ANALISIS DAN IMPLEMENTASI IDS PADA WIRELESS NETWORK SECURITY BERBASIS MIKROTIK DI PT BAYU PARIAMA BATAM

SKRIPSI

Oleh:
Kornelius Harianja
130210328

PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS PUTERA BATAM
2017

ANALISIS DAN IMPLEMENTASI IDS PADA WIRELESS NETWORK SECURITY BERBASIS MIKROTIK DI PT BAYU PARIAMA BATAM

SKRIPSI
Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Oleh:
Kornelius Harianja
130210328

PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS PUTERA BATAM
201

PERNYATAAN

Dengan ini saya menyatakan bahwa:

1. Skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik sarjana, baik di Universitas Putera Batam maupun di perguruan tinggi lain.
2. Skripsi ini adalah murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing.
3. Dalam skripsi ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi.

Batam, Februari 2017

Yang membuat pernyataan,

Materai Rp. 6.000

Kornelius Harianja

130210328

ANALISIS DAN IMPLEMENTASI IDS PADA WIRELESS NETWORK SECURITY BERBASIS MIKROTIK DI PT BAYU PARIAMA BATAM

Oleh:
Kornelius Harianja
130210328

SKRIPSI
Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Telah disetujui oleh Pembimbing pada tanggal
Seperti tertera di bawah ini

Batam, 16 Februari 2017

Very Karnadi, S.Kom.,M. Kom.
Pembimbing

ABSTRAK

Kejahatan dari pencurian informasi atau lebih dikenal dengan sebutan *cybercrime*, mengganggu aktifitas jaringan wireles, dan sampai pengrusakan sistem menjadi permasalahan yang dialami PT.Bayu Pariama Batam. Seringkali jaringan di instansi swasta tersebut mengalami down, koneksi semakin lambat, dan memungkinkan adanya penyusup yang mengakses informasi penting yang ada di perusahaan tersebut. Walau belum dapat dipastikan jaringan trouble dikarenakan kesalahan teknis, yang jelas di PT. Bayu Pariama Batam belum menerapkan keamanan jaringan sehingga keseluruhan sistem jaringan pada saat sekarang masih bisa diakses oleh siapapun dan hal tersebut bisa disalahgunakan oleh pihak yang tidak bertanggung jawab. Untuk itu pada penelitian ini menulis menawarkan sistem keamanan jaringan menggunakan *Intrusion Detection System (IDS)* untuk dipasang di PT Bayu Pariama Batam. IDS ini bertugas sebagai pengawas sistem yang akan melakukan identifikasi akses oleh siapa saja yang menggunakan sistem. mesin *tools* IDS yang akan digunakan pada penelitian ini menggunakan *snort* yang akan diintegrasikan dengan jaringan komputer.

Kata kunci: jaringan *wireless*, *keamanan jaringan, Intrusion Detection System, snort.*

ABSTRACT

The crime information of the thive or known as sybercrime, distrub the activities of the wireless network, and the destruction of the system make at the issue being facing by Bayu Pariama Batam Company. Frequently the network of the private limited agency experience down, the connection in slow, and allow intruders can access the file information of the company. Althougt uncertain troble network due to of the technical errors, obviously Bayu Pariama Batam Company does not implement network security yet so that the whole system of the network until right now, network system can be used by irresponsible parties. Therefore, the research makes offering network security which Intrusion Detection system (IDS) to be installed in Bayu Pariama Batam Company. IDS has function as the regulatory system that will do an identify acces by anyone who uses the system. The tools machine will be used at the system. The tools will be integrated by computer network.

Keywords: Network Security, Intrusion Detection System,Snort.

KATA PENGANTAR

Segala puji syukur penulis panjatkan kehadapan Allah Yang Maha Kuasa atas segala rahmatnya-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Ibu Elfi Husda, S.Kom., M.SI. sebagai Rektor Universitas Putera Batam
2. Ketua Program Studi Teknik Informatika Andi Maslan, S.T., M.SI.
3. Very Karnadi, S.Kom., M.Kom. sebagai pembimbing Skripsi pada Program Studi Teknik Informatika Universitas Putera Batam
4. Dosen dan Staff Universitas Putera Batam.
5. Bapak Sarmudin Sinaga, S.T. sebagai Direktur PT Bayu Pariama Batam
6. Seluruh karyawan dan staff PT Bayu Pariama Batam
7. Istri saya Riana Lumban Raja yang sangat saya sayangi dan saya cintai yang selalu memberi dorongan, dukungan, doa, motivasi dan pengorbananya sehingga penulis dapat menyelesaikan skripsi ini
8. Ibu saya yang sangat saya hormati dan saya sayangi yang selalu memberikan dorongan, mendoakan, memberikan motivasi kepada penulis sehingga penulis dapat menyelesaikan skripsi ini
9. Kedua anak saya Teresa Tiur Harianja dan Bonifasius Bona Harianja yang selalu membuat saya semangat dalam selesainya skripsi ini
10. Buat teman-teman sekelas serta seperjuangan penulis terima kasih atas dukungan dan doanya

11. Terima kasih juga kepada semua pihak yang telah membantu dalam penyelesaian skripsi ini yang tidak dapat disebutkan satu per satu.

Semoga Allah Yang Maha Kuasa membalas kebaikan dan selalu memberkati kita semua, Amin.

Batam, 15 Februari 2017

Penulis

DAFTAR ISI

HALAMAN PERNYATAAN i
HALAMAN PENGESAHAN ii
KATA PENGANTAR iii
ABSTRAK v
AVSTRAK vi
DAFTAR ISI vii
DAFTAR TABEL ix
DAFTAR GAMBAR x
DAFTAR LAMPIRAN xii

BAB I: PENDAHUAN 1
1.1. Latar Belakang Penelitian 1
1.2. Identifikasi Masalah 4
1.3. Pembatasan Masalah 5
1.4. Perumusan Masalah 5
1.5. Tujuan Penelitian 6
1.6. Manfaat Penelitian 6

BAB II: KAJIAN PUSTAKA.....8
2.1. Teori Dasar 8
2.1.1. Jaringan Komputer 8
2.1.2. Standar Jaringan Komputer 9
2.1.2.1. Organisasi Dunia untuk standardisasi Jaringan 9
2.1.3. Jenis Jaringan Komputer 11
2.1.3.1. Berdasarkan Ruang Lingkup 11
2.1.3.2. Berdasarkan Topologi 12
2.1.3.3. Berdasarkan Fungsi 14
2.1.3.4. Berdasarkan Media Penghantar 14
2.1.4. Model OSI *layer* 15
2.1.5. Jaringan wireless 19
2.1.6. Mikrotik Wireless.....20
2.1.7. Model Referensi TCP/IP 21
2.1.8. User Diagram Protokol (UDP) 21
2.2. Teori Khusus 22
2.2.1. Keamanan Komputer 23
2.2.1.1. Tujuan Keamanan Jaringan 24
2.2.2. *Intrusion Detection System* (IDS) 24
2.2.2.1. Peran *Intrusion Detection System* 25
2.2.2.2. Tipe *Intrusion Detection System* 26
2.2.2.3. Analisys Console Intrusion Database 31
2.2.3. Snort 32
2.2.3.1. Komponen-Komponen Snort 34

2.2.3.2. Mode Snort 35
2.2.3.3. Snort Rule 38
2.2.4. Firewall 40
2.3. Tools 43
2.3.1. ISP (Internet Service Provider) 43
2.3.2. Perangkat Keras (Hardware) 44
2.3.3. Sofware dan Aplikasi System 48
2.4. Penelitian Terdahulu 52
2.5. Kerangka Pemikiran 55

BAB III: METODOLOGI PENELITIAN 57
3.1. Desain Penelitian.....57
3.2. Analisis Jaringan Lama 61
3.3. Analisis Jaringan Yang Dibangun 62
3.4. Lokasi dan Jadwal Penelitian 64
3.4.1. Lokasi Penelitian 64
3.4.2. Jadwal Penelitian..... 64

BAB IV: HASIL PENELITIAN DAN PEMBAHASAN 66
4.1. Hasil Penelitian 66
4.1.1 Implementasi 66
4.1.1.1. Tahap Penginstalan Aplikasi *snorrt* 68
4.1.1.3. Tahap Konfigurasi *Snort* 73
4.1.1.3. Tahap Instalasi *Wireshark* 82
4.1.1.4. Tahap Pengujian *Snort* 86
4.2. Pembahasan..... 91

BAB V: KESIMPULAN DAN SARAN 92
5.1. Kesimpulan 92
5.2. Saran 92

DAFTAR PUSTAKA 94
DAFTAR RIWAYAT HIDUP
SURAT KETERANGAN PENELITIAN
LAMPIRAN

DAFTAR TABEL

Tabel 2.1 Tabel perbandingan NIDS dan HIDS 30
Tabel 2.2 Spesifikasi *Hardware Client* 44
Tabel 3.1 Jadwal Penelitian 58
Tabel 4.1 IP Address pada jaringan PT Bayu Pariama Batam 67

DAFTAR GAMBAR

Gambar 2.1 Susunan *Layer* OSI 15
Gambar 2.2 *Host-Based* IDS 27
Gambar 2.3 Network-*Based* IDS 29
Gambar 2.4 Cara Kerja Snort IDS 33
Gambar 2.5 Internet Service Provider 43
Gambar 2.6 Komputer Server 44
Gambar 2.7 Komputer *Client* 45
Gambar 2.8 Modem ADSL 46
Gambar 2.9 Switch 46
Gambar 2.10 Router Mikrotik RB 750 Gr2 47
Gambar 2.11 Tampilan *Snort* 48
Gambar 2.12 Tampilan *Wireshark* 49
Gambar 2.13 Tampilan *WinPcap* 49
Gambar 2.14 Operating *System* 50
Gambar 2.15 Kerangka Pemikiran 55

Gambar 3.1 Langkah *Action Research* 58
Gambar 3.2 Metodologi Penelitian 59
Gambar 3.3 Topologi Implementasi *Snort* 60
Gambar 3.4 Topologi Jaringan PT Bayu Pariama Batam 61
Gambar 3.5 Topologi Jaringan PT Bayu Pariama Batam Yang Baru 62

Gambar 4.1 IP Scanner 68
Gambar 4.2 Instalasi *Snort* 1 69
Gambar 4.3 Instalasi *Snort* 2 69
Gambar 4.4 Instalasi *Snort* 3 70
Gambar 4.5 Instalasi *Snort* 4 70
Gambar 4.6 Instalasi *Snort* 5 71
Gambar 4.7 Instalasi *Snort* 6 71
Gambar 4.8 Instalasi *Snort* 7 72
Gambar 4.9 Instalasi *Snort* 8 72
Gambar 4.10 Instalasi *Snort* 9 73
Gambar 4.11 Konfigurasi *Snort* 1 73
Gambar 4.12 Konfigurasi *Snort* 2 74
Gambar 4.13 Konfigurasi *Snort* 3 74
Gambar 4.14 Konfigurasi *Snort* 4 75
Gambar 4.15 Konfigurasi *Snort* 5 75
Gambar 4.16 Konfigurasi *Snort* 6 76
Gambar 4.17 Konfigurasi *Snort* 7 76
Gambar 4.18 Konfigurasi *Snort* 8 77
Gambar 4.19 Konfigurasi *Snort* 9 77

Gambar 4.20 Konfigurasi *Snort* 10 78
Gambar 4.21 Konfigurasi *Snort* 11 78
Gambar 4.22 Konfigurasi *Snort* 12 79
Gambar 4.23 Konfigurasi *Snort* 13 79
Gambar 4.24 Konfigurasi *Snort* 14 79
Gambar 4.25 Konfigurasi *Snort* 15 80
Gambar 4.26 Konfigurasi *Snort* 16 80
Gambar 4.27 Konfigurasi *Snort* 17 81
Gambar 4.28 Konfigurasi *Snort* 18 81
Gambar 4.29 Konfigurasi *Snort* 19 82
Gambar 4.30 Konfigurasi *Snort* 20 82
Gambar 4.31 Instal *Wireshark* 1 83
Gambar 4.32 Instal *Wireshark* 2 83
Gambar 4.33 Instal *Wireshark* 3 84
Gambar 4.34 Instal *Wireshark* 4 84
Gambar 4.35 Instal *Wireshark* 5 85
Gambar 4.36 Instal *Wireshark* 6 85
Gambar 4.37 Instal *Wireshark* 7 86
Gambar 4.38 IP Address google.com 87
Gambar 4.39 Hasil capture snort dari ping google.com 87
Gambar 4.40 Hasil capture wireshark dari google.com 88
Gambar 4.41 Hasil capture c:\user dari facebook.com 88
Gambar 4.42 Hasil capture snort dari facebook.com 89
Gambar 4.43 Hasil capture wireshark dari facebook.com 89
Gambar 4.44 Hasil capture c:\user ping of death 89
Gambar 4.45 Hasil capture snort mendeteksi ping of death 90
Gambar 4.46 Hasil capture Wireshark mendeteksi ping of death 90
Gambar 4.47 Hasil capture log yang terdeteksi ping of death 90

DAFTAR LAMPIRAN

Lampiran 1 Foto Penelitian
Lampiran 2 Konfigurasi snort

BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Jaringan komputer saat ini memasuki era *wireless* atau nirkabel yang memungkinkan pengguna jaringan bisa memperluas area kerja mereka sehingga tidak terkait dengan penggunaan kabel. Penerapan jaringan *wireless* memberikan kemudahan dalam berkomunikasi atau transaksi data, yang ternyata terdapat beberapa kelemahan pada segi keamanannya. Jaringan *wireless* tidak memiliki jalur pertahanan yang jelas, sehingga setiap komputer pengguna harus siap terhadap gangguan ataupun serangan yang mungkin terjadi.

PT Bayu Pariama Batam adalah sebuah perusahaan swasta yang bergerak di bidang developer real estate yang beralamat di Komplek Pertokoan Kuda Putih Blok A No. 2 Sei Panas Batam. Kecepatan jaringan komputer diperlukan untuk memperlancar karyawan dapat bekerja dengan efektif dan efisien dalam menjalankan tugasnya masing-masing. Keamanan informasi data haruslah mendapat perhatian khusus terutama pada sebuah perusahaan besar yang lalu lintas data nya sangat tinggi. Jaringan *wireless* di PT. Bayu Pariama Batam saat ini sering terdapat keluhan seperti penurunan performa jaringan internet yang selanjutnya dapat berimbas ke semua komputer yang terhubung pada jaringan tersebut. Untuk mengatasi hal tersebut, perlu diterapkan metode pendeteksian terhadap kasus yang terjadi di dalam lingkungan PT Bayu Pariama Batam yang

diharapkan dapat membantu administrator dalam memonitor kondisi jaringannya dan meningkatkan mutu jaringan tersebut.

Keamanan jaringan bergantung pada kecepatan pengaturan jaringan dalam menindaklanjuti sistem saat terjadi gangguan. Penerapan IDS diusulkan sebagai salah satu solusi yang dapat digunakan untuk membantu pengatur jaringan dalam memantau kondisi jaringan dan menganalisa paket-paket berbahaya dalam jaringan tersebut. Keamanan jaringan terus mendapat perhatian yang serius dan diciptakan berbagai *sofware* aplikasi dan *tools* untuk menjaga usaha penyusupan dan pencurian data, banyak *tools* yang ada saat ini memiliki cara kerja yang berbeda. Dalam keamanan jaringan diperlukan *tools* yang berfungsi mendeteksi jaringan atau *Intrusion Detection Sistem* (IDS) salah satu *tools* adalah menggunakan *snort* yang dapat digunakan untuk mendeteksi dan adanya lalu lintas data yang tidak normal. *Tools* ini adalah sistem yang berfungsi sebagai alat pendeteksi serangan yang berusaha masuk ke sistem jaringan, dan jika terdapat serangan *snort* akan memberikan *alert* kepada administrator. Lalu lintas data yang tinggi yang menghasilkan *log* dengan perubahan data per sekian detik, sehingga tidak memungkinkan bagi *network admin* optimal dalam memantau lalu lintas data.

Pada dasarnya IDS terbagi menjadi dua jenis yaitu *host-based* dan *network-based*. Sistem *host-based* bekerja pada host yang akan dilindungi. IDS jenis ini dapat melakukan berbagai macam tugas untuk mendeteksi serangan yang dilakukan pada *host* tersebut, sedangkan *network-based* biasanya berupa suatu mesin yang khusus dipergunakan untuk memonitoring seluruh segmen dari

jaringan. IDS *network-based* akan mengumpulkan paket-paket data yang terrdapat pada jaringan dan kemudian menganalisisnya serta menentukan apakah paket-paket itu berupa suatu paket yang normal atau serangan atau berupa aktifitas yang mencurigakan.

Adapun alasan dalam pemakaian *snort* karena *software* tersebut *open source* dan interfacenya mudah dipahami (GUI) sehingga memudahkan dalam pengoperasiannya. Namun Perlu diingat bahwa saat ini *snort* bekerja dalam modus *Intrusion Detection System* (IDS). *Detection* disini benar-benar hanya berarti mendeteksi dan memberitahu bila terjadi serangan. Tidak ada upaya untuk menanggulangi atau menghindari serangan. Hal ini berguna bila *snort* dipakai dalam *honeypo*t, sebuah sistem yang sengaja menarik perhatian *hacker* guna menganalisa teknik serangan *hacker*. *Intrusion Detection System* seperti *Snort* biasanya berada di lapisan sebelum *firewall* sehingga *packet* dapat dianalisa secara lengkap sebelum diteruskan ke *firewall*. Secara spesifik, aplikasi *Snort* memiliki kemampuan untuk mendeteksi dan menangkal peluang-peluang ancaman terkini, seperti serangan *buffer overflow*, kode-kode berbahaya, serangan *Deniel of Services* (DOS), pemindai port-port, pemindaian kelemahan-kelemahan jaringan sistem, *SMB probes*, OS *figer printing*, serangan berbasisi CGI, serangan aplikasi-aplikasi web, penyusupan, dan usaha-usaha pendobrakan sistem atau *hacking*.

Berdasarkan penelitian Budiman, (2014, ISSN: 2338-6313) yang berjudul "Implementasi Intrusion Detection System (IDS) Pada Server Debian Menggunakan Media Sosial Sebagai Media Notifikasi" setelah dilakukan

pengujian dapat ditarik kesimpulan, bahwa implementasi IDS dengan menggunakan jejaring sosial sebagai media notifikasi dan dapat mengetahui serangan sesuai dengan *rule* yang ditetapkan sehingga jejaring sosial dapat melakukan notifikasi sesuai dengan jenis serangan yang sudah didefenisikan.

Menurut (Ariyus 2007:146), *snort* merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisa paket yang melintas jaringan real time traffic dan logging ke dalam database serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan. *Snort* bisa digunakan pada platform sistem operasi Linux, BSD, SOL *windows*, dan sistem operasi lainnya. *Snort* sudah di-download lebih dari 3 juta orang. Hal ini menandakan bahwa *snort* merupakan suatu *Intrusion Detection System* yang dipakai banyak orang di dunia.

Berdasarkan penjelasan singkat diatas penulis tertarik melakukan penelitian pada PT Bayu Pariama Batam dengan judul **"ANALISIS DAN IMPLEMENTASI IDS PADA WIRELESS NETWORK SECURITY BERBASIS MIKROTIK DI PT BAYU PARIAMA BATAM"**

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan di atas maka pada penelitian ini dapat diidentifikasikan masalah sebagai berikut:

1. Belum adanya evaluasi keamanan jaringan di PT Bayu Pariama Batam.
2. Belum adanya metode pencegahan dengan melakukan pendeteksian serangan secara awal untuk meminimalkan resiko dan kemudian dapat

melakukan pencegahan secara tepat sehingga administrator dapat menentukan tindakan jika terdapat hal yang mengganggu keamanan jaringan.

1.3 Pembatasan Masalah

Sehubungan dengan keterbatasan waktu untuk melakukan penelitian, maka pada penelitian ini dibuat batasan masalah. Adapun batasan masalah yang akan dibahas sebagai berikut:

1. Sistem Operasi yang digunakan dilakukan pada *platform* Windows 7. Untuk melakukan proses penyerangan aplikasi yang digunakan adalah ping attach, Wireshark. Untuk mencegah serangan adalah menggunakan *iptables*.
2. Sistem pendeteksi *intrusi* yang dikembangkan berjenis *Network Intrusion Detection System* (NIDS) untuk mendeteksi dan mengetahui adanya lalu lintas data yang tidak normal didalam jaringan PT Bayu Pariama Batam.

1.4 Perumusan Masalah

Berdasarkan penjelasan di atas, maka merumuskan masalah-masalah sebagai berikut:

1. Bagaimana menerapkan sistem IDS sehingga dapat bekerja dalam melakukan analisis jaringan wireless dari serangan?
2. Bagaimana menentukan rule dan mencegah terjadinya penyusupan atau penyerangan pada sistem jaringan komputer?

3. Bagaimana analisis dan implementasi IDS pada lingkungan windows 7?

1.5 Tujuan Penelitian

Berdasarkan pada rumusan masalah yang telah dikemukakan, maka dapat dirumuskan tujuan dilaksanakannya penelitian ini adalah:

1. Untuk melakuan evaluasi keamanan jaringan wireless di PT Bayu Pariama Batam.
2. Untuk menerapkan, memonitoring keamanan, mamahami kelebihan dan kekurangan IDS pada jaringan wireless.
3. Untuk mengetahui serangan yang terjadi di dalam jaringan sehingga dapat melakukan pendeteksian.

1.6 Manfaat Penelitian

a) Aspek Teoritis

Hasil penelitian ini diharapkan dapat menjadi bahan informasi dan referensi bagi perkembangan ilmu pengetahuan khususnya untuk penelitian lebih lanjut mengenai analisis dan implementasi IDS pada jaringan *wireless* berbasis mikrotik dengan menggunakan aplikasi *Snort* untuk menjaga keamanan jaringan dan mengontrol lalu lintas jaringan.

b) Aspek Praktis

Hasil penelitian ini diharapkan dapat menjadi masukan bagi perusahaan dapat membantu administrator jaringan dalam mengawasi dan mendeteksi serangan dan informasi yang diterima administrator yaitu jumlah serangan

yang ada bisa menjadi bahan pertimbangan untuk mengembangkan tingkat keamanan jaringan di PT Bayu Pariama Batam.

BAB II
KAJIAN PUSTAKA

2.1 Teori Dasar

2.1.1 Jaringan Komputer

Menurut Kustanto & Saputro (2015:1), jaringan komputer adalah kumpulan dua atau lebih komputer yang saling berhubungan satu sama lain untuk melakukan komunikasi data dengan menggunakan protokol komunikasi melalui media komunikasi (kabel atau nirkabel), sehingga komputer-komputer tersebut dapat saling berbagi informasi, data, program-program, dan penggunaan perangkat keras secara bersama. Dalam hal ini komunikasi data yang bisa dilakukan melalui jaringan komputer dapat berupa data teks, gambar, video dan suara.

Menurut Daryanto (2010: 22), jaringan komputer merupakan komputer yang berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya, dua buah komputer dikatakan terkoneksi bila keduanya dapat saling bertukar informasi.

Menurut Sofana (2008: 3), jaringan komputer adalah sekumpulan beberapa komputer (perangkat lain seperti printer, hub, dan sebagainya) yang saling berhubung satu sama lain melalui media perantara, media perantara ini bisa berupa data akan mengalir dari satu komputer ke komputer yang lainnya atau dari komputer keperangkat yang lain, sehingga masing-masing komputer yang terhubung tersebut bisa saling bertukar data atau berbagi perangkat keras. Dari

beberapa pendapat para ahli komputer di atas, maka dalam hal ini yang menjadi pengertian jaringan komputer yang menjadi referensi dalam penelitian ini adalah pendapat Kustanto & Saputro yang menyatakan jaringan komputer adalah jaringan komputer adalah kumpulan dua atau lebih komputer yang saling berhubungan satu sama lain untuk melakukan komunikasi data dengan menggunakan protokol komunikasi melalui media komunikasi (kabel atau nirkabel), sehingga komputer-komputer tersebut dapat saling berbagi informasi, data, program-program, dan penggunaan perangkat keras secara bersama.

2.1.2 Standar Jaringan Komputer

Menurut Pratama (2016: 17), di jaringan komputer khususnya internet , terdapat administrasi yang mengatur agar semua proses dan layanan dapat berjalan dengan baik. Dengan perkembangan teknologi yang makin pesat, menjadikan internet Dan jumlah pengguna internet makin bertambah dan berkembang makin besar. Untuk itu diperlukan adanya administrasi dan standarisasi yang baik, sehingga terjadi keseragaman dan keteraturan , yang berujung pada ketertiban dan kenyamanan internet secara global.

2.1.2.1. Organisasi Dunia untuk Standardisasi Jaringan

Menurut Pratama (2016: 117), Terdapat enam buah organisasi dunia yang mengurusi tentang standardisasi jaringan komputer, khususnya internet . Keenam organisasi dunia tersebut meliputi :

1. ISOC *(Internet Society)*

   ISOC *(Internet Sociaty)* merupakan organisasi dunia yang mengurusi tentang pembuatan standarisasi internasional terkait dengan internet dan isu-isu terkait di dalamnya, pembuatan aturan dan kebijakan terkait dengan implementasi internet, pendidikan tentang internet, tata kelola internet, implementasi internet, teknologi teknologi yang dikembangkan dan digunakan di internet, serta perkembangan beragam aplikasi di internet.

2. IAB *(Internet Architecture Board)*

   IAB *(Internet Architecture Board)* merupakan komite internasional bentukan IETF (*Internet Engineering Task Force*).

3. IETF *(Internet Engineering Task Force)*

   IETF *(Internet Engineering Task Force)* merupakan organisasi dunia yang menjadi wadah bagi seluruh komunitas internet yang meliputi para pengguna koneksi internet, perancangan desain arsitektur jaringan internet, vendor atau provider penyedia layanan akses internet, operator, dan juga para ilmuan atau akademisi yang berkecimpung di bidang jaringan internet, untuk bersama-sama menjadikan internet dunia menjadi lebih baik.

4. IANA *(Internet Assigned Number Authority)*

   IANA *(Internet Assigned Number Authority)* merupakan organisasi dunia yang merupakan bagian (dalam hal departemen) dari organisasi ICANN *(Internet Corporation for Assigned Name and Number)*. Sebagai sebuah departemen bentukan ICANN, IANA bertugas mengurusi permasalahan penamaan domain di dalam jaringan komputer (DNS *root*).

5. ICANN *(Internet Corporation For Assigned Name and Number)*

   ICANN *(Internet Corporation for Assigned Name and Number)* merupakan organisasi dunia non profit yang bertujuan untuk menjaga agar internet dunia tetap aman, stabil, nyaman, sehingga mendukung semua kegiatan bisnis, pendidikan, pemerintahan, dan bidang-bidang lainnya.

6. NIC (*Network Information Center)*

   NIC (*Network Information Center)* merupakan organisasi dunia yang berbentuk profit dan nonprofit yang menyediakan sejumlah layanan jasa *(costumer Support)* dan informasi terkait dengan jaringan internet dunia, khususnya pada *Domain name Service* (layanan domain atau alamat pada jaringan internet).

2.1.3 Jenis Jaringan Komputer

Menurut Utomo (2012:3-12), jenis jaringan dapat dibedakan berdasarkan ruang lingkup, berdasarkan tepologi, berdasarkan fungsi, dan berdasarkan media penghantar.

2.1.3.1. Berdasarkan Ruang Lingkup

Menurut Utomo (2012: 2), yang dimaksud dengan ruang lingkup adalah beberapa banyak dan seberapa besar jaringan komputer tersebut akan dibangun. Berdasarkan ruang lingkupnya, sebuah jaringan komputer dapat dibedakan menjadi tiga bagian yaitu :

1. LAN (*Local Area Network*), merupakan jaringan komputer yang dibangun diruang lingkup kecil seperti sebuah perkantoran, sekolah, rumah, atau instansi tertentu. Pembuatan LAN bisa dilakukan hanya dengan sebuah kartu jaringan atau LAN *Card*, sebuah Hub, dan kabel jaringan.
2. MAN (*Metropolitan Area Network*), jaringan komputer ini dibangun untuk kebutuhan ruang lingkup yang besar, bisa mencakup satu kota, misalnya perusahaan tertentu mempunyai sebuah LAN pada area perusahaannya, kemudia beberapa perusahaan dalam satu kota dapat saling terhubung dan membentuk sebuah MAN.
3. Wide Area Network (WAN), merupakan jaringan komputer dengan cakupan area yang lebih luas dan biasanya akan menghubungkan beberapa kesatuan jaringan komputer yang lebih banyak. Koneksi antar jaringan dengan cakupan yang luas tersebut memudahkan kita berbagi sumber daya yang ada sehingga proses berbagi antar komputer atau jaringan dapat dilakukan secara lintas daerah, kota, Negara bahkan Benua.

2.1.3.2. Berdasarkan Topologi

Menurut Utomo (2012: 4), tepologi adalah gambaran struktur jaringan komputer yang akan dibangun. Berdasarkan tepologi atau gambar struktur jaringan komputer yang akan dibuat, jaringan komputer dapat dibedakan menjadi tujuh bagian yaitu:

1. Topologi *Bus*, jenis topologi ini menghubungkan setiap komputer/node dengan sebuah kabel komunikasi melalui sebuah kartu antarmuka *(card*

interface) komputer, setiap komputer dapat berhubungan dengan komputer yang lain yang ada dalam jaringan tersebut.

2. Topologi Ring, komputer-komputer dalam jenis topologi ini akan dihubungkan dengan sebuah kabel tunggal dan membentuk bagan seperti sebuah cincin. Pada jaringan ini tidak terdapat pusat, sehingga semua komputer mempunyai kedudukan yang sama.
3. Topologi Star, jenis topologi ini beberapa komputer akan dihubungkan dengan satu pusat komputer sehingga semua *control* berbagi sumber daya (*recources)* dalam jaringan yang diperlukan juga akan dipusatkan pada satu titik, ketika akan mengirim data ke komputer ke komputer lainnya, komputer harus melalui komputer pusat terlebih dahulu. Dalam tepologi jenis ini, ketika komputer pusat mengalami gangguan semua komputer *client* juga akan terganggu.
4. Topologi *extended star,* dasar topologi ini adalah tepologi bintang hanya ditambah pengulang (*repeater)* berupa hub atau pengalih *(switch)* sehingga semakin memperluas jaringan yang jaraknya berjauhan.
5. Topologi *Cascading Star,* jenis tepologi ini juga hampir sama dengan bintang diperluas, akan tetapi beberapa jaringan bintang yang dibuat tersebut dihubungkan ke sebuah simpul pusat untuk mengontrol semuanya.
6. Topologi *Mesh*, jaringan jenis topologi ini mempunyai jalur ganda pada setiap node/simpul jaringan. Semakin banyak jumlah komputer yang ada dalam jaringan, semakin sulit pemasangan kabel akan menjadi berlipat ganda.

7. Topologi *Tree*, merupakan kombinasi antara topologi bintang dan topologi bus. Topologi ini terdiri atas kumpulan topologi bintang yang dihubungkan dalam topologi bus sebagai jalur *backbone.*

2.1.3.3. Berdasarkan Fungsi

Menurut Utomo (2012: 10), berdasarkan fungsinya, jaringan komputer dibagi menjadi dua bagian, yaitu:

1. Jaringan *Client-Server,* pada jaringan ini terdapat satu komputer yang disiapkan sebagai komputer *server* yang akan melayani komputer lainnya yang berfungsi sebagai *client.*
2. Jaringan *peer-to-peer*, pada jaringan ini sebuah komputer langsung dihubungkan ke komputer lainnya dan dapat saling berbagi sumber daya masing-masing komputer.

2.1.3.4. Berdasarkan Media Penghantar

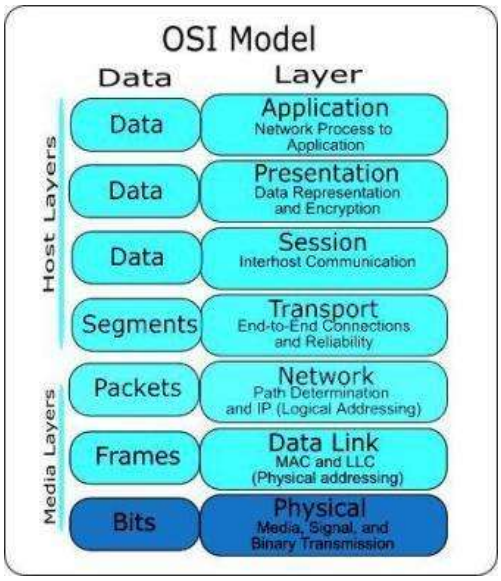
Menurut Utomo (2012 :13), Berdasarkan media penghantarnya, jaringan komputer dapat dibedakan menjadi dua yaitu :

1. Menggunakan media kabel (*wired networking*)**,** jaringan komputer ini menggunakan media kabel sebagai penghantarnya. Data akan mengalir melalu kabel. Kabel yang digunakan bisa berbahan tembaga atau serat optik (*fiber optic*). Bahan tembaga biasa digunakan untuk jaringan LAN, sedangkan jenis MAN atau WAN biasanya menggunakan gabungan antara kabel tembaga dan serat optik.

2. Menggunakan media udara (*wireless*), jaringan komputer ini tidak menggunakan kabel. Media penghantar antar komputernya menggunakan gelombang radio. *Frekuensi* yang digunakan untuk jaringan komputernya tinggi, yaitu 2,4 GHz dan 5 GHz.

2.1.4 Model OSI Layer

Menurut Kristanto (2003: 15), tujuan utama penggunaan model OSI adalah untuk membantu designer jaringan memahami fungsi dari tiap *layer* yang berhubungan dengan aliran komunikasi data. Termasuk jenis-jenis protocol jaringan dan metode transmisi. Model dibagi menjadi 7 *layer*, dengan karakteristtik dan fungsinya masing masing.



Gambar 2.1 Susunan *Layer OSI*
Sumber (Sofana, 2012:96)

Fungsi masing-masing dari tiap *layer* pada OSI :

1) *Application*

Application layer menyediakan jasa untuk aplikasi pengguna, *layer* ini bertanggungjawab atas pertukaran informasi antara program computer, seperti program *e-mail* dan servis lain yang berjalan di jaringan seperti *server* printer atau aplikasi computer lainnya. Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan. Mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. *Protocol* yang berada dalam lapisan ini adalah HTTP, FTP, SMTP, dan NFS.

2) *Presentation*

Presentation layer bertanggung jawab bagaimana data dikonversi dan di format untuk transfer data. Contoh *konversi* format text *ASCII* untuk dokumen, .GIF dan .JPG untuk gambar layer ini membentuk kode *konversi,* translasi data*, enkripsi* dan *konversi.* Berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi kedalam format yang dapat ditransmisikan melalui jaringan. *Protocol* yang berada dalam level ini adalah perangkat lunak *director (redictor Software)*. Seperti llayanan *worksatation* (dalam Windows NT) dan juga Network Shell (semacam *Virtual Network Computing) (VNC)* atau *Remote Dekstop Protocol (RDP).*

3) *Session*

Session layer menentukan bagaimana dua terminal menjaga, memelihara dan mengatur koneksi. Bagaimna mereka saling berhubungan satu sama lain. Koneksi di layer di sebut "*session*". Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara atau di hancurkan. Selain itu, di level ini juga dilakukan resolusi nama.

4) *Transport*

Transport layer bertanggung jawab membagi data menjadi segmen, menjaga koneksi logika "*end – to _ end*" antar terminal, dan menyediakan penanganan error (error handling). Berfungsi untuk memecahkan data kedalam paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan yang telah diterima. Selain itu, pada level ini juga membuat tanda bahwa paket diterima dengan sukses (*acknowledgement*) dan mentransmisikan ulang terhadap paket-paket yang hilang di tengah jalan.

5) *Network*

Network layer bertanggung jawab menentukan alamat jaringan, menentukan rute yang harus diambil selama perjalanan, menjaga antrian tafik di jaringan. Data pada layer ini berbentuk "Paket". Berfungsi untuk mendefinisikan alamat-alamat IP, membuat Header untuk paket-paket dan kemudian melakukan routing melalui *internet-working* dengan menggunakan *router* dan *switch layer* tiga.

6) *Datalink*

Data *link layer* menyediakan link untuk data. Memaketkannya menjadi frame yang berhubungan dengan "*hardware*" kemudian diangkut melalui media komunikasinya dengan kartu jaringan, mengatur komunikasi *layer physical* antara system koneksi dengan penaganan *error.* Berfungsi untuk menentukan bagaimana *bit-bit* data dikelompokan menjadi format yang disebut sebagai *frame*. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamatan perangkat keras (seperti halnya di Media *Access Control Address (MAC Address)*, dan menetukan bagaimna perangkat perangkat jaringan seperti *hub, bridge, repeater* dan *switch layer* 2 beroperasi. Spesifikasi IEEE 802, membagi level ini menjadi dua level anak, yaitu lapisan *Logical Link Control* (LLC) dan lapisan Media Access Control (MAC).

7) *Physical*

Physical layer bertyanggung jawab atas proses data menjadi bit dan mentransfernya melalui media (seperti kabel) dan menjaga koneksi fisik antar system. Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya *Ethernet* atau *token Ring*), topologi jaringan dan pengkabelan. Selain itu, level ini juga mendefinisikan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio.

2.1.5 Jaringan Wireless

Menurut Sopandi (2009: 113), Wireles (jaringan nirkabel) merupakan satu jaringan komunikasi antar komputer dengan menggunakan frekwensi radio. Kadang disebut juga jaringan *Wi-Fi (Wireless* Fidelity).

Wi-Fi tidak hanya dapat digunakan untuk mengakses *internet*, *Wi-Fi* juga dapat digunakan untuk membuat jaringan tanpa kabel di perusahaan. Karena itu banyak orang mengasosiasikan *Wi-Fi* dengan "kebebasan" karena teknologi *Wi-Fi* memberikan kebebasan kepada pemakainya untuk mengakses internet atau transfer data dari ruang meeting, kamar hotel, kampus, dan *café-café* yang bertanda "*Wi-Fi Hot Spot*". Salah satu kelebihan dari *Wi-Fi* adalah kecepatannya yang beberapa kali lebih cepat dari modem kabel. Jadi pemakaian *Wi-Fi* tidak lagi harus berada didalam ruangan kantor untuk bekerja.

Menurut Maslan dan Wangra (2012: 103) , *Wi-Fi* memiliki beragam standar 802.11 yang ditetapkan oleh *IEEE*. Untuk koneksi Wi-Fi antar perangkat, ada tiga jenis jaringan nirkabel yang ditetapkan oleh *IEEE.* Standarnya adalah standar 802.11a dengan frekuensi 5 Ghz dengan kecepatan 54 Mbps dan jangkauan jaringan 300 m, 802.11b dengan *frekuensi* 2,4 Ghz dengan kecepatan 11 Mbps dan jangkauan jaringan 100 m, dan 802.11g dengan *frekuensi* 2,4 Ghz dengan kecepatan 54 Mbps dan jangkauan jaringan 300 m. Yang membedakan masing-masing standar adalah jangkauan frekuensi dan kecepatan transfernya. Kebanyakan perangkat yang dijual saat ini dilengkapi standar 802.11b, meskipun kecepatan transfer datanya lebih lambat daripada kecepatan standar 802.11a.

Pasalnya, kebanyakan istalasi Wi-Fi saat ini dibangun menggunakan standar 802.11b.

Hotspot adalah *definisi* untuk daerah yang dilayani oleh satu *Access Point Wireless* . LAN standar 802.11a/b/g, dimana pengguna (*user*) dapat masuk ke dalam *Access* Point secara bebas dan *mobile* menggunakan perangkat sejenis *notebook*, PDA atau lainnya (Deris Setiawan, *Wireless Fundamental, Instalation & Implemetations*, 2008).

2.1.6 Mikrotik Wireless

Menurut Towidjojo (2013: 31), untuk membangun jaringan *wireless* atau *Wi-FI* yang dapat melayani laptop ataupun *smartphone* sebagai client, tentunya harus menggunakan perangkat router mikrotik delengkapi dengan interface *wireless.* Penggunaan mikrotik *wireless* memungkinkan untuk mengatur pengaksesan terhadap jaringan publik untuk pengguna yang menggunakan jaringan kabel maupun nirkabel, dengan fitu fitur sebagai berikut :

1. Menggunakan server DHCP untuk memberikan alamat IP sementara kepada klien untuk proses otentifikasi
2. Otentifikasi klien menggunakan penyimpanan data lokal seperti radius
3. Pemberian IP tetap setelah proses otentifikasi berhasil.

2.1.7 Model Referensi TCP/IP

Menurut Sopandi (2008: 60), TCP/IP (*Transmision Control/Internet Protocol*) adalah sekumpulan protokol yang didesain untuk melakukan fungsi-fungsi komunikasi data WAN. TCP/IP merupakan nama *protocol* jaringan yang universal terutama pada internet, dan mempunyai kemampuan jaringan yang sangat baik, tetapi *protocol* ini membutuhkan konfigurasi yang cukup suli. TCP/IP terdiri atas bagian bagian tertentu dari komunikasi data . *Protocol* ini merupakan komunikasi sistem apapun yang terhubung kedalamnya, biasanya berkomunikasi dengan sistem lain tanpa harus mempedulikan bagaimana remote system yang lain tersebut bekerja

2.1.8 User Diagram protokol (UDP)

Menurut Ariyus (2007: 75), sebagai tabahan dari TCP, terdapat satu *protocol level transpor*t lain yang umum digunakan sebagai bagian dari *suite protocol* TCP/IP yang disebut dengan *User Datagram Protocol* (UDP). UDP menyediakan nirkoneksi untuk prosedur pada level aplikasi. Pada dasarnya UDP merupakan suatu layanan protokol yang kurang bisa diandalkan karena kurang memberikan perlindungan dalam pengiriman dan duplikasi data. Datagram merupakan suatu paket *switching*, sebuah paket yang terpisah-pisah dari paket lain yang membawa informasi yng memadai untuk *routing* dari *Data Terminal Equipment* (DTE) sember ke DTE tujuan tanpa harus menetapkan koneksi antara DTE dan jaringan.

2.2 Teori Khusus

2.2.1. Keamanan Komputer

Menurut Sofana (2008: 306), masalah keamanan merupakan salah satu aspek terpenting pada sebuah sistem informasi. Masalah keamanan sering kali kurang mendapatkan perhatian dari perancang dan pengelola sistem informasi serta berada di urutan setelah tampilan, atau bahkan menjadi perhatian pada jaringan nirkabel. Keamanan komputer mencakup empat aspek yaitu *privacy, integrity, authentication,* dan *availability.*

a. *Privacy,* mencakup kerahasian informasi yang tidak dapat diakses oleh orang yang tidak berhak. Salah satu yang harus dilakukan yaitu penggunaan enkripsi yang hanya dapat diakses hanya kita sendiri dengan menggunakan "kunci" untuk informasi atau setiap dokumen penting.

b. *Integrity*, menjaga informasi agar tetap utuh. Informasi tidak boleh diubah baik ditambah maupun dikurangi kecuali mendapat izin dari pemilik. Adapun gangguan yang dapat mengubah aspek ini ialah virus dan pemakai lain. Sehingga pengunaan anti virus merupakan solusi untuk mengatasinya.

c. *Authentication,* sebuah keabsahan atas pemilik informasi merupakan hal yang penting bagi pemilik untuk mengetahui bahwa informasi tersebut asli dan dapat diakses oleh pemilik informasi maupun yang berhak atas megirimkan informasi tersebut kepada orang lain.

d. *Availability*, aspek ini merupakan ketersediaan informasi yang dapat dibutuhkan setiap saat. DoS *attack* (*denial of service attack*) merupakan serangan terhadap aspek ini. Sebagai contoh *mailbomb,* dimana seseorang

dikirimi email secara bertubi-tubi sehingga kesulitan untuk mengakses *email*nya.

Menurut Iwan Sofana (2012:307), berkaitan dengan keamanan jaringan tersebut ada beberapa kemungkinan serangan terhadap keamanan jaringan informasi, yaitu *interruption, interception, modification, fabrication*.

a. *Interruption*, ketersediaan informasi diganggu sedemikian rupa sehingga sistem tidak dapat mengakses informasi atau *availability*.

b. *Interception,* seseorang yang tidak berhak atas informasi tersebut berhasil mengakses aset atau informasi yang tersedia. Serangan ini ditujukan ke aspek *integrity*.

c. *Modification,* jika pihak yang tidak berwenang sudah berhasil mengakses informasi, memungkinkan dilakukannya perubahan atas informasi. Serangan ini ditujukan ke aspek *integrity*.

d. *Fabrication,* informasi palsu dikirimkan oleh pihak yang tidak bertanggung jawab dengan menyisipkannya kedalam sistem. Serangan ini ditujukan ke aspek *authentication*.

Ada beberapa menyatakan bahwa keamanan komputer identik dengan keamanan informasi yaitu sama-sama melindungi *privacy, integrity,* dan *availability.* Tetapi ada beberapa perbedaan dianatara keduanya.

Menurut Iwan Sofana (2012:308), perbedaan yang utama terletak pada pendekatan, metode dan kajiannya. Keamanan informasi memfokuskan diri dimana data tersebut disimpan. Sedangkan keamanan komputer memfokuskan diri kepada proses yang dilakukan oleh sistem komputer.

2.2.1.1. Tujuan Keamanan Komputer

Menurut Ariyus (2007: 25), Dewasa ini IDS menjadi solusi untuk mengatasi masalah tersebut. Pada dasarnya tujuan keamanan komputer, yang disingkat dengan CIA, yang merupakan singkatan dari:

1. *Confidentility,* merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Confidentiality biasanya berhubungan dengan informasi yang diberikan ke pihak lain.

2. *Integrity,* kesalahan pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan tersebut.

3. *Avability,* aspek *avaibility* atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan.

2.2.2. Intrusion Detection System(IDS)

Menurut Ariyus (2007: 27), *Intrusion Detection System* (IDS) merupakan penghambat semua serangan yang akan mengganggu sebuah jaringan. Kemampuan dari IDS memberikan peringatan kepada administrator *server* saat terjadi sebuah aktivitas tertentu yang tidak diinginkan administrator sebagai penanggung jawab sebuah sistem.

Intrusion Detection System (IDS) dapat didefinisikan sebagai *tool*, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi,

memberikan laporan terhadap aktifitas jaringan komputer. *Intrusion Detection System* secara khusus berfungsi sebagai proteksi secara keseluruhan dari sistem yang telah diinstal IDS. IDS tidak berdiri sendiri dalam melindungi suatu sistem.

Ada beberapa alasan untuk memperoleh menggunakan IDS, diantaranya adalah :

1. Mencegah resiko keamanan yang terus meningkat, kareena banyak ditemukan kegiatan ilegal yang diperbuat oleh orang-orang yang tidak bertanggungjawab dan hukuman yang diberi atas kegiatan tersebut
2. Mencegah serangan dan pelanggaran keamanan sistem jaringan yang tidak bisa dicegah oleh sistem yang umum dipakai, seperti firewall.
3. Mendeteksi serangan awal (biasanya *network probe* dan aktivitas *doorknob rattling*)
4. Mengamankan file yang keluar dari jaringan
5. Sebagai pengendali untuk *security design* dan administrator, terutama bagi perusahaan yang besar
6. Menyediakan informasi yang akurat terhadap gangguan secara langsung, meningkatkan *diagnosis*, *recovery*, dan mengoreksi faktor faktor penyebab serangan.

2.2.2.1. Peran *Intrusion Detection System*

Menurut Ariyus (2007:34), IDS Juga memiliki peran penting untuk mendapatkan arsitektur *defence-in-depth* (pertahanan yang mendalam dengan melindungi akses jaringan internet, sebagai tambahan dari parameter *defence)*.

Hal-hal yang dilakukan IDS *(Intrusion Detection System)* pada jaringan internal adalah sebagai berikut:

1. Memonitor akses database, ketika mempertimbangkan pemilihan kandidat untuk penyimpanan data, suatu perusahaan akan memilih database sebagai solusi untuk menyimpan data-data yang berharga.
2. Melindungi e-mail server, IDS *(Intrusion Detection System)* juga berfungsi untuk mendeteksi virus *e-mail* seperti QAZ, *Wrom*, NAVIDAD *worm*, dan versi terbaru *ExploreZip.*
3. Memonitor *policy security*, jika kelonggaran terhadap policy security maka IDS *(Interusion Detection System)* akan memberitahu bahwa telah terjadi sesuatu yang tidak sesuai dengan yang ada.

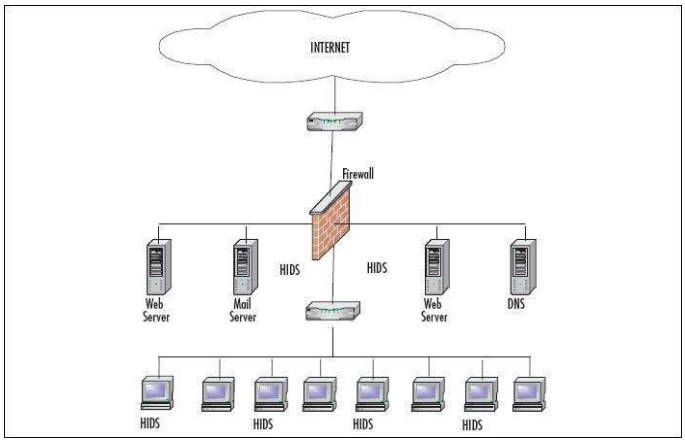
2.2.2.2. Tipe Intrusion Detection System (IDS)

Menurut Ariyus (2007: 36-48), pada dasarnya terdapat dua macam IDS, yaitu:

1. *Host- Based Intrusion Detection System* (HIDS)

   IDS *host-based* bekerja pada host yang akan dilindungi. IDS jenis ini dapat melakukan berbagai macam tugas untuk mendeteksi serangan yang dilakukan pada host tersebut. *Host-Based Intrusion Detection System* memperoleh informasi dari sebuah sistem computer yang diamati. Data *host-based* IDS biasanya berupa log, yang dihasilkan dengan memonitor sistem file, event, dan keamanan pada Windows NT dan *syslog* pada lingkungan sistem operasi UNIX. Saat terjadi perubahan pada log tersebut

maka dilakukan analisis apakah sama dengan pola serangan yang ada pada pasisi data IDS.



Gambar 2.2 Host-Based IDS
Sumber (Ariyus, 2007:40)

Host-based IDS tidak secepat *network-based* IDS dalam mendeteksi adanya serangan. *Host-based* IDS memiliki beberapa kelebihan yang tidak dapat dimiliki *network-based* IDS. Kelebihan tersebut termasuk analisis forensik yang lebih kuat, fokus terhadap sebuah *host*, dan lainnya. Beberapa kelebihan host-based IDS adalah :

a. Menguji keberhasilan atau kegagalan serangan
b. Memonitor aktifitas sistem tertentu. Sistim ini memonitor aktivitas pengguna dan akses terhadap file, termasuk pengaksesan file, penggantian atribut file, percobaan untuk mengakses *service privileged*.
c. Mendeteksi serangan yang lolos dari network-based IDS.
d. Cocok untuk lingkungan *encrypt dan switch.*
e. Deteksi dan respons secara *near real-time*

f. Tidak memerlukan tambahan perangkat keras.Host-based IDS berada di dalam insfrastruktur jaringan yang ada, termasuk server file, *server web*, dan sumber daya lain pada jaringan seperti yang dilakukan *network-based* IDS.

Beberapa kelemahan dari host-based diantaranya adalah:

a. Manajemen yang rumit, informasi harus dikonfigurasi untuk setiap host yang ada.

b. Sedikit sumber informasi, karena host-based berada pada host yang menjadi target suatu serangan.

c. Host-based tidak cocok untuk mendeteksi jaringan atau monitoring terhadap suatu jaringan karena IDS hanya memonitor paket yang diterima pada host tersebut.

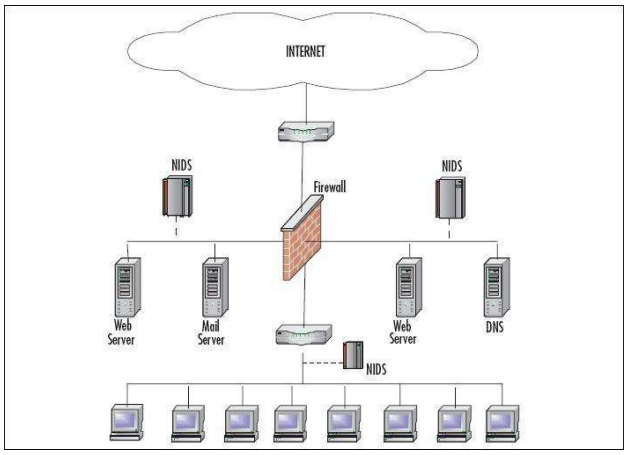
d. *Host-based* IDS menggunakan sistem operasi audit sebagai sumber informasi yang akan memberikan ruang tambahan pada hardisk.

e. *Host-based* IDS menggunakan sumber daya komputer untuk melakukan monitoring terhadap paket-paket yang merugikan sehingga akan menambah biaya dari sumber daya itu sendiri.

2. ***Network - Based Intrussion Detection System*** **(NIDS)**

IDS jenis ini akan mengumpulkan paket - paket data yang terdapat di seluruh bagian jaringan. *Network-based* IDS menggunakan *network adapter* sebagai alat untuk menangkap paket-paket yang akan dipantau. Network adapter berjalan pada mode *prosmicuou*s untuk memonitor dan melakukan analisis paket paket yang ada yang berjalan dalam jaringan. *Network-based*

IDS akan mengumpulkan paket data yang terdapat pada jaringan dan kemudian menganalisisnya serta menentukan apakah paket tersebut normal atau paket serangan.



Gambar 2.3. *Network-Based* IDS
Sumber (Ariyus, 2007:43)

Beberapa cara yang digunakan untuk mengenali serangan pada Network-bsed IDS ini antara lain :

a. Pola data, expresi atau pencocokan secara bytecode.

b. Frekuensi atau pelanggaran ambang batas.

c. Kolerasi yang dekat dengan sebuah event.

d. Deteksi anomali secara statistik.

Beberapa kelebihan dari Network- Based IDS adalah :

a. Biaya yang lebih rendah

b. Deteksi serangan yang tidak terdeteksi oleh Host-based IDS

c. Kesulitan bagi penyerang untuk menghapus jejak Network- Based IDS menggunakan data *live network traffic* untuk mendeteksi serangan secara real time.

d. Deteksi dan respons secara real time.

e. Deteksi serangan yang gagal dan kecenderungan serangan Network-based IDS yang ditempatkan di luar firewall dapat mendeteksi serangan yang sebenarnya telah dicegah firewall.

f. Tidak tergantung pada sistem operasi.

Kekurangan dari network-based IDS adalah sebagai berikut:

a. *Network-based* IDS sulit untuk memproses semua paket yang besar dan jaringan yang sibuk sehingga gagal dalam mendeteksi serangan yang terjadi jika suatu jaringan sangat sibuk (aktifitas yang tinggi).

b. Banyak keuntungan IDS tidak berlaku untuk jaringan yang menggunakan metode switch-based yang lebih modern.

c. *Network-based* IDS tidak bisa menganalisis paket yang telah dienkripsi.

d. Kebanyakan *network-base* IDS tidak bisa memberitahukan apakah suatu serangan telah berhasil mendapatkan sistem, hanya dapat memberitahukan bahwa serangan sedang terjadi.

Perbedaan antara NIDS dan HIDS **(**Mellander, 2004**)** :
Tabel 2.1 Perbandingan NIDS dan HIDS

NIDS	HIDS
Ruang lingkup yang luas, mengamati semua aktivitas jaringan	Ruang lingkup yang terbatas, mengamati hanya aktivitas pada host tertentu
Lebih mudah melakukan setup	Setup lebih rumit
Lebih baik untuk mendeteksi serangan yang berasal dari luar jaringan	Lebih baik untuk mendetaksi serangan yang berasal dari dalam jaringan
Lebih murah untuk diimplemantasikan	Lebih mahal untuk diimplementasikan
Pendeteksian berdasarkan pada apa yang direkam dari aktifitas jaringan	Pendeteksian berdasarkan pada single host yang diamati semua aktifitasnya
Menguji packet header	Paket header tidak diperhatikan
OS independen	OS spesifik
Mendeteksi serangan terhadap jaringan serta payload untuk dianalisis	Mendeteksi serangan lokal sebelum mereka memasuki jaringan
Mendeteksi usaha dari serangan yang gagal	Memverifikasi sukses atau gagalnya suatu jaringan

2.2.2.3. ACID (*Analysis Console Intrusion Database*)

Menurut Ariyus (2007:214), *Analysis Console Intrusion Database (*ACID) merupakan PHP-based *analysis engine* yang berfungsi untuk mencari dan mengolah database dari *alert network sekurity* yang dibangkitkan oleh perangkat lunak pendeteksi *intrusi* (IDS). Dapat diimplementasikan pada sistem yang

mendukung PHP seperti linux, BSD, Solaris, dan OS lainya. ACID adalah perangkat lunak yang open *source* dan didistribusikan dibawah lisensi GPL.

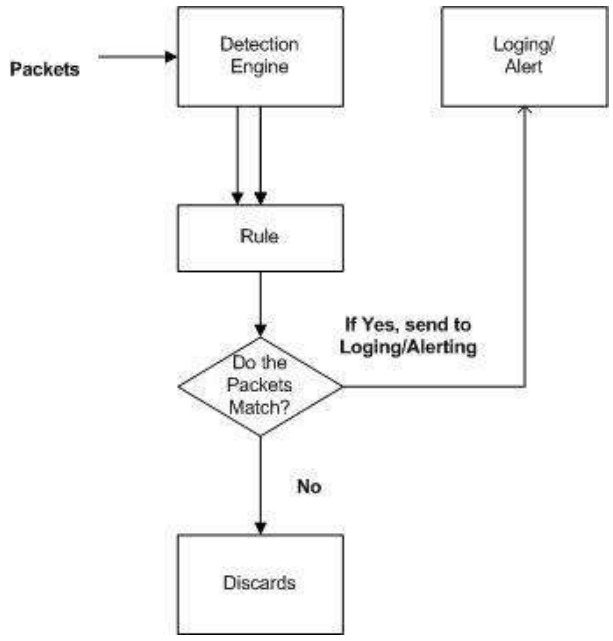
ACID merupakan

2.2.3. Snort

Menurut Ariyus (2007:146), *snort* merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisa paket yang melintas jaringan real time traffic dan logging ke dalam database serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan. *Snort* bisa digunakan pada platform sistem operasi Linux, BSD, SOL windows, dan sistem operasi lainnya. *Snort* sudah di-download lebih dari 3 juta orang. Hal ini menandakan bahwa *snort* merupakan suatu Intrusion Detection System yang dipakai banyak orang di dunia. *Snort* bisa di operasikan dengan tiga model yaitu:

1. Paket sniffer, untuk melihat paket yang lewat di jaringan.
2. Paket logger, untuk mencatat semua paket yang lewat di jaringan untuk dianalisi di kemudian hari.
3. NIDS, deteksi penyusup pada network. Pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini diperlukan setup dari berbagai rules atau aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan.

Menurut Nishhidh et all (2013: 411), cara kerja *snort* IDS adalah seperti gambar di bawah ini :



Gambar 2.4. Cara kerja *snort* IDS
Sumber (Nishidh *et al*., 2013:411)

Dari gambar cara kerja *snort* IDS diatas dapat dijelaskan mengenai fungsi dari tiap komponen adalah sebagai berikut:

1. *Detection engine,* bagian yang menangani paket data dengan menggunakan *detection plug-ins,* dan paket data akan diperiksa sesuai dengan *rules*, jika sesuai dengan *rules,* maka akan dikirimkan ke *alert preprocessor.*
2. *Rule,* file teks yang berisi daftar aturan yang sintaksnya sudah diketahui, sintaks ini meliputi *protocol, address, output plug-ins* dan hal-hal yang berhubungan dengan berbagai hal.

2.2.3.1. Komponen-Komponen *Snort*

Menurut Ariyus (2007:146), komponen-komponen dasar yang bekerja saling berhubungan satu dengan yang lain seperti berikut ini:

1. *Decoder*, sesuai dengan paket yang di-capture dalam bentuk struktur data dan melakukan identifikasi protokol, decode IP dan kemusian TCP dan UDP tergantung informasi yang dibutuhkan, seperti port number, IP address. Snort akan memberikan alert jika menemukan suatu paket yang cacat.
2. *Prepocessors*, merupakan suatu saringan yang mengidentifikasi berbagai hal yang harus diperiksa seperti Detection Engine. Pada dasarnya preprocessors berfungsi mengambil paket yang mendetection engine untuk dikenali polanya.

   Example : HTTPInspect

   HTTPInspect menggantikan http_decode sebagai preprocessor yang bertanggung jawab untuk men-decode-kan lalu lintas http dan mendeteksi lapisan aplikasi serangan eksploit http design atau implementasi. Hal ini akan terlihat dalam buffer data paket yang berusaha mencari celah-celah lalu-lintas http dan berusaha melakukan normalisasi data.

   HTTPInspect mempunyai dua bagian:
3. *Global Section*, mengijinkan untuk mapping file IIS Unicode, Configure alert untuk proxy server dengan proxy_alert atau konfigurasi deteksi lalu-lintas HTTP pada nonauthorized port dengan menggunakan

detect_anomalous_traffict. Global section HTTPInspect preprocessor bisa dikonfigurasi pada snort.conf.

4. *Server Section*, mengijinkan untuk setting HTTP server profiles yang berbeda untuk beberapa server yang berbeda. Konfigurasi tipe serangan dan menormalisasi berdasarkan server yang ada.
5. *Rules Files*, merupakan suatu file teks yang berisi daftar aturan yang sintaks-nya sudah diketahui. Sintaks ini meliputi protokol, address, output plug-ins dan hal-hal yang berhubungan dengan berbagai hal. Rules file akan selalu diperbaharui setiap ada kejadian di dunia maya. Rules snort lebih dari 100 tipe. Setiap hari bisa di-update melalui situs resmi snort www.snort.org atau dari forum-forum yang disediakan oleh komunitas snort.
6. *Detection Engine*, menggunakan detection plug-ins, jika ditemukan paket yang cocok maka snort akan menginisialisasi paket tersebut sebagai suatu serangan.
7. *Output plug-ins* merupakan suatu modul yang mengatur format dari keluaran untuk *alert dan* file *logs* yang bisa diakses dengan berbagai cara, seperti *console, exteren files, database.*

2.2.3.2. Mode Snort

Menurut Rafiudin (2010: 43), terdapat beberapa konsep dasar yang dapat dipahami tentang mode *Snort* akan dikonfigurasikan untuk berjalan pada mode berikut ini :

a. Sniffer Mode

Mode ini praktis membaca paket-paket dari jaringan dan memperlihatkan dalam bentuk aliran yang tidak terputus pada layar. Jika hanya ingin melihat paket-paket *header* dari TCP/IP pada layar dapat digunakan perintah:

./snort – v

perintah ini akan menjalankan *snort* dan hanya menampilkan *header* IP dan TCP/UDP/ICMP, tidak yang lainnya. Jika ingin melihat data-data aplikasi yang lewat, digunakan perintah:

./snort –vd

perintah diatas mengintruksikan *snort* agar menampilkan data sebagaimana dalam *header.*

b. Packet Logger Mode

Jika ingin menyimpan paket-paket kedalam disk, perlu mencantumkan direktori *logging* yaitu dimana data-data disimpan. Melalui perintah *snort* akan secara otomatis berjalan pada mode pencatatan paket:

./snort –dev –l ./log

Saat berjalan pada *logger* mode ini, snort mengumpulkan setiap paket dan menempatkannya dalam sebuah hirarki direktori berdasarkan IP address dari salah satu *host* di dalam data diagram.

Untuk mencatat keterkaitan dengan network, digunakan perintah berikut:

./snort- dev –l./log.h 192.168.1.0/24

Konfirmasi ini akan mengintruksikan *snort* untuk mencetak data link dari number TCP/IP sebagaimana data aplikasi kedalam direktori */log,* dan mencatat paket-paket yang terhubung ke jaringan kelas C 192.168.10.0/24

c. *Network Intrusion Detection System* (NIDS) Mode

Untuk mengaktifkan *Network intrusion detection System* (NIDS) digunakan perintah:

./smort –dev –l ./log –h 192.168.1.0/24 –c snort conf terhadap setiap paket yang ditemukan, untuk memutuskan tindakan apa yang harus diambil berdasarkan *rule* yang telah ditetapkan tersebut. Terdapat beberapa cara untuk konfigurasi output *snort* dalam mode NIDS. Mekanisme peringatan *(alerts)*, dan pecatatan *(logging)default* adalah dengan mencatatkan laporan dalam bentuk ASCII dan menggunakan pesan peringatan sebagai tambahan dalam *header* paket.

d. *Inline* Mode

Snort menyertakan kemampuan *Intrusion Pervention System (IPS)* dari *snort inline. Snort inline* mengambil paket dari *iptables,* dan menggunakan jenis *rule* baru untuk membantu *iptables* melakukan *pass* atau *drop* paket-paket berdasarkan *rule snort.* Ada tiga jenis *rule* yang bisa gunakan saat menjalankan *snort* dengan *snort inline :*

1. *Drop,* jenis *rule drop* akan membuat *iptables* membuang , paket dan mencatat *log* melalui perangkat *snort.*

2. *Reject,* jenis *rule reject* akan membuat *iptables* membuang paket, mencatat *log* melalui perangkat *snort,* dan mengirimkan sinyal TCP *reset* jika termasuk *protocol* tersebut berupa UDP.
3. *Sdrop, rule sdrop* akan membuat *IPTables* membuang paket tetapi tidak ada *log* yang dicatat.

2.2.3.3. Snort Rule

Menurut Rafiudin (2010: 57), *rule snort* adalah aturan-aturan atau kondidi-kondisi yang dibuat oleh *administrator* yang bertujuan mengklasifikasi aktivitas-aktifitas jaringan/internet yang normal dan berbahaya atau tidak diinginkan.

Menurut Ariyus (2007: 157), *rules file* merupakan suatu *file* teks yang berisi daftar aturan yang sintaksnya sudah diketahui, sintaks ini meliputi protokol, *address, output plug in,* dan hal-hal yang berhubungan dengan berbagai hal. Rile ini akan selalu diperbaharui setiap ada kejadian.

Menurut Rafiudin (2010: 57), *rule-rule snort* secara terstruktur terdiri atas dua bagian utama , yaitu:

1. *Rule Header,* merupakan bagian *rule* dimana aksi-aksi *rule* diidentifikasi

   Beberapa bagian dari *rule header,* yaitu:

   a. *Rule Action, rule header* mengandung informasi yang menetapkan siapa, dimana, paket apa, beserta apa, beserta apa yang harus dilakukan saat sebuah event cocok dengan atribut-atribut yang termasuk dalam *rule.* Terdapat lima tindakan default yang etrsedia dalam *snort* yaitu *alert, log, pass, activate, dynamic.*

b. *Protocols,* ada empat protokol yang sekarang ini dianalisis oleh snor terhadap prilaku-prilaku mencurigakan, yaitu TCP,UDP,ICMP, dan IP.

c. *IP Address,* merupakan *rule header* yang berhubungan dengan *IP Address* dan informasi *port, Snort* tidak memiliki mekanisme untuk menyediakan *lokup hostname* untuk *field* IP *address* didalam *file rule.*

d. *Port Numbers, port number* bisa ditetapkan menggunakan beberapa cara, seperti nilai *any* (semua *port), port statis, range port* tertentu, atau oleh pelarangan/pengecualian.

e. *Direction Operator,* dilambangkan dengan "≥" yang mengidentifikasikan orientasi, atau arahan, pada trafik yang diaplikasikan *rule* tersebut. IP *address* dan angka port pada sisi kiri dan *operator direction* dianggap sebagai trafik yang datang dari *host* number, sedangkan informasi *address* dan *port* pada sisi kanan operator adalah *host* tujuan.

f. *Rule Activate/Dynamic,* memberi *snort* kemampuan yang besar, bisa memiliki *rule* yang mampu mengaktifkan *rule* lainnya saat aksi tersebut dijalankan terhadap sejumlah sel paket.

2. *Rule Option,* merupakan bagian *rule* dimana pesan-pesan peringatan *(alert message)* diidentifikasi. Rule option dari mesin pendeteksi penyusupan *snort* menggabungkan kemudahan penggunaan dengan kekuatan dan fleksibilitas, semua opsi *rule snort* masing-masing dipisahkan dengan karakter semocolon. Menurut Rafiudin (2010:65-116), terdapat empat kategori utama *rule option, yaitu:*

a. *General,* opsi ini menyediakan informasi tentang *rule,* tetapi tidak memberikan efek apapun selama pendeteksian, terdapat beberapa perintah. Opsi-opsi *rule general* yaitu *msg, reference, gid, sid, rev, classtype, priority, metadata*

b. *Payload Detection, iopsi ini mencari data didalam payload* paket dan bisa dihubungkan dengan tool yang lain, terdapat beberapa perintah dalam payload yaitu *content, nocase, rawbytes, depts, offset, distance, within_client_body,http_cookie, http_header, http_method, http_uri, fast_pattern, urilen, isdataat, pcre, byte_test, byte_jump, ftpbounce, cvs.*

c. *Non payload,* opsi ini mencatat data *non_payload,* terdapat beberapa perintah dalam *non payload* yaitu, *fragoffset, ttl, tos, id, ipopts, fragbits, dsize, flags, flow, flownits, seq, ack, window, itype, icode, icmp_id_sec, ip_proto, dameip, stream_size.*

d. *Post Detection,* opsi ini merupakan pemicu *rule* tertentu yang berjalan setelah *rule* tersebut diaktifkan. Terdapat beberapa perintah pada *post detection iantara lain, logto, session, resp, react, tag, activates,activated_by, count.*

2.2.4. Firewall

Menurut Ariyus (2006:307), *firewall* adalah alat yang digunakan untuk mencegah orang luar memperoleh akses ke suatu jaringan. Firewal pada umumnya merupakan suatu kombinasi dari perangkat lunak dan perangkat keras. *Firewall*

biasanya menerapkan pengeluaran rencana atau perintah untuk menyortir alamat yang tak dikehendaki dan diinginkan.

Konfigurasi dari firewall bergantung kepada kebijaksanaan (policy) dari organisasi yang bersangkutan, yang dapat dibagi menjadi dua jenis :

1. Apa-apa yang tidak diperbolehkan, secara eksplisit dianggap tidak diperbolehkan *(prohibitted)*
2. Apa-apa yang tidak dilarang, secara eksplisit dianggap diperbolehkan *(permitted)*

Menurut Ariyus (2006:308), untuk memahami bagaimana firewalls bekerja, pengesahan pertama yang paling sederhana adalah memeriksa prosedur penggunaan IP alamat sebagai suatu index. IP alamat merupakan index identifikasi universal pada internet, baik alamat statis maupun alamat yang dinamis.

Karakteristik dari firewall memiliki tujuan sebagai berikut :

1. Segala lalu lintas jaringan, baik dari dalam maupun dari luar harus melalui firewall. Hal tersebut menghalangi semua akses dalam bentuk apa pun kecuali melalui firewall.
2. Kebijakan keamanan hanya memberikan izin untuk memasuki server atau jaringan komputer yang memenuhi syarat tertentu.

3. Firewall sendiri bebas terhadap penetrasi, yang menandakan bahwa suatu sistem dapat dipercaya dan menjamin keamanan dari sistem operasi.

Hal-hal yang dilakukan firewall secara ringkas dibawah ini :

1. *Firewall* berfungsi sebagai dinding penghambat yang tidak mengijinkan user yang tidak memliki hak terhadap jaringan untuk melakukan akses guna melindungi jaringan dari hal-hal yang tidak diinginkan, seperti IP spoofing, serangan terhadap router.

2. *Firewall* berfungsi sebagai monitor atas kejadian-kejadian yang berhubungan dengan keamanan sistem, yang akan memberikan keterangan kepada sistem serta mencatat ke file log, alarm yang diimplemantasikan oleh sistem *firewall.*

3. *Firewall* juga berfungsi sebagai platform dari fungsi internet yang tidak aman, yang meliputi penerjemahan alamat jarinagn, dari alamat lokal ke alamat internet.

4. *Firewall* melayani paltform untuk Ipsec menggunakan tunnel mode dan firewall juga digunakan oleh *Virtual Private Network* (VPN).

Hal- hal yang tidak bisa diatasi *firewall* adalah :

1. Serangan yang dilakukan dengan mem-bypass *firewall*

2. Firewall tidak bisa melindungi serangan yang dilakukan di dalam sistem (internal)

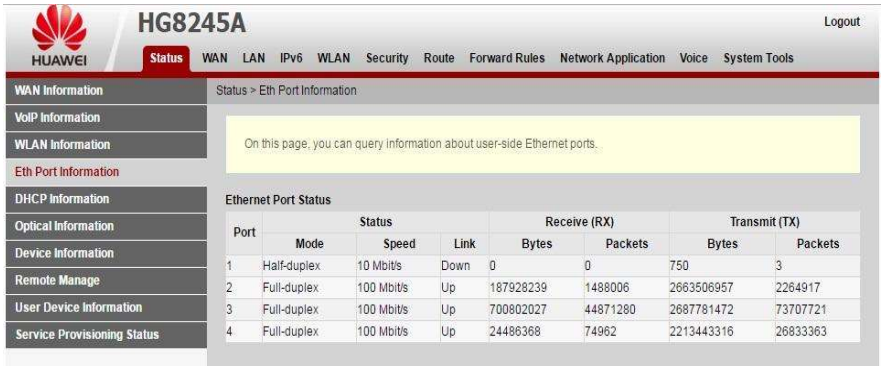
3. *Firewall* tidak bisa melindungi pengiriman virus yang disisipkan ke suatu program atau file. Firewall tidak bisa melakukan scanning terhadap file, program, dan e-mail yang berisi virus.

2.3 Tools

Untuk melakukan penelitian ini dijelaskan tools dan sofware yang digunakan yaitu:

2.3.1. ISP (*Internet Service Provider*)

ISP yang digunakan dalam penelitian ini adalah Telkom Indihome 10 Mbps, alasan utama dalam memilih ISP Telkom Indihome adalah harga *bandwidth* yang cukup murah dibandingkan dengan provider lain selain itu Telkom Indihome memberikan fasilitas *modem* gratis untuk setiap konsumen yang menggunakan ISP Telkom Indihome, serta kemudahan dalam konfigurasi *modem* membuat administrator perusahaan menggunakan ISP ini.



Gambar 2.5. *Internet Service Provider*
Sumber (Hasil Olahan sendiri, 2017)

2.3.2. Perangkat Keras (Hardware)

1. Komputer Server

PT Bayu Pariama Batam memiliki 1 komputer *server* yang bertugas melayani, mengatur, mengelola, semua suatu hal yang terkait dengan komputer *client*, dengan spesifikasi *hardware* sebagai berikut :

Gambar 2.6 Komputer *Server*
Sumber (Hasil Olahan sendiri, 2017)

2. Client

PT Bayu Pariama Batam memiliki 15 komputer *client* yang digunakan untuk melakukan aktifitas kerja staff maupun karyawan, dengan spesifikasi *hardware* sebagai berikut :

Tabel 2.2 Spesifikasi *Hardware Client*

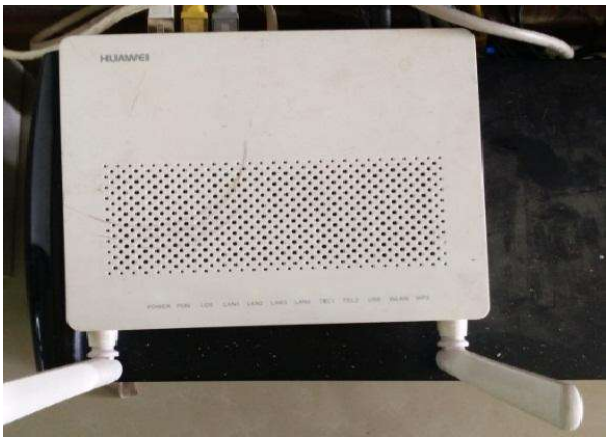
Unit	Perangkat	Spesifikasi
15	Motherboard	HP Compaq dx2300 Microtower

	Processor	Intel(R) 946GZ @ 1.80 GHz
	RAM	Kingston 2gb ddr2
	Hardisk	Seagate 250gb
	VGA Card	NVidia GeForce 9500GS 512mb 128bit
	Monitor	LCD Acer 19 inch

Gambar 2.7 Komputer *Client*
Sumber (Hasil Olahan sendiri, 2017)

3. Modem ADSL

Modem ADSL yang digunakan pada PT Bayu Pariama Batam adalah *modem* ADSL Huawei dengan tipe HG 8245A , *modem* tersebut diberikan oleh PT Telekomunikasi Indonesia (TELKOM) secara gratis pada saat dilakukan pemasangan jaringan optik indihome telepon dan setelah terdaftar sebagai konsumen Telkom Indonesia.



Gambar 2.8 Modem ADSL
Sumber (Hasil Olahan sendiri, 2017)

4. Switch

Switch yang digunakan pada PT Bayu Pariama Batam adalah D-LINK dengan tipe DES-1024D memiliki 24 *port ethernet*.

Gambar 2.9 Switch
Sumber (Hasil Olahan sendiri, 2017)

5. *Router*

Router yang akan digunakan pada PT Bayu Pariama Batam adalah mikrotik dengan tipe RB 750 Gr2 memiliki 5 *port ethernet*.

Gambar 2.10 Router Mikrotik RB 750 Gr2
Sumber (Hasil Olahan sendiri, 2017)

6. *Akses Point*

Akses point merupakan *repeater yang* berfungsi untuk memperluas cakupan dan kekuatan sinyal, dengan distribusi layanan *wireless* teknologi dengan menghubungkan beberapa jalur akses. Pengguna dapat jaringan wireless tanpa kabel yang lebih luas dan lebih banyak pengguna seperti di perkantoran, hotel, cafe.

2.3.3. Sofware dan Aplikasi System

Dalam penelitian ini sofware dan aplikasi yang diperlukan adalah:

1. Snort

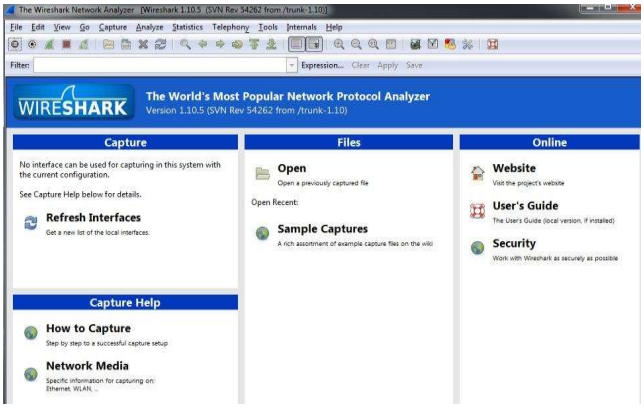
Snort merupakan salah satu tool *Network Intrusion Prevention System* dan *Network Intrusion Detection System* (NIDS). Dalam prakteknya, snort sangat andal untuk membentuk loging paket-paket dan analisis trafik-trafik secara *real-time* dalam jaringan-jaringan berbasis TCP/IP. Snort ditulis oleh Martin Roesch dan sekarang dikelola oleh Sourcefire, dimana Roesch bertindak sebagai pendiri dan CTO(Chief of technical Officer- Kepala Tim Teknis). Dalam penelitian ini snort yang digunakan adalah snort 2.9.7.6.

Gambar 2.11 Tampilan Snort
Sumber (https://www.snort.org)

2. Wireshak

Wireshak merupakan salah satu tools atau aplikasi *Network Analyzer* atau penganalisa jaringan. Penganalisaan kinerja jaringan itu dapat melingkupi

berbagai hal, mulai dari proses menangkap paket-paket data atau informasi yang berlalu-lalang dalam jaringan, sampai pada digunakan untuk *sniffing*. *Wireshark* merupakan *free tools* untuk *Network Analyzer* yang ada saat ini yang terbilang bersahabat dengan *user* karena menggunakan tampilan grafis atau GUI (*Graphical User Interface*).



Gambar 2.12 Tampilan Wireshark
Sumber (https://www.wireshark.org)

3. WinPcap

WinPcap merupakan seperangkat packet procedure yang memperbolehkan aplikasi berinteraksi dengan network secara langsung. *Procedure* yang digunakan bermanfaat sebagai contoh untuk aplikasi capture yang membutuhkan data yang masuk melalui network tanpa proses dari kernel.

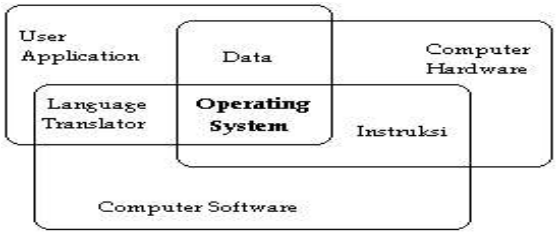
Gambar 2.13 Tampilan WinPcap
Sumber (https://www.**winpcap**.org)

4. Ping Attack

Menurut Sukmaaji dan Rianto (2008: 165), Ping of death merupakan suatu serangan Daniel Of Service (DoS) tehadap suatu server atau komputer yang terhubung dalam suatu jaringan. Serangan ini memanfaatkan fitur yang ada si TCP/IP yaitu paket *fragmentation* atau pemecahan paket, dan juga kenyataan batas ukuran paket di protokol IP adalah 65536 byte atau 64 kilobite. Penyerangan dapat mengirimkan berbagai paket ICMP yang terfragmentasi sehingga untuk paket-paket tersebut disatukan kembali, maka ukuran oaket seluruhnya melebihi batas 65536 byte. Contoh sederhana adalah sebagai berikut : C:\windows>ping 192.168.1.1-l 65540.

5. Windows 7

Sistem Operasi (OS) merupakan bagian dari software komputer yang berfungsi sebagai interface (penghubung) antara aplikasi user, hardware komputer, dan software komputer.



Gambar 2.14 *Operating System*

Karena itu, sistem operasi harus memilki kemampuan untuk bertindak sebagai :

1. *Coordinator*, yaitu menyediakan fasilitas sehingga instruksi yang kompleks dapat dikerjakan dalam tingkatan tertentu.
2. *Guardian*, memiliki access controls untuk melindungi file dan mengadakan restriksi terhadap reading/writing/executing data dan program
3. *Gatekeeper*, mengendalikan siapa saja yang dapat masuk ke dalam sistem momputer tersebut.
4. *Accountant*, menjaga kerja CPU, penggunaan memory, termasuk media penyimpan (storage devices).
5. *Server*, melayani aplikasi yang dibutuhkan oleh user.

Sistem operasi yang dikeluarkan oleh perusahaan Microsoft Inc. Microsoft Windows adalah software sistem informasi yang paling populer untuk para pengguna PC. Melihat perkembangan Windows yang sangat pesat yang dimulai dari awal tahun sembilan puluhan dengan mengeluarkan Windows versi 3.11 lalu disusul dengan Windows 95, 98, 2000, Me, dan Windows XP. Semakin baru dari versi maka akan semakin memudahkan para penggunanya dalam menggunakan sistem operasi tersebut maupun dengan dukungan dari software aplikasi yang lain.

Windows jauh lebih diminati karena kemampuannya yang lebih handal. Windows di desain sebagai OS yang sangat users-friendly. Demikian pula dalam hal tampilannya yang berbasis grafis. Windows juga adalah OS yang dirancang sedemikian rupa sehingga user yang belum kenal komputer sama sekali dalam waktu yang relatif singkat dapat mengoperasikan komputer. Selain itu, Windows juga memiliki kemampuan multitasking, sehingga user akan dapat lebih

menghemat waktu untuk menjalankan beberapa aplikasi. Bandingkan dengan DOS di mana kita harus menghafal perintah-perintah yang ada.

2.4 Penelitian Terdahulu

Sebagai pertimbangan dan acuan untuk penelitian yang akan dilakukan maka penulis menggunakan penelitian terdahulu tentang analisis dan implementasi IDS pada jaringan wireless berbasis Mikrotik, berikut ini akan dikemukakan hasil penelitian terdahulu sesuai dengan yang berkaitan dengan IDS dan keamanan jaringan adalah:

1. **Sahid Aris Budiman, Catur Iswahyudi, Muhammad Sholeh**(2014) Jurnal JARKOM Vol. 2 No. 1 Desember 2014 ISSN: 2338-6313**,** dengan judul ***"Implementasi Intrusion Detection System (IDS) Pada Server Debian Menggunakan Jejaring Sosial Sebagai Media Notifikasi"*** Setelah melakukan pengujian scanning, DoS Attack, SSH dan FTP. Hasil pengujian menunjukkan bahwa setiap ada serangan yang datang dari luar menuju host atau server yang didalamnya terdapat IDS yang sedang berjalan, maka secara otomatis akan mendeteksi dan memberitahukan kepada administrator berupa notifikasi yang dikirim melalui jejaring sosial, sehingga administrator dapat melakukan tindak lanjut terhadap jenis serangan yang dilakukan oleh intruder,
2. **Nishidh D Patel et al**, (2013) vol 1, issue 3, dipublikasikan oleh *International Journal For Scientific Research and develoment, ISSN: 2321-*

0613), dengan judul AN ANALISYS OF NETWORK INTRUSION DETECTION SYSTEM USING SNORT. Penelitian ini dilakukan untuk mengetahui performa dari snort yang digunakan pada *MIT Lincon laboratories, snort* dianalisis berdasarkan adanya pemberitahuan setiap hari. Hasil dari penelitian ini adalah diperlakukannya meningkatkan kinerja *snort* dalam mendeteksi dan mengurangi kesalahan *alerts* yang dilakukan *snort*.

3. **V.P.Kshirsagar et al** (2012), Vol 1, ISS 4, dipublikasikan oleh International Journal Of Computer Science And Informatics, ISSN: 2231-5292, dngan judul "APPROACHES FOR IMPROVING THE PERFORMANCE OF SNORT INTRUCTION DETECTION SYSTEM". Penelitian ini dilakukan untuk mengetahui bagaimana implementasi *Snort* dalam meningkatkan *Intrusion Detection System,* penelitian ini difokuskan pada arsitektur dari *snort* dan *rule snort.* Hasil penelitian ini adalah tiga metode yaitu, *rule matching algorithm base on dynamic adjustment, NAPI, logic analyser for tweaking snort security adn performance.*
4. **Vinod Kumar dan Om Prakash Sagwan,** (2012), Vol 1, Issue III, dipublikasikan oleh International Journal Of Computer Aplications and Information Technology, ISSN: 2278-7720, dengan judul "SIGNATURED BASED INTRUSION DETECTION SYSTEM USING SNORT". Pada penelitian ini dilakukan inplementasi *snort* didalam sistem operasi Debian, *Snort* dapat mendeteksi dan menganalisis serangan secara real time, jika diidentifikasi kan sebuah serangan maka *Snort* akan mengirimkan sebuah *alert* kepada administrator. Hasil dari penelitian ini adalah *snort* perlu

dikembangkan dimasa yang akan datang dalam model *prototype* untuk menyaring, menghapus serangan secara otomatis dan *real time* didalam jaringan.

5. **Adi Wibowo** (2014)**,** Naskah Publikasi Sekolah Tinggi Manajemen Informatika Dan Komputer Amikom Yogyakarta dengan judul **"ANALISIS DAN IMPLEMENTASI IDS MENGGUNAKAN SNORT PADA CLOUD SERVER DI JOGJA DIGITAL VALLEY".** Menggunakan Snort Pada Cloud Server Di Jogja Digital Valley" dapat dipaparkan hasil penelitian sebagai berikut :

   a. Distribusi IP Public pada infrastruktur dan jaringan cloud server JDV memberikan kemudahan untuk diakses kapan saja dan dimana saja. Sedangkan kondisi saat ini masih terdapat beberapa default port yang terbuka, hal inilah yang rentan dimanfaatkan oleh attacker.

   b. Cara mengembangkan infrastruktur jaringan Jogja Digital Valley saat ini adalah dengan membangun IDS server sehingga dapat mengirim alert berupa log ketika terjadi serangan kepada administrator

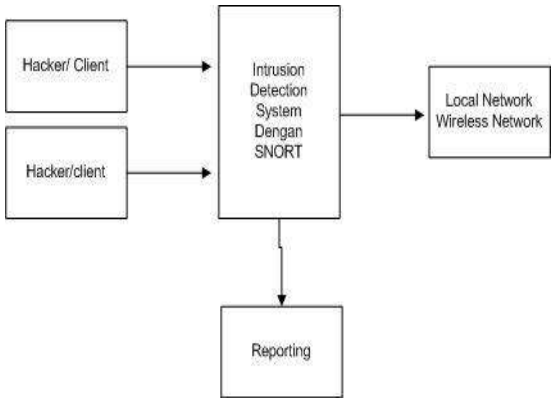
   c. Sistem deteksi penyusup yang digunakan adalah Snort dan dapat mendeteksi pola serangan baik dari dalam (local) atau luar (internet) sesuai dengan rules yang telah dibuat sebelumnya.

   d. Data dan log dari Snort disajikan dalam bentuk Graphical User Interface (GUI) menggunakan aplikasi Snorby sebagai sistem monitoring.

e. Secara umum Snort bekerja hanya sebagai sistem deteksi dan tidak mampu menahan serangan, sehingga memerlukan kombinasi menggunakan Iptables firewall sebagai tindak pencegahan serangan.

2.5 Kerangka Pemikiran

Kerangka pemikiran adalah suatu pemikiran terhadap alur yang dipahami sebagai acuan dalam pemecahan masalah yang diteliti secara logis dan sistematis, pada penelitian yang membahas analisis wireless *network security* dengan metode *snort* IDS. Uraian dalam kerangka konsep menjelaskan hubungan dan keterkaitan antar pokok-pokok penelitian. Pokok-pokok penelitian dijelaskan secara mendalam dan relevan dengan permasalahan yang diteliti, sehingga dapat dijadikan dasar untuk menyusun kerangka pemikiran.



Gambar 2.15 Kerangka Pemikiran
Sumber (Olahan sendiri, 2017)

Dari gambar kerangka pemikiran diatas dapat dijelaskan setiap bagian komponen sebagai berikut :

Hacker atau *Client* sebagai komponen yang dapat melakukan pengiriman serangan data atau ancaman serangan pada jaringan komputer. Serangan dari hacker atau client akan dideteksi oleh *Intrusion Detection System* (IDS) dengan aplikasi snort. *Snort* IDS yang di instal di dalam sistem operasi *windows* akan memberikan bantuan untuk melakukan identifikasi , memberi laporan terhadap aktifitas jaringan *wireless network*, dan *local network* dalam jaringan komputer tersebut. *Intrusion Detection System* secara khusus berfungsi sebagai proteksi secara keseluruhan dari sistem yang diinstal IDS. *Snort* secara real time akan mencatat seluruh aktifitas yang terjadi pada jaringan komputer pada *loging* report berupa alert yang akan dianalisis oleh *administrator server*.

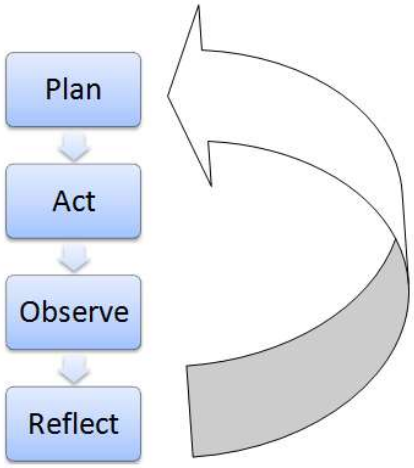
BAB III
METODE PENELITIAN

3.1. Desain Penelitian

Menurut Noor (2012: 107), desain penelitian bertujuan untuk melaksanakan penelitian sehingga dapat diperoleh suatu logika, baik dalam pengujian hipotesis maupun dalam membuat kesimpulan. Menurut Hasibuan (2007: 60), desain penelitian merupakan pedoman dalam melakukan proses penelitian diantaranya dalam menentukan instrumen pengambilan data, penentuan sampel, pengumpulan data serta analisis data.

Penelitian ini menggunakan metode *action research* atau sering disebut penelitian tindakan. Menurut Hasibuan (2007:79), penelitian tindakan (*action research)* merupakan penelitian kuantitatif maupun kualitatif dimana cara meneliti terjun langsung ke daerah penelitian. Menurut Darmadi (2011:244), penelitian tindakan merupakan salah satu model penelitian yang muncul ditempat kerja, tempat dimana melakukan pekerjaan sehari-hari.

Menurut Darmadi (2011: 246), terdapat empat langkah penting dalam penelitian tindakan dapat ditunjukkan pada gambar di bawah ini :



Gambar 3.1 Langkah *Action Research*
Sumber (Darmadi, 2011:246)

1. Rencana, merupakan serangkaian tindakan terencana untuk meningkatkan apa yang terjadi, dalam penelitian tindakan, rencana tindakan harus berientasi ke depan.
2. Tindakan, merupakan langkah kedua yang perlu diperhatikan, tindakan dalam penelitian harus hati hati dan merupakan kegiatan praktis yang terencana
3. Observasi, observasi pada penelitian yang diberikan kepada subjek, oleh karena itu observasi harus mempunyai berbagai macam unggulan seperti memiliki orientasi presfektif, memiliki dasar-dasar reflektif waktu sekarang dan masa yang akan datang
4. Reflektif, merupakan sarana untuk melakukan pengkajian kembali tindakan yang telah dilakukan terhadap objek penelitian dan telah dicatat dalam observasi.

Guna mengumpulkan informasi mengenai kebutuhan sistem maka penulis melakukan pengumpulan data dengan cara observasi ditempat penelitian, yaitu pada PT Bayu Pariama Batam, bulan Januari 2017, dengan Bapak Budi yang bertindak sebagai administrator jaringan PT Bayu Pariama Batam, tentang bagaimana implementasi jaringan saat ini.

Gambar 3.2 Desain Penelitian
Sumber (Olahan sendiri , 2017)

Berikut adalah pembahasan dari gambar di atas :

a. Observasi lapangan bertujuan untuk meninjau secara langsung masalah yang akan diteliti dan mengetahui kondisi jaringan di lapangan.

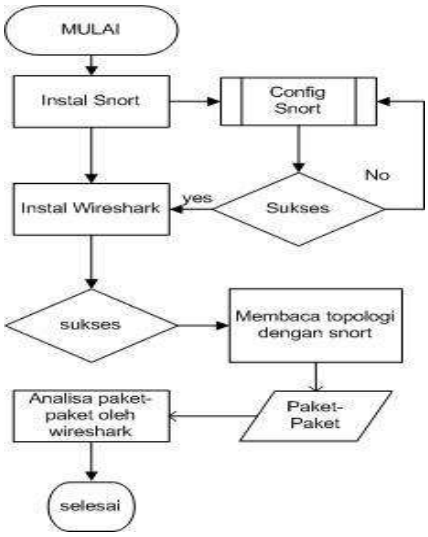
b. Identifikasi masalah, merupakan dasar pokok dalam penelitian.

c. Studi Literatur bertujuan untuk mengumpulkan data-data yang dilakukan dengan cara membaca dan mempelajari buku-buku yang berkaitan dengan

permasalahan yang akan menunjang terhadap materi pembahasan masalah yang diteliti.

d. Evaluasi jaringan bertujuan untuk memahami pokok masalah yang ada dan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah tersebut.

e. Perancangan, dalam tahap penelitian ini merupakan analisa terhadap kebutuhan sistem. Pengumpulan data dalam tahap ini bisa melakukan sebuah penelitian wawancara dan studi literatur. Dalam hal ini PT Bayu Pariama Batam memiliki sebuah masalah yaitu bagaimana mereka mendeteksi sebuah penyusup yang masuk kedalam jaringan mereka dan akan mengirimkan alert atau pemberitahuan ketika memang terjadi suatu masalah. Dalam tahap ini akan memberikan saran pada perusahaan untuk memakai snort yang berfungsi sebagai IDS. Berikut ini merupakan desain perencanaan pembuatan IDS:



Gambar 3.3 Topologi Implementasi *Snort*
Sumber (Olahan sendiri , 2017)

Dari gambar diatas dijelaskan bagaimana perancangan membuat sistem IDS dan bagaimana sistem itu bekerja. Untuk membaca isi dari paket yang terdeteksi oleh IDS dibutuhkan *wireshark*. *Wireshark* berperan penting dalam menganalisa paket yang masuk ke jaringan.

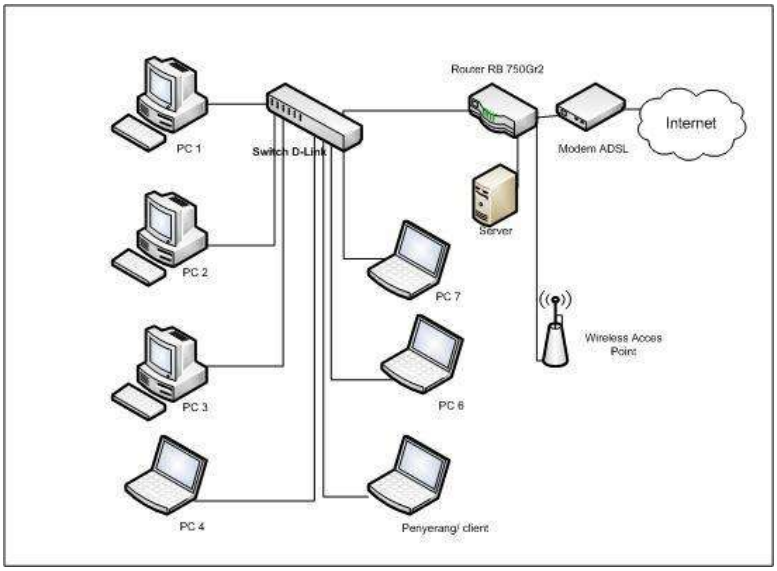
f. Implementasi, dalam tahap ini akan mengimplementasikan IDS dengan menginstal *snort*, konfigurasi *snort*, menginstal *wireshark*, uji coba *snort*, dan analisa paket.

g. Kesimpulan

h. Pelaporan, meliputi dokumen skripsi

3.2. Analisis Jaringan lama

Jaringan PT. Bayu Pariama Batam yang ada saat ini dapat dilihat pada gambar di bawah ini :

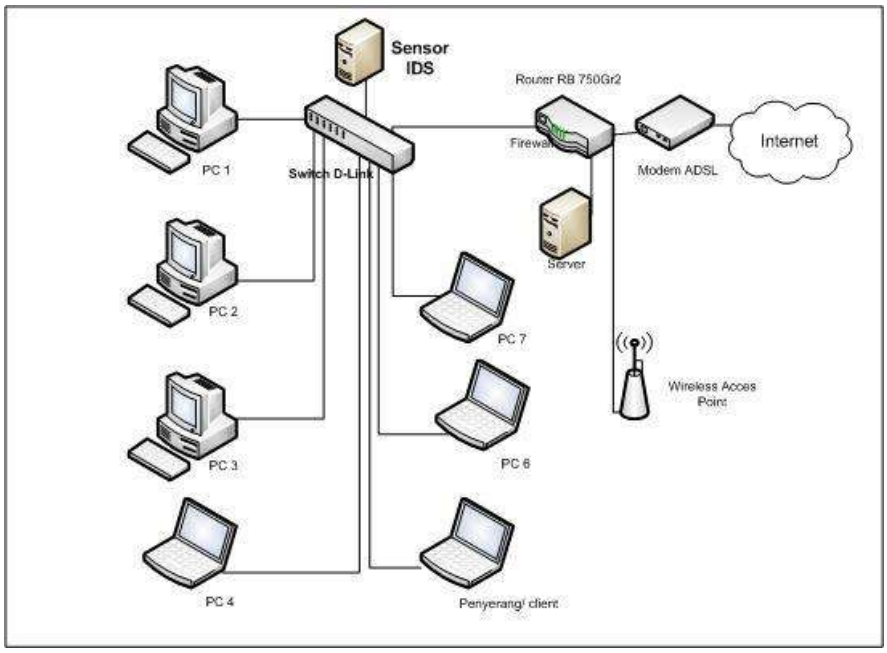


Gambar 3.4 Topologi Jaringan PT Bayu Pariama Batam
Sumber (Olahan sendiri , 2017)

Dilihat dari topologi diatas, topologi yang digunakan adalah topologi *star*, dimana setiap node terhubung langsung ke *switch*. Di topologi tersebut, belum adanya penambahan *Intrusion Detection System* (IDS). Belum adanya keamanan jaringan yang digunakan, sehingga tingkat keamanan jaringan masih minimal, sehingga tidak menutup kemungkinan apabila serangan datang dari luar maka sistem yang ada dalam jaringan akan terganggu dan jaringan yang lambat.

3.3. Rancangan jaringan yang dibangun

Jaringan komputer PT Bayu Pariama Batam yang akan diusulkan dan dirancang baru yaitu :



Gambar 3.5 Topologi Jaringan PT Bayu Pariama Batam Yang Diusulkan
Sumber (Olahan sendiri , 2017)

Tahapan pengembangan yang dilakukan dalam penelitian meliputi :

1. Topologi Jaringan pada PT Bayu Pariama Batam menggunakan topologi star, dimana setiap node terhubung langsung ke *switch*
2. Seluruh alamat internet protocol yang digunakan adalah kelas C
3. Menentukan kebutuhan hardware yang akan digunakan dalam penelitian. Agar sistem IDS dapat berjalan dengan semestinya, komputer yang digunakan server harus memiliki spesifikasi sebagai berikut :
    a. Processor 3.0 Ghz
    b. Motherboard dengan slot PCI
    c. 4 GB RAM
    d. Hardisk 160 GB
    e. 2 buah Network Interface Card (NIC)
4. Spesifikasi perangkat lunak membutuhkan perangkat lunak pendukung antara lain :
    a. Sistem Operasi Windows
    b. Winpcap versi 4.1.3 (http://www.winpcap.org/install/).
    c. Snort versi 92.9.7.6 (https://www.snort.org/downloads#snort).
    d. Wireshark (https://www.wireshark.org/#download.

Sistem pendeteksi intrusi yang dikembangkan berjenis NIDS (*Network Intrusion Detection System*), karena IDS jenis ini ditempatkan di sebuah titik yang strategis untuk melakukan pengawasan terhadaf traffic yang menuju dan berasal dari alat alat dalam jaringan. Idealnya semua traffic yang berasal dari luar dan dari

dalam jaringan dilakukan di scan. IDS ditempatkan pada jaringan nirkabel PT Bayu Pariama Batam untuk mengamati aktifitas para pengguna *wireless*. Semua paket dari atau menuju klien akan melalui mikrotik Hotspot, sehingga untuk dapat mengamati lalu-lintas IDS ditempatkan pada Interface publik monitoring mikrotik hotspot pada router RB 750Gr2. Semua paket yang masuk ataupun keluar jaringan interface publik mikrotik hotspot akan dicerminkan ke IDS untuk kemudian dianalisis.

3.4. Lokasi dan Jadwal Penelitian

3.4.1. Lokasi Penelitian

Lokasi penelitian dilakukan di PT Bayu Pariama batam. Alasan pemilihan lokasi penelitian adalah karena Perusahaan yang berlokasi di Komplek Pertokoan Kuda Putih Blok A No. 2 Sei Panas-Batam, saat ini sudah tersedia koneksi internet yang memadai untuk melakukan penelitian.

3.4.2. Jadwal Penelitian

Penelitian ini dilakukan dari bulan September 2016 hingga Januari 2017 dimulai dengan pengajuan judul penelitian sampai dengan akhir penelitian yaitu pengumpulan skripsi dengan jadwal sebagai berikut:

Tabel 3.1 Jadwal Penelitian

Tahap	Uraian	Bulan															
		Oktober 2016				November 2016				Desember 2016				Januari 2017			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Pengajuan judul penelitian																
2	Bimbingan dosen pembimbing																
3	Studi kepustakaan																
4	Pengajuan surat penelitian ke PT Bayu Pariama Batam																
5	Rancangan penelitian																
6	Pengumpulan data di lapangan																
7	Analisis data																
8	Penyimpulan hasil																
9	Pengumpulan skripsi																