



**RANCANG BANGUN SISTEM MAINTENANCE KEAMANAN JARINGAN
KOMPUTER BERBASIS WEB PADA KANTOR BKN REGIONAL VI
MEDAN**

Disusun Dan Diajukan Untuk Memenuhi Persyaratan Ujian Akhir
Memperoleh Gelar Sarjana Komputer Pada Fakultas Sains Dan Teknologi
Universitas Pembangunan Panca Budi
Medan

SKRIPSI

OLEH

NAMA : RAHMA DAYANI
N.P.M : 1414370349
PROGRAMSTUDI : SISTEM KOMPUTER

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

ABSTRAK

RAHMA DAYANI
RANCANG BANGUN SISTEM MAINENANCE KEAMANAN JARINGAN
KOMPUTER BERBASIS WEB PADA KANTOR BKN REGIONAL VI
MEDAN
2019

Monitoring jaringan komputer adalah proses pengumpulan dan melakukan analisis terhadap data – data yang terjadi pada lalu lintas jaringan. Pada penelitian ini dirancang sebuah aplikasi monitoring yang berbasis website yang diimplementasikan dalam jaringan BKN Sumut yang bertujuan untuk memonitor kondisi trafik dengan parameter pengukuran yaitu: IPS (*Intrusion Prevention System*), koneksi, dan tidak koneksi. Metode yang digunakan adalah IPS (*Intrusion Prevention System*) sebagai metode pengamanan pada jaringan lokal. Adapun tujuan dari penelitian ini adalah menghasilkan sebuah hal ternatif sistem maintenance keamanan jaringan komputer secara local yang di kantor BKN Regional VI Medan dan membantu upaya pembuatan sistem maintenance dan keamanan jaringan untuk melakukan pencegahan terjadinya peretasan legal di Kantor BKN Regional VI Medan. Dari hasil penelitian ini dapat disimpulkan bahwa kondisi jaringan di BKN Sumut masih dalam kategori normal dan dengan adanya website monitoring jaringan ini pihak BKN menjadi mudah dalam monitoring jaringan.

Kata kunci : BKN Regional VI Medan, Firewall Keamanan Jaringan Komputer, Monitoring Jaringan.

DAFTAR ISI

	Halaman
LEMBAR JUDUL	
LEMBAR PENGESAHAN	
ABSTRAK	
KATA PENGANTAR.....	i
DAFTAR ISI.....	iii
DAFTAR GAMBAR.....	vi
DAFTAR TABEL.....	vii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Metodologi Penelitian	5
1.7 Sistematika Penulisan.....	7
BAB II LANDASAN TEORI	9
2.1 Kamanan Komputer	9
2.2 <i>Intrusion Prevention System</i>	9
2.3 <i>Intrusion Detection System</i>	10
2.4 <i>Firewall</i>	11
2.5 Jenis Serangan pada Sistem Komputer.....	13
2.5.1 Spoofing.....	14
2.5.2 Ddos.....	14
2.5.3 <i>Denial of Servis</i>	15
2.5.4 <i>Information Theft</i>	16
2.6 Jenis Program Pencurian Informasi.....	16
2.6.1 <i>Sniffer</i>	16
2.6.2 <i>Intelligence</i>	16

2.6.3	<i>Back Door</i>	16
2.6.4	<i>Cyber Espionage</i>	17
2.6.5	<i>Social Engineering</i>	17
2.7	Jenis Penyerang.....	17
2.7.1	<i>Joyriders</i>	17
2.7.2	<i>Vandal</i>	17
2.7.3	<i>Hacker</i>	18
2.8	Metode Pendeteksi Intrusi.....	18
2.9	Jaringan Komputer.....	19
2.10	PPDIOO SISCO.....	22
2.11	<i>Unified Modeling Languager</i>	24
2.11.1	Bagian-Bagian UML	25
2.11.2	<i>Use Case Diagram</i>	27
2.11.3	<i>Class Diagram</i>	28
2.11.4	<i>Sequence Diagram</i>	29
2.11.5	<i>State Machine Diagram</i>	31
2.11.6	<i>Activity Diagram</i>	31
2.12	Bagian Alir.....	33
2.13	Web.....	34
2.14	PHP.....	35
2.15	MySql.....	36
2.16	Xampp.....	37
BAB III METODE PENELITIAN		39
3.1	Sistem Yang Sedang Berjalan.....	39
3.2	Analisis System yang di usulkan.....	40
3.3	Analisi kebutuhan Non-Fungsional.....	43
3.4	Diagram Konteks	44
3.5	Data Flow Diagram	45
3.6	Struktur Tabel.....	45
3.7	Entity Relationship Diagram.....	46
3.8	Perancangan Tampilan	47
3.8.1	Desain From Login.....	48
3.8.2	Desain From Halaman Admin.....	49
3.8.3	Desain From Halaman Monitoring.....	49

3.8.4 Desain From Halaman Tambah Client.....	50
3.8.5 Desain From Halaman Tambah Stasiun.....	50
BAB IV HASIL PENELITIAN DAN PEMBAHASAN.....	51
4.1 Implementasi Sistem	51
4.2 Tujuan Implementasi Sistem.....	51
4.3 Komponen Utama Dalam Sistem.....	51
4.3.1 <i>Hardware</i>	52
4.3.2 <i>Software</i>	52
4.3.3 <i>Brainware</i>	53
4.4 Tampilan Website	53
4.4.1 Tampilan Log In Sistem.....	53
4.4.2 Halaman Tampilan Halaman Admin.....	54
4.4.3 Halaman Tampilan Halaman Info Stasiun.....	55
4.4.4 Halaman Tampilan Halaman Daftar Stasiun.....	55
4.4.5 Halaman Tampilan Monitoring Stasiun.....	55
4.5 Pengujian <i>Black Box</i>	56
4.6 Kelebihan Dan Kekurangan Sistem	57
BAB V PENUTUP	58
5.1 Kesimpulan	58
5.2 Saran	58
DAFTAR PUSTAKA	
BIOGRAFI PENULIS	
LAMPIRAN	

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Ilustrasi Firewall	13
Gambar 2.2 <i>PPDIOO Cisco Lifecycle Service</i>	22
Gambar 2.3 Penampilan XAMPP	38
Gambar 3.1 Flowchart Maintenance Jaringan di BKN.....	41
Gambar 3.2 Diagram Konteks.....	44
Gambar 3.3 Data Flow Diagram Level 0.....	45
Gambar 3.4 Entity Relationship Diagram.....	46
Gambar 3.5 Rancangan Flow Map Monitoring Jaringan Website.....	47
Gambar 3.6 Rancangan Halaman Login	48
Gambar 3.7 Rancangan Halaman Admin	49
Gambar 3.8 Rancangan Tampilan Halaman Monitoring	49
Gambar 3.9 Rancangan Tampilan Halaman Tambah Client	50
Gambar 3.10 Rancangan Tampilan Halaman Tambah Stasiun	50
Gambar 4.1 Halaman Log In Account	54
Gambar 4.2 Halaman Admin.....	54
Gambar 4.3 Halaman Tampilan Halaman Info Stasiun.....	55
Gambar 4.4 Halaman Tampilan Halaman Daftar Stasiun.....	55
Gambar 4.5 Halaman Tampilan Halaman Monitoring Stasiun.....	56

DAFTAR TABEL

	Halaman
Tabel 2.1 <i>Use Case Diagram</i>	28
Tabel 2.2 <i>Class Diagram</i>	29
Tabel 2.3 <i>Sequence Diagram</i>	30
Tabel 2.4 <i>State Machine Diagram</i>	32
Tabel 2.5 <i>Activity Diagram</i>	32
Tabel 3.1 Tabel User	45
Tabel 3.2 Tabel Log	46
Tabel 3.3 Tabel Client	46
Tabel 4.1 Penguji <i>Black Box</i>	57

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan dalam bidang teknologi dan informasi semakin pesat, ini terbukti dengan semakin banyaknya manusia yang menggunakan layanan internet. Seiring dengan perkembangan internet yang sedemikian pesat menjadikan keamanan suatu data atau informasi pada server yang terhubung dengan publik menjadi sangatlah penting. Menurut Yusep, kerentanan terhadap serangan kejahatan lewat dunia maya di Indonesia masih terjadi. Pada 2012, jaringan internet negara indonesia mengalami lebih dari satu juta serangan. Serangan itu berupa pencurian data, pemalsuan data, pengubahan data (misalnya halaman muka situs web), *phising*, pembocoran data, spionase industri, penyalahgunaan data oleh orang dalam, dan kejahatan.

Keamanan jaringan komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya (Arriyus, 2007). Keamanan sebuah jaringan komputer dapat dikelompokkan menjadi dua bagian yaitu keamanan yang bersifat fisik dan bersifat non fisik. Keamanan fisik lebih cenderung terhadap segala sesuatu yang berhubungan dengan fisiknya sedangkan keamanan non fisik adalah keamanan dimana suatu kondisi keamanan yang menitik beratkan pada kepentingan secara sifat, sebagai contoh yaitu pengamanan data, misalnya data sebuah perusahaan yang sangat penting. Keamanan suatu jaringan seringkali terganggu dengan

adanya ancaman dari dalam ataupun dari luar. Serangan tersebut berupa serangan hacker yang bermaksud merusak jaringan komputer yang terkoneksi pada internet ataupun mencuri informasi penting yang ada pada jaringan tersebut.

Selama ini keamanan pada jaringan lokal yang ada di sekitar kita kurang di perhatikan dari ancaman yang mungkin saja ada untuk merusak, maupun mencuri data yang ada di lingkungan kantor BKN Regional VI Medan dengan menggunakan perangkat pribadi, seperti *smartphone* mau pun *personal komputer* membuka peluang bagi para pelaku tindak kejahatan. Kejahatan yang di lakukan dapat berupa pengiriman paket data secara besar besaran, atau bisa di sebut *flooding* yang bertujuan mengganggu transmisi data di jaringan *sniffing*, yaitu tindakan untuk mencari data yang berada di jaringan untuk mendapatkan informasi yang memungkinkan rahasia bersifat *privacy*. Karyawan maupun Pegawai yang terhubung di jaringan lokal juga sering malakukan *folder sharing* untuk memudahkan mereka dalam pengiriman data yang tanpa di sadari telah membuka pertahanan perangkat mereka dengan mematikan *firewall* dan memberikan hak penuh untuk melakukan perubahan pada data mereka. Hal ini pula yang menyebabkan cepatnya penyebaran *virus* ataupun *malware* dalam sebuah jaringan dengan pertahan terbuka. Sudah tidak di pungkiri lagi bahwa pegawai atau karyawan pada saat ini banyak menggunakan sarana *electronic mail* biasa di sebut *e-mail* dalam kegiatan di duni maya, seperti untuk sekedar membuat akun sosial, mengirim tugas, maupun untuk sekedar bertukaran informasi. Tak jarang informasi yang di kirim merupakan penting yang bersifat rahasia seperti hasil penyidikan, data pribadi maupun data laporan. Dari

permasalahan dan atas maka tertarik untuk mengangkat judul “**RANCANG BANGUN SISTEM MAINTENANCE KEAMANAAN JARINGAN KOMPUTER BERBASIS WEB PADA KANTOR BKN REGIONAL VI MEDAN**”.

1.2 Rumusan Masalah

Pada pembuatan tugas akhir ini terdapat beberapa rumusan masalah. Hal ini dilakukan agar hasil penelitian sesuai dengan tujuan. Pada tugas akhir ini, Penulis merumuskan beberapa masalah antara lain:

- a. Bagaimana melakukan upaya untuk menghasilkan sebuah sistem keamanan pada jaringan komputer di lingkungan Kantor BKN Regional VI Medan?
- b. Bagaimana melakukan upaya maintenance pada jaringan komputer di lingkungan Kantor BKN Regional VI Medan?
- c. Bagaimana melakukan upaya peningkatan keamanan jaringan komputer di lingkungan Kantor BKN Regional VI Medan?

1.3 Batasan Masalah

Pada pembuatan tugas akhir ini terdapat beberapa batasan masalah. Hal ini disebabkan agar hasil penelitian sesuai dengan tujuan. Pada pembuatan tugas akhir ini penulis merumuskan beberapa masalah antara lain:

- a. Penelitian menggunakan IPS (*Intrusion Prevention System*) sebagai metode pengamanan pada jaringan lokal.
- b. Pengamanan dan maintenance hanya dilakukan pada jaringan komputer secara lokal yang ada di Kantor BKN Regional VI Medan.
- c. Tidak membahas keamanan secara fisik.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut yaitu:

1. Menghasilkan sebuah hal ternatif sistem maintenance keamanan jaringan komputer secara local yang di kantor BKN Regional VI Medan.
2. Melakukan upaya pembuatan sistem maintenance dan keamanan jaringan untuk melakukan pencegahan terjadinya peretasan legal di Kantor BKN Regional VI Medan.
3. Melakukan upaya pengawasan jaringan komputer local di kantor BKN Regional VI Medan.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut yaitu :

- a. Untuk mengaplikasikan ilmu yang telah diperoleh selama menempuh pendidikan di Universitas Pembangunan Panca Budi Medan dengan membuat laporan penelitian secara ilmiah dan sistematis.
- b. Dapat mengidentifikasi kebutuhan-kebutuhan informasi yang diperlukan untuk meningkatkan Keamanan Jaringan Komputer pada Kantor Bkn IV Medan
- c. Dapat di bangun sebuah sistem keamanan yang handal dalam pendeteksian dan pencegahan hal yang mengganggu Keamanan Jaringan Komputer pada Kantor BKN VI Medan sehingga tercipta rasa aman dalam melakukan kegiatan dalam dunia maya.

1.6 Metode Penelitian

Pada penelitian ini menggunakan pendekatan R&D (*Research and Development*), maka berikut ini adalah metode penelitiannya yaitu sebagai berikut:

a. Teknik Pengumpulan Data

Adapun beberapa teknik yang digunakan dalam pengumpulan data dari penelitian yaitu:

1) Observasi

Observasi merupakan teknik pengumpulan data dengan melakukan tinjauan langsung ke tempat studi kasus dimana akan dilakukan penelitian. Dalam hal ini peneliti melakukan observasi Kantor BKN Regional VI Medan.

2) Wawancara

Teknik wawancara ini dilakukan untuk mendapatkan informasi tambahan dari pihak-pihak yang memiliki wewenang dan berinteraksi langsung dengan sistem yang akan dirancang sebagai sumber data.

3) Studi Kepustakaan

Studi kepustakaan merupakan salah satu elemen yang mendukung sebagai landasan teoritis peneliti untuk mengkaji masalah yang dibahas. Dalam hal ini, peneliti menggunakan beberapa sumber kepustakaan diantaranya: Buku, Jurnal Nasional, Jurnal Internasional dan sumber-sumber lainnya.

b. Teknik Perancangan Sistem

Sesuai dengan rumusan masalah yang menggunakan pendekatan *Classic or Waterfall Algorithm* maka berikut ini adalah teknik perancangan sistem yang digunakan.

1) Analisis Masalah dan Kebutuhan

Mempelajari proses-proses identifikasi data-data yang dibutuhkan dalam perancangan suatu aplikasi informasi. Sehingga dapat memenuhi kebutuhan dan kemudahan dalam hal ini untuk meningkatkan pelayanan efisiensi dari keputusan.

c. Perancangan Sistem dan Pemodelan

Melakukan desain sistem secara detail, mulai dari *flowchart* sistem, *context* diagram, desain tabel dan lain sebagainya sehingga membentuk sistem lengkap sesuai dengan fungsi-fungsi yang dikehendaki.

d. Pengkodean

Melakukan *coding* untuk merealisasikan desain fungsi yang telah dibuat. Lama pengerjaan, kerumitan dan jumlah baris *coding*.

e. Percobaan

Melakukan beberapa testing dengan uji perilaku (*behavior testing*), fokus terhadap *input* dan *output* dan testing terhadap fungsionalitas sistem.

f. Implementasi

Sebelum aplikasi program dijalankan oleh user. Pihak pengembang juga berkewajiban memberikan informasi yang benar dan terbuka sehingga tidak menyulitkan para pengguna aplikasi selanjutnya.

1.7 Sistematika Penulisan

Sistematika penulisan rancang bangun sistem maintenance keamanan jaringan komputer berbasis web pada kantor BKN Regional VI Medan dibagi atas 5 bab yaitu

BAB I : PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang pemilihan judul, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini membahas masalah yang berhubungan dengan peancangan aplikasi serta teori lainnya yang mendukung pembuatan aplikasi sistem maintenance keamanan jaringan komputer berbasis web.

BAB III : METODE PENELITIAN

Bab ini menjelaskan bagaimana menganalisis dan merancang sistem yang akan dibangun.

BAB IV : HASIL DAN PEMBAHASAN

Bab ini menjelaskan bagaimana mengimplementasikan sistem dan dilanjutkan dengan menguji aplikasi yang dibuat.

BAB V : PENUTUP

Dalam bab ini diuraikan kesimpulan dari masalah yang dihadapi oleh penulis dan memberikan saran-saran untuk kemajuan pengembangan dimasa yang akan datang.

BAB II

LANDASAN TEORI

2.1 Keamanan Komputer

Gollmann pada tahun 2013 dalam bukunya “Computer Security” menyatakan bahwa, “Keamanan komputer adalah berhubungan dengan pencegahan dini dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam sistem komputer”. Pencegahan dapat menggunakan *firewall*, sedangkan pendeteksian dapat menggunakan IDS (*Intrusion Detection System*) dan penggabungan dari kedua metode itu adalah IPS (*Intrusion Prevention System*).

2.2 Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS), adalah pendekatan yang sering digunakan untuk membangun sistem keamanan komputer. IPS mengkombinasikan teknik *firewall* dan metode *Intrusion Detection System* (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor, di saat serangan telah teridentifikasi, IPS menolak akses (*block*) dan mencatat (*logging*) semua paket data yang teridentifikasi tersebut. Jadi IPS bertindak seperti layaknya *firewall* yang melakukan *allow* dan *block* yang dikombinasikan seperti IDS yang dapat mendeteksi paket secara detail. IPS menggunakan *signatures* untuk mendeteksi *traffic* di jaringan dan terminal, di mana pendeteksian paket yang masuk dan keluar (*inbound-outbound*) dapat

dideteksi sedini mungkin sebelum merusak atau mendapatkan akses ke dalam jaringan lokal. (Dony Arius, 2014 : 15)

2.3 *Intrusion Detection System (IDS)*

IDS (*Intrusion Detection System*) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS (*Intrusion Detection System*) sendiri mempunyai beberapa pengertian yaitu: (Dony Arius, 2014 :20)

- a. Sistem untuk mendeteksi adanya *intrusion* yang dilakukan oleh *intruder* (pengganggu atau penyusup) dalam jaringan. Pada awal serangan, *intruder* biasanya hanya mencari data. Namun, pada tingkat yang lebih serius *intruder* berusaha untuk mendapat akses ke sistem seperti membaca data rahasia, memodifikasi data tanpa permisi, mengurangi hak akses ke system sampai menghentikan sistem.
- b. Sistem keamanan yang bekerja bersama *firewall* untuk mengatasi *Intrusion*. *Intrusion* itu sendiri didefinisikan sebagai kegiatan yang bersifat *anomaly*, *incorrect*, *inappropriate* yang terjadi di jaringan atau di *host* tersebut. *Intrusion* tersebut kemudian diubah menjadi *rules* ke dalam IDS (*Intrusion Detection System*).
- c. Sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan.

Ada dua jenis IDS pada Dony Arius, (2014 : 21) pada buku *Intrusion Detection System, Sistem Pendeteksi Penyusupan Pada Jaringan Komputer* yaitu :

- a. NIDS (*Network Based Intrusion Detection System*) *Network-based Intrusion Detection System* adalah ketika semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. NIDS umumnya terletak di dalam segmen jaringan penting di mana *server* berada atau terdapat pada "pintu masuk" jaringan. Kelemahan NIDS adalah bahwa NIDS agak rumit diimplementasikan dalam sebuah jaringan yang menggunakan *switch* Ethernet, meskipun beberapa *vendor switch* Ethernet sekarang telah menerapkan fungsi IDS di dalam *switch* buatannya untuk memonitor *port* atau koneksi.
- b. HIDS (*Host Based Intrusion Detection System*) *Host-based Intrusion Detection System* adalah ketika aktivitas sebuah *host* jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS sering diletakkan pada *server - server* kritis di jaringan, seperti halnya *firewall*, *web server*, atau *server* yang terkoneksi ke internet.

2.4 Firewall

"Firewall adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah firewall diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (*gateway*) antara jaringan lokal dan jaringan lainnya. Firewall umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak

luar. Saat ini, istilah firewall menjadi istilah generik yang merujuk pada sistem yang mengatur komunikasi antar dua jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke Internet dan juga tentu saja jaringan korporat di dalamnya, maka perlindungan terhadap aset digital perusahaan tersebut dari serangan para hacker, pelaku spionase, ataupun pencuri data lainnya, menjadi esensial." Sumber : (Ibisa, 2011:136)

Firewall pada dasarnya merupakan suatu alat yang bersifat melindungi, jika seseorang akan berhubungan dengan jaringan komputer dan ingin mendapat hak akses yang aman, *firewall* merupakan salah satu pelindung yang dibutuhkan. Pada dasarnya ada tiga hal yang perlu dilindungi, di antaranya :

a. Data (Informasi)

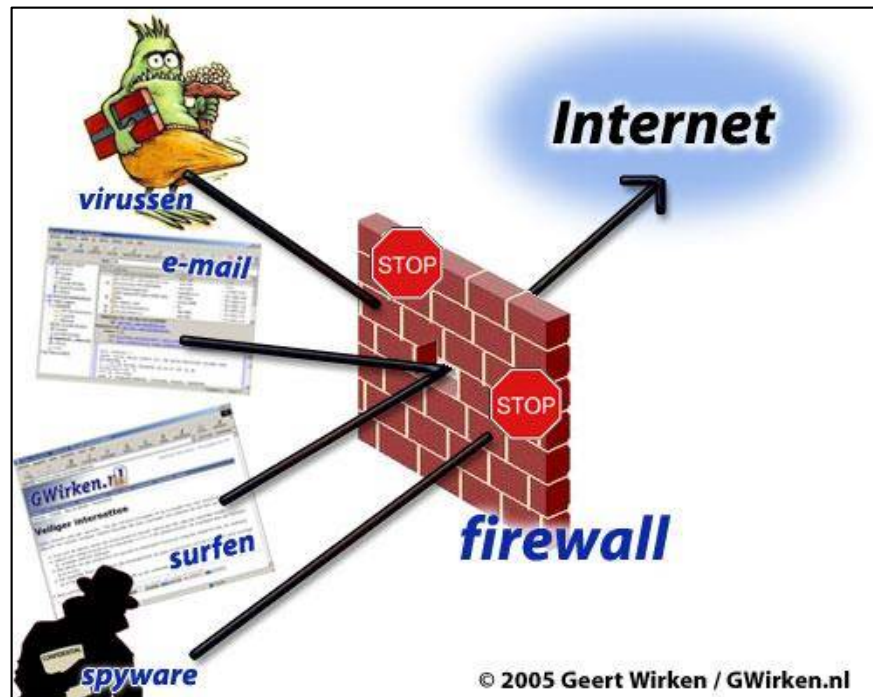
Data merupakan hal yang berharga yang perlu untuk dilindungi, pertukaran data di dunia maya (internet) merupakan hal yang sering dimanfaatkan oleh orang yang tidak bertanggung jawab, sebagai contoh, jika suatu perusahaan mengirim data yang mempunyai rahasia dan dalam pengirimannya disadap atau dihancurkan oleh orang lain, maka rahasia dari perusahaan tersebut akan menjadi milik umum.

b. *Resources* (Sumber Daya)

Pada organisasi sosial banyak memberikan ruang *hardisk* untuk umum dengan mengharapkan terima kasih dan publisitas, namun bukan berarti mereka aman dari gangguan.

c. Reputation

Hacker biasanya menggunakan identitas orang lain untuk melakukan kejahatan pada jaringan komputer sehingga membuat reputasi dari orang tersebut rusak.



Gambar 2.1 Ilustrasi Firewall

Sumber : Ahmad Muammar. W. K.2004 : 125. *Firewal*

2.5 Jenis Serangan pada Sistem Komputer

Ada banyak jenis serangan yang terjadi pada sistem komputer, di antaranya:

2.5.1 Spoofing

Spoofing adalah Teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi, dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka

adalah *host* yang dapat dipercaya. Hal ini biasanya dilakukan oleh seorang hacker/ cracker.

Macam-Macam Spoofing

1. **IP-Spoofing** adalah serangan teknis yang rumit yang terdiri dari beberapa komponen. Ini adalah eksploitasi keamanan yang bekerja dengan menipu komputer dalam hubungan kepercayaan bahwa anda adalah orang lain.
2. **DNS spoofing** adalah mengambil nama DNS dari sistem lain dengan membahayakan domain name server suatu domain yang sah.
3. **Identify Spoofing** adalah suatu tindakan penyusupan dengan menggunakan identitas resmi secara ilegal. Dengan menggunakan identitas tersebut, penyusup akan dapat mengakses segala sesuatu dalam jaringan

2.5.1 Ddos (Distributed Denial of Service)

Serangan DOS (*Denial-Of-Service attacks*) adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

Dalam sebuah serangan *Denial of Service*, si penyerang akan mencoba untuk mencegah akses seorang pengguna terhadap sistem atau jaringan dengan menggunakan beberapa cara, yakni sebagai berikut:

1. Membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. Teknik ini disebut sebagai *traffic flooding*.
2. Membanjiri jaringan dengan banyak request terhadap sebuah layanan jaringan yang disediakan oleh sebuah host sehingga request yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanan tersebut. Teknik ini disebut sebagai *request flooding*.
3. Mengganggu komunikasi antara sebuah host dan kliennya yang terdaftar dengan menggunakan banyak cara, termasuk dengan mengubah informasi konfigurasi sistem atau bahkan merusak fisik terhadap komponen dan server.

2.5.3 Denial of Service

Merupakan suatu istilah yang diberikan untuk upaya serangan dengan cara menurunkan kinerja suatu sistem komputer secara terus menerus. Serangan seperti ini bertujuan untuk membuat *server* korban menjadi kewalahan dalam melayani permintaan yang terkirim dan berakhir dengan penghentian aktivitas komputer. DoS juga merupakan serangan yang dilancarkan melalui paket tertentu dengan jumlah yang sangat banyak dengan maksud mengacaukan jaringan target.

3. Information Theft

Pada umumnya *information theft* merupakan suatu kejahatan komputer yang bertujuan mencari informasi dari komputer korban.

2.6 Jenis Program Pencurian Informasi

Program-program yang berhubungan dengan pencurian informasi ini banyak terdapat di internet seperti yang tertulis dalam buku (Sinaga, Dian, 2014:35. “Kejahatan Terhadap Buku dan Perpustakaan)” :

2.6.1 *Sniffer*

Suatu program yang sifatnya melakukan pencurian atau penyadapan data. Meskipun data tidak dicuri secara fisik (hilang), *sniffer* sangat berbahaya karena dia dapat digunakan untuk menyadap *password* dan informasi yang sensitive. Ini merupakan serangan terhadap aspek *privacy*.

2.6.2 *Intelligence*

Intelligence merupakan *hacker* atau *cracker* yang merupakan suatu kegiatan mengumpulkan segala informasi yang berkaitan dengan sistem target.

2.6.3 *Back Door*

Merupakan suatu akses yang khusus dibuat oleh seorang *programmer* sehingga dapat masuk ke dalam sistem. Tidak semua *programmer* mengerti perintah dalam sistem operasi, di dalam sistem operasi inilah programmer memasukkan perintah tertentu (yang biasanya disisipkan dalam program yang tidak jelas) namun tidak terlalu mengganggu kinerja sistem pada awalnya. Pada saat dibutuhkan *listing* program ini dijalankan dan dengan menggunakan fasilitas jaringan komputer untuk mendapatkan akses yang sama dengan pemilik yang sah.

2.6.4 Cyber Espionage

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran.

2.6.5 Social Engineering

Mencari berbagai informasi yang berhubungan dengan target/korban dari semua detail kehidupannya baik dari dunia maya maupun dunia nyata. Biasanya informasi tersebut digunakan untuk melakukan *brute-forcing* (memasukkan *password* secara acak) untuk mendapatkan hak akses baik *email* maupun akun lainnya.

2.7 Jenis Penyerang

Menurut Sinaga, Dian, 2014:45. Jenis – jenis penyerang yang banyak terdapat di internet seperti:

2.7.1 Joyriders

Penyerang yang merasa iseng dan ingin memperoleh kesenangan dengan cara menyerang sistem.

2.7.2 Vandal

Penyerang bertujuan untuk merusak sistem yang bertujuan untuk mendapatkan uang, kepopuleran, data penting, dan menghancurkan atau menghapus informasi yang tersisa dalam sistem tersebut.

2.7.3 Scorekeeper / Script Kiddies

Penyerang jenis ini hanya bertujuan untuk mendapatkan reputasi dengan cara meng-*crack* sistem sebanyak mungkin.

2.7.4 Cryptanalysis

Merupakan bagian dari kriptografi, dan merupakan orang yang mencobamemecahkan kode yang ada.

2.7.5 Developed Kiddie

Sebutan untuk kelompok yang masih remaja, mereka membaca metode dan cara *hack* hingga berhasil dan memamerkan keberhasilannya. Pada umumnya masih menggunakan GUI (*Graphic User Interface*) tanpa mampu menemukan lubang pada keamanan sistem operasi.

2.7.6 Hacker

Seseorang yang mencari kelemahan dan sangat memahami logika pemrograman dan konsep jaringan komputer. Aktivitas mereka disebut *hacktivism* yang dilakukan untuk mencari simpati tertentu.

2.8 Metode Pendeteksian Intrusi

Metode yang banyak digunakan dalam pendeteksian menurut *Dony Arius*, (2014 : 45) antara lain:

a. Signature Based Intrusion Detection System

Pada metode ini, telah tersedia daftar *signature* yang dapat digunakan untuk menilai apakah paket yang dikirimkan berbahaya atau tidak. Sebuah paket data akan dibandingkan dengan daftar yang sudah ada. Metode ini melindungi sistem dari jenis-jenis serangan yang sudah diketahuisebelumnya. Oleh karena itu, untuk tetap menjaga keamanan system jaringan komputer, data *signature* yang ada harus tetap ter-*update*.

b. *Anomaly Based Intrusion Detection System*

Pada metode ini, terlebih dahulu harus melakukan konfigurasi terhadap IDS dan IPS, sehingga IDS dan IPS dapat mengetahui pola paket seperti apa saja yang akan ada pada sebuah sistem jaringan komputer. Sebuah paket anomaly adalah paket yang tidak sesuai dengan kebiasaan jaringan komputer tersebut. Apabila IDS (*Intrusion Detection System*) dan IPS (*Intrusion Prevention System*) menemukan ada anomali pada paket yang diterima atau dikirimkan, maka IDS dan IPS akan memberikan peringatan pada pengelola jaringan (IDS) atau menolak paket tersebut untuk diteruskan (IPS). Untuk metode ini, pengelola jaringan harus terus menerus memberitahu IDS dan IPS bagaimana lalu lintas data yang normal pada sistem jaringan komputer tersebut, untuk menghindari adanya salah penilaian oleh IDS (*Intrusion Detection System*) atau IPS (*Intrusion Prevention System*).

2.9 Jaringan Komputer

Jaringan komputer adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling bertukar data. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (*service*). Pihak yang meminta/menerima layanan disebut klien (*client*) dan yang memberikan/mengirim layanan disebut pelayan (*server*). Desain ini disebut dengan sistem *client-server*, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

Dua buah komputer yang masing-masing memiliki sebuah kartu jaringan, kemudian dihubungkan melalui kabel maupun nirkabel sebagai medium transmisi data, dan terdapat perangkat lunak sistem operasi jaringan akan membentuk sebuah jaringan komputer yang sederhana. Apabila ingin membuat jaringan komputer yang lebih luas lagi jangkauannya, maka diperlukan peralatan tambahan seperti *Hub, Bridge, Switch, Router, Gateway* sebagai peralatan interkoneksinya. *Dony Arius, (2014 : 57)*

a. TCP/IP

Beberapa materi yang digunakan adalah *subnetting* atau pembagian kelas IP. *Subnetting* adalah suatu proses untuk memecah suatu jaringan IP ke SubJaringan yang lebih kecil atau juga dapat diartikan sebagai metode yang dilakukan untuk membagi blok setiap alamat IP address menjadi beberapa blok IP address. TCP/IP membagi IP menjadi lima kelas, yaitu:

1. Kelas A 8 bit pertama merupakan *bit network* sedangkan 24 bit terakhir merupakan *bit host*.
2. Kelas B 16 bit pertama merupakan *bit network* sedangkan 16 bit terakhir merupakan *bit host*.
3. Kelas C 24 bit pertama merupakan *bit network* sedangkan 8 bit terakhir merupakan *bit host*.
4. Kelas D digunakan untuk *multicast address*, yakni sejumlah komputer yang memakai bersama suatu aplikasi. Penggunaan *multicast address* yang sedang berkembang saat ini adalah aplikasi *real-time video*

conference yang melibatkan lebih dari dua *host* (*multipoint*), menggunakan *Multicast Backbone* (MBone).

5. Kelas E (4 bit pertama adalah 1111 atau sisa dari seluruh kelas). Pemakaiannya dicadangkan untuk kegiatan eksperimental.

b. Topologi Jaringan

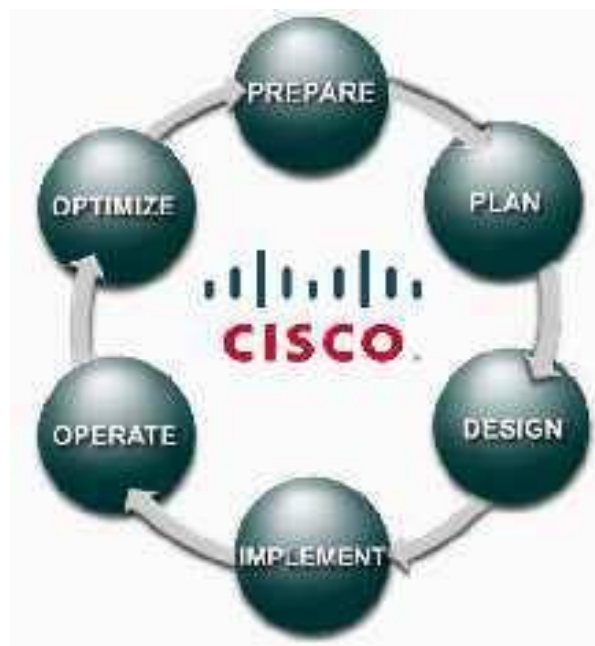
Topologi jaringan atau arsitektur jaringan adalah gambaran perencanaan hubungan antar komputer dalam *Local Area Network*, yang umumnya menggunakan kabel sebagai media transmisi, dengan konektor, *ethernet card* dan perangkat pendukung lainnya. Topologi jaringan memberikan gambaran bagaimana komputer-komputer dan perangkat jaringan komputer lainnya saling dihubungkan.

1. Topologi *Star* Karakteristik dari topologi jaringan ini adalah *node* (*station*) berkomunikasi langsung dengan *station* lain melalui *central node* (*hub/switch*), *traffic data* mengalir dari *node* ke *central node* dan diteruskan ke *node* (*station*) tujuan. Jika salah satu segmen kabel putus, jaringan lain tidak terputus. Keuntungan:

- a. Akses ke *station* lain (*client* atau *server*) cepat
- b. Dapat menerima *workstation* baru selama port di *central node* (*hub/switch*) tersedia.
- c. *Hub/switch* bertindak sebagai konsentrator.
- d. *Hub/switch* dapat disusun seri (bertingkat) untuk menambah jumlah *station* yang terkoneksi di jaringan.
- e. *User* dapat lebih banyak dibanding topologi *bus*, maupun *ring*.

- f. Bila *traffic* data cukup tinggi dan terjadi *collision*, maka semua komunikasi di tunda, dan koneksi akan di lanjutkan atau di persilahkan dengan cara *andom*, apabila *hub/switch* mendeteksi tidak ada jalur yang sedang di pergunakan oleh *node* lain.

2.10 PPDIOO (CISCO Lifecycle Service)



Gambar 2.2 PPDIOO Cisco Lifecycle Service

PPDIOO adalah sebuah metode yang digunakan oleh Cisco dalam melakukan pelayanan yang terus menerus. Dalam hal ini peneliti menggunakannya dalam melakukan layanan system maintenec keamanan jaringan pada Kantor BKN Regional VI Medan, Ada enam tahap yang dilakukan ketika menerapkan metode PPDIOO yaitu *prepare*, *plan*, *design*, *implementation*, *operate* dan, *optimize*. Sugeng winarno, (2010 : 35)

a. Prepare (Persiapan)

Pada fase ini peneliti menetapkan kebutuhan dari jaringan Kantor BKN Regional VI Medan pada bagian keamanan sesuai dengan *issue* yang telah terjadi dan yang akan terjadi. Dengan merencanakan strategi yang didukung dengan sumber daya yang tersedia di Kantor BKN Regional VI Medan.

b. Plan (Perencanaan)

Pada fase ini peneliti melakukan identifikasi jaringan berdasarkan tujuan, fasilitas (sumber daya), dan kebutuhan. Perencanaan penelitian untuk tugas yang dikelola, pihak yang bertanggung jawab, *milestones*, dan semua kebutuhan untuk melakukan desain dan implementasi. Fase ini terus diperbarui sesuai dengan siklus yang sedang berjalan.

c. Design (Desain)

Desain jaringan yang dikembangkan sesuai dengan perencanaan yang telah dibuat. Hasil dari fase ini adalah diagram jaringan dan daftar peralatan yang digunakan. Tahap ini harus disetujui untuk segera melakukan tahap implementasi.

d. Implementation (Implementasi)

Melakukan instalasi dan konfigurasi sesuai dengan desain. Perangkat mengganti atau menambah sumber daya yang ada, setiap langkah yang dilakukan harus memiliki deskripsi, rincian pelaksanaan, dan perkiraan waktu penyelesaian. Evaluasi dilakukan dan apabila terjadi kegagalan maka dilakukan *rollback* atau pengulangan langkah – langkah dan pencarian

informasi sebagai referensi tambahan. Pada tahap ini harus dilakukan pengujian (dengan *penetration test*, maupun penggunaan aplikasi seperti BASE) sebelum dilanjutkan ke fase operasional.

e. Operate (Operasional)

Pengelolaan dan *monitoring* pada komponen jaringan, pemeliharaan *routing, upgrading*, identifikasi dan koreksi jika terjadi kesalahan pada jaringan. Tahap ini adalah pengujian dari desain yang telah dibuat, dengan memantau kinerja, stabilitas, deteksi kesalahan, koreksi konfigurasi, dan pengumpulan data untuk digunakan pada fase optimalisasi.

f. Optimize (Optimalisasi)

Mempelajari data yang telah ada untuk selanjutnya melakukan identifikasi dan penyelesaian masalah sebelum mengganggu jaringan secara luas. Pada fase ini dimungkinkan untuk melakukan modifikasi desain jaringan jika terlalu banyak masalah yang ditimbulkan, dan melakukan perbaikan pada bagian aplikasi (*software*). Dan jika telah dilakukan modifikasi akan menuntun perkembangan jaringan tersebut ke awal fase pada siklus PPDIOO. (Sugeng winarno, 2010 :35, Jaringan Komputer dengan TCP/IP, Modula).

2.11 UML (*unified modeling language*)

UML (*Unified Modeling Language*) merupakan pengganti dari metode analisis berorientasi object dan design berorientasi object (OOA&D) yang dimunculkan sekitar akhir tahun 80-an dan awal tahun 90-an. UML merupakan gabungan dari metode Booch, Rumbaugh (OMT) dan Jacobson. Tetapi UML ini akan mencakup lebih luas dari pada OOA&D. Pada pertengahan

pengembangan UML dilakukan standarisasi proses dengan OMG (Object Management Group) dengan harapan UML akan menjadi bahasa standar pemodelan pada masa yang akan datang.

UML disebut sebagai bahasa pemodelan bukan metode. Kebanyakan metode terdiri paling sedikit prinsip, bahasa pemodelan dan proses. Bahasa pemodelan (sebagian besar grafik) merupakan notasi dari metode yang digunakan untuk mendesain secara cepat. Bahasa pemodelan merupakan bagian terpenting dari metode. Ini merupakan bagian kunci tertentu untuk komunikasi. Jika anda ingin berdiskusi tentang desain dengan seseorang, maka Anda hanya membutuhkan bahasa pemodelan bukan proses yang digunakan untuk mendapatkan desain. (Rosa A.s2014:137)

2.11.1 Bagian-bagian UML (*unified modeling language*)

Bagian-bagian utama dalam UML adalah :

1. *View* digunakan untuk melihat sistem yang dimodelkan dari beberapa aspek yang berbeda. *View* bukan melihat grafik, tapi merupakan suatu abstraksi yang berisi sejumlah diagram. Beberapa jenis view sebagai berikut:

- a. *Usecase view*

Mendeskripsikan fungsionalitas sistem yang seharusnya dilakukan sesuai yang diinginkan external actors. Actor yang berinteraksi dengan sistem dapat berupa user atau sistem lainnya. View ini digambarkan dalam use case diagrams dan kadang-kadang dengan activity

diagrams. View ini digunakan terutama untuk pelanggan, perancang (designer), pengembang (developer), dan penguji sistem (tester).

b. *Logical view*

Mendeskripsikan bagaimana fungsionalitas dari sistem, struktur statis (class, object, dan relationship) dan kolaborasi dinamis yang terjadi ketika object mengirim pesan ke object lain dalam suatu fungsi tertentu. View ini digambarkan dalam class diagrams untuk struktur statis dan dalam state, sequence, collaboration, dan activity diagram untuk model dinamisnya. View ini digunakan untuk perancang (designer) dan pengembang (developer).

c. *Component view*

Mendeskripsikan implementasi dan ketergantungan modul. Komponen yang merupakan tipe lainnya dari code module diperlihatkan dengan struktur dan ketergantungannya juga alokasi sumber daya komponen dan informasi administrative lainnya. View ini digambarkan dalam component view dan digunakan untuk pengembang (developer).

d. *Concurrency view*

Membagi sistem ke dalam proses dan prosesor. View ini digambarkan dalam diagram dinamis (state, sequence, collaboration, dan activity diagrams) dan diagram implementasi (component dan deployment diagrams) serta digunakan untuk pengembang (developer), pengintegrasian (integrator), dan penguji (tester).

e. *Deployment view*


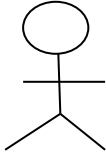
Mendeskripsikan fisik dari sistem seperti komputer dan perangkat (nodes) dan bagaimana hubungannya dengan lainnya. View ini digambarkan dalam deployment diagrams dan digunakan untuk pengembang (developer), pengintegrasi (integrator), dan penguji (tester).

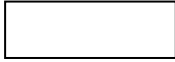


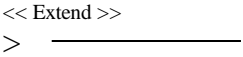
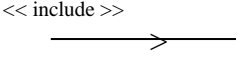
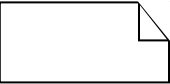

2. Diagram berbentuk grafik yang menunjukkan simbol elemen model yang disusun untuk mengilustrasikan bagian atau aspek tertentu dari sistem. Sebuah diagram merupakan bagian dari suatu view tertentu dan ketika digambarkan biasanya dialokasikan untuk view tertentu. Adapun jenis diagram antara lain.

2.11.2 Use case diagram

Use case adalah deskripsi fungsi yang disediakan oleh sistem dalam bentuk teks sebagai dokumentasi dari *use case symbol* namun dapat juga dilakukan dalam activity diagrams. *Use case* digambarkan hanya yang dilihat dari luar oleh actor bukan bagaimana fungsi yang ada di dalam system.

Tabel 2.1 simbol-simbol use case diagram

Nama Komponen	Keterangan	Gambar
<i>Use case</i>	Menerangkan “ apa” yang dikerjakan sistem, bukan “bagaimana” sistem mengerjakannya.	
<i>Actor</i>	Menggambarkan orang, sistem atau eksternal entitas/stakeholder yang menyediakan atau menerima informasi dari sistem.	

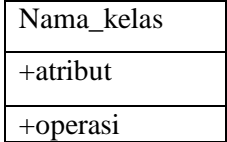
<i>Sistem Boundary</i>	Menggambarkan Jangkauan system	
<i>Association</i>	Menggambarkan bagaimana aktor terlihat dalam <i>use case</i> .	
<i>Generalization</i>	Dibuat ketika ada sebuah keadaan yang lain/perlakuan khusus.	
<i>Extend</i>	Perluasan dari <i>use case</i> lain jika kondisi atau syarat terpenuhi	
<i>Include</i>	Menjelaskan bahwa <i>use case</i> termasuk didalam <i>use case</i> lain.	
<i>Note</i>	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi	
<i>Collaboratin</i>	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan prilaku yang lebih besar dari jumlah elemen-elemenya	

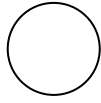


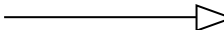
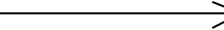

Sumber : Rosa A.s (2014:156)

2.11.3 Class Diagram

Diagram kelas adalah diagram UML yang menggambarkan kelas-kelas dalam sebuah sistem dan hubungannya antara satu dengan yang lain. Berikut daftar simbol-simbol dari *Class Diagram* :

Tabel 2.2 Simbol-sombol *class diagram*

Nama	Simbol	Deskripsi
Kelas		Kelas pada struktur sistem

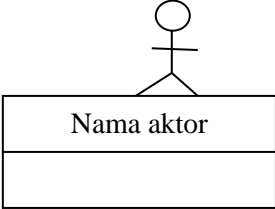

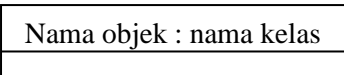
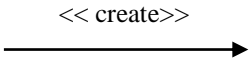
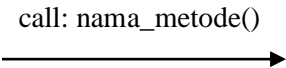
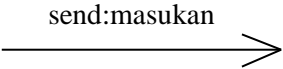
Antar muka / <i>interface</i>	 Nama_interface	Sama dengan konsep interface dalam pemograman yang berorientasi
Asosiasi / <i>assocition</i>		Relasi antarkelas dengan makna umum, asosiasi biasanya juga disertai dengan <i>multiplicity</i>
Asosiasi berarah / <i>directed association</i>		Relasi antar kelas dengan makna yang satu digunakan oleh kelas yang lain, saosiasi biasanya juga disertai dengan <i>multiplicity</i>
Generalisasi		Relasi antar kelas dengan makan generalisasi-spesialisasi (umum khusus)
Kebergantungan / <i>dependency</i>		Relasi antarkelas dengan makna keberuntungan antarkelas
Agregasi / <i>agregation</i>		Relasi antar kelas dengan makna semua-bagian (<i>whole-part</i>)

Sumber : Rosa A.s (2014: 146)

2.11.4 Sequence diagram

Diagram sequence menggambarkan kelakuan objek pada use case dengan mendeskripsikan waktu hidup objek dan message yang dikirimkan dan diterima antar objek. Oleh karena itu untuk menggambarkan diagram sequence maka harus diketahui objek-objek yang terlibat dalam sebuah use case beserta metode-metode yang dimiliki yang diintiasiasi menjadi objek itu. Berikut adalah simbol-simbol yang ada pada diagram sekuen :

Tabel 2.3 simbol-simbol diagram *sequence*



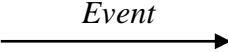

Nama	Simbol	Deskripsi
Aktor		Orang, proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat di luar sistem informasi itu sendiri, jadi walaupun simbol dari aktor adalah gambar orang, tapi aktor belum tentu orang, biasanya dinyatakan menggunakan kata benda diawal frase nama aktor
Garis hidup / lifeline		Menyatakan kehidupan suatu objek
Objek		menyatakan objek yang berinteraksi pesan
Pesan tipe <i>create</i>		Menyatakan suatu objek membuat objek yang lain, arah panah mengarah pada objek yang dibuat
Pesan tipe <i>call</i>		Menyatakan suatu objek yang memanggil suatu operasi/metode yang ada pada objek lain atau dirinya sendiri, arah panah mengarah pada objek yang memiliki operasi/metode, karena ini memanggil operasi/metode yang dipanggil harus pada diagram kelas sesuai dengan kelas objek yang berinteraksi.
Pesan tipe send		Menyatakan bahwa objek mengirim data/masukan informasi ke objek lainnya,arah panah mengarah pada objek dikirim

Sumber :Rosa A.s (2014:165)

2.11.5 State Machine Diagram

State machine diagram atau *statechart diagram* atau dalam bahasa Indonesia disebut diagram mesin status atau sering juga disebut diagram status digunakan untuk menggambar perubahan status atau transisi status dari sebuah mesin atau sistem atau objek. *State machine diagram* merupakan pengembangan dari diagram *Finite State Automata* dengan penambahan beberapa fitur dan konsep baru. Berikut adalah simbol-simbol yang ada pada *state machine diagram* :

Tabel 2.4 simbol-simbol diagram state machine

Nama	Simbol	Deskripsi
<i>Start/ status awa (initial state)</i>		Start atau initial state adalah state atau keadaan awal pada saat sistem mulai hidup
<i>End/status akhir (Final state)</i>		Enda atau final state adalah state keadaan akhir dari daur hidup suatu sistem.
<i>Event</i>		Event adalah kegiatan yang menyebabkan suatu mesin
<i>State</i>		Sistem pada waktu tertentu, state dapat berubah jika ada event tertentu yang memicu perubahan tersebut


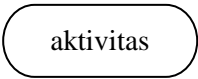
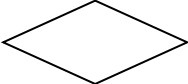

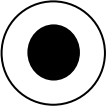
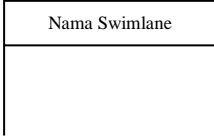
Sumber :Rosa A.s (2014:164)

2.11.6 Activity diagram

Activity Diagram adalah lebih focus kepadamenggambarakan proses bisnis dan urutan aktivitas dalam sebuah proses.bisnis. Memiliki manfaat yaitu apabila kiata membuat diagram ini terlebih dahulu lebih memodelkan sebuah proses untuk membantu memahami proses secara keseluruhan. Dan *activity* dibuat berdasarkan

sebuah atau beberapa *use case* dan *use case diagram*. Yang perlu diperhatikan disini adalah bahwa diagram aktivitas menggambarkan aktivitas sistem yang bukan apa yang dilakukan aktor, jadi aktivitas yang dilakukan oleh sistem. berikut adalah simbol-simbol yang ada pada diagram aktivitas :

Tabel 2.5 Simbol-simbol *activity diagram*

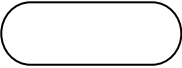


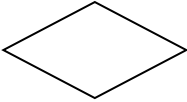

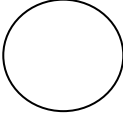
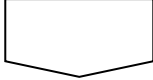
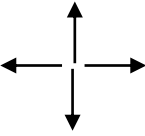
Nama	Simbol	Deskripsi
Status awal		Status awal aktivitas sistem, sebuah diagram aktivitas memiliki sebuah status awal
aktivitas		Aktivitas yang dilakukan sistem, aktivitas biasanya diawali dengan kata kerja
Percabangan/ <i>decision</i>		Asosiasi percabangan dimana jika ada pilihan aktivitas lebih dari satu
penggabungan/ <i>join</i>		Asosiasi penggabungan dimana lebih dari satu aktivitas digabungkan menjadi satu
Status akhir		Status akhir yang dilakukan sistem, sebuah diagram aktivitas memiliki sebuah status akhir
Swimlane		Memisahkan organisasi bisnis yang bertanggung jawab terhadap aktivitas yang terjadi

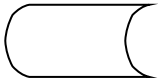
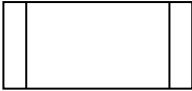
Sumber : Rosa A.s (2014:162)

1.12 Bagan Alir (*Flowchart*)

Flowchart adalah skema atau bagan yang menggambarkan arus dan urutan suatu kegiatan programkerja secara keseluruhan dari system secara logika mulai dari awal hingga akhir. Simbol-simbol yang digunakan adalah sebagai berikut:

Tabel 2.6 Simbol-simbol *flow chart*

No	Simbol	Deskripsi
1		Terminal, untuk memulai atau mengakhiri suatu program
2		Proses suatu simbol yang menunjukkan setiap pengolahan yang dilakukan
3		Input-output untuk memasukan data ataupun menunjukkan hasil dari suatu proses
4		Decesion, suatu kondisi yang akan menghasilkan beberapa kemungkinan jawaban atau pilihan
5		Preparation, proses suatu simbol yang menyediakan tempat-tempat pengolahan dalam storage
6		Conector, suatu prosedur akan masuk atau keluar melalui simbol ini dalam lembar yang sama
7		Off-page Conector, merupakan simbol masuk atau keluarnya suatu prosedur pada lembar kertas lainnya
8		Flow, arus dari pada prosedur yang dapat dilakukan atas kebawah dan bawah keatas, dari kiri kekanan ataupun dari kanan ke kiri

9		Stored data, penyimpanan data secara sementara
10		Predifined process, untuk menyatakan sekumpulan langkah proses yang ditulis sebagai procedure

Sumber : Rosa A.s (2014:175)

2.13 Web

Awal perkembangan web dimulai pada bulan maret 1989 saat tim berner-lee yang bekerja di laboratorium fisika partikel eropa atau yang dikenal dengan nama CERN (*conseil european pour la recherche nuclaire*) yang terletak di Genewa Swiss, mengajukan protokol (bahasa atau prosedur yang digunakan untuk menghubungkan antara komputer yang satu dengan lainnya) sistem distribusi informasi internet yang digunakan untuk berbagai informasi di antara para fisikawan. Protokol inilah yang selanjutnya dikenal sebagai protokol *world wide web* dan dikembangkan oleh *world wide web consortium* (w3c). w3c adalah konsorsium dari sejumlah organisasi yang berkepentingan dalam pengembangan berbagai standar yang berkaitan dengan web.

Sumber daya yang ada di Internet jumlahnya sangat banyak, seperti *Chatting*, *E-mail*, *Milis*, dan sebagainya. Salah satu sumber daya internet yang perkembangannya sangat pesat adalah *www* (*world wide web*) atau sering disebut dengan istilah web saja. *Web* didistribusikan dengan menggunakan pendekatan *hypertext*. Dimana hanya dengan menggunakan suatu teks yang tidak terlalu banyak/singkat bisa dijadikan acuan untuk membuka dokumen yang lain. melalui pendekatan *hypertext* ini seorang *user* dapat memperoleh informasi yang

diinginkan dengan cepat. Caranya bisa berpindah dari suatu dokumen ke dokumen yang lain. Dokumen-dokumen yang diperlukan informasinya tersebut dapat terletak dilokasi manapun, asalkan terletak pada jaringan internet.

2.14 PHP

PHP diciptakan pertama kali oleh Rasmus Lerdorf pada tahun 1994. Awalnya PHP Digunakan untuk mencatat jumlah serta untuk mengetahui siapa saja pengunjung pada homepage-nya. Rasmus Lerdorf adalah seorang pendukung open source. Oleh karena itu, ia mengeluarkan *Personal Home Page Tools* versi 1.0 secara gratis, kemudia menambahkan kemampuan PHP 1.0 dan meluncurkan PHP 2.0.

Pada tahun 1996, PHP telah banyak digunakan dalam website didunia. Sebuah kelompok pengembang software yang terdiri dari Rasmus, Zeew Suraski, Andi Gutman, Stig Bakten, Shane Caraveo, dan Jim Winstead bekerja sama untuk menyempurnakan PHP 2.0. Akhirnya, pada tahun 1998, PHP 3.0 diluncurkan. Penyempurnaan terus dilakukan sehingga pada tahun 2000 dikeluarkan PHP 4.0. Tidak berhenti sampai disitu, kemampuan PHP terus ditambah, dan sampai saat ini versi terbaru PHP yang telah dikeluarkan adalah PHP 5.0.x.

PHP memiliki banyak kelebihan yang tidak dimiliki oleh bahasa script sejenis. PHP difokuskan pada pembuatan *script server-side*, yang bisa melakukan apa saja yang dapat dilakukan oleh CGI, seperti mengumpulkan data dari form, menghasilkan isi halaman web dinamis, dan kemampuan mengirim serta menerima *cookies*, bahkan lebih dari pada kemampuan CGI.

PHP dapat digunakan pada semua sistem operasi, antara lain Linux, Unix (termasuk variannya HP-UX, Solaris, dan Open BSD), Microsoft Windows, Mac OS, RISC OS. PHP juga mendukung banyak Web Server, seperti Apache, Microsoft Internet Information Server (MIIS), Personal Web Server (PWS), Netscape and iPlanet servers, O'Reilly Website Pro Server, audium, Xitami, OmniHTTPd, dan masih banyak lagi lainnya, bahkan PHP dapat bekerja sebagai suatu CGI Processor. PHP tidak terbatas pada hasil keluaran HTML (*Hyper Text Markup Language*). PHP juga memiliki kemampuan untuk mengolah keluaran gambar, file PDF, dan movie flash. PHP juga dapat menghasilkan text seperti XHTML dan file XML lainnya.

Salah satu fitur yang dapat diandalkan oleh PHP yakni dukungannya terhadap banyak database seperti Adabas D, dBase, Direct MS-SQL, Empress, FrontBase, Hyperwave, IBM DB2, Informix, Ingres, Interbase, MSOL, MySQL, ODBC, Oracle, Ovrimos, PostgreSQL, Solid, Sybase, Unix DBM dan Velocis. Umumnya database MySQL digunakan untuk bekerja sama dengan PHP. (Kusuma Ardhana, 2017:1)

2.15 Mysql

Mysql adalah sebuah perangkat lunak sistem manajemen basis data SQL (*database management system*) atau DBMS yang multithread, multi-user, dengan sekitar 6 juta instalasi di seluruh dunia. MySQL AB membuat MySQL tersedia sebagai perangkat lunak gratis di bawah lisensi GNU General Public License (GPL), tetapi mereka juga menjual dibawah lisensi komersial untuk kasus-kasus

dimana penggunaannya tidak cocok dengan penggunaan GPL. Beberapa kelebihan yang dimiliki oleh MySQL sebagai berikut :

a. Gratis

Sama dengan PHP, MySQL bersifat opensource, semua orang bebas menggunakannya tanpa harus membayar sepeser pun

b. Cross Platform

MySQL dapat digunakan under windows, ataupun under linux.

c. Lengkap dan Cepat

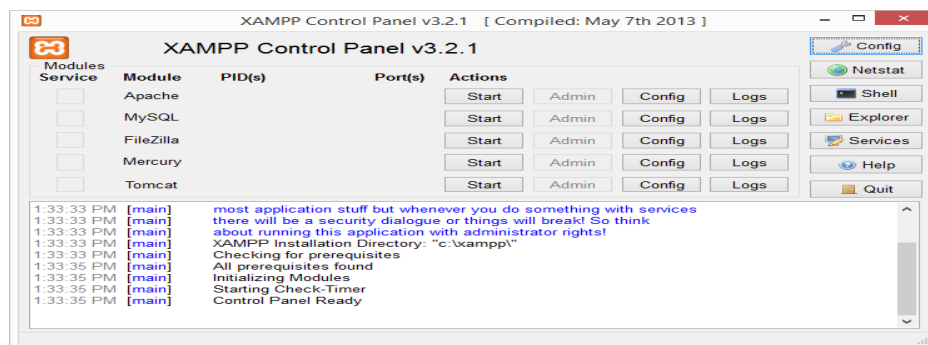
Pasangan yang cocok dengan PHP. Wajar jika banyak hosting saat ini mendukung adanya PHP dan MySQL karena kecepatan, gratis, dan dapat dijalankan di sistem operasi manapun.

2.16 Xampp

XAMPP adalah perangkat lunak gratis yang bebas digunakan. XAMPP berfungsi sebagai server yang berdiri sendiri (localhost), yang terdiri dari Apache HTTP Server, MySQL database dan penerjemah bahasa yang ditulis dengan bahasa pemrograman PHP dan XAMPP dikembangkan oleh perusahaan apache friends yang memiliki kelebihan bisa berperan sebagai server web apache untuk simulasi pengembangan website.

XAMPP banyak mendukung sistem operasi, merupakan kompilasi dari beberapa program. Fungsinya adalah sebagai server yang berdiri sendiri (localhost), yang terdiri atas program Apache HTTP Server, MySQL database, dan penerjemah bahasa yang ditulis dengan bahasa pemrograman PHP dan Perl. Nama XAMPP merupakan singkatan dari X (empat sistem operasi apapun),

Apache, MySQL, PHP dan Perl. Program ini tersedia dalam GNU General Public License dan bebas, merupakan web server yang mudah digunakan yang dapat melayani tampilan halaman web yang dinamis. Untuk mendapatkannya dapat mendownload langsung dari web resminya.



Gambar 2.3 Penampilan XAMPP

Sumber : Yosef Murya Kusuma Ardhana, 2017:7

BAB III

METODE PENELITIAN

3.1 Sistem Yang Sedang Berjalan

Analisis system yang sedang berjalan pada system pengamanan jaringan komputer pada Kantor Badan Kepegawaian Negara (BKN) di Medan, Bertujuan untuk mengetahui lebih jelas bagaimana cara kerja system tersebut dan masalah yang dihadapi system tersebut untuk dapat dijadikan system yang baru agar terkomputerisasi system yang sedang berjalan yang dilakukan berdasarkan urutan kejadian yang ada dan dari urutan kejadian tersebut dapat dibuat diagram aliran dokumen (*flowmap*), prosedur penanganan masalah jika terjadi permasalahan pada jaringan komputer maka perlu di lakukan *maintenance* sehingga proses kerja bagi staff dapat berjalan dengan baik, maka dapat di deskripsikan sebagai berikut:

1. Sering terjadi gangguan jaringan komputer pada saat jam kerja diakibatkan banyaknya pengguna jaringan.
2. Penanganan untuk melakukan perbaikan jaringan komputer masih terkesan lamban dikarenakan system yang di rancang sebelumnya belum terintergerasi pada server secara menyeluruh.
3. Router dan switch di lantai dua belum ada sehingga jaringan komputer sering bermasalh diakibatkan switch yang digunakan dari lantai 1 dan

. mengakibatkan kabel internet yang digunakan semakin panjang sehingga membuat gangguan jaringan pada saat jam kerja sibuk.

Penelitian ini menggunakan metode studi kasus di Badan Kepegawaian Negara (BKN) Medan beralamat di jalan Gatot Subroto Kecamatan Medan Petisah Propinsi Sumatra Utara. Penelitian ini di laksanakan dalam tanggal 16 April 2018. Rancang bangun system *maintenance* keamanan jaringan komputer di kantor BKN melalui beberapa proses agar system yang di buat mendapat hasil yang baik dan sesuai dengan tujuan dalam mengamankan data di Kantor BKN agar proses kerja dapat berjalan dengan baik tanpa ada gangguan dari jaringan komputer.

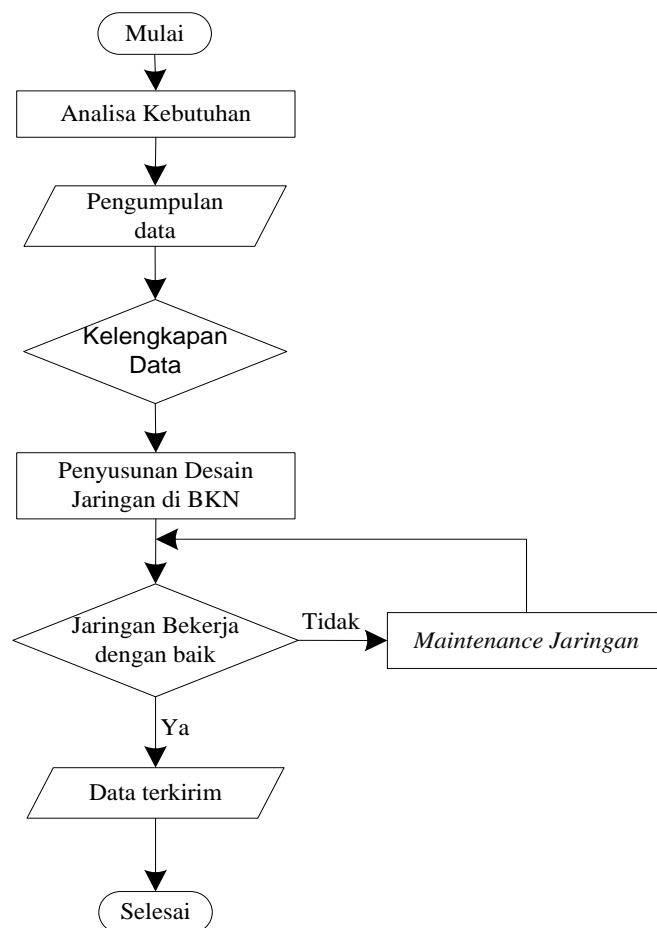
3.2 Analisis Sistem Yang Diusulkan.

Pengamanan jaringan komputer di kantor BKN ynag saat ini terpasang hanya mencakup sebagian gedung sehingga kantor yang lain belum terintergaris oleh karena itu perancangan jaringan untuk keamanan system yang di gunakan belum memadai kerena server terbagi-bagi, maka dengan dilakukannya perancangan jaringan komputer untuk menganalisis jika terjadinya gangguan jaringan diakibatkan proses kerja kepegawaian menjadi terganggu maka dapat lebih muda dilakukan *maintenance* sehingga keamanan jaringan lebih terjamin.

Untuk gedung BKN bagian pepegawaian bias mencakup sebagian gedung lain dikarenakan *aces point* terletak di dekat ruangan tata usah, hal ini membuat setiap ruangan kepegawaian yang berada di dalam gedung tidak bias mengakses jaringan. Sedangkan untuk gedung lain sudah ada jaringan tapi masih belum

semua dapat terjangkau jaringan tersebut sehingga sering terjadi gangguan saat pengiriman data, maka dari perluh dibuat suatu *maintenance* jaringan yang mudah mendeteksi jika terjadi gangguan pada jaringan komputer di Kantor Kepegawaian Negara Medan

Proses Rancangan bangun system *maintenance* keamanan jaringan komputer disimulasikan dalam sebuah *flowchart* seperti pada gambar 4. Di bawah ini :



Gambar 3.1 Flowchart Maintenance Jaringan di BKN

Gambar 3.1 Menjelaskan alur perancangan jaringan di kantor BKN Medan, yaitu sebagai berikut :

- 1) Analisis kebutuhan, dalam tahap ini penelitian menganalisa kebutuhan baik *software*, *hardware* serta data yang diperlakukan dalam penelitian.
- 2) Pengumpulan data, dalam tahap ini peneliti mencari dan mengumpulkan data-data yang dibutuhkan dalam penelitian yang akan diimplementasikan secara langsung di kantor BKN Medan. Pengumpulan data dilakukan dengan metode, yaitu:
 - a. Studi pustaka, yaitu data yang dapat didapat dari buku, artikel, jurnal, dan sebagaimana yang sesuai dengan penelitian sebagai pendukung pembuatan skripsi hingga penyusunan laporan.
 - b. Obsevasi yaitu data yang diperoleh dengan melakukan pengamatan secara lansung.
 - c. Wawancara yaitu data yang didapat dengan cara bertanya kepada pihak kantor BKN yang sesuai dengan bidangnya dalam pengamanan jaringan
- 3) Kelengkapan data yaitu, tahap mengidentifikasi kelengkapan data yang telah diperoleh, jika data telah lengkap, maka dilanjutkan ke tahap desain jaringan dan apabila data belum lengkap, maka dilakukan pengumpulan data kembali.
- 4) Penyusunan desain jaringan dengan simulasi, pada bagian penelitian mendesain topologi sesuai dengan data . Jaringan bekerja dengan baik, jika system yang telah diimplemetasikan akan diuji dengan beberapa percobaan, apabila system masih error. Maka dilakukan perbaikan system dan akan diuji kembali.

3.3 Analisis Kebutuhan Non-Fungsional

Analisis kebutuhan non fungsional merupakan analisis yang dibutuhkan untuk menentukan spesifikasi kebutuhan sistem. Spesifikasi ini juga meliputi elemen atau komponen – komponen apa saja yang dibutuhkan untuk sistem yang akan dibangun sampai dengan sistem tersebut diimplementasikan. Analisis kebutuhan ini juga menentukan spesifikasi masukan yang diperlukan sistem, keluaran yang akan dihasilkan sistem dan proses yang dibutuhkan untuk mengolah masukan sehingga menghasilkan suatu keluaran yang diinginkan.

a. Analisis Perangkat Keras (Hardware)

Perangkat keras minimum yang digunakan untuk membangun Sistem Monitoring Jaringan ini adalah sebagai berikut:

1. Processor berkecepatan 2.0 Ghz
2. RAM 2 Gb
3. Hardisk minimal 10 Gb untuk menyimpan data
4. LAN Card
5. Keyboard dan Mouse
6. Monitor 14.

b. Analisis Perangkat Lunak (Software)

Untuk mendukung dalam penyimpanan informasi, dibutuhkan suatu fasilitas yang memadai. Yaitu berupa perangkat lunak (software) yang dirancang untuk memudahkan dalam pembangunan dan menjalankan sisten nantinya.

Adapun perangkat lunak yang digunakan adalah sebagai berikut :

1. Microsoft Windows 7 , Windows XP sebagai sistem operasi
2. Mozila Firefox version 3.5 sebagai browser
3. Modem untuk koneksi ke internet
4. ArcGIS Server 10 sebagai Web Server

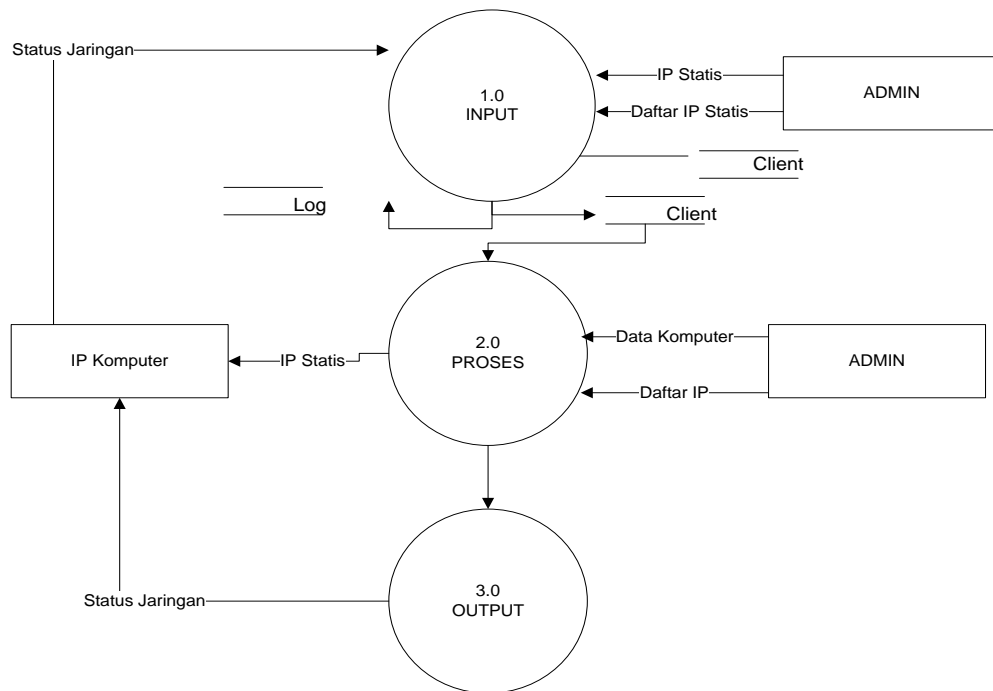
3.4 Diagram Konteks

Diagram Konteks adalah diagram yang menggambarkan secara umum yang menjadi masukan, proses dan keluaran yang terjadi dalam sebuah sistem. Diagram konteks untuk sistem monitoring jaringan yang akan dibangun adalah sebagai berikut :



Gambar 3.2 Diagram Konteks

3.5 Data Flow Diagram (DFD) Level 0



Gambar 3.3 DFD Level 0

3.6 Struktur Tabel

Berikut adalah struktur tabel dari website monitoring Jaringan komputer:

Tabel 3.1 Tabel User

No	Field Name	Type	Length	Keterangan
1	Iduser	Int	11	Primary Key
2	Emailuser	Varchar	150	
3	Passworduser	Varchar	20	
4	NamaUser	Varchar	20	

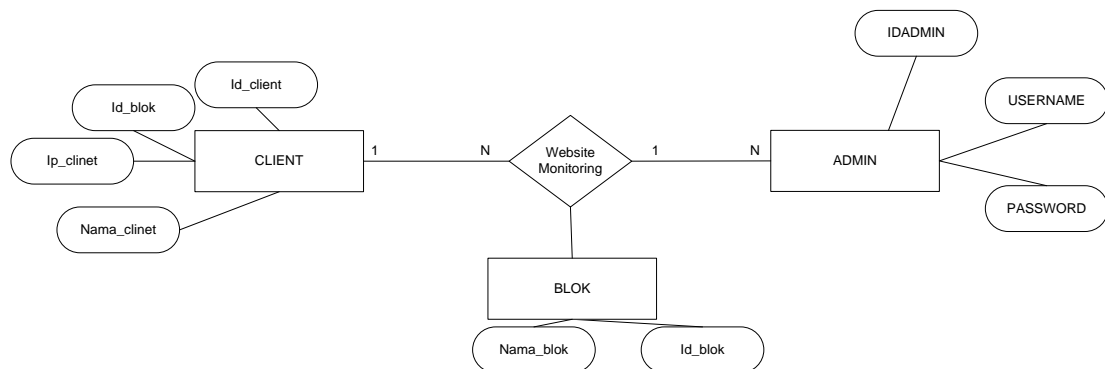
Tabel 3.2 Tabel Log

No	Field Name	Type	Length	Keterangan
1	Id_log	Int	11	Primary Key
2	Id_clinet	Varchar	150	
3	Date_log	Varchar	50	
4	Hour_log	Varchar	50	
5	status_log	Int	50	

Tabel 3.3 Tabel Client

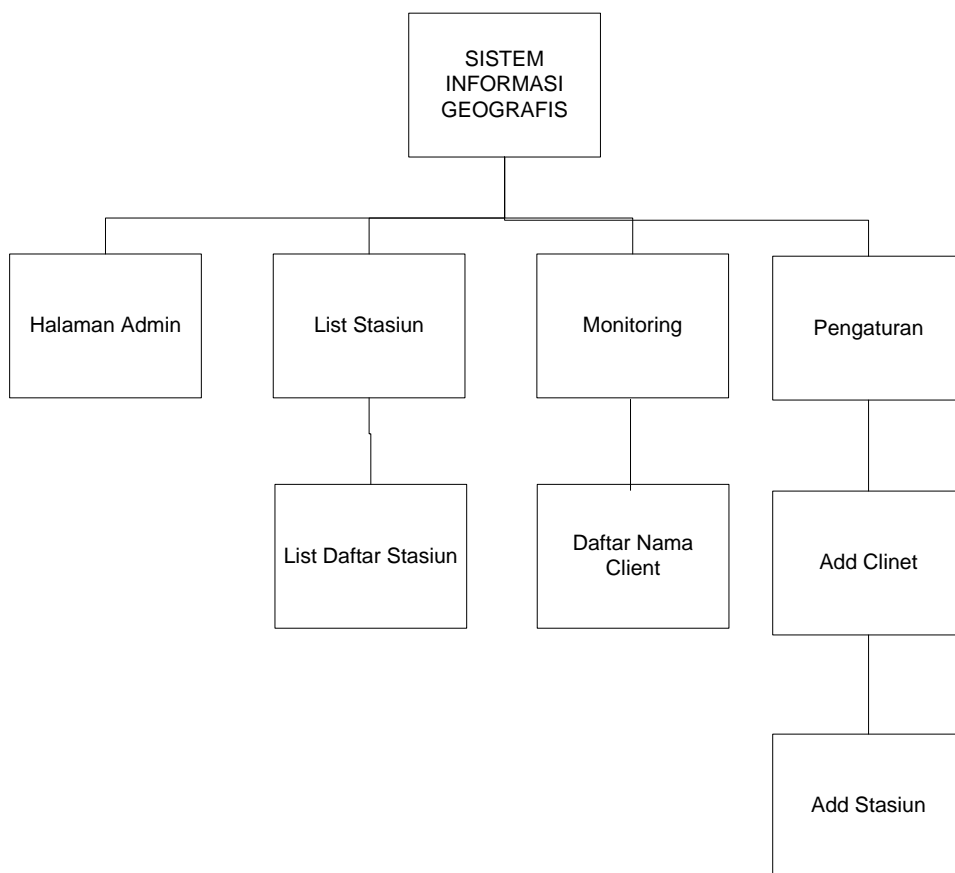
No	Field Name	Type	Length	Keterangan
1	Id_clinet	Int	11	Primary Key
2	Id_blok	Varchar	150	
3	Ip_client	Varchar	50	
4	Nama_client	Varchar	50	
5	Status_client	Varchar	50	

3.7 Entity Relationship Diagram

**Gambar 3.4 Entity Relationship Diagram**

3.8 Perancangan Tampilan

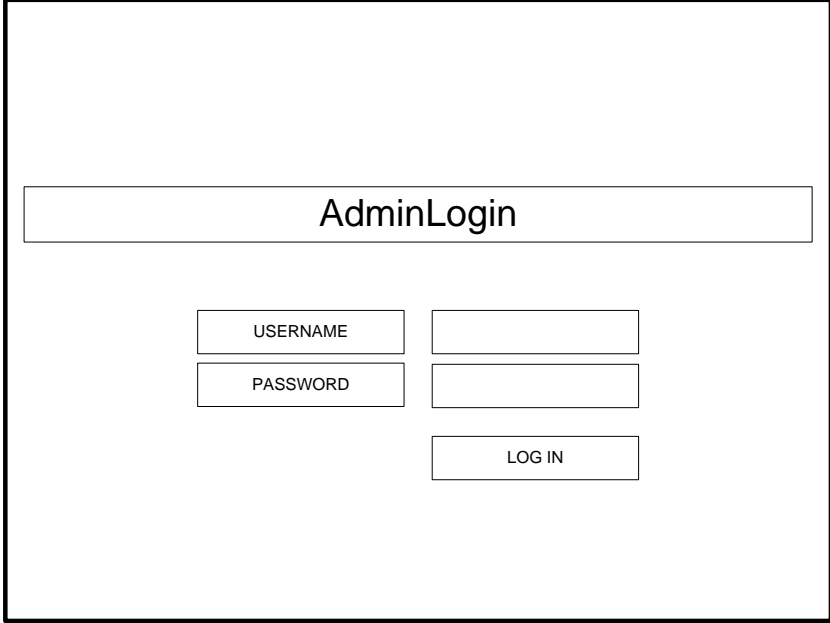
Sebelum dilakukannya proses perancangan tampilan pada website monitoring jaringan pada BKN Sumut, maka terlebih dahulu dilakukan flowmap pada perancangan sistem, adapun flowmap ada website monitoring jaringan adalah sebagai berikut:



Gambar 3.5 Rancangan FlowMap Monitoring Jaringan website

Perancangan merupakan bagian yang paling penting dalam merancang sistem. Adapun bentuk website monitoring jaringan pada kantor BKN Sumut adalah sebagai berikut:

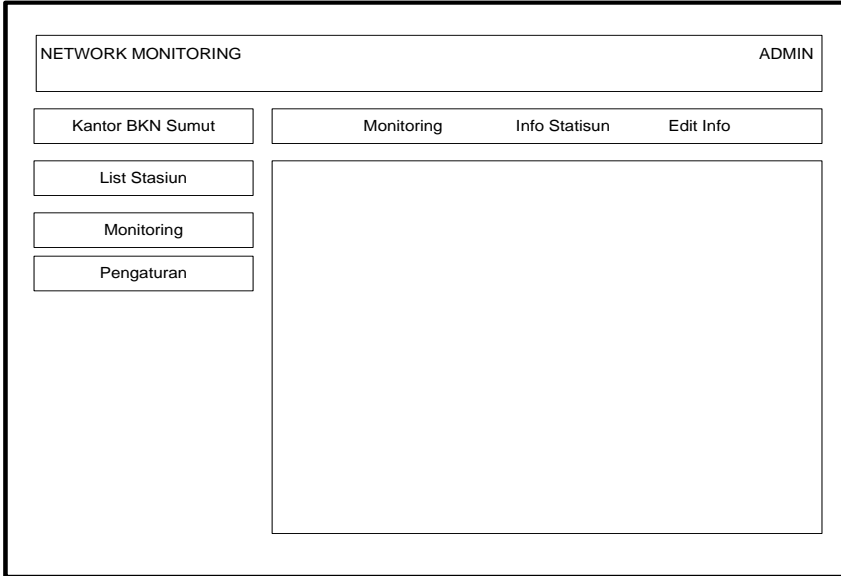
3.8.1 Desain Form Halaman Login



The image shows a wireframe for an AdminLogin page. At the top center, there is a rectangular box containing the text "AdminLogin". Below this, there are two rows of input fields. The first row has a label "USERNAME" on the left and an empty input box on the right. The second row has a label "PASSWORD" on the left and an empty input box on the right. Below these two rows, there is a single button labeled "LOG IN" centered horizontally.

Gambar 3.6 Rancangan Halaman Login

3.8.2 Desain Form Halaman Admin



The image shows a wireframe for an Admin dashboard. At the top, there is a header bar with "NETWORK MONITORING" on the left and "ADMIN" on the right. Below the header, there is a navigation bar with four buttons: "Kantor BKN Sumut", "Monitoring", "Info Stasisun", and "Edit Info". On the left side, there is a vertical sidebar with three buttons: "List Stasiun", "Monitoring", and "Pengaturan". The main content area is a large empty rectangular box.

Gambar 3.7 Rancangan Halaman Admin

3.8.3 Desain Form Halaman Monitoring

The wireframe shows a page titled "NETWORK MONITORING" with "ADMIN" in the top right corner. Below the title is a button labeled "Kantor BKN Sumut". To the left of the main content area are three buttons: "List Stasiun", "Monitoring", and "Pengaturan". The main content area features a table with the following headers: "No", "Nama Client", "IP Client", "Status", and "Aksi". Below the table header are four empty rows, representing the data table.

Gambar 3.8 Rancangan Tampilan Halaman Monitoring

3.8.4 Desain Form Halaman Tambah Client

The wireframe shows a page titled "NETWORK MONITORING" with "ADMIN" in the top right corner. Below the title is a button labeled "Kantor BKN Sumut". To the right of this button are three buttons: "Monitoring", "Info Statisun", and "Edit Info". Below these buttons are three input fields: "Host Name", "Ip Client", and "Stasiun". Below the input fields is a "Simpan" button. To the left of the main content area are three buttons: "List Stasiun", "Monitoring", and "Pengaturan".

Gambar 3.9 Rancangan Tampilan Halaman Tambah Client

3.8.5 Desain Form Halaman Tambah Stasiun

NETWORK MONITORING ADMIN

Kantor BKN Sumut Monitoring Info Stasisun Edit Info

List Stasiun Nama Stasiun

No Telp

Monitoring Alamat

Pengaturan

Simpan

Gambar 3.10 Rancangan Tampilan Halaman Tambah Stasiun

BAB IV

HASIL DAN PEMBAHASAN

4.1 Implementasi Sistem

Implementasi sistem adalah langkah-langkah atau prosedur-prosedur yang dilakukan dalam menyelesaikan desain sistem yang telah disetujui, untuk menguji, menginstal dan memulai sistem baru atau yang diperbaiki untuk menggantikan sistem yang lama. Adapun langkah-langkah yang dibutuhkan dalam implementasi sistem adalah:

1. Mendapatkan software dan hardware yang tepat/sesuai untuk merancang website.
2. Menyelesaikan rancangan sistem.
3. Menulis, menguji, mengontrol dan mendokumentasikan website.
4. Mendapatkan persetujuan.

4.2 Tujuan Implementasi Sistem

Tujuan Implementasi Sistem adalah sebagai berikut:

1. Menyelesaikan desain sistem yang telah disetujui sebelumnya.
2. Memastikan bahwa pemakai (user) dapat mengoperasikan sistem baru.
3. Menguji apakah sistem baru tersebut sesuai dengan pemakai.

Memastikan bahwa konversi ke sistem baru berjalan yaitu dengan membuat rencana, mengontrol dan melakukan instalasi baru secara benar.

4.3 Komponen Utama Dalam Sistem

Untuk menjalankan sistem yang telah dirancang, dibutuhkan beberapa komponen, antara lain:

4.3.1 Hardware

Merupakan suatu komponen yang sangat dibutuhkan dalam mewujudkan sistem yang diusulkan. Dalam hal ini, dapat dirincikan spesifikasi komponen hardware yaitu:

1. PC dengan processor minimal Intel Pentium III 733 MHz.
2. Hard disk 20 GB.
3. Monitor Super VGA.
4. Memory minimal 128 MB.
5. Keyboard.
6. Mouse.
7. Printer.

4.3.2 Software

Hardware tidak akan memecahkan suatu masalah tanpa adanya komponen software. Adapun software yang sering digunakan dalam pembuatan website ini adalah:

1. Sistem operasi Ms. Windows XP.
2. XAMPP Version 1.7.7 software yang merangkum Apache 2.2.21 sebagai web server, PHP 5.3.8 sebagai web programming dan MySQL 5.0.8 sebagai database server.
3. Adobe Dreamweaver CS5 sebagai web editor.

4. Adobe Photoshop CS5 sebagai desain layout.

4.3.3 Brainware

Brainware adalah semua pihak yang bertanggung jawab dalam pengembangan informasi, pemrosesan dan penggunaan keluaran informasi.

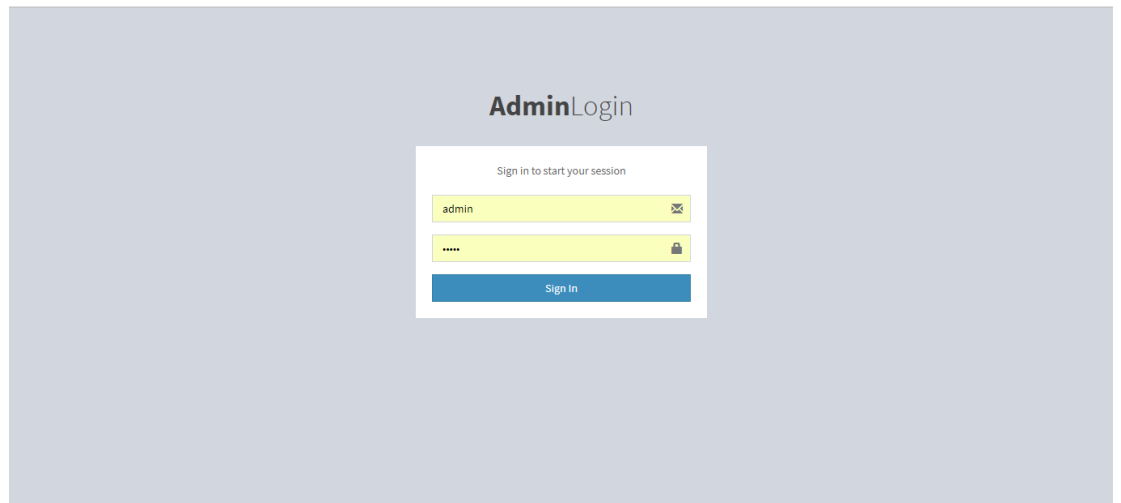
Brainware dalam sistem ini terbagi atas:

1. Sistem analis: orang yang menganalisa sistem dengan mempelajari masalah- masalah yang timbul dan menentukan kebutuhan-kebutuhan pemakai dan mengidentifikasi pemecahan yang beralasan.
2. Programmer: orang yang membuat sistem dengan menggunakan salah satu bahasa pemrograman yang dikuasainya.
3. Operator: orang yang menggunakan dan memanfaatkan sistem.

4.4 Tampilan Website

4.4.1 Halaman Log In Sistem

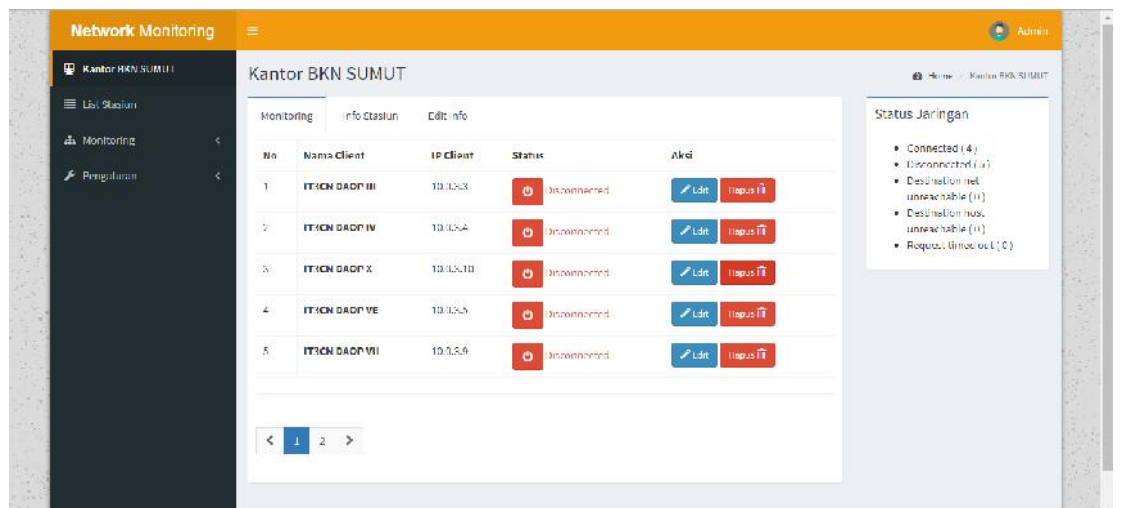
Halaman ini apabila admin ingin melakukan monitoring jaringan, maka admin harus login terlebih dahulu.



Gambar 4.1 Halaman Log In Account

4.4.2 Halaman Tampilan Halaman Admin

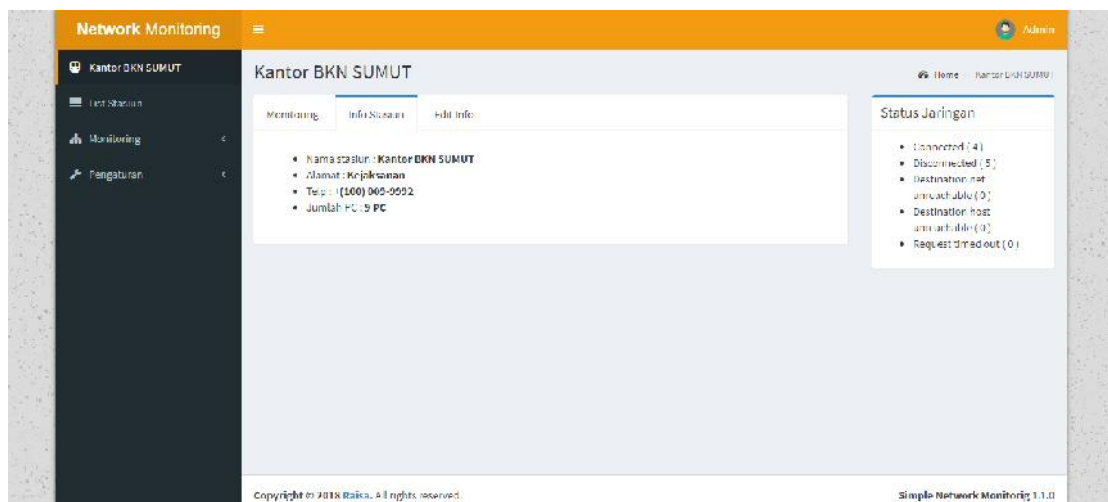
Halaman ini adalah halaman admin untuk monitoring jaringan pada kantor BKN Sumatera Utara:



Gambar 4.2 Halaman Admin

4.4.3 Halaman Tampilan Halaman Info Stasiun

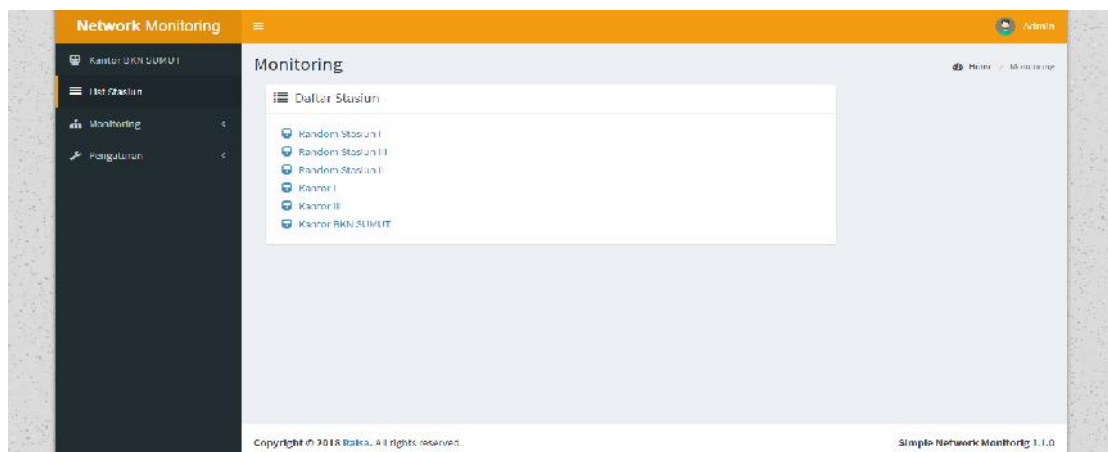
Halaman ini adalah halaman info untuk mengetahui alamat kantor BKN Sumatera Utara:



Gambar 4.3 Halaman Info Stasiun

4.4.4 Halaman Tampilan Halaman Daftar Stasiun

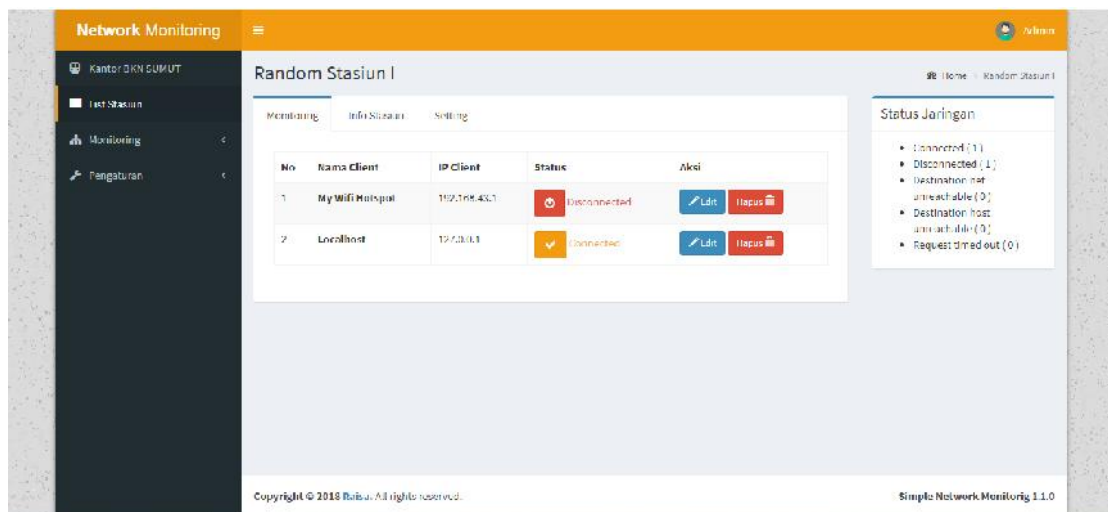
Halaman ini adalah halaman daftar untuk mengetahui daftar stasiun di kantor BKN Sumatera Utara:



Gambar 4.4 Halaman Daftar Stasiun

4.4.5 Halaman Tampilan Halaman Monitoring Stasiun

Halaman ini adalah halaman monitoring untuk mengetahui nama-nama client di kantor BKN Sumatera Utara:



Gambar 4.5 Halaman Tampilan Halaman Monitoring Stasiun

4.5 Pengujian Black Box

Untuk dapat menggunakan aplikasi ini dengan baik, dibutuhkan seperangkat komputer dengan spesifikasi minimal. Black Box pengujian adalah metode pengujian perangkat lunak yang menguji fungsionalitas aplikasi yang bertentangan dengan struktur internal atau kerja. Metode uji dapat diterapkan pada semua tingkat pengujian perangkat lunak: unit, integrasi, fungsional, sistem dan penerimaan.

Tabel 5.1 Tabel Pengujian Black Box

No	Rancangan Proses	Hasil Yang Diharapkan	Hasil	Keterangan
1	Halaman Utama Interaktif dan Mudah Digunaka	Halaman Admin (Awal)	Sesuai	-
2	Monitoring Jaringan	Halaman Monitoring	Sesuai	-
3	Monitoring Stasiun Jaringan	Halaman Info Jaringan	Sesuai	-
4	Monitoring Status Jaringan	Halaman Daftar Jaringan	Sesuai	-

4.6 Kelebihan dan Kekurangan Sistem

Adapun kelebihan dan kekurangan dari media pembelajaran ini adalah sebagai berikut:

a. Kelebihan Sistem

- Lebih mudah diakses.
- Proses Monitoring menjadi lebih gampang.
- Proses perbaikan jaringan menjadi cepat dan bisa di control dari website.

b. Kekurangan Sistem

- Masih bersifat jaringan local.
- Sebaiknya dapat digunakan pada Android.

BAB V

PENUTUP

5.1 Kesimpulan

Adapun kesimpulan dari penelitian yang dilakukan di kantor Badan Kepegawaian Negara (BKN) di Sumut, dapat ditarik kesimpulan sebagai berikut :

- a. Hasil Web telah dapat menghubungkan semua lantai yang terdapat di kantor BKN VI Medan, baik dari Lantai I ke Lantai II dan Lantai III.
- b. Hasil Web ini juga berguna untuk pemeliharaan dan pengembangan jaringan di Kantor Badan Kepegawaian Negara Wilayah VI Medan.

5.2 Saran

Setelah melakukan penelitian di Kantor Badan Kepegawaian Negara Wilayah VI Medan, maka penulis memberikan beberapa saran sebagai pertimbangan jika suatu saat ingin mengembangkan sistem perbaikan dan keamanan jaringan. Saran yang diusulkan sebagai berikut :

- a. Melakukan pengamanan fisik dari perangkat keras jaringan atau hardware agar terhindari kerusakan fisik dan mengurangi resiko perangkat keras bersinggungan langsung dengan benda disekitar.
- b. Meningkatkan sistem keamanan jaringan dengan melakukan pemantauan atau pun memperbarui konfigurasi sistem secara berkala jika diperlukan.

DAFTAR PUSTAKA

- Ahmad Muammar.W.K. 2004. Firewall keamanan jaringan. Penerbit jasakom.
- Al-Fattah, Hanif, 2007, "Analisis dan Perancangan sistem informasi untuk keunggulan bersaing perusahaan dan organisasi modern", Yogyakarta: Andi Offset.
- Andrian, Yudhi, and Purwa Hasan Putra. "Analisis Penambahan Momentum Pada Proses Prediksi Curah Hujan Kota Medan Menggunakan Metode Backpropagation Neural Network." Seminar Nasional Informatika (SNIF). Vol. 1. No. 1. 2017.
- Ariyus, Dony, 2006, Computer Security, Penerbit Andi, Yogyakarta.
- Ariyus, Dony, 2014 Intrusion Detection System, Sistem Pendeteksian Penyusupan
- Aryza, S., Irwanto, M., Lubis, Z., Siahaan, A. P. U., Rahim, R., & Furqan, M. (2018). A Novelty Design Of Minimization Of Electrical Losses In A Vector Controlled Induction Machine Drive. In IOP Conference Series: Materials Science and Engineering (Vol. 300, No. 1, p. 012067). IOP Publishing.
- Barus, S., Sitorus, V. M., Napitupulu, D., Mesran, M., & Supiyandi, S. (2018). Sistem Pendukung Keputusan Pengangkatan Guru Tetap Menerapkan Metode Weight Aggregated Sum Product Assesment (WASPAS). Jurnal Media Informatika Budidarma, 2(2).
- Batubara, Supina. "Analisis perbandingan metode fuzzy mamdani dan fuzzy sugeno untuk penentuan kualitas cor beton instan." IT Journal Research and Development 2.1 z, Supina, Sri Wahyuni, and Eko Hariyanto. "Penerapan Metode Certainty Factor Pada Sistem Pakar Diagnosa Penyakit Dalam." Seminar Nasional Royal (SENAR). Vol. 1. No. 1. 2018.
- Fachri, Barany. "Perancangan Sistem Informasi Iklan Produk Halal Mui Berbasis Mobile Web Menggunakan Multimedia Interaktif." Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika) 3 (2018): 98-102.
- Gollmann, 2013, Computer Security. Penerbit jasakom.

- Hongdoyo, Fandy, 2013, "Perancangan Bodi Sepeda Motor Jupiter MX Yang Sesuai Dengan Keinginan Konsumen Kelompok Umur 17 – 23 Tahun". *Jurnal Ilmiah Mahasiswa Universitas Surabaya* Volume 2 No. 1.
- Jogiyanto, Hm. 2015,"Analisis dan Desain Sistem Informasi Pendekatan Terstruktur", edisi ketiga. Yogyakarta: Andi Offset.
- Kendall Keneth E, Kendal Julie E, 2006, Analisis dan Perancangan Sistem edisi lima jilid 1, Gramedia, Jakarta
- Khairul, K., IlhamiArsyah, U., Wijaya, R. F., & Utomo, R. B. (2018, September). Implementasi Augmented Reality Sebagai Media Promosi Penjualan Rumah. In *Seminar Nasional Royal (Senar)* (Vol. 1, No. 1, pp. 429-434).
- Kurniawan, H. (2018). Pengenalan Struktur Baru untuk Web Mining dan Personalisasi Halaman Web. *Jurnal Teknik dan Informatika*, 5(2), 13-19
- Kusrini, 2007, Konsep dan Aplikasi Sistem Pendukung Keputusan, CV Andi Offset, Yogyakarta
- Mayasari, Nova. "Comparison of Support Vector Machine and Decision Tree in Predicting On-Time Graduation (Case Study: Universitas Pembangunan Panca Budi)." *Int. J. Recent Trends Eng. Res* 2.12 (2016): 140-151.
- Media Komputindo.
Pada Jaringan Komputer. Penerbit Andi, Yogyakarta.
- Putra, Randi Rian, and Cendra Wadisman. "Implementasi Data Mining Pemilihan Pelanggan Potensial Menggunakan Algoritma K Means." *INTECOMS: Journal of Information Technology and Computer Science* 1.1 (2018): 72-77.
- Rahardho, Nurlita Caesariany, 2013, "Pembuatan Sistem Informasi Geografis (SIG) Pencarian Lokasi Bengkel". *Jurnal Ilmiah Mahasiswa Universitas Surabaya* Volume 2 No. 2.
- Rahim, R., Supiyandi, S., Siahaan, A. P. U., Listyorini, T., Utomo, A. P., Triyanto, W. A., ... & Khairunnisa, K. (2018, June). TOPSIS Method Application for Decision Support System in Internal Control for Selecting Best Employees. In *Journal of Physics: Conference Series* (Vol. 1028, No. 1, p. 012052). IOP Publishing.
- Rosa.A.S.M.Shalahuddin (2014) *Pemodelan system Rekayasa perangkat lunak*. Jakarta: PT. Elex Media Komputindo
- Sari, R. D., Supiyandi, A. P. U., Siahaan, M. M., & Ginting, R. B. (2017). A Review of IP and MAC Address Filtering in Wireless Network Security. *Int. J. Sci. Res. Sci. Technol*, 3(6), 470-473.

- Sheren, 2013, “ Aplikasi Web Manajemen Proyek Sistem Informasi”. Jurnal Mahasiswa Universitas Surabaya Volume 2 No. 2.
- Siahaan, A. P. U., Aryza, S., Nasution, M. D. T. P., Napitupulu, D., Wijaya, R. F., & Arisandi, D. (2018). Effect of matrix size in affecting noise reduction level of filtering.
- Siahaan, MD Lesmana, Melva Sari Panjaitan, and Andysah Putera Utama Siahaan. "MikroTik bandwidth management to gain the users prosperity prevalent." Int. J. Eng. Trends Technol 42.5 (2016): 218-222.
- Sidik, A. P. (2018). Algoritma RSA dan Elgamal sebagai Algoritma Tambahan untuk Mengatasi Kelemahan Algoritma One Time Pad pada Skema Three Pass Protocol.
- Simarmata Janner, 2010, Rekayasa Perangkat Lunak, Andi Offset, Yogyakarta.
- Sinaga, Dian , 2014, Jenis Program Pencurian Informasi. Penerbit Andi, Yogyakarta.
- Sinaga, Dian, 2014, Jenis Penyerangan. Penerbit Andi, Yogyakarta
- Sugeng winarno, 2010, Jaringan Komputer dengan TCP/IP, Modula, Bandung.
- Sutanta, Edhy. 2011. Sistem Informasi Manajemen Database. Jakarta : Penerbit
- Tasril, V. (2018). Sistem Pendukung Keputusan Pemilihan Penerimaan Beasiswa Berprestasi Menggunakan Metode Elimination Et Choix Traduisant La Realite. INTECOMS: Journal of Information Technology and Computer Science, 1(1), 100-109.
- Thersia Arie Prabawati, 2011, Keamanan Sistem Informasi/IBISA. Penerbit Andi,
- Uning Lestari, Marwoto, Agustus 2012, “Aplikasi Sistem Informasi Geografis Pemetaan Digital Loop Carrier”. Jurnal Teknologi Technoscientia Volume 5 No.1.
- Yosef Murya Kusuma Ardhana, 2017. Script PHP. Penerbit, Jasakom