*. Sistem desain dengan diagram *use case* dalam penelitian ini ditunjukkan pada Gambar 4.



Gambar 4. *Use Case* Diagram Sistem

Use case diagram sistem yang ditunjukkan pada Gambar 4 menggambarkan bahwa terdapat 1 (satu) aktor yaitu *Administrator* yang menjalankan sistem dan dapat mengakses menu proses sistem operasi, mengakses perangkat keras dan informasi dari *server*, mengakses statistik jaringan, serta mengakses informasi tentang kami, yaitu informasi tentang pembangun sistem.

Selanjutnya adalah desain aliran data dalam sistem baru menggunakan *flowchart*. Untuk *flowchart* sistem ditunjukkan pada Gambar 5.



Gambar 5. *Flowchart* Sistem

Gambar 5 adalah desain *flowchart* dalam sistem yang akan dibangun. Penjelasan gambar tersebut diawali dengan menu PROSES yang merupakan data hasil proses aliran data dalam sistem operasi di dalam jaringan komputer. Sedangkan pada menu INFO akan menampilkan data dari spesifikasi komputer *server*. Menu NETSTAT menampilkan data *port* dan protokol jaringan komputer yang digunakan baik menggunakan TCP atau UDP. Dan menu terakhir dari bagan alur dalam sistem ini adalah TENTANG adalah informasi tentang pembuat sistem.

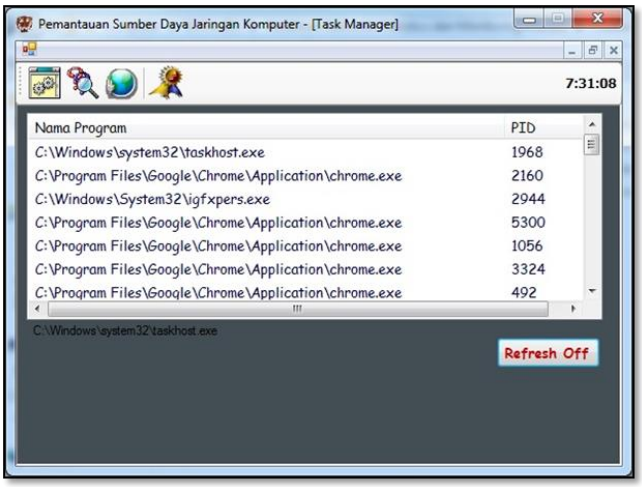
- Implementasi dan Pengujian

  Tahap selanjutnya adalah implementasi dan pengujian sistem. Penjelasan tahap ini terdapat pada Bab IV Hasil dan Pembahasan.

IV. HASIL DAN PEMBAHASAN

Pembahasan ini berisi implementasi desain sistem dan diskusi tentang pengujian sistem. Implementasi dan pengujian sistem ini dijelaskan melalui *print screen* gambar pada setiap halaman aplikasi dan tabel hasil analisa disertai dengan penjelasannya.

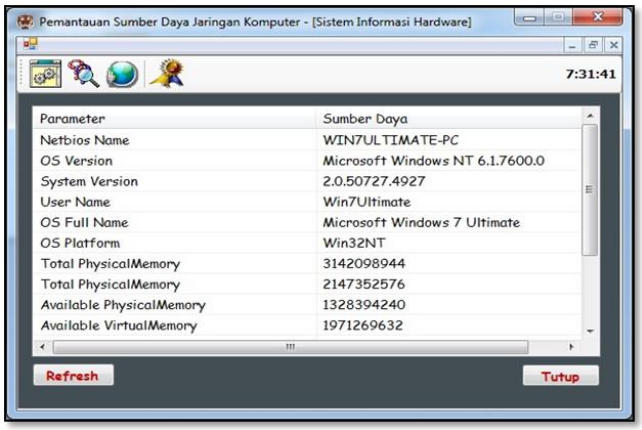
Hasil dari penelitian ini menghasilkan beberapa fasilitas yaitu pemantauan proses pada sistem operasi, sistem pemantauan perangkat keras, dan sistem pemantauan jaringan. Fasilitas pertama dari sistem ini adalah halaman untuk memantau proses yang terjadi di sistem operasi. Halaman ini sudah disediakan oleh Mandau Registry Tools and Information System. Penjelasan ini ditemukan pada Gambar 6.



Gambar 6. Halaman Proses Sistem Informasi

Halaman proses sistem operasi yang terdapat pada Gambar 6 adalah fasilitas yang digunakan untuk pemantauan proses pada sistem operasi. Fungsionalitas halaman ini mirip dengan Windows Task Manager.

Fasilitas lain yang terdapat dalam sistem pemantauan jaringan komputer ini adalah informasi tentang perangkat keras komputer. Fasilitas ini ditunjukkan pada Gambar 7.

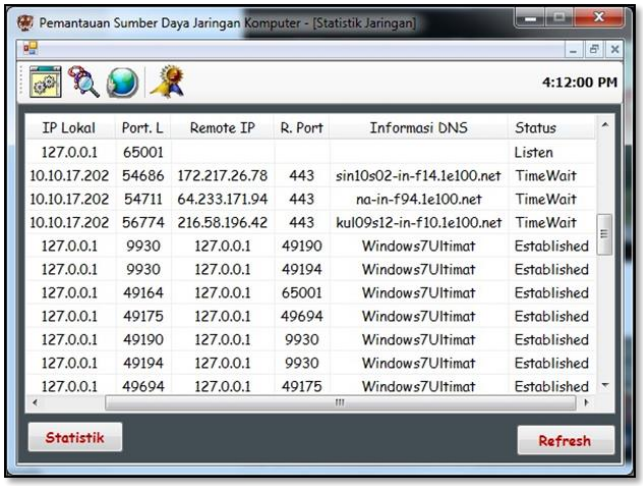


Gambar 7. Halaman Informasi *Hardware*

Gambar 7 berisi informasi rinci tentang perangkat keras *server* komputer. Informasi pada halaman ini antara lain jenis sistem operasi, kondisi RAM, dan kondisi *harddisk* yang membantu *administrator* dalam memantau kondisi perangkat keras.

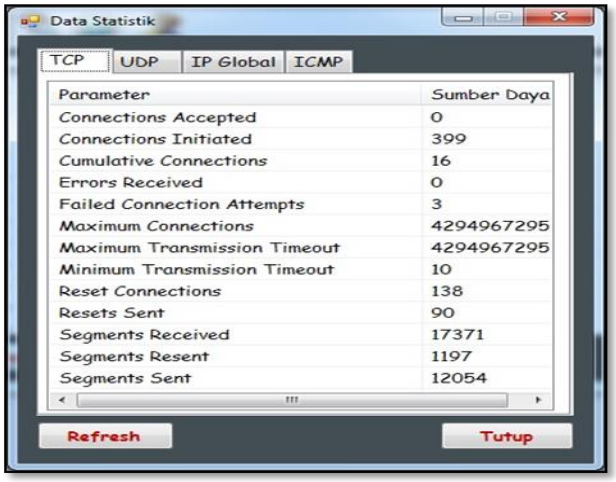
Fasilitas tambahan yang dihasilkan dari modifikasi Mandau Registry Tools and Information System dalam penelitian ini

adalah halaman statistik jaringan yang berfokus pada pemantauan *port* jaringan komputer lengkap dengan status *port* tersebut, protokol yang digunakan, dan informasi DNS. Hasil dari fasilitas ini ditunjukkan pada Gambar 8.



Gambar 8. Hasil Modifikasi (Halaman Statistik *Port* Jaringan)

Gambar 8 adalah fasilitas untuk melihat informasi tentang statistik *port*. Sistem dan fitur baru yang dihasilkan dalam penelitian ini dapat memindai 65.536 *port* dan memantau sekitar *port* dengan status terbuka. Terdapat beberapa status *port* di *Local Area Network* (LAN) yang "*Listen*" di *port* 65001 yang berarti *port* tersebut siap untuk terhubung. Sementara beberapa *port* memiliki status "*Time Wait*" seperti pada *port* 54686, 54711, dan 56774 yang berarti bahwa *port* sedang menunggu koneksi *internet* dari IP lain. Sementara status "*Established*" digunakan pada *port* yang sedang melakukan transfer data. Status lain adalah "*Open*" yang berarti *port* tersebut perlu penanganan keamanan lebih lanjut. Fitur lain di halaman ini yaitu terdapat pula tombol statistik yang merupakan fitur yang digunakan untuk melihat informasi rinci tentang TCP, UDP, dan protokol IP yang digunakan. Penjelasan ini ditemukan pada Gambar 9.



Gambar 9. Hasil Modifikasi (Halaman Statistik Data)

Halaman pada Gambar 9 adalah informasi terperinci yang perlu diketahui *administrator* tentang protokol yang digunakan, IP yang digunakan, dan informasi *ping* jaringan menggunakan protokol ICMP.

Setelah tahap perencanaan, analisis, desain, dan implementasi telah dilaksanakan, maka pada tahap akhir dalam penelitian ini adalah metode pengujian sistem agar sistem yang dibangun dapat berjalan dengan baik dan sesuai dengan tujuan penelitian. Fase pengujian sistem menjadi tolok ukur peneliti untuk mengakomodir kebutuhan *administrator* jaringan komputer di Universitas Semarang. Kriteria yang digunakan untuk menguji sistem baru di sini akan menggunakan metode validasi untuk membuktikan validitas sistem yang akan digunakan oleh *administrator*. Hasil tahap ini tercantum dalam Tabel 3 berikut ini.

TABLE III. HASIL PENGUJIAN SISTEM

Poin yang Diuji	Validasi *Input*	Hasil Pengujian
Menu Proses	Klik Mouse	Muncul proses yang sedang berjalan di sistem operasi
Menu Informasi	Klik Mouse	Muncul informasi perangkat keras
Menu Statistik Jaringan	Klik Mouse	Muncul statistik port, IP, dan data DNS
Menu Tentang Kami	Klik Mouse	Muncul informasi pembuat sistem
Tombol Statistik pada Menu Statistik Jaringan	Klik Mouse	Muncul informasi TCP, UDP, dan ICMP data protokol

Hasil dari pengujian terhadap sistem baru hasil modifikasi dari Mandau Registry Tools and Information System pada Tabel 3 adalah bahwa sistem yang dibangun berfungsi dengan baik.

Tahap pengujian lain adalah membandingkan pula kemampuan sistem baru yang dihasilkan dalam penelitian ini dengan sistem perangkat lunak pemantauan *port* yang digunakan dalam penelitian-penelitian sebelumnya. Data komparasi perangkat lunak tersebut terdapat pada Tabel 4.

TABLE IV. DATA KOMPARASI SOFTWARE

Software	*Port* Terpantau	*Port* Terbuka	Waktu	Antar Muka	*Platform*
NMAP	65536	15	102	Command line, GUI	Linux, Windows, Mac Os
Advanced Port Scanner	65536	9	109	Command line, GUI	Linux, Windows
Atelier Web Sequrity Port Scanner	65536	4	95	Command line, GUI	Linux, Windows, Mac Os
Mandau Registry Tools and Information System ***(Custom Configuration)***	65536	11	114	GUI	Windows

Hasil pengujian komparasi dengan perangkat lunak lain pada Tabel 4 membuktikan bahwa NMAP adalah *tools* terbaik dalam pemantauan *port* jaringan, tetapi belum menjawab tujuan dan permasalahan dalam penelitian ini yaitu kebutuhan akan sistem yang terintegrasi dengan fitur yang lengkap, lebih efektif, dan efisien untuk membantu pekerjaan *administrator* karena NMAP belum mempunyai fitur untuk memantau kondisi *hardware* dan sistem operasi seperti yang dimiliki Mandau Registry Tools and Information System.

Dari hasil modifikasi Mandau Registry Tools and Information System pada penelitian ini menghasilkan sistem baru yang memiliki fitur lebih lengkap untuk pemantauan proses, pemantauan *hardware*, pemantauan sistem operasi, serta pemantauan *port* jaringan komputer. Sistem baru hasil modifikasi Mandau Registry Tools and Information System mempunyai performa yang cukup baik pula dalam hal pemantauan *port* terbuka yaitu sejumlah 11 saat *scanning* dilakukan dengan jumlah seluruh *port* yang terpantau berjumlah 65536 buah sehingga kebutuhan akan pemantauan *port* jaringan dapat terpenuhi dengan akurat. Selain itu integrasi fitur yang telah dibangun dari modifikasi Mandau Registry Tools and Information System dalam penelitian ini membuktikan bahwa performa dari sistem baru dapat dikatakan cukup baik jika dibandingkan dengan *tools* pemantauan *port* lain seperti NMAP. Hal ini dapat dapat dibuktikan dari hasil pengujian dalam penelitian ini yang terdapat pada Tabel 3 dan Tabel 4.

Setelah melakukan *scanning por*t dengan sistem baru hasil penelitian ini, maka *administrator* dapat melakukan *discover open port* melalui *router* dan melakukan *Access Control Lists* (ACLs) terhadap alamat IP yang pernah melakukan serangan terhadap *Local Area Network* (LAN) di Fakultas Teknologi Informasi dan Komunikasi (FTIK) Universitas Semarang. Dalam penelitian ini telah dibangun pula suatu sistem untuk melakukan *Access Control Lists* (ACLs) menggunakan Fail2Ban. Hasil *banned* IP yang telah melakukan serangan terhadap *Local Area Network* (LAN) selama 1 (satu) hari yaitu pada tanggal 27 September 2018 terdapat pada Gambar 10.

```
2018-09-27 15:54:51,847 fail2ban.actions: WARNING [ssh] Ban 125.65.42.178
2018-09-27 16:00:33,461 fail2ban.actions: WARNING [ssh] Unban 106.43.254.90
2018-09-27 16:09:06,055 fail2ban.actions: WARNING [ssh] Ban 61.184.247.2
2018-09-27 16:14:38,641 fail2ban.actions: WARNING [ssh] Unban 125.65.42.179
2018-09-27 16:19:04,953 fail2ban.actions: WARNING [ssh] Ban 61.184.247.7
2018-09-27 16:22:06,403 fail2ban.actions: WARNING [ssh] Unban 137.74.148.234
2018-09-27 16:25:39,653 fail2ban.actions: WARNING [ssh] Unban 125.65.42.180
2018-09-27 16:27:22,777 fail2ban.actions: WARNING [ssh] Unban 61.184.247.6
2018-09-27 16:31:04,034 fail2ban.actions: WARNING [ssh] Unban 61.184.247.8
2018-09-27 16:36:17,394 fail2ban.actions: WARNING [ssh] Ban 116.31.116.51
```

Gambar 10. Hasil *Access Control Lists* (ACLs)

Dari Gambar 10 dapat dibuktikan bahwa sistem keamanan *Local Area Network* (LAN) di Fakultas Teknologi Informasi dan Komunikasi (FTIK) Universitas Semarang menjadi lebih baik dan aman daripada sebelumnya dengan implementasi pemantauan proses, pemantauan *hardware*, pemantauan sistem operasi, serta pemantauan *port* jaringan komputer hasil modifikasi Mandau Registry Tools and Information System serta penerapan *Access Control Lists* (ACLs) terhadap alamat IP yang pernah melakukan serangan dengan Fail2Ban.

V. PENUTUP

Setelah mengamati hasil penelitian eksperimental dengan menggunakan beberapa rangkaian hasil evaluasi yang menghasilkan sistem pemantauan statistik *port* pada *Local Area Network* (LAN) dan implementasi *Access Control Lists* (ACLs) terhadap alamat IP yang pernah melakukan serangan, peneliti dapat menarik kesimpulan bahwa sistem hasil penelitian ini dapat digunakan untuk memberikan informasi rinci tentang kondisi *Local Area Network* (LAN) terutama dalam hal pemantauan *port* jaringan. Dengan modifikasi Mandau Registry Tools and Information System dari yang semula merupakan sistem untuk implementasi pemantauan proses, pemantauan *hardware*, dan pemantauan sistem operasi menjadi sistem yang lebih lengkap dengan penambahan fitur baru yaitu pemantauan *port* jaringan komputer. Sistem ini dapat membantu *administrator* dalam proses deteksi kerusakan dan serangan dengan melihat status dan jumlah *port* terbuka yang dihasilkan oleh sistem ini karena memiliki sensitivitas tinggi terhadap status *port* terbuka. Selain itu dengan implementasi *Access Control Lists* (ACLs) terhadap alamat IP yang pernah melakukan serangan membuat *Local Area Network* (LAN) di Fakultas Teknologi Informasi dan Komunikasi (FTIK) Universitas Semarang menjadi lebih baik dan aman daripada sebelumnya.

Penelitian yang telah dilakukan masih belum dapat dikatakan sempurna, sehingga masih diperlukan beberapa pengembangan lebih lanjut untuk mendapatkan hasil yang maksimal. Dari hasil komparasi perangkat lunak yang dilakukan pada Tabel 4, beberapa saran pengembangan yang dapat dilakukan antara lain adalah sistem operasi yang kompatibel selain sistem operasi Windows, waktu pemindaian *port* lebih cepat, dan penambahan fitur sistem seperti pemantauan jenis serangan yang melanda *Local Area Network* (LAN).

UCAPAN TERIMAKASIH

Terimakasih kepada Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Semarang yang telah membiayai penelitian ini dengan kontrak penelitian nomor : 298/USM.H9/L/2017.

DAFTAR PUSTAKA

[1] R. Weaver, "Identifying Anomalous Port-Specific Network Behavior," *Program*, no. May, 2010.

[2] S. M. Musa, J. Shepard, and C. M. Akujuobi, "Nonconventional Network Security Measures for Intrusion Detection," *Ijasre*, vol. 3, no. 9, pp. 48–58, 2017.

[3] M. J. Arshad *et al.*, "A Study of Internet Threats, Avoidance, and Biometric Security Techniques-Comparison of Biometric Techniques," *J. Fac. Eng. Technol.*, vol. 21, no. 2, pp. 135–146, 2014.

[4] N. El-nazeer and K. Daimi, "Evaluation of Network Port Scanning Tools," 2011.

[5] T. A. Ahanger, "Port Scan - A Security Concern," *Int. J. Eng. Innov. Technol.*, vol. 3, no. 10, pp. 241–246, 2014.

[6] R. Kaur and G. Singh, "Analysing Port Scanning Tools and Security Techniques," vol. 1, no. 5, pp. 58–64, 2014.

[7] J. Biswas, "An Insight in to Network Traffic Analysis using Packet Sniffer ANALYSIS : DISCUSSION ON WHERE," vol. 94, no. 11, pp. 39–44, 2014.

[8] A. Rahman, K. R. Kawshik, A. A. Sourav, and A. Gaji, "Advanced Network Scanning," no. 6, pp. 38–42, 2016.

[9] W. Wang and S. Lian, "Network Traffic Monitoring, Analysis and Anomaly Detection," *Netw. Traffic Monit. Anal. Anom. Detect.*, no. June, pp. 6–7, 2011.

[10] P. Aar and A. K. Sharma, "Analysis of Penetration Testing Tools," no. 9, pp. 36–41, 2017.

[11] M. Nunes, "Statistical Analysis of Network Data with R," *J. Stat. Softw.*, vol. 66, no. August, pp. 1–6, 2015.

[12] E. Zam, "Buku Sakti Wireless Hacking," 2016.

[13] P. S. Code, "PlanetSourceCode, 'Update: Mandau (Registry Tools and Information System Include Netstat)', [Online], Available : http://www.planet-source-code.com/vb/scripts/ShowCode.asp?txtCodeId=5249&lngWId=10, [accessed on August 30, 2017].," p. 5249, 2017.

[14] J. W. Creswell, *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*, vol. 4. 2012.

[15] R. Khan, "An Efficient Network Monitoring and Management System," *Int. J. Inf. Electron. Eng.*, vol. 3, no. 1, 2013.

[16] P. C. S. Nimodia and P. S. S. Asole, "A Survey on Network Monitoring and Administration Using Email and Android Phone," vol. 3, no. 4, pp. 83–87, 2013.

[17] F. Wahyu and M. Sani, "Enhancement Network Monitoring System Functionality by Implementing an Android-based Notification System to Monitor Virtual Servers on Cloud Computing Network," vol. 02, no. 01, pp. 0–3, 2018.

[18] F. W. Christanto *et al.*, "Pemantauan Sumber Daya Virtual Server Pada Cloud Computing Universitas Semarang Menggunakan Network," *SIMETRIS (Jurnal Tek. Mesin, Elektro, dan Ilmu Komputer)*, vol. 8, no. 2, pp. 629–638, 2017.