PENERAPAN INTRUSION PREVENTION SYSTEM UNTUK KEAMANAN JARINGAN

SKRIPSI

Oleh:
Tohap Sitohang
150210232

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
2019

PENERAPAN INTRUSION PREVENTION SYSTEM UNTUK KEAMANAN JARINGAN

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Oleh:
Tohap Sitohang
150210232

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
2019

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, 03 Agustus 2019

Yang membuat pernyataan,

Materai Rp. 6.000

Tohap Sitohang

150210232

PENERAPAN INTRUSION PREVENTION SYSTEM UNTUK KEAMANAN JARINGAN

Oleh:
Tohap Sitohang
150210232

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Telah disetujui oleh Pembimbing pada tanggal
seperti tertera di bawah ini

Batam, 03 Agustus 2019

Cosmas Eko Suharyanto, S.Kom., M.MSI..
Pembimbing

ABSTRAK

Jaringan komputer adalah telekomunikasi yang memungkinkan komputer untuk bertukar informasi. Tidak adanya sistem untuk mengambil tindakan pencegahan telah menyebabkan kebutuhan untuk sistem pencegahan dalam jaringan komputer. Dalam hal ini ada beberapa sistem yang dirancang untuk pencegahan dan dapat dilihat melalui, grafik peringatan Wireshar dan port digunakan sebagai server aplikasi *INTRUSION PREVENTION SISTEM*,yang dapat mengoptimalkan potensi kerusakan pada sistem, yang dipengaruhi oleh kegiatan dan kegiatan dan PPDIOO (mempresentasikan,merencanakan,merancang,mengimplementasikan,mengoperasi kan, menjalankan dan mengoptimalkan) CISCO adalah metode yang tepat untuk merancang sistem keamanan jaringan. Penelitian ini membangun keamanan jaringan protoype menggunakan Snort dan peringatan grafik menggunakan Wireshark, dengan Server, BASE (Analisis Dasar, dan Mesin Keamanan) untuk mengambil tindakan untuk mencegah intrusi. Beberapa fitur dapat dilihat di notifikasi email dan analisis data menggunakan Splunk. Hasil pengujian membuktikan bahwa Server Sistem Pencegahan Intrusi berjalan dengan baik, dan dapat diandalkan. Ini dapat dilihat dengan memblokir intrusi dengan aturan yang telah dibuat dan tidak ada sistem crash.

Kata kunci: *Intrusion Prevention System, Snort, PPDIOO, Wireshark, email, Splunk.*

ABSTRACT

Computer networks are telecommunications that allow computers to exchange information. The absence of a system for taking precautionary measures has led to a need for prevention systems in computer networks. In this case there are several systems that are designed for prevention and can be seen through, warning graphics Wireshar and ports are used as application servers Intrusion Prevention system, which can optimize potential damage to the system, which is influenced by activities and activities and PPDIOO(presenting, planning, designing, implementing, operating, running and optimizing) CISCO is the right method for designing network security systems. This research builds protoype network security using Snort and graphics warnings using Wireshark, with Server, BASE (Basic Analysis, and Security Engine) to take action to prevent intrusion. Some features can be seen in e-mail notifications and data analysis using Splunk included. The test results prove that the Intrusion Prevention System Server is running well, and is reliable. This can be seen by blocking intrusions with rules that have been created and no system crashes.

***Keywords**: Intrusion Prevention System, Snort,PPDIOO, Wireshark, email notification, Splunk*

KATA PENGANTAR

Segala puji syukur penulis panjatkan kehadapan Allah SWT atas segala rahmat dan hidayah-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. Rektor Universitas Putera Batam.
2. Ketua Program Studi Teknik Informatika Universitas Putera Batam.
3. Bapak Cosmas Eko Suharyanto, S.Kom., M.MSI. selaku pembimbing Skripsi pada Program Studi Teknik Informatika Universitas Putera Batam.
4. Seluruh Dosen Teknik Informatika.
5. Dosen dan Staff Universitas Putera Batam.
6. Bapak Joe Hasriato SE selaku IT dan Aministarasi di Dinas Kependudukan dan pencatatan Sipil,dan Ibu Miftahul Ashar selaku pengelola dan penyajian data Kependudukan dan Pencatatan Sipil kota Batam.
7. Istri dan Anak saya yang selau meberikan semagat,dan selau mendoakan mendorong.meberikan motivasi.dan juga pengorbanan baik moral sehinga penulis dapat meyelesaikan skripsi ini.
8. Kedua orang tua saya yang saya sayangi dan saya cintai yang selalu memberikan dorongan, mendoakan, memberikan motivasi dan pengorbanannya baik dari segi moril, materi kepada penulis sehingga penulis dapat menyelesaikan skripsi ini.

9. Buat teman-teman satu pekerjan yang selalu memberi semagat dan motivasi kepada saya,trimakasi atas dukugan dan doanya.
10. Buat teman-teman sekelas serta seperjuangan penulis terima kasih atas dukun dan doanya.
11. Terima kasih juga kepada semua pihak yang telah membantu dalam penyelesaian skripsi ini yang tidak dapat disebutkan satu per satu.

Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan Berkat dan Kasihnya, Amin.

Batam, 03Agustus 2019

Penulis :Tohap Sitohang.

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

Halaman

DAFTAR TABEL

Halaman

BAB I
PENDAHULUAN

1.1 Later Belakang Masalah

Seperti yang kita ketahui sekarang ini kemajuan jaman teknologi ilmu telekomunikasi sekarang ini begitu cepat dan sangat banyak teknologi munculan di kota Batam.Teknologi baru yang lahir memberikan banyak kecanggihan dan kemudahan bagi penggunanya di bandingkan sebelunya. Ini merupakan Tantangan untuk penyedia informasi adalah bagaimana menmberikan informasi dengan baik dan tepat. Internet merupakan jaringan komputer terluas. Salah satuya adalah dengan adanya jaringan internet sebagai media informasi untuk menjawab tantangan tersebut. Internet merupakan jaringan komputer terluas, dengan cakupan seluruh planet bumi ini. Internet menghubungkan semua atau untuk menjembatani pertukaran informasi, pertukaran data dalam beberapa jaringan yang tidak sama atau diberi nama *Wide Area Network* (WAN), WAN (*Wide Area Network*) merupakan jaringan komputer yang lebih luas dari MAN (*Metropolitan Area Network),* dengan cakupan area luas sebuah Negara atau Benua. WAN (*Wide Area Network*) terdiri atas dua atau lebih MAN (*Metropolitan Area Network*) di dalamnya. Setiap MAN (*Metropolitan Area Network*) tersebut terdiri atas dua atau lebih LAN (*Local Area Network*) di dalamnya. Sehingga dapat dikatakan bahwa WAN (*Wide Area Network*) ini merupakan gabungan dari sejumlah jaringan komputer yang berada dalam satu kawasan seluas sebuah Negara ataupun Benua.

Misalkan saja WAN (*Wide Area Network*) di Negara Indonesia maupun WAN (*Wide Area Network*) sejumlah kota besar di Australia, Eropa, Amerika Serikat yang saling terhubung satu sama lain Pratama (2015: 35). internet iyalah sudah menjadi bagaian dari kebutahan untuk seluruh manusia.Sesuai dengan era yang sagat pesat menutut menigkanya kualitas keaman jaringan dan semakin banyakya ilmu pengetahuan tentang *hacking* dan *craking* yang di dukun oleh *tools*,yang mudah di dapat dengan mudah dan gratis.selain itu beberapa tutoriya dan buku.dan sangat banyak media dan juga sumber yang boleh di pelajari tentang berbagi pengetahuan untuk mempelajari, dan mengetahuai tentang *hackin* yang meyedikan.*virus,macicous,Trojan,worm,dossnniping*dan,*spammping,*dan juga lainya.hal ini lah yang menancam keaman sebuah system jaringang dimna data dapat dengan mudah di ambil,dan dirusak oleh *intruder* dan *attacker.*Ancaman mungkin saja ada,untuk merusak dan mencuri data,kejahatan yang sering terjadi biasanya berupa,pengiriman paket data yang besar dan biasanya di sebut *flooding,*bertujuan mengganggu tranmisi data di jaringan computer,*sniffing* untuk mencari data yang berada di jaringan computer untuk mendapatakn informasi yang bersifat rahasia atau bersifat *privacy,*hal ini pula yang menyebabkan cepatnya penyebaran *virus* ataupun *malware* sebuah jaringan computer dengan pertahan terbuka.Pada saat ini tidak bisa di pungkiri lagi bahwa masayarakyat, apalagi di kalangan pelajar dan mahasiwa banyak mengunakan sarana *electron mail* atu bisa di sebut *e-mail,*dalam kegiatan di dunia maya.seperti membuat akun sosial,mengirim tugas -tugas,kuliah,maupunmendapatakn informasi.seperti hasil penelitian,biodata pribadi,data laporan,ataupun laporan yang besifat pribadi. Di

dunia maya Sangat banyak tindak kriminal yang terjadi.dengan penaganan yang pasti dan perawatan yang berkala dapat memperkecil kemungkinan buruk resiko yang akan terjadi. *Intrusion prepention System* dalam dunia keamanan computer memiliki arti *Intrusion prepention System.* Yang berfungsi untuk melakukan pemeriksan terhadap lalu lintas data di jaringan mendeteksi aktifasi menjalankan pengencekan secepat mungkin kepada terjadinya suatu masalah yang menyebabkan lalu lintas tidak berjalan dengan semestinya.Keaman jaringan kompter adalah memang penting untuk menjaga validitas dan integritas data serta menjamin layanan bagi pengunaya dalam penelitian ini.penulis membahas mengenai jaringan komputer pada jaringan internet sering terjadi permasalahan diantaranya seperti lambatnya koneksi pada saat pegawai melakukan akses internet dan terkadang pegawai juga mengalami putus koneksi internet sesaat bahkan juga ada beberapa pegawai yang tidak dapat melakukan akses ke internet sama sekali. Hal ini biasanya terjadi saat ada beberapa Pegawi melakukan proses download maupun upload data pada sebuah website dalam waktu yang hampir bersamaan. Dalam penelitian ini, penulis juga melihat pada saat jam kerja terdapat beberapa pegawai yang melakukan aktivitas browsing ke media sosial dan juga streaming ke beberapa situs penyedia film dan video secara online. Hal ini di nilai penulis,dapat menyebabkan bayakya serangan Masuk ke dalam jaringan dan Membuat beberpa komputer error. Dan komputer mati mendadak,atau pun susah dalam koneksi dan membuat produktivitas Pegawi dalam bekerja karena Pegawai tidak menggunakan waktu kerja secara optimal dan Pegawai tidak menggunakan fasilitas internet sesuai dengan kepentingan yang berhubungan dengan pekerjaan.Untuk

menyelesaikan permasalahan tersebut, maka pertama penulis akan mengatasi permasalahan mengenai koneksi internet dengan mengatur penggunaan *bandwidth* pada jaringan dengan melakukan manajemen *bandwidth*. yang dilakukan dalam penelitian ini adalah dengan menggunakan aplikasi untuk memudahkan operator jaringan memantau penggunaan internet yang dilakukan oleh masing-masing Pegawai pada Dinas Kependudukan Dan Pencatatan Sipil Kota BATAM.tidak dapat melakukan akses ke internet sama sekali. Hal ini biasanya terjadi saat ada beberapa Pegawai melakukan proses *download* maupun *upload* data pada sebuah website dalam waktu yang hampir bersamaan.Berdasarkan later belakan penulis tertantang untuk terjun mejalankan penelitian menerapkan *keamanan jaringan* ketika melakukan pengunduhan (*download*) dan mengunggah (*upload*) pada WAN dengan judul ***Penerapan Intrusion prepention System*** **Menggunakan *Wireshark dan Snort*.**

1.2 Identifikasi Masalah

Dari later belakang dapat di defenisikan beberapa masalah di antaranya sebagai berikut :

1. Ancaman dan keaman jaringan dan penyusup,banyak ditemukan seperti contoh *virus.malicious,dos,Troimming,crackrs*
2. Ancaman untuk merusak,dan mencuri *data* dan mengancam system,Disaat terjadi penyerangan jaringan.

1.3 Pembatasan Masalah

Berdasarkan identifikasi masalah,peneliti membatasi masalah,di antaranya:

1. Peneliti mengunakan ***Intrusion prepention System dan wireshark,Snort*** sebagai metode pengaman.
2. Pengamanan hanya di Dinas Kependudukan Pencatatan Sipil Kota Batam.
3. Peneliti tidak mebahas keaman secara fisik.

1.4 Perumusan Masalah

Sistem dalam pencegahan, tindakan peretasan yang mukin akan di Lakukan dalam mengamankan suatu jaringgan,sehinga di butuhkan sistem dalam pencegahan tindakan *intrusidi*,sehinga bisa meminimalisasi potensi pengerusakan di jaringan maka demikin di butuhkan penganan peningkatan keamana jaringan Setelah melakukan analisa timbul beberapa pertanyaan :

1. Bagaimana menghasilkan sebuah system lalu lintas jaringan?
2. Bagaimana upaya penegawasan pada lalu lintas jaringan?
3. Bagaimana upaya pencegahan pada lalu lintas jaringan?
4. Bagaimana upaya peningkatan keamana pada lalu lintas jaringan?

1.5 Tujuan Penelitian

1.5.1 Secara Teoritis:

1. Menghasilkan suatu sistem keaman jaringan yang dapat di gunakan.
2. Melakuan upaya pembuatan system dalam pengaman jaringan.

3. Meningkatkan keamana jaringan/pengawasan jaringan.

1.5.2 Secara Praktis :

1. Menggembangkan ilmu tentang jaringan.
2. Meninkatakan ilmu pengetahuan,peneliti dalam lingkup *networking.*

1.6 Manfaat Penelitian

1.6.1 Manfaat Teoritis

1. Menambah Pengalaman ilmu tentang terjadinya serangan pada jaringan
2. Memberikan gambaran tentang konsep mengenai serangan pada jaringan
3. Dapat menjadi referensi mahasiswa khusnya teknik informatika yang tertarik mengenai kinerja ***Intrusion prepention System dan wireshark***

1.6.2 Manfaat Praktis

1. Membantu pengguna jaringan yang sering mengalami serangan saat berkerja mengunakan media komputer .
2. Meningkatkan pengetahuan kinerja pada jaringan ***Intrusion prepention System dan wireshark*** dalam keaan jaringan.
3. Penelitian ini bisa memperoleh panduan sebagai awal untuk penelitian selanjutnya dalam keaman jaringan. ***Intrusion prepention System dan wireshark.***

BAB II
KAJIAN PUSTAKA

2.1 Teori Dasar

Berdasarkan penelitian yang dilakukan menyimpulkan bahwa jaringan komputer itu sendiri adalah kumpulan dari beberapa atau banyak komputer, printer dan perangkat lainnya yang terhubung dalam satu kesatuan. Kemudian ada sebuah paket data yang dialirkan dengan mengunakan sambugan *wire/kabel* agar *user* atau *konsumen* dapat saling berbagi informasi bersama-sama menggunakan perangkat keras dan perangkat lunak *terkoneksi* kejaringan. Setiap komputer, *printer dan periferal* atau perangkat tambahan yang terhubung dengan jaringan disebut node. (Ardianto & Akbar, 2017)

2.1.1 Jaringan Komputer

Menurut Pratama (2015: 12) terdapat banyak defenisi oleh para ahli mengenai jaringan komputer, penulis menggunakan referensi utama dari buku karya Forouzan Sehingga defenisi jaringan komputer disepakati sesuai dengan defenisi dari Forouzan. Menerut Forouzan di dalam bukunya yang berjudul *Computer Network A Top Down Approach*, disebutkan bahwa jaringan komputer adalah hubungan dari sejumlah perangkat yang dapat saling berkomunikasi satu sama lain (*a network is a interconnection of a set of devices capable of communication*). Perangkat yang dimaksud pada defenisi ini mencakup semua

jenis perangkat komputer (komputer desktop, komputer jinjing, smartphone, PC tablet) dan perangkat penghubung *(router, switch, modem, hub).*

Menurut Maslan (2012: 2) Jaringan Komputer merupakan kesatuan dari komputer, printer, dan peralatan laiannya yang terkoneksi satu kumpulan dan membuat suatu jaringan yang mempuyai sistem tertentu. semua Informasi berjalan megunakan *wire/kabel* ataupun tanpa *wire/kabel* sehingga memungkin pengguna jaringan komputer bias saling berbagi informasi data mencetak yang sama dan dapat secara simultan memakai sistem yang sama.

2.1.2 Standar Jaringan Komputer

IEEE dan WI-FI adalah dua hal yang berbeda, atau lebih tepatnya merupakan dua organisasi yang berbeda. IEEE (*Institute Of Electrial And Electronics Engineers*) merupakan organisasi non-profit yang mendedikasikan kerja kerasnya demi kemajuan teknologi. Organisasi ini mencoba membantu banyak sekali bidang teknologi penerbangan, elektronik, biomedical, dan tentu saja komputer juga termasuk didalamnya. Keanggotaan organisasi IEEE diklaim mencapai 370.000 orang yang berasal dari 160 negara di dunia. Pada tahun 1980 bulan 2, IEEE membuat sebuah bagian yang mengurusi standirisasi LAN (*Local Area Network*) dan MAN (*Metropolitan Area Network*). Bagian ini kemudian dinamakan sebagai 802. Bener, angka 80 menunjukan tahun dan angka 2 menunjukkan bulan dibentuknya kelompok kerja ini. Lalu apa itu WI-FI,IEEE sudah meluncura standar jaringan *wireless* namun standar itu diperkirakan kurang

baik dalam memenuhi kebutuhan dalam bidang bisnis. Organisasi ini berkerja memastikan semua peralatan yang mendapatkan label WI-FI bisa bekerjasama dengan benar sehingga membantu penguna dalalm memakai produknya. Anggota WI-FI sehingga mereka berkuasa *Cisco, Micorsoft, Dell, Texas Instrumens, Apple, AT & T*, dan masih banyak lagi yang tidak dituliskan satu persatu.Maka secara umum, Anda bisa menyamakan WI-FI dengan standarisasi *wireless* yang dilakukan oleh IEEE karena WI-FI mengambil spesifikasi yang telah dilakukan oleh IEEE. Pada buku ini, saya menyamakan WI-FI dengan jaringan *wireless* 802.11x menurut (S'to 2015: 5-8).

2.1.3 Jenis Jaringan Komputer

2.1.3.1 Berdasarkan geografis

Menurut Pratama (2015: 32-37) jaringan komputer bersifat *Scalable*, yaitu dapat membesar dan mengecil sesuai kebutuhan.Ini berarti bahwa sebuah jaringan computer dapat di perluas untuk menjangkau sebanyak mungkin pengguna di berbagai wilayah geografis hingga dipersempit untuk dapat digunakan sebagai pribadi oleh satu pengguna atau beberapa pengguna pada satu lokasi saja.Berdasarkan cakupan lokasi geografis inilah, jaringan Komputer dapat diklasifikasikan menjadi empat kelompok. Keempat kelompok tersebut meliputi LAN (*Local Area Network*), MAN (*Metropolitan Area Network*), WAN (*Wide Area Network*), dan Internet. Keempat disajikan secara detail pada setiap subbab dibawah ini. LAN (*Local Area Network*)

2.1.3.2 LAN (*Local Area Network)*

Gambar 2.1 *Local Area Network*

(Wongkar et al., 2015)

Merupakan jaringan komputer terkecil untuk pemakaian pribadi. LAN (*Local Area Network*) memiliki skala jangkauan mencakup 1 km hingga 10 km, dalam bentuk koneksi *wired* (kabel), *wireless* (nirkabel), maupun kombinasi keduanya. Umumnya LAN (*Local Area Network*) lebih banyak di terapkan di dalam sebuah ruangan maupun sebuah gedung,sebagai contoh:

a. Jaringan lokal diperpustakaan untuk penyedian *repository ebook* dan layanan sistem informasi perpustakaan.
b. Jaringan lokal pada laboratorium untuk sarana riset, penelitian, maupun bertukar data dan informasi.
c. Jaringan lokal pada kantor swasta, instansi emerintah, kampus/perguruan tinggi, dan sekolah, untuk pengguna bersama, printer, sistem informasi, pertukaran data, dan lain-lain.

2.1.3.3 MAN *(Metropolitan Area Network)*

Gambar 2.2 *Metropolitan Area Network*

(Wongkar et al., 2015)

MAN *(Metropolitan Area Network)* adalah Jaringan MAN atau *Metropolitan Area Network* merupakan jenis jaringan komputer dengan wilayah jaringan komputer dalam suatu kota. Biasanya jaringan MAN memiliki kecepatan pengiriman data yang besar untuk menyatukan tempat misalnya kantor,sekolah, dan kampus. MAN (*Metropolitan Area Network*) merupakan jaringan computer yang memiliki cangkupan area dan luas yang lebih besar dibandingkan LAN (*Lan Area Network*). MAN (*Metropolitan Area Network*) memiliki jarak jangkauan anatara 10 km hingga 50 km. wilayah jangkauan MAN (*Metropolitan Area Network*) dapat mencakup sebuah wilayah kota, yang didalamnya terdapat banyak gedung dan pemukiman. Ini berarti di dalam sebuah MAN (*Metropolitan Area Network*) telah banyak LAN yang berasal dari berbagai gedung dan pemukiman yang ada. Beberapa kota, terutama yang menerapkan *Smart City*, mulai banyak yang mengimpementasikan MAN (*Metropolitan Area Network*). Misalkan saja di Surabaya, Denpasar, Jakarta, Bandung, serta sejumlah kota besar di Eropa, Amerika, Asia, dan Australia. Penjelasan mengenai *Smart City* dapat Anda simak secara dlebih detail pada buku *Smart City* karangan penulis (pada penerbit yang sama, yaitu informatika).

2.1.3.4 WAN (*Wide Area Network*)

Gambar 2.3 *Wide Area Network*

(Wongkar et al., 2015)

WAN *(Wide Area Network)* adalah Jaringan WAN atau *Wide Area Network* suatu jenis jaringan komputer yang menjangkau daerah yang sangat luas.bentuk jaringan tersebut biasanya dipakai dalam menyatukan jaringan suatu negara dengan negara lainnya. (Wongkar et al., 2015)WAN (*Wide Area Network*) merupakan jaringan komputer yang lebih luas dari MAN (*Metropolitan Area Network),* dengan cakupan area luas sebuah Negara atau Benua. WAN (*Wide Area Network*) terdiri atas dua atau lebih MAN (*Metropolitan Area Network*) di dalamnya. Setiap MAN (*Metropolitan Area Network*) tersebut terdiri atas dua atau lebih LAN (*Local Area Network*) di dalamnya. Sehingga dapat dikatakan bahwa WAN (*Wide Area Network*) ini merupakan gabungan dari sejumlah jaringan computer yang berada dalam satu daerah sebesar sebuah Negara ataupun Benua. Misalkan saja WAN (*Wide Area Network*) di Negara Indonesia maupun WAN

(*Wide Area Network*) sejumlah kota besar di Australia, Eropa, Amerika Serikat yang saling terhubung satu sama Bentuk komunikasi antara computer di dalam WAN (*Wide Area Network*) memerlukan adanya perangkat penghubung, sakah satunya berupa *router*. Fungsi dari *router* adalah membant di dalam merutekan jalur yang akan di tempuh oleh plaket data di dalam proses transmisi paket data dan komunikasi antarkomputer di dalam WAN (*Wide Area Network*) tersebut. Pembahasan lebih lanjut mengenai *router* akan di sajikan detail pada bab lainnya di buku ini.

2.1.3.5 Internet

Sekarang internet sudah salah satu kebutuhan pokok manusia,apalagi orang yang berhubungan dengan Teknologi komunikasi dan informasi. Internetpun salah satu bagian dari jaringan Komputer, yang menyatukan semua computer dan penmakai Komputer di seluruh benua.*Internet* atau *internetworking* secara umum didefenisikan sebagai jaringan komputer terluas di benua dan menghubungakn seluruh jaringan yang ada. dan internet juga sudah menjadi kebutuhan semua orang di dunia.apalagi di masa sekarang *internet* sudah menjadi salah satu kebutuhan yang utama.terlebih di kalangan orang yang bekerja mengunakan media internet.dan internet sangat banjak menbantu semua kalangan di mana pun berada di sampin sangat mudah di dapatkan dan di akses.

2.1.3.6 Berdasarkan Media Transmisi

Menurut Iwan Sofana (2013: 06) berdasarkan media transmisi,dapat dibagi dua jenis, yaitu :

- ***Wire network***

Wire network merupakan jaringan komputer yang menggunakan kabel sebagai media penghubung. Jadi, mengalir pada kabel, kabel yang umum digunakan pada komputer biasanya berbahan dasar tembaga. Ada juga jenis kabel yang menggunakan bahan sejenis *fiber* yang disebut *fiber optic* atau *optik*.

- ***Wireless network***

Wireless network adalah jaringan tanpa kebl yang menggunakan media penghantar gelombang radio atau cahaya infrared atau laser. Saat ini sudah semakin banyak publik area atau lokasi tertentu yang menyediakan layanan *wireless network*. Sehingga pengguna dapat dengan mudah melakukan akses *internet* tanpa kabel. Frekunsi yang digunakan pada radio untuk jaringan komputer biasanya dikisarkan 2,4GHz dan 5,8GHz.

2.1.3.7 Macam Jaringan Topologi Pada Jaringan Komputer

Menurut Pratama (2015: 19) pada jaringan komputer, dikenal setidaknya Enam buah topologi pada jaringan komputer. Keenam jenis topologi pada jaringan komputer tersebut memiliki karakteristik, kelebihan dan kekurangan masing-masing. Keenam topologi pada jaringan komputer ini meliputi.Topologi jaringan merupakan sebuah aturan dalam menghubungkan komputer satu sama lain secara fisik dan pola hubungan antara komponen-komponen yang berkomunikasi melalui media atau perangkat jaringan, seperti *server*, *workstation* dan switch. Topologi

jaringan memiliki beberapa jenis diantaranya adalah topologi *bus*, topologi *star* dan topologi *ring*. (Widodo et al., 2018).

Sedangkan menurut Utomo (2012: 4) topologi yang dimaksud disini adalah gambaran struktur jaringan komputer yang Akan dibuat. Berdasarkan topologinya, sebuah jaringan komputer dapat dibedakan menjadi tujuh, yaitu:

1. Topologi Jaringan

Topologi jaringan merupakan sebuah aturan dalam menghubungkan komputer satu Sama lain dengan cara fisik dan pola hubungan komponen dan saling meberi informasi melalui media atau perangkat jaringan, seperti *server*, *workstation* dan switch. Topologi jaringan memiliki beberapa jenis diantaranya adalah topologi *bus*, topologi *star* dan topologi *ring*. (Widodo et al., 2018).

2. Topologi *Bus*

Jenis topologi ini menghubungkan setiap komputer atau node dengan sebuah kabel komunikasi melalui sebuah kartu antara muka (*card interface*) komputer. setiap jaringan komputer dapat terhubung dengan komputer lain yang ada dalam jaringan tersebut. Artinya, semua komputer mempunyai kedudukan yang sama dalam jaringan dan tidak tergantung pada komputer *server* pusat.

3. Topologi *Ring*

Komputer-komputer dalam jenis topologi ini akan dihubungkan dalam sebuah kabel tunggal dan membentuk bagan seperti sebuah cincin. Pada komputer ini tidak dapat komputer pusat sehingga semua komputer mempunyai kedudukan yang sama.

4. Topologi bintang atau *Star*

Dalam jenis topologi ini, beberapa komputer akan dihubungkan dengan satu pusat komputer sehingga semua control berbagai sumber daya (*resource*) dalam jaringan yang diperlukan juga akan dipusatkan pada satu titik. Ketika akan mengirim data ke komputer lainnya, komputer harus melalui komputer pusat terlebih dahulu. Dalam topologi ini, ketika pusat mengalami gangguan, semua komputer klien juga terganggu.

5. Topologi bintang diperluas atau *Extended Star*

Dasar jenis topologi ini adalah topologi bintang, hanya ditambah pengulang (*repeater*) berupa *hub* atau pengalih (*switch*) sehingga semakin memperluas jaringan yang jaraknya bejauhan.

6. Topologi bintang bertingkat atau *Cascading Star*

Jenis topologi ini juga hamper sama dengan bintang diperluas, namun beberapa jaringan bintag yang dibuat tersebut dihubungkan ke sebuah simpul pusat untuk mengontrol semuanya.

7. Topologi *Mesh*

Jaringan dengan jenis topologi ini mempunyai jalur ganda pada setiap node atau simpul jaringan, semakin banyak jumlah komputer yang ada dalam jaringan, semakin sulit pemasangan kabel-kabelnya, pemasangan kabel akan menjadi berlipat ganda. Oleh karena itu, pada topologi jaringan jenis ini setiap perangkat jaringan dihubungkan satu sama lain menggunakan jalur ganda untuk *hub* utama sebagai jalur cadangan ketika terjadi masalash pada jalur utama.

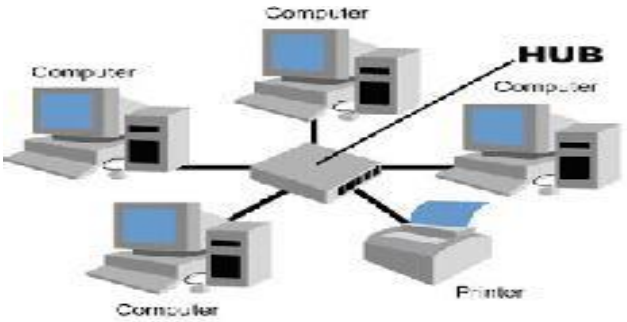
8. Topologi pohon atau *tree topology* atau bertingkat

Topologi jenis ini merupakan kombinasi antara topologi bintang dan topologi bus. Topologi ini terdiri atas kumpulan topologi bintang yang dihubungkan dalam satu topologi bus sebagai jalur tulang punggung atau *backbone*. Komputer-komputer dihubungkan ke *hab,* sedangakan hub yanglain dihungkan sebagai jalur tulang punggung. topologi ini sering dipakai untuk antara koneksi antarasentral dengan hierarki tidak sama. Hierarki yang kecil di uraikan pada tempat kecil dan makin keatas hieraekinya pasti lebih tinggi.

2.1.3.8 Jaringan Komputer Berdasarkan Fungsi

Menurut Iwan Sofana (2013: 07) berdasarkan pada oprasional atau mamfattnya, jaringan bisa dibagi menjadi dua, yaitu :

1. ***Client server***



Gambar 2.4 *Client-Server*

(Zunaidi et al., 2014)

Client-Server, Berbeda dengan jaringan peer to peer, pada jaringan client-server terdapat sebuah komputer yang berguna untuk server atau pusat data dan komputer lainnya berguna untuk client. Server disini berkerja untuk meberi seluruh *request* data dari komputer *client* yang termasuk dalam jaringan tersebut. (Zunaidi et al., 2014) *Client server* merupakan jaringan komputer yang mengharuskan salah satu (atau lebih) komputer digunakan untuk *server* atau *central*. *Server* melayani komputer lain yang dikatakan *client*. Layanan yang diserahkan dapat berupa akse*s Web, e-mail, file*, dang yang lain. *Client server* sangat banyak di temui pada jaringan *internet*. Dan LAN atau jaringan yang lainpum bisa menneraapkan *client server*. Hal tersebut bisa tergantung untuk kegunaan masing-masing.

2. *Peer to Peer*

Gambar 2.5 *Peer Peer*

(Zunaidi et al., 2014)

dimana setiap komputer dapat menjadi *server* sekaligus *client*.ketika tidak ada komputer yang lebih unggul dibanding komputer lain. Setiap komputer dapat menerima dan memberikan *access* dari atau ke komputer lain. *Peer to Peer* banyak diimplementasikan pada jaringan LAN, meskipu bias di terapkan pada WAN, MAN dan *internet* dan dengan cara kerja peer to peer,bias saling berbagi infomasi atu berbagi data untuk melangsukan komunikasi data karna setiap computer bias menjadi sever dan juga sekaligus bias juga menjadi *clien*.jadi dengan koneksi ini sangat lebih muda dalam mebagikan informasi dan juga menerima infomasi dari komputer yang lain dan sangat cepat dalam meberi dan menerima data ,jadi dalam hal ini Komputer yang satu dengan yang lain bias berkomunikasi dengan mudah .

2.1.4 Model OSI Layer

Model OSI Layer atau *Open System Interconnection* Layer merupakan sebuah model referensi jaringan terbuka dari arsitektural jaringan yang diperbesar oleh lembaga ISO *(International Organization for Standardization)* di Eropa pada tahun 1977. Model OSI Layer biasa dikenal dengan sebutan bentuk tujuh tingkat atau *OSI seven layer model* karena memiliki struktur tujuh tingkat bersamaan dengan protokol data unit pada setiap tingkatan. Pada model OSI standar, protokol dibagi menjadi 7 layer atau lapisan diantaranya adalah *Physical Layer*, *Data Link Layer*, *Network Layer*, *Transport Layer*, *Session Layer*, *Presentation Layer*, dan *Application Layer*. (Sondakh et al., 2014)

2.1.4.1 Pemodelan Layer OSI

Dalam jaringan komputer, terdapat permodelan secara hirarki untuk menggambarkan secara jelas tugas dari setiap lapisan pada jaringan komputer, terkait dengan proses pengiriman dan penerimaan paket data dari komputer pengirim ke komputer penerima. Selain itu, pemodelan secara hirarki ini juga turut menjelaskan fungsi-fungsi dari setiap lapisan di dalamnya terkait dengan jaringan komputer, yang meliputi perangkat keras jaringan komputer (*hardware*) dan perangkat lunak jaringan komputer (*software*). Lapisan-lapisan inilah yang disebut dengan pemodelan *layer* pada jaringan komputer (*layering model*). Pratama (2015: 45).Secara umum pemodelan *layer* pada jaringaan komputer memiliki duah buah model utama. Kedua model utama tersebut meliputi pemodelan *layer* OSI (*open system interconnection*) dan pemodelan *layer* TCP/IP (*transmission control*

protocol/internet protocol). Pemodelan *layer* TCP/IP kemudian terbagai atas pemodelan *layer* TCP/IP versi umum dan pemodelan *layer* TCP/IP versi Forouzan.

1. *Physical Layer*

Physical Layer (layer fisik) suatu layer di tingkatan pertama (terendah) pada pemodelan layer OSI. Sesuai dangan pangilannya, lapisan (layer) ini lebih banyak mengelola perangkat fisik (*hardware*) pada jaringan komputer. Termasuk juga di dalamnya pengolahan sinyal, bagus digital maupun analog.

2. *Data link layer*

Data link layer merupakan layer di lapisan kedua dan berada satu lapisan di atas *physical layer. Data link layer* memiliki sejumlah fungsi penting di dalam jaringan komputer, khususnya terkait dengan control data dan kesalah, pengalamatan fisik, serta dengan perangkat keras dan perangkat lunak.

3. *Network layer*

Network layer merupakan layer di lapisan ketiga dan berada satu lapisan atas *data link layer*. *Network layer* memiliki sejumlah fungsi penting di dalam jaringan komputer.

4. *Transport layer*

Transport layer merupakan layer di lapisan keempat (diatas *network layer*) dan berada satu lapis di atas *network layer*. *Transport layer* memiliki sejumlah fungsi penting di dalam jaringan komputer.

a. Memecahkan paket ke dalam beberapa buah unit paket data.

b. Membuat penomoran untuk smua pecahan paket data.

c. Membantu di proses datagram paket data,dan juga pemecahan paket data menjadi unit terkecil, pembungkusan pemecahan paket (*encapsulation*) dan pembukaan bungkusan pada packet data tersebut dengan *segment*.

5. *Session layer*

merupakan layer lapis kelima berada diatas tansport layer. Sesuai dengan namanya, session layer memiliki sejumlah fungsi penting terkait dengan sesi penting di dalam jaringan komputer. Antara lain sebagai berikut:

a. Melakukan proses pendefinisian dan pembuatan koneksi.

b. Melakukan pemeliharaan koneksi.

c. Melakukan penghacuran koneksi (*destroy*).

6. *Presentation layer*

Presentation layer merupakan layer di lapis keenam yang berada diatas *session layer*. Sesuai dengan namanya, *Presentation layer* bertugas menerjmahkan data yang ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan oleh jaringan komputer. penerjemah data yang ditransmisikan oleh perangkat

lunak di dalam jaringan komputer ke dalam format standar yang dapat dipahami oleh komputer penerima maupun entitas lainnya di dalam jaringan komputer, sangat diperlukan dan penting. Untuk itulah *presentation layer* bertuga untuk melakukan penerjemahini di dalam proses transmisi paket data.

7. *Application layer*

Application layer merupakan layer di lapis ketujuh (teratas). *Application layer* memiliki sejumlah fusngsi penting di dalam jaringan komputer. beberapa fungsi tersebut antara lain:

a. mendefenisikan spesifikasi aplikasi untuk dapat berkomunikasi di dalam jaringan komputer.
b. sebagai antara muka (*interface*) aplikasi dengan jaringan.
c. Membantu di dalam pengaksesan jaringan.

2.1.4.2 Fungsi Pemodelan *Layer OSI*

Menurut Maslan (2012: 38) Suatu jaringan komputer WAN dirancang dengan melihat arsitktur standar dibuat lembaga standar *industry* dunia. Standar jaringan yang sekarang diakui adalah *The Open System Conection* atau OSI yang dirancang oleh lembaga ISO (*The Internasional Organitation*), Amerika Serikat. Semua kegunaan tugas jaringan komputer dan hubungan antar terminal dalam standar ini. OSI suatu standar hubungan antara mesin yang terdiri atas tujuh tingkat. Ke tujuh tingkat ini itu memiliki tanggung jawab yang tidak sama Setiap *layer* bertanggung jawab secara khusus komunikasi data.

Tabel.2 1 Model layer OSI

Application	Application
Presentation	Presentation
Session	Session
Transport	Transport
Network	Network
Data link	Data link
Physical	Physical
OSI Model	OSI Model

(Zunaidi et al., 2014)

2.1.4.3.Pemodelan Layer TCP/IP

Menurut Pratama (2015: 53-55) Pemodelan *Layer* TCP/IP lahir karena banyak kekurangan pada Pemodelan *Layer* TCP/IP serta Pemodelan *Layer* TCP/IP sudah tidak mengikuti kemajuan perkembangan zaman, terutamnya Sofware dan jaringan komputer itu sendiri. Walaupun secara konsep, Pemodelan *Layer* OSI masih selalu digunakan di dalam ilmu jaringan komputer. Pemodelan *Layer* TCP/IP lebih simple dan ringkas hanya empat *layer* saja di dalamnya. Pemodelan *Layer* TCP/IP menggunakan konsep protocol TCP/IP yang mempunyai empat subprotokol di dalamnya, yang kemudia menjadi keempat *layer* pada Pemodelan *Layer* TCP/IP.

1. *Link layer (data link/network access)*

*Link layer (data link/network access)*layer terbawah pada Pemodelan *Layer* TCP/IP. *Link layer* berfungsi menjelaskan protocol yang digunakan pada topologi jaringan, *interface* yang digunakan , *flow control* dan sebagainya. Secara umum layer ini berfungsi untuk mendefenisikan beragam metode di dalam jaringan ke dalam lingkup *link* lokal jaringan pada komputer yang sedang berkomunikasi. Pada layer ini unit data disebut dengan *frame*, yang terdiri atas *frame header*, *frame data*, dan *frame footer*, *link layer* (*data link/network access*).

3. *Internet layer*

Internet layer adalah layer tingkat kedua (di atas *link layer/data link/network access*) yang berguna untuk pergantian datagram pada jaringan. *Layer* ini menberikan *interface* jaringan yang sama, dengan menghubungkan topologi yang dipakai. *layer* ini juga memberi pengalamatan dan *routing*. Itu sebabnya pada *layer* terdapat IP *header* dan IP data. Internet layer bisa disertakan dengan *network layer* pada pemodelan *layer* OSI.

4. *Transport layer*

Transport layer adalah *layer* di tigkat ketiga (di atas *internet layer*) yang berguna dalam memberi hubungan antaraproses (*end to and service*), *channel* penukaran data untuk aplikasi, *transmisi end to end massege*,bisa memakai protokol TCP (untuk *connection oriented*) dan UDP (untuk *connectionless*). *Transport layer* bisa dimasukan dengan *transport layer* pada pemodelan *layer* OSI.

5. *Application layer*

Application layer adalah ayer tertingi berguna dalam hubungan data antara sofware dan komputer (ini di sebut *peer*). beberapa protokol jaringan bekerja di *layer* ini, antara lain: SMPT, HTTP, FTP. *Application layer* serta dengan *session layer*, *presentation layer*, dan *application layer* pada pemodelan *layer* OSI.

2.1.4.4 Model referensi TCP/IP

TCP/IP yaitu standar komunikasi data yang dipakai konsumen internet dalam proses pertukaran data dari komputer ke komputer lain di dalam jaringan Internet (Iwan Sofana, 2010). standar yang dipakai komputer-komputer dalam lingkungan sistem operasi UNIX dan berguna untuk mengkoneksikan jaringan dan memberi alamat perjalanan jaringan..Sedangkan *internet protocol* adalah aturan yang mengatur aktivitas *internet* dan menfasilitasi penyelesaian berbagai tindakan pada WWW *(World Wide Web)*. (Hasrul & Lawani, 2017)

TCP/IP terdiri atas 4 (empat) layer yaitu:

1. *Application layer*

Protokol pada layer aplikasi TCP/IP menberikan servis bagi. *Software-software* yang berkerja pada direct. *Layer* aplikasi tidak memberikan *software* itu sendiri tapi hanya memberikan *servis* yang di dipergunakan oleh software.

2. *Transport Layer*

Transport layer terbagi dari 2 buah direct utama yaitu TCP dan *User DatagramProtocol* (UDP). *Transport layer* memberikan servis yang akan dipakai oleh*Application Layer Internet Layer* memeberikan kegunaan IP addressing, routing penentuan.

1. Network Access Layer mengangatikan direct-protokol dan hardware yang dipakai penghantaran data.

Tabel.2 2 Model Layer TCP/IP

Aplication	Applications
Presentation	
Session	Transport
Transport	(host to host)
Network	Internet
Data Link	Network accsess
Physical	

(Zunaidi et al., 2014)

2.1.4.5 OSI /TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) merupakan sekelompok protokol komunikasi yang saat ini secara luas dipakai untuk komunitas jaringan komputer. TCP/IP merupakan protokol standar yang dipakai komputer-komputer dalam lingkungan sistem operasi UNIX dan berfungsi untuk menghubungkan jaringan komputer dan mengalamati lalu lintas jaringan,Sedangkan *internet protocol* adalah aturan yang mengatur aktivitas *internet* dan menfasilitasi penyelesaian berbagai tindakan pada WWW *(World Wide Web)*. (Hasrul & Lawani, 2017)

2.1.4.6 Defenisi Protocol Dan Manfaat Protokol Pada Jaringan Komputer

Menurut Pratama (2015: 73-76) protokol memberikan banyak sekali manfaat di dalam jaringan komputer, baik dalam bentuk layanan, integrasi dengan aplikasi, kemudahan pada pengembang aplikasi,serta konsumen umum terdapat empat belas kegunaan yang didapat pada protokol secara general di dalam jaringan komputer yaitu:

1. Menolong di dalam proses *Flow Control* dalam jaringan komputer.
2. Menolong di dalam proses *Error Control* dalam jaringan komputer.
3. Menolong di dalam proses *multiplexing* dalamjaringan komputer.
4. Menolong di dalam transmisi paket data dalam jaringan komputer.
5. Menolong di dalam melakukan kontrol terhadap koneksi di dalam jaringan komputer (*Connection Control*).

6. Menolong di dalam proses pemecahan paket data ke dalam unit-unit paket data (*Fragmentasi*) serta penyusunan kembali paket data tersebut (*Reassembly*).
7. Menolong di dalam menyerahakan alamat (pengalamatan) pada jaringan komputer.
8. Menolong perintah dan menjalankan perintah di dalam jaringan komputer.
9. Menolong di dalam pengiriman dan transmisi paket data di dalam jaringa computer.
10. Menolong di dalam proses pembungkusan paket data dan unit paket data (*Encapsulation*) serta pembukaan bungkusan (*Decapsulation*).
11. Menjadi dasar di dalam pemodelan layer pada jaringan komputer.
12. Menolong di dalam penyediaan layanan secara tepat pada jaringan kompter tanpa perlu pengecekan di dalamnya. Misalkan layanan *streaming audio* dan *video* memanfaatkan (*User Datagram Protocol*).
13. Menolong di dalamnya penyedian layanan berbasis *web* dan elektronik,
14. Layanan keamanan dan adanya enkripsi dan kriptografi, misalkan pada transaksi elektronik, menggunakan protokol SSL (*Secure Socket Layer*)

2.4 TEORI KHUSUS

2.4.1 *INTRUSION PREVENTION SYSTEM (IPS)*

adalah perangkat lunak atau perangkat keras yang berjalan demi memantau trafik menemukan kegiatan yang tidak wajar dan menjalankan pencegahan lebih awal penyusupan atau masalah yang membuat jaringan menjadi tidak bekerja

biasanya.Suatu pendekatan yang selalu di pergunakan agar merancang sistem keamanan komputer, mengombinasikan teknik *firewall* dan metode *intrusion detection system* (IDS) dengan cukup bagus. Teknologi ini bias dipakai dalam membatalkan serangan yang dating ke jaringan lokal dan melihat dan menulis seluruh,paket data serta mengenali paket dengan sensor saat seragan dikenali. Jadi Intrusion Prevention System bertindak seperti layaknya *firewall* yang akan mengizinkan atau menolak paket data. (Raven Alder, 2007) *Intrusion Prevention system (IPS)* yaitu suatu pendekatan yang selalau dipakai dalam merancang sebuah system keamanan komputer mengabungkan metode *firewall* dan metode *Intrusion detection sytem (IDS)* dengan sangat bagus Teknologi ini di peroleh di gunakan dalam memblok serangan yang datang dari jaringan local dan mengenali dan menuliskan semua paket data dan mndeteksi paket dengan sensor,ketika serangan telah di kenal,dan memblok jalur dan menadai semua paket data yang sudah di kenal tersebut.jadi *Intrusion Prevention System (IPS*) bekerja sebagai layaknya *Firewall* yang melakuakan *allow* dan *block* yang di kombinasikan seperti *Intrusion detection sytem (IDS)* yang dapat mendeteksi paket secara lengkap *Prevention System (IPS*)menggunakan *signatures* untuk mengenali *traffic* di jaringan dan terminal paket yang masuk dan keluar dapat di deteksi secepat mungkin sebelum merusak dan mendaptkan jalan kedalam jarigan computer.

2.4.2 INTRUSION DETECTION SYTEM (IDS)

Intrusion Detection sytem (IDS) yaitu salah satu system software perangakat lunak atau perangkat keras yang dapat mengenal aktifitas yang tidak wajar di sebuah system jaringan.IDS di pergunakan untuk mengenali suatu tindakan mencurigakan di sebuah system jaringan.IDS memiliki beberapa pengertian di anataranya adalah :

1. Sistem untuk mengenali suatau intrusion di lakuakan oleh *intruder* (pemakai ataupun penyeludup)bagian jaingan.di awal serangan *intruder* biasayan hanya mencari data.namun pada tingakat yang lebih serius *intruder* berusaha mendapatakan jalan ke system contoh melihat data rahasia diubah tanpa meberi tahu,mengurangi jalan kesistem sampai memmatikan system.
2. Sistem keamana yang berjalan dengan *firewall* mengawasi *intrusion intrusion* dapat di defenisikan sebagai kegiatan yang terjadi di sebuah jaringan ataupun di *host* tersebut. *Intrusion* tersebut akan di ubah menjadi rules ke dalam IDS (*Intrusion Detection Sytem).*
3. Suatu *sofware* perangakat lunak ataupuan perangakat keras yang dapat mengenali semua aktivitas atau kegiatan yang asing (mencurigakan)

1. *NETWORK BASED INTRUSION DETECTION SYTEM(NIDS)*

yaitu ketika seluruh interaksi yang berjalan kesemua system jaringan akan di analis untuk mennemukan apakah pencoban seranagan atau penyusutan ada masuk ke system jaringan.*NIDS* umumnya terdapat di bagian sekmen jaringan yang paling penting di mana keberadan *server* atau berada ketika awal masuk system jaraingan.ini juga mempuyai kelemahan di mana *NIDS* agak rumit untuk di inplementasikan di dalam system sebuah jaringan,yang mengunakan *switch* Ethernet,walaupun beberapa *vendor switch* Ethernet telah menerapakan fungsi IDS di dalam *switch* buatanya untuk memeonitor *port* atau koneksi

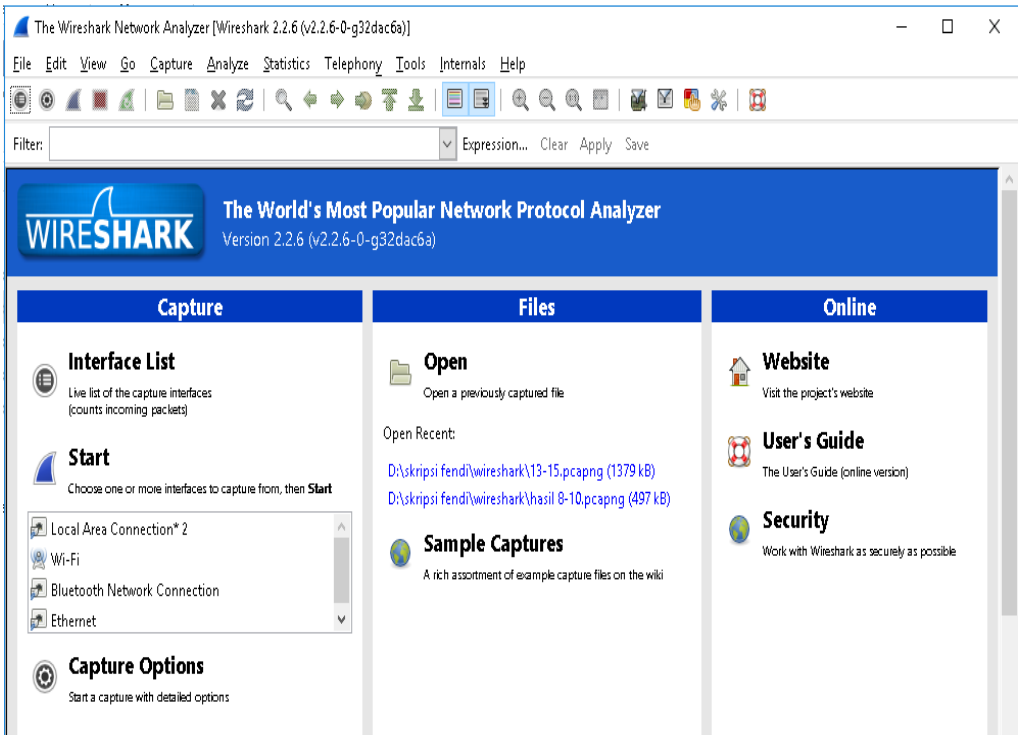
2. *HOST BASED INTRUSION DETECTION SYTEM (HIDS)*

Host based intrusion detection sytem adalah ketika aktivasi sebuah *host* jaringan individual akan di pantau apakah terjadi sebuah pencoban serangan atau penyusupan dalam jaringan system *HIDS* sering di letakan pada server – server kritis di jaringan system,seperti hanya seperti *Firewall*,*web server* atau sever yang terkoneksi ke internet.

2.3 TOOLS

2.3.1 Wireshark

Wireshark adalah salah suatu aplikasi untuk umum untuk mendapatkan komunikasi data dalam jaringan dengan mengontrol mengunakan protokol dan *port-port* yang digunakan. Wireshark iyalah salah merupakan sekian banyak *tool network analyzer* yang banyak dipakai oleh network administrator untuk menganalisa jalanya jaringannya. Wireshark banyak disukai karena interfacenya yang menggunakan graphical user interface (GUI) atau tampilan grarfis (Agus Kurniawan, 2012).

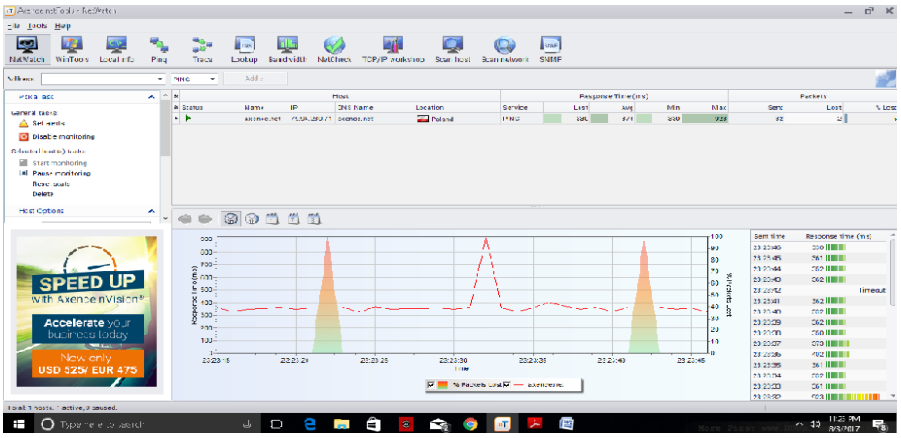


Gambar 2.6 Tampilan Wireshark

Sumber: Penelitian (2019)

Menurut jurnal *wireshark* merupakan *software* untuk melakukan aktivitas jaringan komputer yang mengunakan fungsi yang bermafaat untuk profesional jaringan,administrator,peneliti, hingga memperluas piranti lunak jaringan. Tools dapat berjalan secara real time dalam mendapatkan data/informasi yang berjalan dalam jaringan.keseluruhan paket informasi dalam berbagai format protokol pun akan dengan gampang didapat dan dianalisa (Diansyah, Informatika, Tinggi, & Harapan, 2015).

2.3.2 NetTools



.

Gambar 2.7 *Tampilan* NetTools

Sumber: Penelitian (2019)

Menurut klopototolia (2012 : 01) *NetTools* adalah Merupakan salah satu *network monitoring tools* yang mengukur performa jaringan, pemindaian jaringan, keamanan, alat *administrasi* dan dapat mendiagnosa persoalan jaringan, *NetTools* terdiri atas beberapa *tool* popular seperti *trace*, *lookup*, *port scanner*, *network scanner*, dan *SNMP browser*. Yang membuat *NetTools* menjadi unik adalah

NetTools mempunyai *user interface* yang memudahkan untuk penggunanyaBaris *navigasi* digunakan untuk memilih *tool* yang ingin digunakan sedangkan *address bar* digunakan untuk memasukkan nama *DNS* (atau *IP*) *host* yang akan di periksa atau di-*scan*. *Slidebar* biasanya terdiri atas informasi umum (seperti jumlah paket yang dikirinkan) dan *option.* Main *area* berisi tampilan hasil *monitoring* tergantung pada *tool* yang dipilih. *Tool* yang tersedia pada *NetTools* meliputi *NetWatch,WinTools, Localinfo, Ping, Trace, Lookup, Bandwidth, NetCheck, TCP/IP workshop, Scan host, Scan network, dan SNMP*. *NetWatch* adalah Untuk memonitor *host* dapat digunakan *toolNetWatch. NetWatch* akan memeriksa *host* dengan menggunakan *ICMP (ping)* dan menyimpan waktu respon serta persen paket yang hilang untuk analisis selanjutnya. *NetWatch* tidak hanya memonitor *host* tetapi juga dapat memberi peringatan tentang permasalahan yang terjadi melalui pesan tertentu.Untuk memonitor *host* dapat dimulai dengan :

2 Memilih *tool NetWatch* pada baris navigasi.

3 Kemudian memasukkan *DNS host* atau *IP address* pada *address bar*.

4 Lalu klik tombol Add atau tekan *Enter.*

2.3.3 FIREWALL

Firewall adalah berupa alat yang sifatya melindungi,jika seseorang akan berhubungan dengan jaringan computer dan ingin mendapatkan akses yang aman.*firewall* merupakan salah satu pelindung yang sangat di butuhkan.pada umumnya ada tiga hal yang pelu di lindungi,di antaranya adalah:

1. Data (informasi)

Data adalah hal yang berhaga yang sangat perlu untuk di lindungi,pertukaran data di dalam dunia maya (internet) merupakan hal yang di mamfatakan orang oleh orang yang tidak bertanggung jawab,misalya jika suatau perusahan mengirimkan data yang mempuyai rahasia dalam pengirimanya di sadap atau di hancurkan oleh orang yang tidak bertangung jawab maka rahasia dari perusahan tersebut akan menjadi milik umum.

2.4 Penelitian Terdahulu

Untuk melengkapi penelitian ini ada beberap penelitian terdahulu sebagai berikut:

1. Sistem keamanan jaringan suatu hal yang perlu untuk menjaga sebuah jaringan, penyerang yang bisa mengaggu dan juga merusak sistem koneksi antar kemanan jaringan. *Intrusion Prevention System* (*IPS*) ataupun menagkap serangan dan melakukan drop pada serangan. Melakukan penerapan pada sistem operasi Linux memakai Snort untuk mode inline dan juga mencegah dari serangan yang dapat mengancam.Kata Kunci: *Keamanan Jaringan, Intrusion Prevention System, Denial Of Service, Linux, Snort* **.**

2. Perkembangan teknologi yang sangat pesat menuntut meningkatnya kualitas keamanan jaringan. *hacking* dan *cracking* yang didukung oleh *tools* yang bisa didapatkan dengan mudah dan gratis. Selain itu ancaman keamanan jaringan

komputer juga datang dari virus, *malicious*, trojan, *worm*, *DOS*, *spoofing*, *sniffing*, *spamming*, dan lainnya. Hal – hal inilah yang akan mengancam keamanan sebuah sistem jaringan dimana data dapat dengan mudah diambil bahkan dirusak oleh *intruder* atau *attacker* (Pradipta, Yoga Widya, 2017).

3. Sejalan Perkembangan Teknologi Informasi menjadikan keamanan suatu informasi sangatlah penting terlebih lagi pada suatu jaringan yang terkoneksi dengan internet.. Karena itu telah berkembang teknologi *IDS* dan *IPS* sebagai pembantu pengaman data pada suatu jarigan komputer. Dengan iyalah *Intrusion Detection System* (IDS) dan *Instrusion Prevention System* (IPS), maka serangan-serangan tersebut lebih dapat dihalagi ataupun dihilangkan. IDS bermafat untuk mengkap adanya serangan dari penyusup (serangan dari dalam), sedangkan IPS bermafat dalam menagkap serangan dan menindak lanjutinya dengan pemblokan (filter) serangan (Alamsyah, 2011). Kata Kunci : *Instrusion Detection System (IDS), Instrusion Prevention System (IPS), Firewal*

4. Teknologi *firewall* sebagai tembok penghalang dalam kejahatan Internet dirasa tidak selalu efektif terhadap percobaan intrusi. Karena biasanya firewall dirancang. perangkat keras jaringan (*ethernet card*, *token ring*, *bridge*, *modem*, dan lainnya). sekali ditemukan oleh *user* seperti *virus, Malicious, Trojan, Worm, DoS, Hacker, Spoofing, Sniffing, Spamming, Crackers* dan lain sebagainya, yang membuat *performance* (kinerja) *Availability* (ketersediaan) suatu *internetwork*. serta mencegah segala yang dapat membahayakan jaringan tersebut, hal ini

bertujuan untuk mengatasi segala ancaman seperti *hacker, cracker* dan user yang tidak dikenal (Mohamad Nurul Huda Monoarfa, Xaverius B.N. Najoan, ST., MT., Alicia A.E. Sinsuw, ST., 2016).

5. Keamanan jaringan komputer merupakan bagian dari sebuah sistem yang sangat penting untuk menjaga *validitas* dan *integritas* data serta menjamin ketersediaan layanan bagi penggunanya. Sistem deteksi penyusup jaringan yang ada saat ini umumnya mampu mendeteksi berbagai serangan tetapi tidak mampu mengambil tindakan lebih lanjut. Namun disatu sisi manusia sudah sangat tergantung dengan sistem informasi. Hal itu yang menyebabkan statistik insiden keamanan jaringan terus meningkat tajam dari tahun ke tahun. Ini disebabkan karena kepedulian masyarakat yang sangat kurang terhadap sistem keamanan jaringan. Maka dari itu dibutuhkan sebuah sistem yang dapat membantu network administrator untuk digunakan sebagai monitor trafik jaringan dengan *Intrusion Prevention System* (IPS)kombinasi antara fasilitas *blocking capabilities* dari *Firewall. Kata kunci: firewall, Intrusion Prevention System, router mikrotik.* Pada sisi lain timbul masalah serius yaitu faktor keamanannya, namun disatu sisi manusia sudah sangat tergantung dengan sistem informasi. Hal itu yang menyebabkan statistik insiden keamanan jaringan terus meningkat tajam dari tahun ke tahun.Dalam perkembangan teknologi sekarang yang sudah semakin pesat, kebutuhan akan keamanan jaringan tentunya meningkat seiring dengan berkembangnya ilmu pengetahuan tentang masalah *hacking* dan *cracking* yang bersifat *free* dan ada pula yang dikomersilkan. Kemudian dari sisi *software*

pendukung pun sudah banyak *tool-tool* yang bersifat *free* yang kemampuannya sudah bisa dikatakan mumpuni untuk digunakan sebagai alat penyerangan oleh kalangan *intruder* dan *attacker* (Arta, Syukur, & Kharisma, 2018).

6. Keamanan menjadi salah satu teknologi yang perlu diperhatikan ketika suatu sistem yang terkoneksi dengan system jaringan komputer menjadi hal yang sangat krusial. Pada saat ini kebutuhan manusia sangat tergantung dengan adanya informasi ataupun data, khususnya informasi atau data digital. Semakin besar kebutuhan adanya informasi semakin meningkat pula insiden atau gangguan keamanan terhadap system jaringan yang meningkat tajam. Hal ini umumnya terjadi dikarenakan masih kurangnya kepedulian terhadap keamanan sebuah sistem khususnya pada infrastruktur *hardware* jaringan komputer yang masih sangat kurang. Dikutip dari sebuah sumber yang membahas tentang serangan *cyber* pada sebuah system keamanan bahwa terjadi peningkatan selama tahun 2015 dan tahun 2016 dengan jumlah serangan sebanyak 5,197 dan 6,068. Data ini mengemukakan bahwa jumlah kenaikan yang dramatis terhadap teknologi *cloud cyber security* yang berbasis *cloud* telah membantu beberapa perusahaan melihat pola serangan yang rumit untuk terdeteksi secara manual. Dengan total kenaikan jumlah serangan yang mengakibatkan beberapa *attacker* berpotensial melakukan serangan terhadap sebuah teknologi yang berbasikan *cloud*, ini mengindikasikan bahwa kejadian serangan *cyber* terhadap system keamanan cenderung meningkat pada rentang tahun 2015 dan 2016[1]. Perkembangan dari teknologi komunikasi yang mengarah ke IoT (*internet of things*) juga tidak luput juga dari ancaman para *attacker* yang

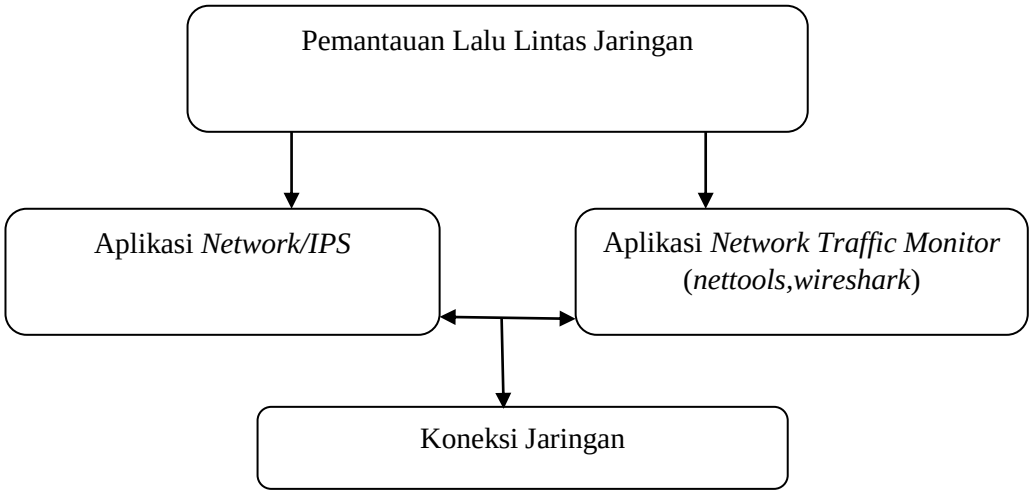
bisa juga mencegat pesan yang lewat dari sumber ke tujuan sehingga privasi dari sebuah messange bisa bocor dan isi pesan juga rentan dimodifikasi, sehingga pengiriman pesan yang aman diperlukan.Salah satu teknologi yang memanfaatkan jaringan adalah *cloud computing*. *Cloud computing* merupakan teknologi komputasi modern yang mulai berkembang penggunaanya pada tahun 2005 yang menggunakan layanan jaringan komputer atau jaringan internet. Di dalam teknologi *cloud computing* menyediakan

3 layanan yaitu, *Software as a Service* (SaaS), *Platform as a Service* (PaaS) dan *Infrastructure as a Service* (IaaS). IaaS merupakan salah satu layanan *cloud computing* yang menyediakan perangkat keras berupa pemroses, penyimpan, jaringan dan beberapa *resource* yang lain mengenai komputasi dasar. Perusahaan seperti Oracle dan Amazon yang memulainya teknologi *cloud computing modern*, dimana oracle mengembangkan perangkat lunak CRM yang berbasikan SaaS, sedangkan amazon menghasilkan EC2 (*elastic computer cloud*). Meskipun teknologi *cloud computing* modern menyajikan layanan yang sangat menarik dan juga manfaat yang dapat memberikan penggunanya dapat menghemat biaya, akan tetapi juga memberikan risiko dan peluang baru untuk eksploitasi bidang keamanan system di dalamnya. Pembahasan pada jurnal ini membahas teknik monitoring dan pencegahan keamanan *cloud computing*. Salah satu faktor keamanan adalah melindungi infrastruktur di dalam *cloud computing* dari serangan jaringan. Selain itu, sistem *firewall* juga merupakan salah satu perangkat lunak yang mampu mencegah beberapa serangan dari luar, namun *firewall* tidak dapat memberikan peringatan terhadap serangan yang cukup kompleks seperti, D-Dos dan serangan

pada port-port tertentu. Lebih spesifik lagi, system yang dirancang ini menggunakan *Intrusion Prevention System* (IPS) berbasis jaringan atau disebut NIPS (*network intrusion prevention system*) untuk layanan *Infrastrukture as a Service* (IaaS) yang diimplementasikan pada aplikasi *open cloud computing*. Tujuanya digunakan untuk memantau dan memproteksi serangan penyusup dari luar yang hendak masuk ke system, dan selanjutnya memberikan laporan ke administrator jaringan jika terdapat serangan yang terjadi di dalam lingkungan *cloud*(Khadafi, Meilani, & Arifin, 2017).

2.5 Kerangka Pemikiran

Untuk memudahkan pemahaman keseluruhan rangkaian ini, maka disusunlah kerangka pemike penelitian sebagai berikut



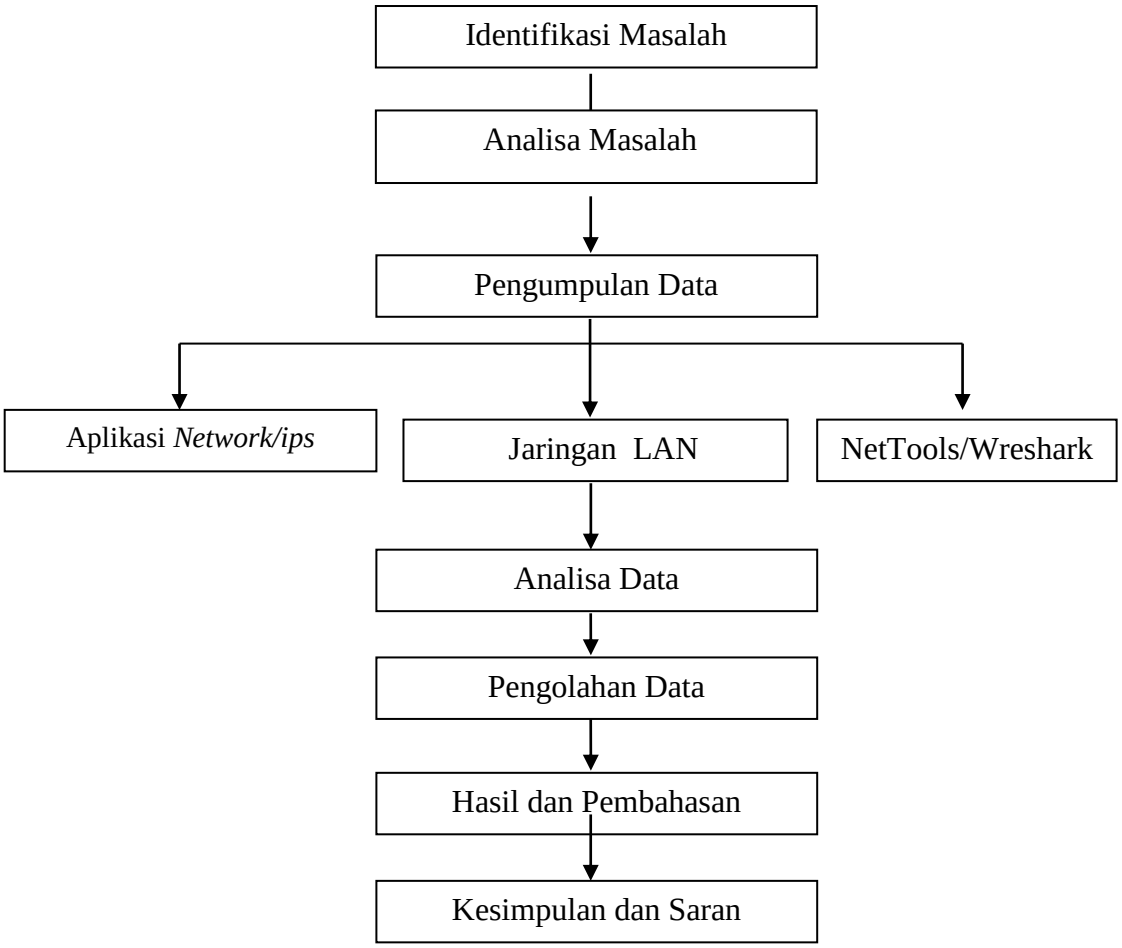
Gambar 2.8 Kerangka Pemikiran

Sumber: Penelitian (2019)

BAB III
METODE PENELITIAN

3.1 Desain Penelitian

Pada desain penelitian, seorang peneliti akan membuat langkah atau struktur dalam menjelaskan sebuah proses penelitian dengan menggunakan berbagai bentuk bagan, menurut (martono, 2010: 131).



Gambar 3.1 Desain Penelitian

Sumber:Penelitian (2019)

1. Identifikasi masalah

Peneliti akan menerangkan masalah dan variable yang diteliti, dengan mengabil data dan cara mengumpulkan yang didapatkan dari tempat penelitian.

2. Analisis masalah

Merupakan pengambilan gambaran konseptual untuk masalah penelitian serta keterkaitan dengan penelitian sebelumnya.

3. Pengumpulan data

Mencari data langsung dari tempat yang ada di kantaor yang berhubungan dengan judul penelitian.sumber yang terkait dengan penelitian yang dilakukan berdasarkan buku dan jurnal ilmiah,di pahami agar mendukung proses penelitaan.

4. Analisa data

Penulis melakukan analisa data yang diperoleh dari tempat intansi/lembaga yang akan dilakukan perhitungan yang sesuai dengan metode penerapan ***Intrusion Prevention System*** untuk keaman jaringan.

5. Pengolahan data

Tahap ini keseluruhan analis data penulis kumpulkan,penulis akanmelakukan analiss untuk memperoleh data diproses menggunakan aplikasi *Intrusion Prevention System* dan *wirshark*

6. Implementasi

Adalah.Pada tahap implementsi setelah semua dilakukan maka sistem yang dibuat akan di implementasikan yang akan membantu mengurangi terjadinya serangan pada jaringan di dinas kependudukan dan pencatatan sipil.kota batam.

7. Hasil

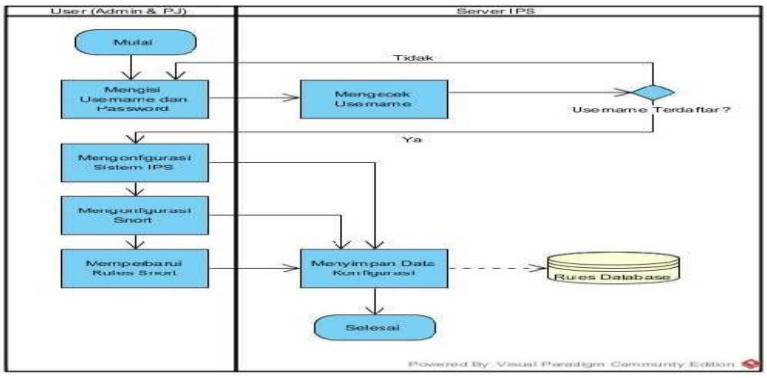
Setelah dilakukan semua proses maka didapatkan hasil atau output dari hasil penelitian ini adalah menunjukkan bahwa dengan memanagemen *bandwidth* pada suatu jaringan dapat meminimalisir adanya serangan.

Ada tiga desain yang peneliti buat yaitu *flow chart diagram, network design*,

3.1.1. Flow Chart

Desain aliran diagram menggunakan *flow chart* yang menggambarkan interaksi dari sistem dan pengguna yang

digambarkan sebagai berikut



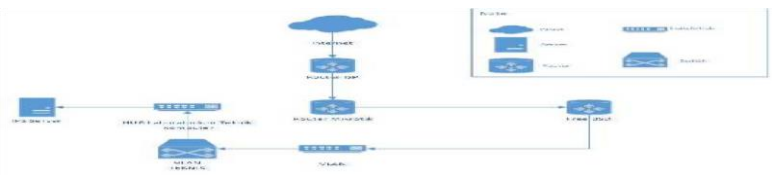
Gambar 3.2 Desain Penelitian

Sumber: Penelitian (2019)

User melakukan *login* ke IPS *server* dan jika terdaftar maka akan diberikan izin untuk masuk ke dalam sistem dan melakukan kofigurasi. Jika salah mengisikan data *login* maka sistem akan meminta untuk memasukkan ulang data. Setelah berhasil melakukan *login* ke dalam sistem maka user dalam melakukan konfigurasi pada sistem IPS dengan melakukan instalasi perangkat lunak yang dibutuhkan dalam melakukan penelitian ini dan semua konfigurasi akan disimpan oleh sistem. Dilanjutkan dengan melakukan konfigurasi pada SNORT dengan mengaktifkan fitur yang diperlukan seperti *data acquisition, rules, configuration file and folder* dan sistem akan menyimpan konfigurasi tersebut dan untuk *rules* akan dituliskan dalam *rules databases*. Aplikasi pengolah *database* yang digunakan adalah MySQL. Ini dapat digunakan ketika SNORT menulis *log* dan menghasilkan sebuah *alert file* yang akan diproses oleh *barnyard2* untuk ditulis ke dalam *database* sehingga dapat ditampilkan pada BASE. *User* yang telah memiliki izin ke sistem juga dapat memperbarui *rules* SNORT jika dibutuhkan.

1. Network Design

Setelah melakukan pembahasan,dilakukan penyesuaian desain penempatan IPS *server* dengan konfigurasi sbb:



Gambar 3.3 Network Design

Sumber: Penelitian (2019)

3.1.2 Cara Kerja *Intrusion Prevention System*

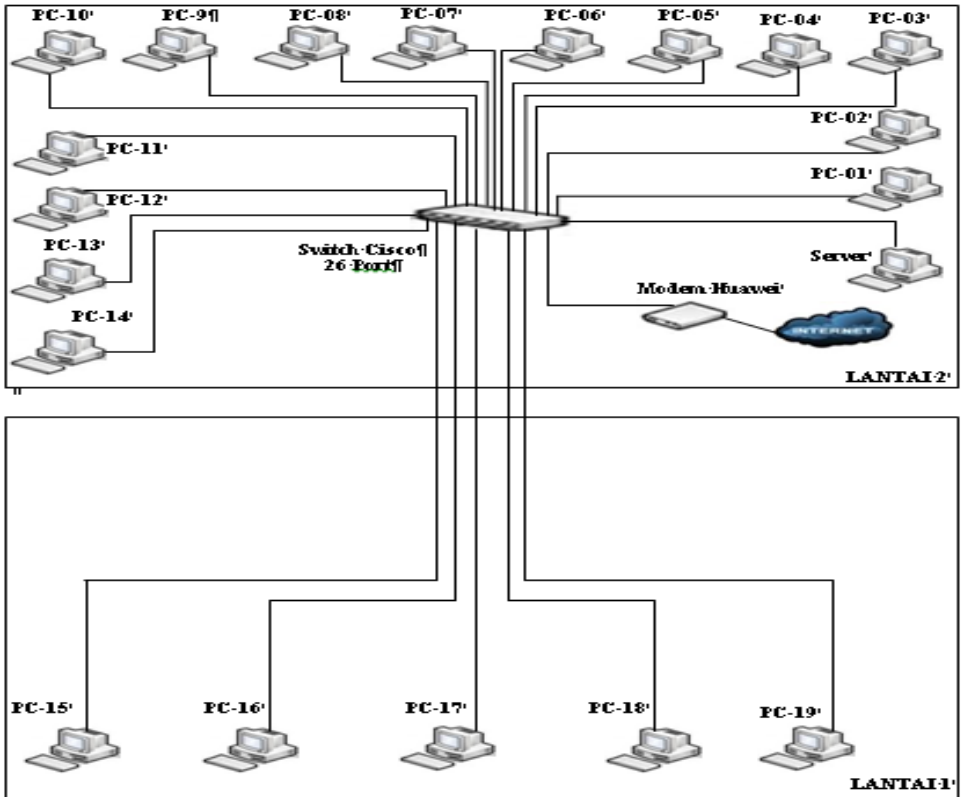
Gambar 3.4 Cara Kerja *Intrusion Prevention System*.

Sumber: Penelitian (2019)

Penyerang melakukan penyerangan dengan beberapa metode seperti, *signatured based attack* (bersifat seperti virus), *anomaly based attack* (contohnya percobaan login berkali-kali), dan pengubahan *database* dalam sistem secara ilegal. *Kerja Intrusion Prevention System* Imendeteksi lalu lintas jaringan yang melewatinya dan melakukan pemeriksaan kesesuaian dengan *database* yang berada dalam sistem. Ketika paket terindikasi sebagai sebuah serangan,*Firewall* melakukan *blocking* terhadap paket tersebut agar ia tidak diteruskan masuk ke dalam *server*.

3.2 Analisis Jaringan Yang Lama/Yang Sedang Berjalan

Demikian gambar dari topologi jaringan kantor dinas kependudukan dan pencatatan sipil kota Batam yang sedang berjalan saat ini dapat dilihat pada gambar dibawah ini.



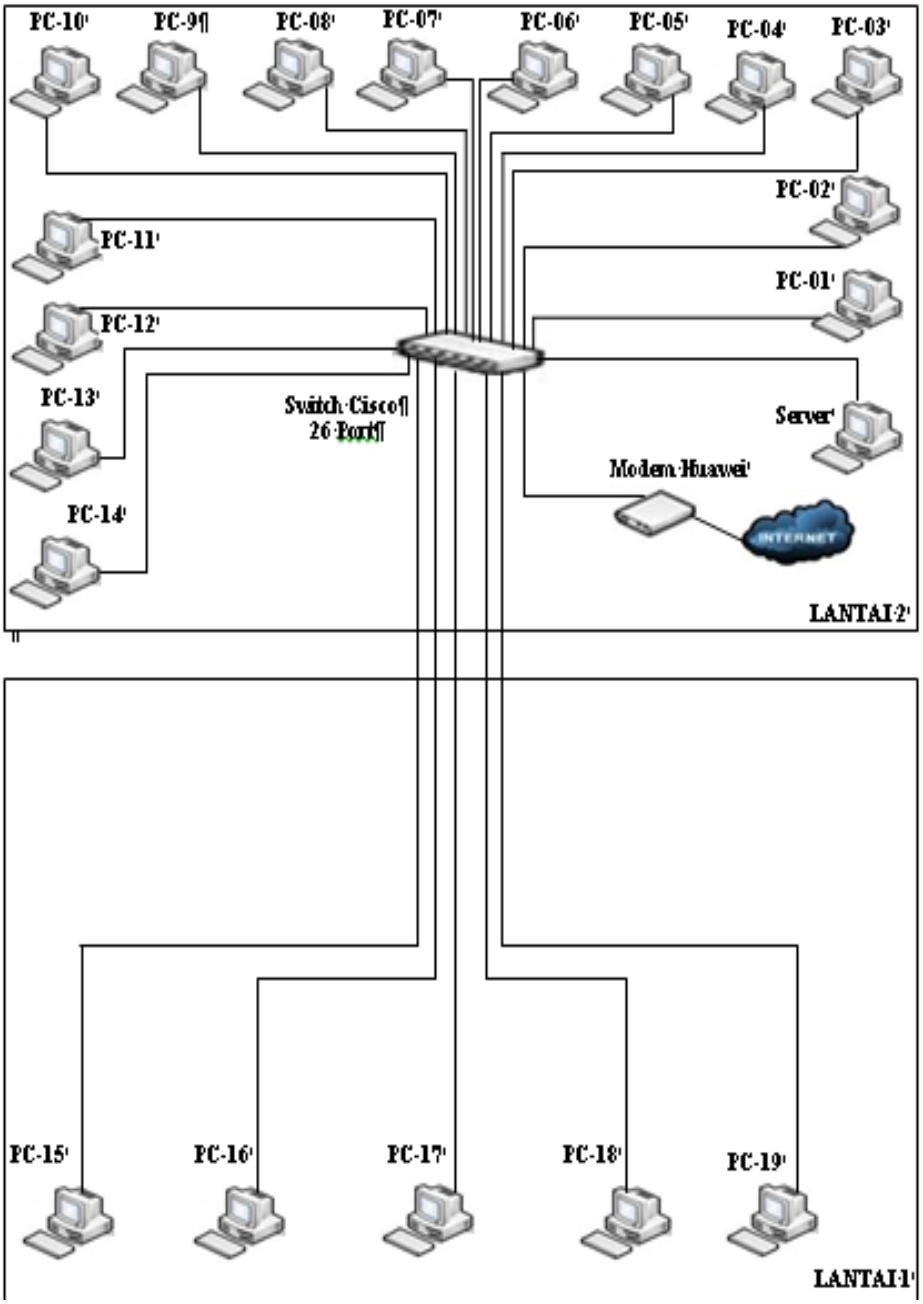
Gambar 3.5 Topologi Jaringan Yang Sedang Berjalan

Sumber: Penelitian (2019)

3.2. Rancangan Jaringan Yang Di Bagun/Di Usulkan

3.2.1. Topologi Jaringan Yang Baru

Perancangan jaringan komputer Kantor Dinas Kependudukan Dan Pencatatan Sipil Kota Batam yang baru yaitu dengan melakukan manajemen *bandwidth* dengan metode ***Intrusion Prevention System*** Demikian gambar perancangan topologi jaringan yang baru setelah dilakukan penambahan perangkat jaringan. Perancangan topologi jaringan dapat dilihat pada gambar dibawah ini:



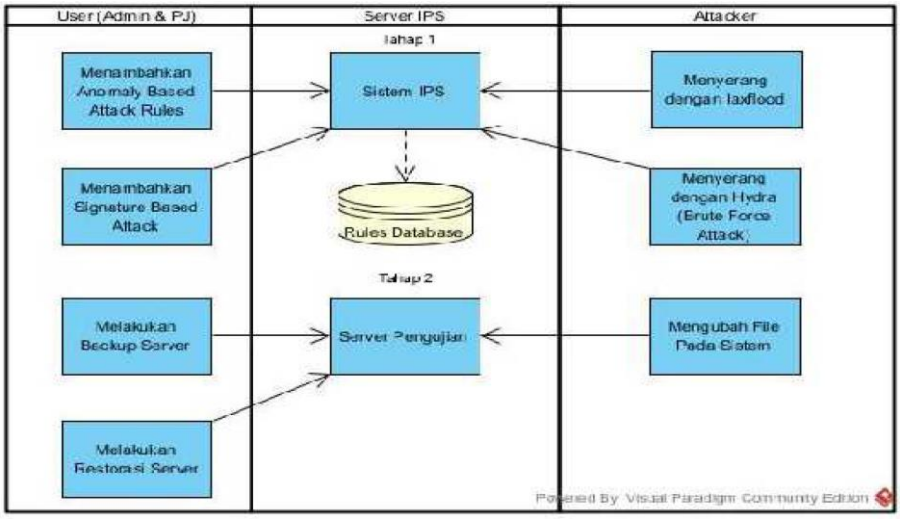
Gambar 3.6 Perancangan Topologi Jaringan

Sumber: Penelitian (2019)

1. Topologi Jaringan

Tahapan kerja yang dimaksud yaitu menghubungkan perangkat Inisialisasi Perangkat dan Implementasi Sistem Konfigurasi Router Berhenti Mulai Menentukan Topologi Jaringan Identifikasi Pengujian Sistem Konfigurasi Jaringan Management *Bandwidth*.Topologi jaringan adalah gambaran sturktur jaringan komputer yang dibuat (Utomo, 2012: Hal 4). berdasarkan identifikasi terhadap data – data yang diperoleh secara langsung dibawah ini adalah arsitek topologi jaringan yang digunakan pada Dinas Kependudukan Dan Pencatatan Sipil Kota Batam. Laptop dengan OS Kali Linux melakukan serangan dengan dua buah *penetration tools* yaitu Hydra dan Iaxflood melakukan serangan ke *server.* SNORT akan bereaksi dengan paket data yang dikirim oleh peretas dengan melakukan identifikasi kesesuaian dengan daftar *rules* yang ada pada *file* local.rules (*rules* yang digunakan mengacu pada community.rules yang didapat dari fitur ekstensi SNORT yaitu Pulled Pork).Setelah itu diteruskan ke *firewall* untuk melakukan tindakan apakah di hentikan atau di lewatkan. GID yang dibuat pada *rules* mengaktifkan *message generator* dan menghasilkan *file* Alert dan *log* berupa snort.u2.xxxx. Alert dapat digunakan oleh Splunk untuk dapat memberikan tampilan alternatif untuk analisis *data*, dan juga digunakan oleh Swatch yang terpicu ketika ada kata kunci yang telah dikonfigurasi untuk selanjutnya dikirim ke *e-mail*.*File* snort.u2.xxxx digunakan oleh Barnyard2 untuk selanjutnya di-*input* ke dalam snort *databases*. BASE menggunakan *tables* yang ada pada snort *databases* untuk selanjutnya ditampilkan sebagai laporan detail kejadian yang dapat digunakan untuk melakukan analisis.

1. SkenarioPengujian



Gambar 3.7 Skenario Pengujia

Sumber: Penelitian (2019)

1. Pengujian.1.(*Attacker* belum berhasil masuk ke dalam *system*)

1. *Attacker* melakukan metode penyerangan dengan *burstattack/ping flood* pada salah satu *server* yag tersimpan di *server*
2. *Sysadmin* melakukan pengamanan dengan menambahkan *rule anomaly based attack* pada *database* SNORT dari sistem IPS
3. *Attacker* mencoba *penetration test* dengan salah satu perangkat lunak yang ada pada Kali Linux yaitu *brute force login* dengan aplikasi hydra untuk mendapatkan akses ke dalam sistem.
4. *Sysadmin* melakukan pengamanan dengan menambahkan *rule signature based attack* pada *database* SNORT dari sistem IPS.

2. Pengujian.2. (*Attacker* telah berhasil masuk ke dalam *system*)

1. *Sysadmin* melakukan *server backup* dengan memindahkan *alert file*maupun SNORT *folder* yang dilindungi.
2. *Attacker* diposisikan telah berhasil masuk ke dalam sistem dan menghapus *alert file* pada *server* untuk menghilangkan catatan *log*.
3. Sistem IPS memberikan peringatan kepada *sysadmin* dan setelah itu melakukan tindakan yang dibutuhkan yaitu restorasi *server* dan *rules update* sesuai dengan *threat* yang berhasil lolos.

3.2.2 Inisialisasi Peralatan Dan Implementasi Sistem

Sebelum membuat kofigurasi.biasnya setiap jaringan,membutuhkan perlengkapan yang menujang.dalam penyelesaian kofigurasi.adapun alat yang di perlukan.yakni *hadware,*yang bermafata untuk mengelola data dan juga,melakukan konfigurasi peralatan yang di pergunakan,dan juga *software* tersebut diperlukan untuk menanalisis,data jaringan yang sudah terkoneksi dengan baik.

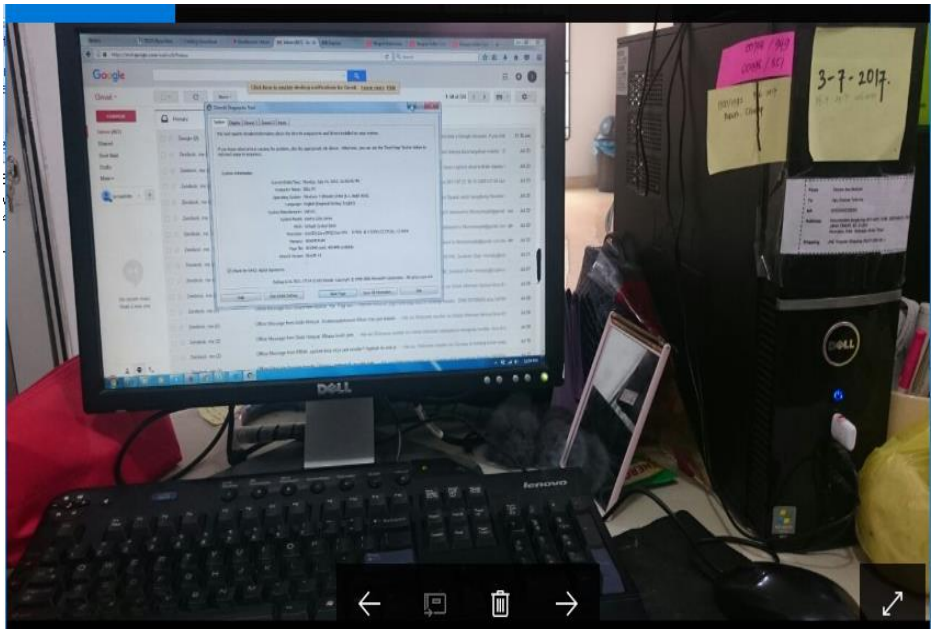
3.2.3 Peralatan yang di pergunakan untuk *Server*

Computer name	: Hybrid Master
Operating system	: Prosesor intel xeon
System manufacturer	: Hewlett Packard
System model	: s5780d
Bios	: 11/05/10 15:07:18 Ver: 6.14
Processor	: Prosesor intel xeon

2.2.4 Perangkat yang digunakan untuk Client

1. ***Client* 1**

Computer name	: DellPC
Operating system	: Windows 7 Home Premium 32-bit (16.1 Build 7600)
System manufacturer	: System Manufacturer
System model	: System Product Name
Bios	: 11/26/17 17:11:35 Ver: 08.00.10
Processor	: Intel ® Pentium ® Dual Core E2180 @2.00 Ghz(2CPUs)
Memory	: 2560 MB RAM

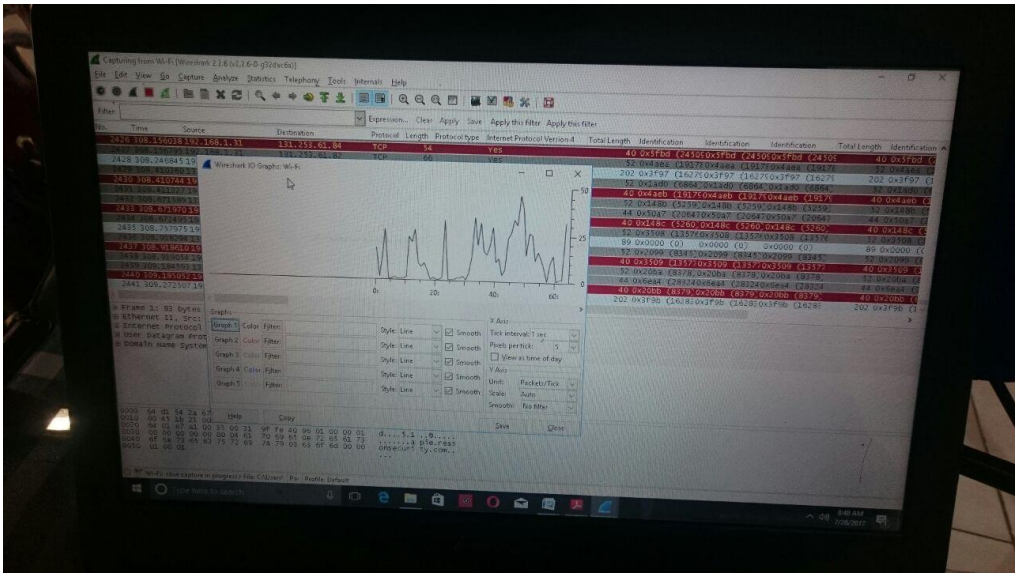


Gambar 3.8 Client 1

Sumber: Penelitian (2019)

***2. Client* 2**

Computer name	: Acer Pc
Operating system	: Windows 7 utimate 64-bit (6.1,Build 7601)
System manufacturer	: Acer
System model	: Aspire X1700
Bios	: Default System Bios
Processor	: Intel ® Core™ 2Duo CPU E6750@2.66GHz(2 CPUs), ~2,7HGz
Memory	: 3072 MB RAM

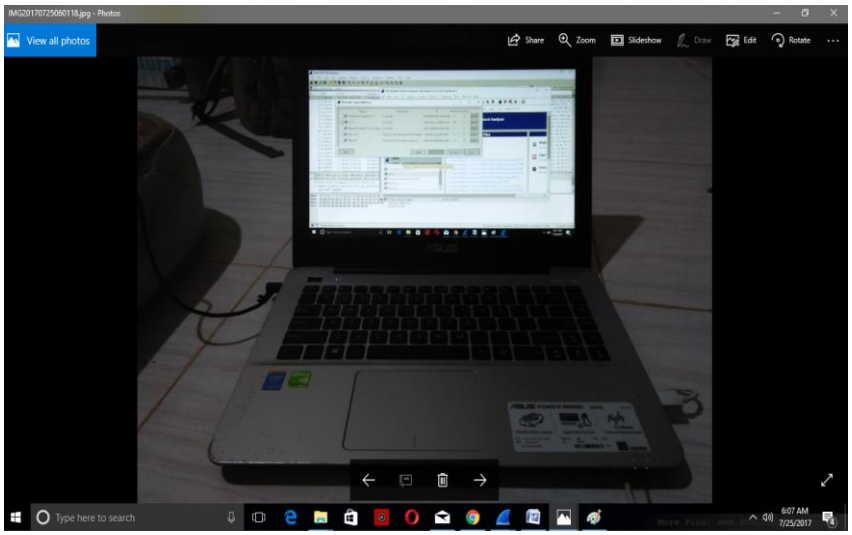


Gambar 3.9 Client 2

Sumber: Penelitian (2019)

3.2.5 Perangkat Yang Digunakan Untuk Analisis Data

Computer name	: Asus
Operating system	: Windows 10 Home Singkle Language 64 bit(10.0, bulif 14393)
System manufacturer	: ASUSTek Computer Inc.
System model	: X455LJ
Bios	: X455LJ.205
Processor	: Intel ® Core ™ I3–5010U CPU @2.10GHz (4CPUs), ~ 2.1GHz
Memory	: 4096 MB RAM



Gambar 3.10 Perangkat Analisa Data

Sumber: Penelitian (2019)

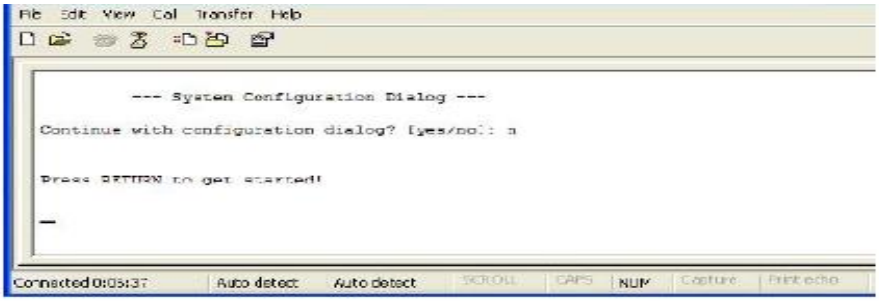
3.2.6 Infrastruktur *Hardware*

Perangkat yang digunakan pada jaringan Kantor Dinas Kependudukan Dan Pencatatan Sipil yaitu :

- ✓ *Switch / Hub*
- ✓ *Router*
- ✓ NIC (*Network interface card*)
- ✓ Kabel UTP
- ✓ *Access point*

3.2.7 Konfigurasi *Router*

Di buat mengunakan Accr Pc dan aplikasi yang di pakai dalam menjalankan konfigurasi untuk router yang *hayper, Hyper terminal* yang ada tersedia dalam sisterm *windows-10*. Untuk menggunakan *hyper* terminal terlebih dahulu klik *start* kemudian *all programs* lalu pilih *accessories*, masuk ke *communications* dan *hyperterminal*. Kemudian menuliskan nama dan menentukan *serial port* yang dihubungkan dengan kabel *console*.



Gambar 3.11 Konfigurasi Router

Sumber: Penelitian (2019)

3.2.8 Menentukan *Hostname*

Dalam mengkonfigurasi *router* hal pertama yang dilakukan yaitu memberi Nama pada *router*. Pemberian Nama pada *router* dilakukan agar setiap komputer dapat berkomunikasi antara satu dengan lainnya. *Router* diberi Nama Ro_1. Perintah *command line interface* (CLI) yang digunakan untuk memberi nama pada Ro_1 adalah sebegai berikut

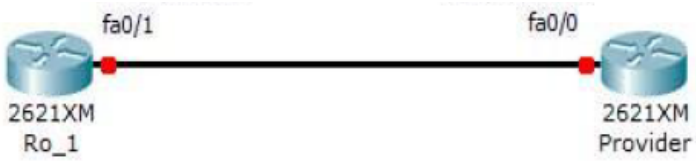
```
Router>enable
Router#conf t
Router(config)#hostname Ro_1
Ro_1 (config)#
```

Gambar 3.12 Menentukan Hostname

Sumber: Penelitian (2019)

3.4.1 *Setting IP Address Router*

Melakukan konfigurasi *router* IP *address* dengan IP *address interface* *fastethernet*0/1 Ro_1 adalah 192.168.119.2 dan *fastethernet*0/0 Ro_1 adalah 192.168.10.1. Kedua *router* akan disabungkan dengan masing-masing IP *address*



interfae adalah 192.168.119.1 dan 192.168.119.2 dengan *netmask* standar.

Gambar 3.13 Konfigurasi IP Address

Sumber: Penelitian (2019)

Perintah CLI yang digunakan untuk melakukan konfigurasi IP *address* adalah sebagai berikut:

```
Ro_1(config)#int fa0/0
Ro_1(config-if)#IP address 192.168.10.1 255.255.255.0
Ro_1(config-if)#no shut
Ro_1(config-if)#int fa0/1
Ro_1(config-if)#IP address 192.168.111.2 255.255.255.0
Ro_1(config-if)#no shut
Ro_1(config-if)#exit
```

Gambar 3.14 Setting IP Address

Sumber: Penelitian (2019)

3.4.2 Menentukan IP *Route*

Routing protocol Akan menentukan jalur yang dijalani oleh data melalui sebuah *internetwork*. Jalur pertama yang harus dilalui data untuk dapat masuk ke *network* yang lain. Pada Ro_1 jika ingin mencapai *clip ip route* pada *router* sebagai Berikut :

```
Ro_1(config)#IP route 0.0.0.0 0.0.0.0 192.168.111.1
```

Gambar 3.15 Menentukan IP Route

Sumber: Penelitian (2019)

3.4.3 *Dynamic Host Configuration Protocol* (DHCP)

DHPC digunakan untuk memberikan nomor IP kepada komputer yang memintanya. Komputer yang memberikan nomor IP disebut sebagai DHCP *server*,Sedangkan komputer yang meminta nomor IP disebut sebagai DHCP *client*. Dengan demikian administrator tidak perlu lagi harus memberikan nomor IP secara manual DHCP saat konfigurasi TCP/IP, tapi cukup dengan memberikan referensi kepada DHCP *server*.

Pada saat kedua DHCP *client* Dihidupkan , maka komputer tersebut melakukan request ke DHCP-*Server* untuk mendapatkan nomor IP. DHCP menjawab dengan memberikan nomor IP yang ada di database DHCP. DHCP-*Server* setelah memberikan nomor IP, maka *server* meminjamkan (lease) nomor IP yang ada ke DHCP-Client dan mencoret nomor IP tersebut dari daftar *pool*. Nomor IP diberikan bersama dengan *subnet mask* dan *default gateway*. Jika tidak ada lagi nomor IP yang dapat diberikan, maka *client* tidak dapat menginisialisasi TCP/IP, dengan sendirinya tidak dapat tersambung pada jaringan tersebut.

```
Ro_1(config)#IP dhcp pool LAN_KELAS
Ro_1(dhcp-config)#network 192.168.10.0 255.255.255.0
Ro_1(dhcp-config)#default-router 192.168.10.1
Ro_1(dhcp-config)#dns-server 192.168.20.3
Ro_1(dhcp-config)#exit
Ro_1(dhcp-config)#IP dhcp excluded-address 192.168.10.1
```

Gambar 3.16 Dynamic Host Configuration Protocol (DHCP)

Sumber: Penelitian (2019)

3.4.4 Mengaplikasikan ACL

ACL berfungsi untuk mengatur grafik dan menjamin akses dari suatu jaringan. Perintah ACL yang digunakan untuk mengizinkan grafik yang berasal dari IP *address* 192.168.10.1 yaitu:

```
Ro_1(config)#access-list 1 permit 192.168.10.1
```

Gambar 3.17 Mengaplikasikan ACL

Sumber: Penelitian (2019)

3.4.5 Konfigurasi *Network Address Translation*

Network Address Translation (NAT) iyalah cara untuk menghubungkan jaringan private ke internet menggunakan satu IP *public*.

1. *FastEthernet0* (fa0/0) dengan IP. 192.168.10.1. *Interface* ini terhubung ke jaringan yang akan di NAT.
2. *FastEthernet1* (fa0/1) dengan IP. 192.168.119.2. *Interface* ini terhubung ke *internet*.

```
Ro_1(config)#ip nat inside source list 1 interface fa0/1
overload
Ro_1(config)#int fa0/1
Ro_1(config-if)#ip nat outside
Ro_1(config-if)#int fa0/0
Ro_1(config-if)#ip nat inside
Ro_1(config-if)#exit
```

Gambar 3.18 Konfigurasi Network Address Translation

Sumber: Penelitian (2019)

3.5Managemen *Bandwidth*

Management *bandwidth* yaitu suatu cara yang digunakan untuk memanagemen dan memaksimalkan suatu jaringan. Managemen *bandwidth* bertujuan untuk mengatur *bandwidth* jaringan dan memberikan limit sesuai dengan kebutuhan. Adapun langkah yang di lakukan untuk memanagemen *bandwidth* pada *router* yaitu :

3.5.1 Menentukan *Class-Map*

Class-map digunakan untuk mengklasifikasikan atau membagi lalu-lintas data (*traffic*) menjadi beberapa bagian. Pengaturan ini berfungsi agar jaringan memiliki kemampuan menyediakan jaminan. Untuk membuat c*lass-map* printah yang digunakan yaitu :

```
Ro_1>enable
Ro_1#conf t
Ro_1(config)#class-map LAN_KELAS
Ro_1(config-cmap)#match protocol LAN_KELAS
```

Gambar 3. 19 Menentukan Class-Map

Sumber: Penelitian (2019)

Match protokol digunakan untuk penghubung antar protokol sehingga dapat diberikan prioritas.

3.5.2 Menentukan Aturan *Traffic*

Perintah *traffic* dipakai untuk mengetahui besar *bandwidth* yang akan diberikan pada kelompok yang telah dibuat pada *class-map*. Adapun perintah yang digunakan yaitu :

```
Ro_1(config-cmap)#bandwidth percent 50
Ro_1(config-cmap)#exit
```

Gambar 3.20 Menentukan Aturan Traffic

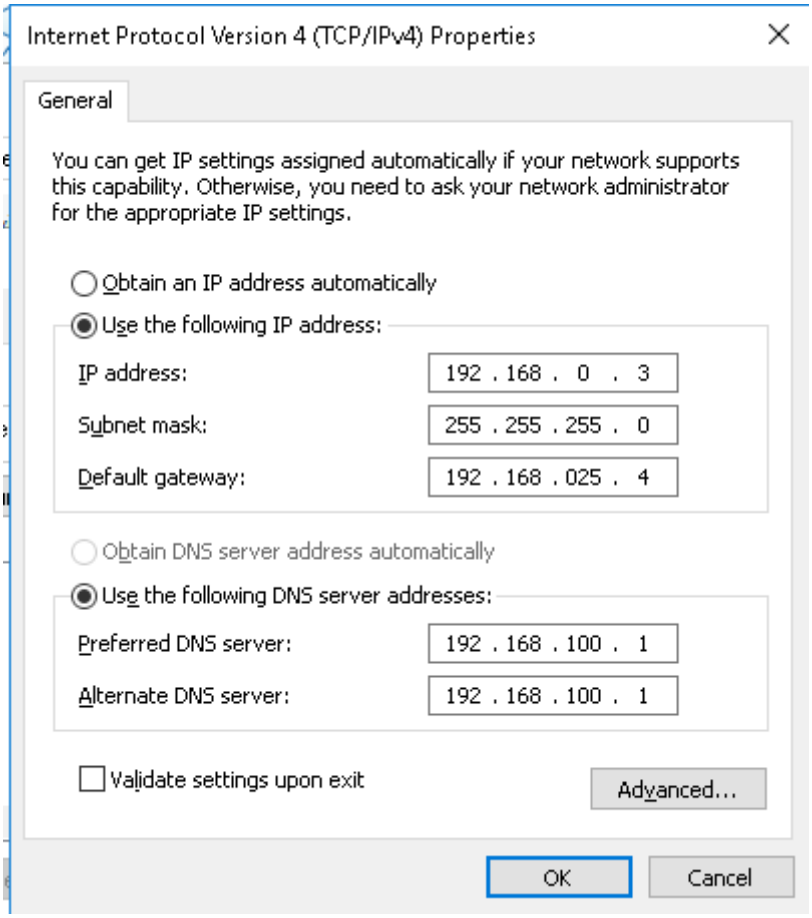
Sumber: Penelitian (2019)

3.5.3 Konfigurasi Jaringan

Sebelum *wireshark* di pakai sebagai aplikasi untuk menganalisa data maka terlebih dulu melakukan *setting* IP *address* pada Acer PC, agar wireshark dapat membaca paket data yang melalui jaringan.

3.5.4 *Setting IP address PC*

Pada gambar dibawah ini menerangkan cara dalam pengaturan IP *address* dengan cara masuk ke *network conection* sesudah itu tekan *wired conection* pada tab wired, tekan *edit* dan masuk ke tab IP*v4 Settings*, pada *Method* ganti *Automatic* (DHCP) dengan manual, dan masukkan IP *Address* sesuai dengan IP *address* yang telah di konfigurasi pada *router* sebelumnya.



Gambar 3.21 Setting IP Address

Sumber: Penelitian (2019)

Dibawah ini menjelaskan cara menambahkan IP *Address* manual, klik *add* kemudian mengisi *address, Netmask, Gateway dan DNS servers.*Pada penelitian ini penulis menggunakan IP *address* kelas C, yaitu IP *address* 192.168.0.3 maka *netmask* nya otomatis 255.255.255.0, *Gateway* dan *DNS server* di *setting* berdasarkan konfigurasi *router*. Setelah melakukan settingan IP *address* pada PC maka *wireshark* sudah bisa di gunakan untuk menganalisa paket data yang melalui jaringan.

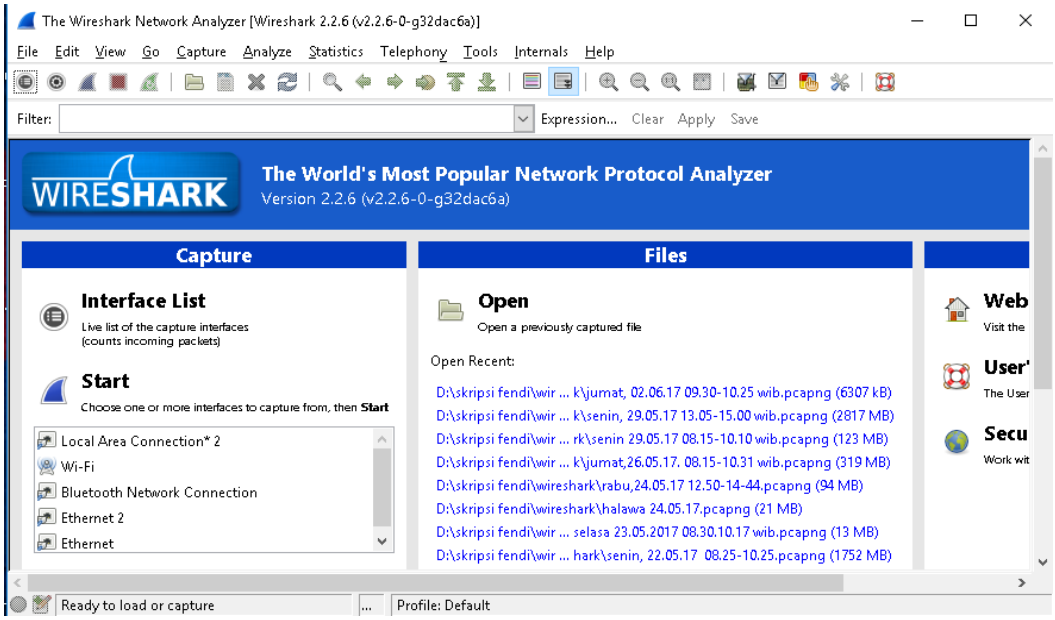
3.6.2 Infrastruktur *Software*

Adapun Infrastruktur alat yang dipakai pada proses pengukuran jaringan agar mendapatkan kinerja jaringan seperti pada parameter *QoS (Quality of Service)* yaitu *bandwidth, delay,* dan *packet loss* menggunakan *software wireshark 2.2.6* dan *software Axence net tools v 5.0.*

3.6.2.1 Melakukan instalasi *Wireshark*

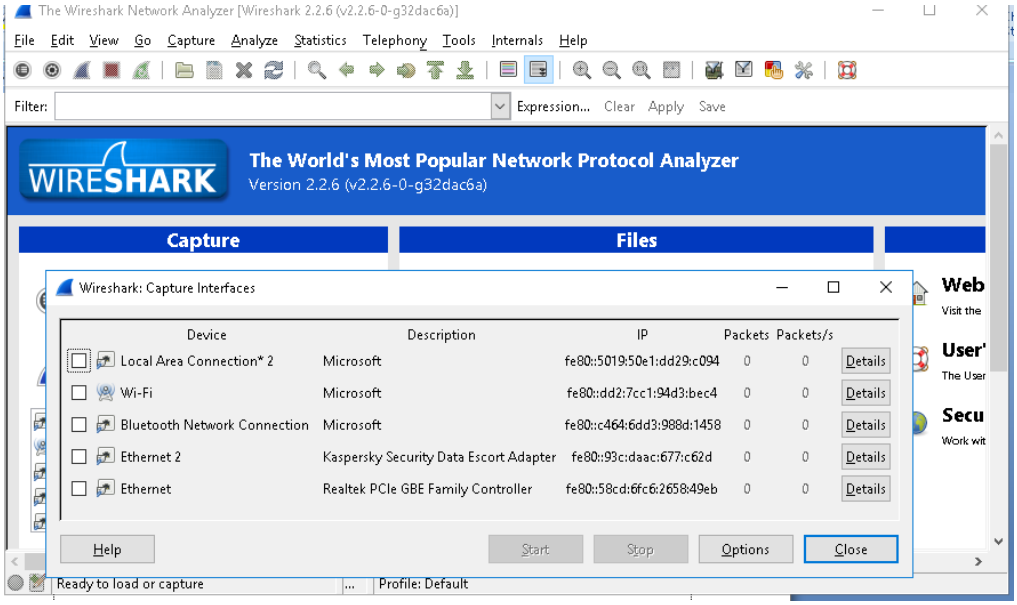
Dalam melihat data yang berisi informasi mengenai apa saja yang sudah berjalan pada suatu jaringan, termasuk mengidentifikasi data yang hilang maka kita akan melakukan analisis paket data dengan munggunakan aplikasi *wireshark* yang telah di *install*.

Berikut tampilan ini iyalah ketika memilih menu *capture*,sesudah itu tekan *interface*. Pada bagian kotak dialog terlihat daftar antarmuka jaringan yang ada. dalam antarmuka ini penguna bisa melakukan konfigurasi dengan mennekan tombol *options* dalam kota dialog *wireshark capture interfaces*.



Gambar 3.22 *Melakuakan instalasi Wireshark*

Sumber: Penelitian (2019)



Gambar 3.23 Memilih Jaringan

Sumber: Penelitian (2019)

3.6.2.2 Uji Coba Jaringan

Ada beberapa poin yang dilakukan dalam pengujian jaringan yaitu sebagai berikut :

1. Melakukan konfigurasi *router*

   Router yang dikonfigurasi diberi akses oleh *router* admin berhasil dijalankan dengan benar.

2. *Packet interface goppher* (PING)

   Ping dilakukan ke *router* admin berjalan dengan lancar tanpa adanya masalah.

3.6.2.3 Identifikasi Pengujian Pada *Wireshark*

Berikut adalah poin yang dilakukan dalam melakukan pengujian pada *wirshark* :

1. *Wireshark capture interfaces*

   Wireshark capture interfaces pada sistem operasi pada *windows* tidak bisa langsung mendeteksi *interface* yang ada pada PC, perlu penambahan beberapa baris perintah agar *interface* dapat terdeteksi oleh *wirehark.*

2. Melakukan pengujian

   Dalam pengujian ini, aplikasi *wireshark* berjalan dengan baik dan dapat menampilkan hasil penangkapan *file*. Setelah melakukan pengujian sistem sesuai dengan spesifikasi alat yang digunakan, maka keluaran yang dihasilkanpun telah sesuai dengan rancangan. Untuk analisa dari hasil yang diperoleh dapat dilihat pada bab IV.

3.2.9 PENERAPAN *INTRUSION PREVENTION SYTEM* UNTUK KEAMANA JARINGAN.

Langkah-langkah yang diambil dalam penerapan interusion prevention sytem ini dilakukan dengan cara mengikuti yang sebagaimana telah dipakai oleh peneliti dan tahapan sebagai berikut:

1. Tahapan Pertama (*Action Planning*)

Pada tahap kedua ini peneliti akan memulai melakukan rencana pengukuran dimana penulis akan menyusun rencana tindakan seperti akan memulai mengukur/mendeteksi serangan. Pengukuran ini akan dilakukan selama 1 (satu) bulan (senin – jumat) dimana waktu tersebut akan dimulai pada jam sibuk antara pukul 08.30 WIB sampai pukul 11.30 WIB dan pada jam sibuk antara pukul 13.00 WIB sampai dengan pukul 15.30 WIB .

Tabel.3 1 Jadwal Pengukuran

Hari/Tanggal	Waktu (WIB)
Senin	08.30 - 11.30 13.00 - 15.30
Selasa	08.30 - 11.30 13.00 - 15.30
Rabu	08.30 - 11.30 13.00 - 15.30
Kamis	08.30 - 11.30 13.00 - 15.30
Jumat	08.30 - 11.30 13.00 - 15.30
Sabtu	08.30 - 11.30 13.00 - 15.30

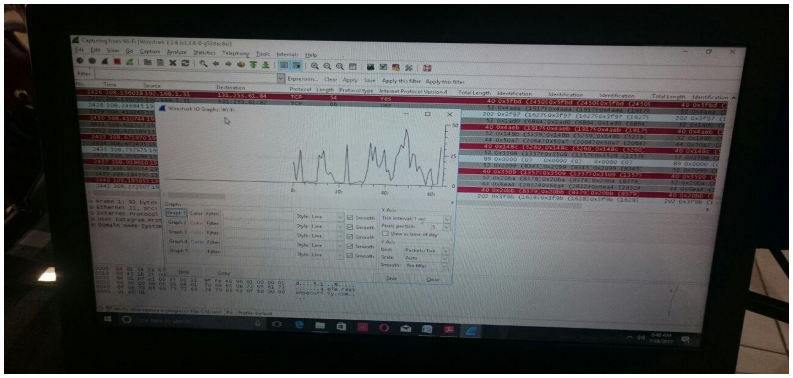
Sumber: Penelitian (2019)

Tabel di atas jelaskan jadwal pengukuran dalam satu pengukurannya dilakukan pada jam padat atau jam sibuk sebanyak 2 kali, dengan 08.00 – 11.30 dan 13.00 – 15.00

Adapun *software* yang digunakan dalam pengukuran ini adalah *Axence NetTools* dan IO *Graph (wireshark)* yaitu:

Gambar 3.24 Axence Nettools

Sumber: Penelitian (2019)



Gambar 3.25 IO Graph

Sumber: Penelitian (2019)

2. Tahap Kedua *(action taking)*

Tahap kedua ini peneliti akan melakukan tindakan dengan melakukan penerapan *Interusion Prevention Sytem* terhadap jaringan *LAN di* Dinas Kependududkan Dan Pencatatan Sipil Kota Batam. Pengujian ini akan dilakukan pada lantai 1 pada 2.model sistem pengotrolan yang di pakai untuk *Penerapan Interusion Prevention Sytem* pada jaringan *LAN* adalah *monitoring application*.

3. *Monitoring Application*

Monitoring Application bekerja untuk antar muka pemakai aplikasi jaringan. Komponen ini berguna medapatkan informasi berjalanya data yaitu memantau, menganalisa, dan hasil mengontrol kepada penguna. Berdasarkan analisis tersebut, seorang pengguna jaringan dapat melakukan operasi yang lain.

4. *intrusion prevention sytem Monitoring*

Mekanisme *IPS Monitoring* untuk pengukur parameter *IPS* pada skema jaringan LAN menggunakan *Axence NetTools* sesuai dengan skema jaringan LAN pada Dinas kependudukan dan pencatatan sipil. kegiatan pengukuran parameter *IPS* adalah dengan menggunakan *Axecen NetTools* yaitu dengan cara mendeteksi seranagan pada alamat IP untuk setiap perangkat dan menunggu respon dari *node* serangan- serangan (*source)* kepada *node* di serang (*destination)* di *layer-layer* IP pada skema jaringan yang akan terdeteksi.

3.8 Lokasi dan Jadwal Penelitian

3.4 Lokasi Penelitian

Dalam melakukan penelitian ini penulis mengambil lokasi di Dinas kependudukan dan pencatanatan sipil.seikupang Batam.Penulis melakukan penelitian berdasarkan data-data yang diperoleh dari analisa jaringan yang ada atau digunakan pada DINAS KEPENDUDUKAN DAN PENCATANATAN SIPIL.SEIKUPANG BATAM.

Gambar 3.26 Lokasi penelitian

Sumber: Penelitian (2019)

3.4.1. Jadwal Penelitian

Jadwal penelitian untuk mendapatkan data dan informasi dilaksanakan bulan April; 2019 sampai bulan Agustus 2019. Berikut jadwal penelitian dibawah ini.

Tabel 3.2 Jadwal Peneliti

Kegiatan	**Jawal Kegiatan**																			
	April				**Mei**				**Juni**				**Juli**				**Agustus**			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
PemilihanTopik																				
PengajuanJudul																				
Mengerjakan BAB I																				
Mengerjakan BAB II																				
Mengerjakan BAB III																				
MengerjakanBAB IV																				
Mengerjakan BAB V																				

Sumber: Penelitian (2019)