IMPLEMENTASI INTRUSION DETECTION SYSTEM SNORT MENGGUNAKAN LINUX UBUNTU 16.04 PADA JARINGAN PT SUMBER INOVASI SEJATI

SKRIPSI

Oleh:
Ricky Gunawan
150210040

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

IMPLEMENTASI INTRUSION DETECTION SYSTEM SNORT MENGGUNAKAN LINUX UBUNTU 16.04 PADA JARINGAN PT SUMBER INOVASI SEJATI

SKRIPSI
Untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana

Oleh:
Ricky Gunawan
150210040

PROGRAM STUDI TEKNIK INFORMATIKA
FALKUTAS 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, dan/atau magister), 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 telah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi.

Batam, 7 Agustus 2019

Yang membuat pernyataan,

Ricky Gunawan
150210040

IMPLEMENTASI INTRUSION DETECTION SYSTEM SNORT MENGGUNAKAN LINUX UBUNTU 16.04 PADA JARINGAN PT SUMBER INOVASI SEJATI

Oleh:
Ricky Gunawan
150210040

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Telah disetujui oleh Pembimbing pada tanggal
seperti tertera di bawah ini

Batam, 9 September 2019

Andi Maslan, S.T., M.SI.
Pembimbing

ABSTRAK

Pada Pt. Sumber Inovasi Sejati perusahaan yang bergerak dibidang distributor Valve, memiliki puluhan komputer yang terhubung dalam sebuah jaringan. Pada perusahaan ini hanya memiliki satu jaringan dengan router, switch dan sebuah komputer server yang saling terhubung, tetapi saya akan mengimplementasikan dengan menggunakan 2 komputer, seorang administrator memiliki tanggung jawab terhadap keamanan sistem dari waktu ke waktu, memastikan sistem dan jaringan dapat terjaga dengan baik, sehingga di butuhkan sistem dalam menangani penyalahgunaan jaringan atau ancaman yang akan terjadi. Salah sistem yang dapat mendeteksi jaringan secara real-time terhadap serangan atau gangguan jaringan adalah *Intrusion Detection System* yang disebut juga dengan IDS, salah satunya mengunakan *snort.* Keunggulan dari implementasi snort adalah dapat digunakan pada banyak sistem operasi, Selain itu snort juga menghemat biaya karena bersifat gratis dan mudah dikonfigurasi. Snort dapat memberikan *Alert* jika adanya penyerangan keamanan terhadap sistem jaringan dan hasil peringatan ini dapat digunakan sebagai acuan untuk menentukan kebijakan keamanan jaringan. Dari hasil pengujian yang didapat snort mampu mendeteksi adanya serangan *Nmap, Dos*. Semua aktifitas akan di rekam dengan menggunakan *Barnyard2,* dan dapat men salin semua aktifitas yang terdeteksi oleh *snort dan* menyimpan *Alert* dalam bentuk *Log* kedalam *file log* Dengan tingkat keberhasilan sebesar 98.55% dari 70 serangan yang dilakukan, 69 serangan dapat terdeteksi oleh snort.

Kata kunci: *Intrusion Detection System*, *Snort*, *Alert*,*Barnyard2*

ABSTRACT

At Pt. Sumber Inovasi Sejati, a company engaged in Valve distributor, has dozens of computers connected in a network. In this company only has one network with routers, switches and a server computer that are interconnected, but I will implement it using 2 computers, an administrator has responsibility for the security of the system from time to time, ensuring the system and network can be maintained properly, so that the system is needed to deal with network abuse or threats that will occur. One system that can detect network in real-time against network attacks or interference is the Intrusion Detection System , also called IDS, one of which uses snort. The advantage of snort implementation is that it can be used on many operating systems, besides that it also saves costs because it is free and easy to configure. Snort can provide alerts if there is a security attack on the network system and the results of this warning can be used as a reference to determine network security policies. From the test results obtained snort is able to detectattacks Nmap, Dos. All activities will be recorded using Barnyard2, and can copy all activities detected by snort and save Alerts in the form of Logs into log files With a success rate of 98.55% of 70 attacks, 69 attacks can be detected by snort.

Keywords : Intrusion Detection System, *Snort*, *Alert*,*Barnyard2*

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan YME yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan skripsi yang merupakan salah satu persyaratan untuk gelar sarjana.

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 Ibu Dr. Nur Elfi Husda, S.Kom,. M.SI.
2. Ketua Program Studi Teknik Informatika Bapak Andi Maslan, ST., M.SI.
3. Bapak Andi Maslan,S.T.,M.SI. selaku pembimbing Skripsi pada Program Studi Teknik Informatika Universitas Putera Batam.
4. Algifanri Maulana, S.SI., M.MSI.. selaku pembimbing akademik selama program studi Teknik Informatika Universitas Putera Batam.
5. Dosen dan Staff Universitas Putera Batam.
6. Kedua orang tua penulis yang selalu mendoakan dan menyemangati penulis hingga penulisan skripsi ini selesai.
7. Keluarga penulis yang selalu mendoakan dan memberikan motivasi kepada penulis agar penelitian ini selesai tepat waktu.
8. Teman-teman seperjuangan yang bersedia membagi ilmunya dan *sharing* pendapat dalam rangka pembuatan skripsi ini.

9. Semua pihak yang telah bersedia meluangkan waktu, tenaga dan pikirannya dalam memberikan data/informasi selama penulis membuat skripsi yang tidak dapat penulis sebutkan satu-persatu.

Batam, 7 Agustus 2019

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Pada era perkembangan teknologi berita yg semakin luas, dengan adanya jaringan internet yang bisa memudahkan setiap orang dapat berkomunikasi dimanapun tanpa batasan waktu dan jarak, maka dari itu siaapun dapat mengakses atau mendapatkan informasi yang di perlukan. Dalam jaringan komputer yang akan berkaitan dengan keamanan, keamanan jaringan adalah hal yang sangat penting untuk diperhatikan, karena akan berdampak pada hal yang dapat menggangu keamanan dan kestabilan koneksi pada jaringan komputer. Maka menggunakan cara sistem wajib pada lindungi dari segala macam serangan atau perjuangan penyusupan berasal pihak yang tidak bertanggung jawab. Macam-macam serangan pada jaringan saat ini seperti serangan Malware, Ddos, Sniffing, spoofing, backdor, trojan, ransomware dan lainya.

Sesuai jenis serangan diatas maka survei pada dunia Corporate IT security risk 2015 yg dilakukan sang B2B internasional dengan kaspersky bahwa satu agresi Ddos dapat menyebabkan kerugian keuangan mulai sebesar US$53-417ribu. Serangan Ddos atau Distributed-Denial-of-service merupakan serangan terhadap personal komputer atau server didalam jaringan internet sehingga dapat menyebabkan komputer atau server tidak bisa bekerja dengan baik. Data dari asal Akamay Report menyatakan bahwa sebanyak 79% asal total serangan Ddos di

triwulan IV 2017 lebih ke software permainan sedangkan perangkat lunak seperti telekomunikasi serta jasa finansial jua mendapatkan peningkatan 2 kali lipat dari sebelumnya 6% dan 4%. Akibatnya perseolan keamanan merupakan salah satu bagian terpenting dalam sebuah sistem infomas, keamanan sistem menjadi hal yang harus di perhatikan. Maka diperlu kan sebuah sistem agar dapat dapat mendeteksi jaringan secara real-time terhadap serangan atau gangguan jaringan agar dapat bertindak lanjut sebelum serangan masuk sepenuhnya salah satu yang sistem yang digunakan adalah *Intrusion Detection System* yang disebut juga dengan IDS.

Intrusion Detection System yang disebut dengan IDS adalah cara mengenali adanya penyusupan atau aktivitas mencurigakan dengan melakukan pengamatan trafik secara *real-time* yang memasuki sistem tanpa izin misalkan *cracker* atau gangguan pada sistem yang terjadi karena faktor ketidak sengajaan yang dilakukan seseorang pengelola, dan dapat juga disebabkan oleh pihak ketiga yang mencoba menganggu pengguna jaringan tersebut dengan tujuan melakukan perusakan, penyusupan atau penyalahgunaan data maupun sistem. Secara khusus IDS berfungsi sebagai pemantauan dalam sebuah jaringan. Tanggung jawab IDS adalah untuk mendeteksi sistem yang anggap mencurigakan atau tidak dapat diterima dan aktivitas jaringan dan untuk mengingatkan administrator untuk kegiatan ini. Terdapat dua teknik yang digunakan dalam IDS yaitu NIDS (*Network Intrusion Detection System*) dan HIDS (*Host Intrusion Detection System*). Perangkat IDS yang sering digunakan adalah *snort, snort* adalah sebuah *software* yang bisa digunakan buat memantau serta pencegahan terhadap gangguan pada jaringan personal komputer dan dikembangkan oleh Martin Roesch, dan bersifat *open*

source. Keunggulan dari implementasi *snort* adalah dapat digunakan pada banyak sistem operasi, Selain itu snort juga menghemat biaya pengadaan software karena bersifat gratis dan mudah dikonfigurasi dibandingkan software IDS lain. Dalam *snort* pengaturan paling utama adalah pada jaringan dan *rules snort*. Sebuah serangan dapat di deteksi apa tidak tergantung dari rule yang dibuat dalam *snort. Snort* akan memberikan peringatan jika terdapat terjadinya penyerangan keamanan terhadap sistem jaringan. Dengan adanya peringatan ini bisa dilakuka sebagai tindakan buat menentukan kebijakan dalam keamanan jaringan (Ery Setiyawan Jullev Atmaji, 2016).

Pada PT. Sumber Inovasi Sejati perusahaan yang bergerak dibidang distributor *Valve*, memiliki puluhan komputer yang terhubung dalam sebuah jaringan. Pada perusahaan ini hanya memiliki satu jaringan dengan router, switch dan sebuah komputer server yang saling terhubung. Terdapat keluhan dari administrator yang bekerja di perusahaan tersebut, terjadinya gangguan terhadap jaringan komputer yang menyebabkan jaringan down, akibatnya para user tidak dapat bisa akses sistem dengan baik dan mengalami kesulitan dalam bekerja, ketika di analisa oleh administrator jaringan mengetahui adanya serangan Dos pada jaringan administrator memerlukan waktu cukup lama untuk memulihkan kembali server. Pada perusahaan ini tidak terdapat satu pun sistem keamanan jaringan atau pendeteksi lalu lintas data dan paket-paket jaringan yang masuk pada jaringan terutama untuk *hacker* atau pihak yang tidak bertanggung jawab yang dapat menganalisa atau berusaha melakukan perubahan melalui aplikasi tertentu. Maka diperlukan sebuah sistem mendeteksi serangan pada jaringan, sehingga ketika ada

gangguan yang masuk pada jaringan, maka administrator dapat langsung mengatasi gangguan tersebut, agar dapat menjaga data-data penting serta menjamin pelayanan bagi penggunanya. Dengan membangun Intrution Detection System (IDS) dapat bekerja membaca paket-paket data yang masuk maupun keluar secara otomatis dengan hasil sebuah laporan atau *log* kepada administrator jaringan. Dengan adanya IDS pada jaringan dapat meminimalkan kemungkinan adanya gangguan yang disebabkan oleh pihak ketiga yang sengaja merusak atau menggangu pada sistem, karena setiap jaringan yang terdeteksi oleh IDS akan memberi peringatan atau alert kepada administrator. (Putranto Pancaro & Isnanto Saputra, 2018).

Implementasi ini dibuat nantinya akan sangat berguna untuk mendeteksi lalulintas atau paket mencurigakan yang masuk ke jaringan, sehingga dapat membantu administrator dalam memonitor kondisi jaringan pada perusahaan tersebut.

Berdasarkan uraian diatas, maka penulis melakukan penelitian **"IMPLEMENTASI INTRUSION DETECTION SYSTEM SNORT MENGGUNAKAN LINUX UBUNTU 16.04 PADA JARINGAN PT SUMBER INOVASI SEJATI"**.

1.2 Identifikasi Masalah

Berlandasan latar belakang masalah yang tertuju pada diatas, maka dapat diidentifikasikan permasalahan pada penelitian ini, yaitu:

1. Masih kurangnya perhatian terhadap keamanan jaringan.
2. Terdapat gangguan pada jaringan dengan adanya serangan Dos.

3. User tidak dapat mengakses data di server dengan baik.

1.3 Pembatasan Masalah

Demikian pembatasan masalah mengenai isi dari penelitian yang dilakukan agar pembahasan menjadi lebih terarah, maka penulis perlu membatasinya. Adapun batasan masalah, yaitu:

1. Implementasi menggunakan sistem *linux ubuntu* 16.04
2. Untuk pengujian simulasi proses penyerangan dengan dua macam yaitu menggunakan aplikasi *Loic* sebagai *Distributed-Denial of Service* (Ddos), dan *Sparta* sebagai *Nmap*.
3. Implementasi akan dilakukan pada Pt Sumber Inovasi Sejati.
4. Implementasi sistem hanya dilakukan pada jaringan lokal.
5. Implementasi hanya menggunakan *snort.*

1.4 Perumusan Masalah

Sesuai uraian identifikasi masalah di atas, maka yang menjadi pokok permasalahan yg akan dianalisis dan dibahas dalam penelitian ini adalah:

1. Bagaimana cara mengimplementasikan IDS agar dapat mendeteksi serangan pada jaringan.
2. Bagaimana cara melakukan simulasi Serangan pada jaringan.

1.5 Tujuan Penelitian

Berlandasan sesuai dengan rumusan masalah di atas, maka tujuan penelitian yang ingin dicapai ialah menjadi berikut:

1. Melakukan implementasi *snort* agar dapat memonitoring pada jaringan.
2. Melakukan simulasi deteksi serangan pada jaringan melalui komputer pengguna.

1.6 Manfaat Penelitian

Setelah melaksanakan penelitian ini diharapkan dapat memberikan manfaat antara lain sebagai berikut:

1.6.1. Manfaat Praktis

Adapun manfaat penelitian ini untuk aspek praktis adalah:

1. Memperkuat keamanan pada jaringan dengan biaya yg lebih kecil.
2. Sebagai penembahan wawasan tentang IDS *snort.*
3. Mendapatkan pemberitahuan jika ada penyusupan pada jaringan.

1.6.2. Manfaat Teoritis

Adapun manfaat penelitian ini untuk aspek praktis adalah:

1. Sebagai bahan referensi untuk penelitian lanjut tenntang IDS *Snort*
2. Yang akan terjadi penelitian bisa menyampaikan kontribusi dalam ilmu pengetahuan dan teknologi.

BAB II
KAJIAN PUSTAKA

2.1 Teori Dasar

Dalam teori dasar penulis akan menyebutkan materi pada jaringan komputer serta mengungkapkan sistem yang akan dipergunakan dalam penelitian yang mendukung materi penelitian. Berikut ialah konsep atau penjelasan perihal jaringan serta standart komputer bersertas jenis-jenis serta model lapisan OSI *(Open System Interconnection),* serta *Snort.*

1. Jaringan Komputer

Jaringan komputer ialah sistem komputer yang didesain buat membuatkan sumber daya, berkomunikasi dan mengakses info. Tujuan dari jaringan komputer ialah untuk bisa mencapai tujuannya, setiap bagian asal jaringan komputer dapat meminta serta menyediakan layanan. Jaringan komputer juga bisa dimaknakan menjadi gugusan terminal koneksi yang berlokasi di berbagai lokasi yg terdiri dari asal melebihi berasal satu komputer yang saling terhubung (Koujalagi, 2018).

Dalam jaringan komputer biasanya terdapat satu komputer dengan komputer lain yang saling terhubung bersama yang lain, jaringan sering juga digunakan untuk pengiriman data dari salah satu komputer ke komputer lainnya seperti *Printer,* Pertukaran file, dan bisa saling berkomunikasi secara elektronik. Di setiap komputer memiliki jaringan, dan kemudian terhubung dengan menggunakan kabel

atau nirkabel sebagai medium transmisi data. Informasi data berjalan melalui kabel atau tanpa kabel(Hakim, 2017)

Gambar 2. 1 Jaringan Komputer

2. Standar Jaringan Komputer

Standar jaringan komputer adalah hal yang penting dalam penciptaan dan menjadi jaminan interoperability dalam proses komunikasi, standar ini juga disenggarakan oleh badan dunia lainnya seperti ITU (*Internasional Telecommunication Union),* ANSI *(AmSasaan National Standard Institute),* NCITS *(National Commite for Information Technology Standardization),* bahkan juga disenggarakan oleh badan IEEE *(Institute of Electrical and Electronics Engineers).* Kita bisa melihat badan pekerja yang dibentuk oleh IEEE yang telah banyak membuat standarisasi peralatan telekomunikasi seperti gambar berikut (Maslan & Wangdra, 2012).

Tabel 2. 1 Badan Pekerja Di IEEE

Working Group	Bentuk Kegiatan
IEEE802.1	standarisasi interface lapisan atas HILI dan Data Link *(Medium Access Control dan Logical Link Control).*
IEEE802.2	standarisasi lapisan LLC/*Logical Link Control.*
IEEE802.3	standarisasi lapisan MAC/Medium Access Control untuk CSMA/CD. Standar ini merupakan generasi pertama dari Ethernet dengan kecepatan 10Mbps (Malhotra, Gupta, & Bansal, 2011).
IEEE802.4	Standarisasi lapisan MAC untuk *Token Bus.*
IEEE802.5	Standarisasi lapisan MAC untuk *Token Ring.*
IEEE802.6	Standarisasi lapisan MAC untuk MAN-DQDB (*Metropolitan Area Network-Distributed Queue Dual Bus*.)
IEEE802.7	Grup pendukung BTAG (*Broadband Technical Advisory Group*) pada LAN.
IEEE802.8	Grup pendukung FOTAG (*Fiber Optic Technical Advisory Group*.)
IEEE802.9	Standarisasi ISDN (*Integrated Services Digital Network*) dan IS (*Integrated Services*) LAN.
IEEE802.10	Standarisasi masalah pengamanan jaringan (LAN *security*.)
IEEE802.11	Standarisasi masalah *wireless* LAN dan CSMA/CD bersama IEEE802.3

IEEE802.12	Standarisasi masalah 100VG-AnyLAN
IEEE802.14	Standarisasi masalah *protocol* CATV
IEEE802.15.2	standar yang menggabungkan IEEE802.15 (WPAN) dengan perangkat nirkabel lain yang beroperasi di frekuensi tanpa lisensi.

Sumber: (Maslan & Wangdra, 2012)

3. Jenis Jaringan Komputer

Dalam jaringan komputer terdapat beberapa macam jaringan komputer yang berbeda, berdasarkan jangkauan Diantaranya : (Wongkar, Sinsuw, & Xaverius, 2015)

1. PAN *(Personal Area Network)*

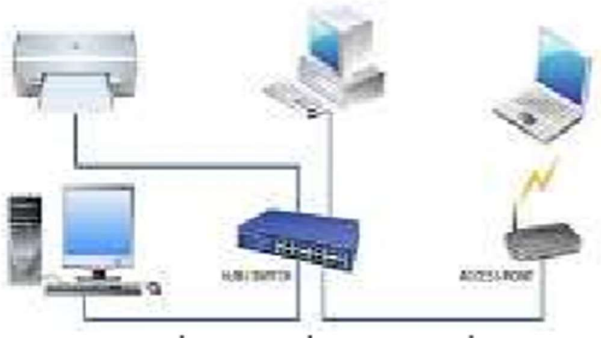
   PAN *(Personal Area Network)* artinya jaringan komputer yang dipergunakan buat tranmisi data antara perangkat langsung seperti personal komputer , serta perangkat hiburan pribadi lainnya. Atau buat menghubungkan perangkat ke jaringan menggunakan tingkat yang lebih akbar dan internet *(Uplink)*.

Gambar 2. 2 PAN (Personal Area Network)

(Wongkar et al., 2015).

2. LAN *(Local Area Network)*

LAN *(Local Area Network)* adalah jaringan komputer yang dapat menghubungkan personal komputer pada area yg terbatas umumnya dipergunakan di suatu daerah mirip sekolah, tempat kerja, warnet atau universitas. Jaringan tersebut dikelolah secara lokal yg membutuhkan korelasi koneksi antara satu komputer menggunakan komputer yang lain, jaringan ini juga sangat di pengaruhi sang topologi jaringannya, bisa dibangun dengan hardware yg relatif murah, seperti Access Point, hub, serta kabel Ethernet. mirip model di sebuah perkantoran dimana semua user harus dapat mengakses file di server sentra atau mencetak dokumen melalui satu printer sentra.

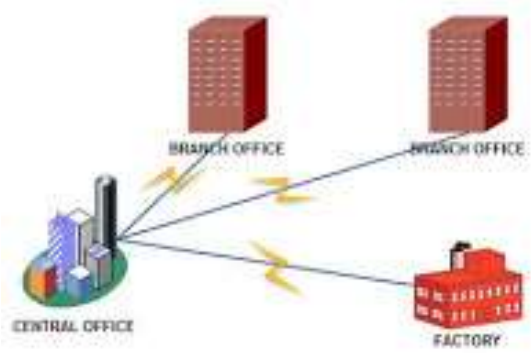


Gambar 2. 3 LAN (Local Area Network)

(Wongkar et al., 2015)

3. MAN *(Metropolitan Area Network)*

MAN *(Metropolitan Area Network)* merupakan jaringan komputer yg menghubungkan para pengguna menggunakan sumber daya personal komputer pada suatu jaringan personal komputer dalam satu kota menggunakan kecepatan tinggi transfer data yang dapat menghubungkan suatu lokasi seperti sekolah, kampus, perkantoran serta pemerintahan. MAN adalah campuran dari beberapa LAN buat membentuk jaringan yang lebih luah, Maka jangkauan MAN dapat mencapai 10-50 kilometer.

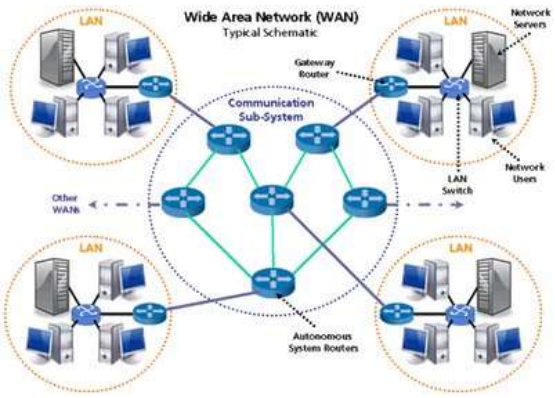


Gambar 2. 4 MAN (Metropolitan Area Network)

(Wongkar et al., 2015)

4. WAN *(Wide Area Network)*

WAN *(Wide Area Network)* merupakan jaringan komputer yg membentang diatas jarak geografis yg sangat luas, contohnya ialah jaringan yg menghubungkan suatu wilayah ataupun satu negara dengan negara lainya, WAN umumnya terdiri asal beberapa jaringan yang kecil seperti LAN atau MAN.



Gambar 2. 5 WAN (Wide Area Network)

(Wongkar et al., 2015)

5. WLAN *(Wireless Local Area Network)*

WLAN *(Wireless Local Area Network)* adalah metode distribusi nirkabel untuk dua atau lebih perangkat yang menggunakan gelombang radio frekuensi tinggi dan sering menyertakan titik akses ke Internet. WLAN memungkinkan pengguna untuk bergerak di sekitar area jangkauan, seringkali rumah atau kantor kecil, sambil mempertahankan koneksi jaringan

Gambar 2. 6 WLAN (Wireless Local Area Network)

Berdasarkan fungsi/pola pengoperasian komputer dalam jaringan maka dapat di bagi menjadi (Varianto & Badrul, 2015) :

a. *Peer to peer*

Jaringan peer to peer dibua waktu 2 atau lebih personal komputer terhubung serta saling berbagi asal daya tanpa melalui personal komputer server yg terpisah, jaringan peer to peer dapat berupa koneksi ad hoc, beberapa komputer terhubung melalui universal serial bus buat melakukan transfer arsip.

b. *Client Server*

Client server merupakan hubungan dimana satu program sebagai klien meminta layanan atau sumber daya dari program lain yaitu server. Saat ini, transaksi komputer dimana *server* memenuhi permintaan yang dibuat oleh klien sangat umum dan model *client server* sudah menjadi salah satu ide sentral dari komputasi jaringn.

Berdasarkan media transmisi dalam jaringan maka terbagi menjadi dua yaitu(Sitohang, 2018) :

a. Jaringan Nirkabel

   Jaringan nirkabel artinya jaringan personal komputer yang tidak terhubung dengan kabel apapun penggunaan jaringan nirkabel memungkinkan perusahaan buat menghindari proses mahal dalam memasukan kabel kedalam gedung atau menjadi koneks antara lokasi peralatan yg tidak selaras. Dasar berasal sistem nirkabel artinya gelombang radio, suatu implementasi yg terjadi di taraf fisik struktur jaringan.

b. Jaringan Kabel

   Kabel jaringan digunakan untuk menghubungkan dalam mentransfer data dan informasi antara komputer. Ada berbagai jenis kabel komunikasi, dan tergantung pada struktur dan topologi keseluruhan arsitektur jaringan. Salah satu kabel yang paling umum digunakan adalah kabel *twisted pair* pada jaringan lokal biasanya seperti lingkugan kantor, situs ritel dan komersial.

4. Model *OSI Layer*

OSI *(Open System Interconnection)* layer adalah suatu deskripsi abstrak mengenai desain lapisan-lapisan komunikasi dan protokol jaringan komputer yang dikembangkan oleh ISO pada tahun 1978. Model OSI bekerja dalam hierarki, menugaskan tugas untuk semua tujuh lapisan. Setiap lapisan bertanggung jawab

untuk melakukan tugas yang ditugaskan dan mentransfer tugas yang telah selesai ke lapisan berikutnya untuk diproses lebih lanjut. Protokol adalah aturan formal dan kesepakatan dengan bagaimana komputer saling bertukar informasi melalui media jaringan. Sebuah protokol mengimplementasikan salah satu lapisan OSI. Model ini juga sering di sebut dengan tujuh lapisan . Berikut adalah tujuh lapisan OSI yaitu :

1. *Physical Layer*

Tugas utama dari lapisan ini adalah untuk mengaktifkan dan mengatur physical interface jaringan komputer. Interface yang digunakan pada lapisan ini adalah 10 BaseT, 100baseTX, V35, X21 dan HSSI. Physical berfungsi dalam pengiriman raw bit ke chace komunikasi. Pada lapisan ini tidak mempunyai protokol yang sepsifik dilayer ini, karena pada layer ini hanya mengirimkan bit data (Setiawan, 2017).

2. *Data Link Layer*

Lapisan kedua dari bagian bawah model OSI. Fungsi utama dari layer ini adalah untuk melakukan deteksi kesalahan dan menggabungkan bit data kedalam frame. Dengan menggabungkan data mentah menjadi byte untuk membingkai dan mentarnsmisikan paket data kelapisan jaringan host tujuan yang di inginkan (Mehta et al., 2016).

3. Network Layer

Lapisan ketiga dari bawah ini memiliki akuntabilitas untuk menyelesaikan paket data dari sumber host ketujuan antara jaringan yang beroperasi pada protokol yang sama atau berbeda. Lapisan ini memiliki tugas menangani sebagian routing dalam jaringan. Lapisan ini berkaitan dengan penerusan paket dan menetapkan rute

yang dilalui paket melalui jaringan. Dalam istilah yang lebih sederhana, Lapisan Jaringan menentukan bagaimana suatu paket melakukan perjalanan ke tujuannya. Protokol seperti TCP / IP , AppleTalk , dan IPX beroperasi pada layer ini.(Mehta et al., 2016).

4. Transport layer

Fungsi dasar pada *transport* layer merupakan menerima data asal *session* layer dan memecahkan data sebagai bagian-bagian yg kecil serta meneruskan data ke *network* layer dan menjamin bahwa semua rabat tersebut bisa datang disisi yang betul. Tujuannya buat melindungi semua lapisan diatasnya teknologi perangkat keras yang mungkin timbul (Setiawan, 2017).

5. *Session layer*

Pada layer ini bertugas untuk mengizinkan para pengguna buat memutuskan *session* dengan pengguna lain. Layer ini membuka dan menutup suatu *session* antar *software*. Fungsi lainya ialah manajemen *token ,* sinkronisasi, penyisipan diperlukan jika akan mengulangi pengiriman yg terjadi dampak crash sehingga akibatnya data tidak perlu diulangi dari awal (Setiawan, 2017).

6. *Presentation Layeri*

Pada lapisan ini dirancang untuk mempersiapkan dan menerjemahkan data dari format jaringan ke format aplikasi atau sebaliknya. Lapisan ini menentukan bagaimana data disajikan untuk masing-masing entitas ini dalam hal sintaks dan struktur. Dalam banyak kasus, Lapisan Presentasi dapat dilihat melalui enkripsi dan dekripsi data. (Mehta et al., 2016).

7. *Application Layeri*

Lapisan ini benar-benar berinteraksi dengan pengguna. Setiap pengguna berinteraksi dengan aplikasi di komputer maka pengguna aktif dilapisan aplikasi. Protokol dari lapisan ini difokuskan pada proses pengguna akhir dan pengiriman aplikasi apa pun yang ingin diakses pengguna.(Mehta et al., 2016).

2.2 Teori Khusus

Teori spesifik menyampaikan penjelasan mengenai variabel-variabel spesifik yg diteliti. Secara teoritis, variabel dapat didefinisikan sebagai objek yang mempunyai variasi antara satu dengan lainnya. Berikut ialah variabel-variabel yg digunakan dalam penelitian ini:

2.2.1 IDS *(Intrusion Detection System)*

IDS (*Intrusion Detection System)* merupakan sebuah perangkat lunak software yg dibuat buat mendeteksi kegiatan komputer menggunakan tujuan menemukan pelanggaran atau mencurigakan terhadap sebuah sistem keamanan jaringan. Intrusion ialah kegiatan tidak sah yang menggangu ketersediaan berasal isu yang terdapat pada sistem. IDS akan memantau lalulintas data di sebuah jaringan, lalu dilakukan di analisa dengan prosedur pemecahan tertentu akan menetapkan buat memberi peringatan kepada seseorang administrator jaringan atau tidak(Gondohanindijo, 2011).

Ada IDS yang berfungsi hanya sebagai pengawas dan pemberi peringatan ketika terjadi serangan dan ada juga IDS yang bekerja dapat melakukan sebuah kegiatan yang merespon adanya percobaan serangan terhadap sistem. IDS sendiri terdiri dari 2 jenis, yaitu:

a. *Network-based Intrusion Detection System* (NIDS) ditempatkan disebuah tempat/ titik didalam sebuah jaringan buat melakukan supervisi terhadap trafik dalam jaringan NIDS akan menganalisa seluruh kemudian lintas yang lewat ke sebuah jaringan yang akan mencari, apakah ada percobaan agresi atau infiltrasi kedalam sistem jaringan. Ideanya semua trafik yg dari dari luar dan dalam jaringan dilakukan di *scan*, namun cara ini dapat mengakibatkan bottleneck yang menggangu kecepatan akses pada seluruh jaringan (Arsin, Yamin, & Surimi, 2017).

b. *Host-based Intrution Detection System* (HIDS) jenis ini berjalan di host yang berdiri sendiri atau perlengkapan pada sebuah jaringan. sebuah HIDS melakukan pengawasan terhadap paket-paket yg asal dari dalam ataupun dari luar hanya di satu indera saja dan lalu memberi peringatan kepada *user* atau *administrator* sistem jaringan bahwa adanya aktivitas yg mencurigakan yang terdeteksi sang HIDS(Arsin et al., 2017).

Berikut ini adalah teknik yang digunakan untuk mendeteksi dalam IDS:

a. *Knowledge-based* atau *misuse detection* Cara kerjanya ialah menyadap paket data kemudian membandingkannya dengan database rule IDS (berisi signature-signature paket agresi). Jika paket data mempunyai pola dengan

keliru satu pola pada database rule IDS, maka data tadi diklaim menjadi agresi(Gondohanindijo, 2011).

b. *Anomaly based atau behavior-based* Cara kerjanya ialah menggunakan mengamati adanya kejanggalan-kejanggalan di sistem, sebagai model adanya penggunaan memori yang meningkat secara terusmenerus atau ada koneksi paralel berasal satu IP pada jumlah banyak dan pada ketika yang bersamaan, kondisi tersebut pada anggap kejanggalan yang selanjutnya sang IDS *Anomaly Based* ini diklaim sebagai agresi(Gondohanindijo, 2011).
c. *Signature based* Cara kerja pada IDS ini akan melakukan pengawasan terhadap paket-paket dalam jaringan serta melakukan perbandingan terhadap paket-paket tersebut dengan berbasis data *signature*, Caran ini hampir sama menggunakan cara kerja anti virus dalam melakukan deteksi terhadap malware. pada dasarnya ialah akan terjadi keterlambatan antara terdeteksinya sebuah serangan pada internet menggunakan *signature* yg digunakan buat melakukan deteksi yg di implementasikan didalam basis data IDS yang dipergunakan.
d. *Passive IDS* Cara kerja pada IDS menjadi pendeteksi dan pemberi peringatan, waktu traffic yang mencurigakan atau membahayakan terdeteksi oleh IDS maka akan membangkitkan sistem pemberi peringatan yang dimiliki dan dikirimkan ke administrator.
e. *Reactive IDS* Cara kerja pada IDS ini tidak hanya melakukan deteksi terhadap *traffic* yg mencurigakan, tetapi juga mengambil tindakan aktif buat merespon terhadap agresi yg ada. biasanya menggunakan melakukan

pemblokiran terhadap *traffic* jaringan lalu asal alamat IP sumber atau *user* yg mencoba buat melakukan agresi lagi terhadap sistem jaringan pada saat selanjutny.

Dalam mendeteksi adanya ancamana pada jaringan komputer IDS menggunakan *signature base* dan *anomali base*. Pada *signature base* IDS akan mendeteksi adanya aktifitas mencurigakan atau penyusupan berdasarkan pada *database* yang telah ada, layaknya virus pada komputer, penyerang memiliki sebuah *signature* yang dapat dikenali, maka berdasarkan *signature* dan *rule* sistem dapat mendeteksi dan membuat catatan aktivitas tersebut dan memberikan peringatan kepada administrator, sedangkan pada *anomali base* IDS melakukan pendeteksian dengan membandingkan pola lalu lintas jaringan yang sedang diawasi denganpola lalu lintas yang biasanya terjadi.

2.2.2 Snort

Snort merupakan salah satu contoh program *Network-based Intrusion Detection System* (NIDS) paling terkenal yaitu suatu *software* yg bisa mendeteksi adanya infiltrasi dan bisa menganalisis paket yang melintas di jaringan secara *real time traffic* dan *logging* kedalam data base serta bisa mengidentifikasi banyak sekali macam serangan yg berasal dari luar jaringan (Kade et al., 2019).

Snort bersifat *open source* dengan lisensi GNU (*General Purpose License*) sehinga perangkat lunak ini dapat digunakan buat mengamankan sistem *server* tanpa harus membayar biaya buat lisensi, snort juga bisa digunakan sebagai bagian tetap asal suatu sistem jaringan. Snort dapat di konfigurasi dan dibiarkan berjalan

buat waktu yg lama tanpa meminta pengawasan atau perawatan bersifat administratif, snort jua dapat dijalankan dibeberapa sistem operasi di *RedHat Linux*, *Debian Linux, MkLinux, HP-UX, Solaris* (*x86* dan *sparc*), *Windows* dan *MacOS X* (Putranto Pancaro & Isnanto Saputra, 2018).

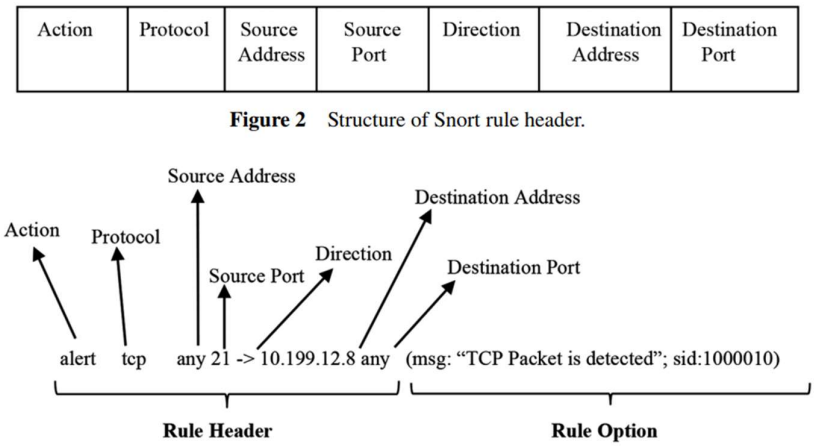
Snort Rules merupakan database yang berisi pola-pola serangan yang berupa *signature* jenis-jenis serangan, dan harus diupdate secara rutin agar ketika ada suatu serangan baru dapat terdeteksi, Suatu serangan dapat dideteksi atau tidak oleh *snort* dikonfigurasi pada pengaturan jaringan dan rule Snort yang ada (Kade et al., 2019).

Cara kerja *Snort Rules* dengan membaca *rules* ke pada struktur atau rantai data internal lalu dicocokan menggunakan paket yg sudah ada. Jika paket sinkron menggunakan *rules* yang ada, maka tindakan akan diambil, kebalikannya bila tidak paket akan dibuang. Tindakan yang diambil bisa berupa *logging* paket atau mengaktifkan *alert* (Ery Setiyawan Jullev Atmaji, 2016).

Pola aturan dalam *snort*, semua aturan snort biasanya di simpan di folder /etc/snort/rules. Pilihan yang biasanya dalam *rules snort* adalah *log* dan *alert*, sedangkan pilihan protokol yang adalah "*tcp, udp*, dan *icmp"* dan berupa Ip address, pilihan *port*. Operator di biasanya digunakan dalam *rules snort* adalah "->", "<-" atau "<>" kalau mau mengatur bi-directional / dua arah.

Peraturan dalam snort terbagi menjadi dua bagian, yaitu *rule header* serta *rule options,* pada *rule header* berisi *alert,* protokol yg di monitoring, alamat IP asal tujuan, netmask, serta angka port asal dan tujuan. Sedangkan rule options berisi pesan- pesan yang ingin di tampilkan, serta bagaimana dari paket yang wajib pada

di amati untuk memilih apakah perlu melakukan *alert* atau tidak, contoh pengertian sebuah rule mirip gambar dibawah ini (Goel, 2017).



Gambar 2. 7 Perintah *rules snort*

Berikut adalah penjelasan dalam *rules snort* (Chan, Weil, & Yeoh, 2018):

1. *Alert* adalah dimana perintah "*Alert"* akan menghasilkan peringatan di ikuti dengan masuknya paket.
2. Tcp adalah protokol yang ditentukan untuk ping, protokol lain juga tersedia seperti icmp dan udp.
3. *Any* adalah variabel port untuk $ EXTERNAL_NET dimana untuk kasus ini akan menjadi port.
4. *Source address* adalah alamat ip yang di tetapkan dalam file konfigurasi untuk mendeteksi pengguna eksternal yang telah di tetapkan "!$ HOME_NET" yang berarti tidak sama dengan jaringan yang akan di lindungi.

5. Tanda “->” adalah Panah yang menunjukkan lalu lintas untuk memverifikasi aturan. Karenanya dalam kasus ini kami memverifikasi ping dari variabel $ EXTERNAL_NET menuju $ HOME_NET
6. *Destination address* adalah Alamat IP yang ditetapkan dalam file konfigurasi untuk dilindungi.
7. *Msg adalah* Pesan yang akan dihasilkan di konsol peringatan ketika NIDS telah mendeteksi pola yang sama seperti yang ditentukan oleh aturan yang ditentukan. Dalam hal ini, itu akan menampilkan pesan "Tcp packet is detected" ketika aturan diaktifkan.
8. *Sid* adalah kependekan dari *snort* ID sederhana untuk melacak jumlah aturan yang bekerja seperti halnya nomor seri. Perubahan "sid" tidak akan memengaruhi cara aturan mendeteksi polanya dalam lalu lintas jaringan.

Ada terdapat 4 jenis mode pada *snort* yang dapat dioperasikan yaitu(Affandi & Setyowibowo, 2013):

1. *Sniffer mode* untuk membaca paket-paket data yang lewat pada jaringan dan memperlihatkan bentuk aliran tak terputus pada konsol (layar).
2. *Logger mode* buat mencatat semua paket-paket data yang lewat pada jaringan kedalam *disk,* maka perlu mencantumkan direktori *logging* supaya bisa menyimpan catatan paket-paket data kedalam *disk*. buat dilakukan analisa dikemudian hari.
3. NIDS *(Network Intrusion Detection System)* pada mode ini *snort* akan berfungi untuk mendeteksi tindakan serangan yang dilakukan melalui jaringan komputer.

4. *Inline mode* untuk membandingkan paket data dengan *rule iptables*, *libpcap* dan kemudian dapat menentukan iptables untuk melakukan drop atau allow paket berdasarkan *rules snort* yang telah ditetapkan.

Snort memiliki beberapa komponen yang bekerja saling berhubungan satu dengan yang lain meliputi (Ery Setiyawan Jullev Atmaji, 2016) :

1. *Rule snort* adalah *database* yg berisi pola agresi pada bentuk signature jenis-jenis pada serangan. Rule snort IDS ini, harus diperbarui secara teratur buat menghindari waktu ada teknik serangan baru.
2. *Snort engine* artinya program yang berjalan menjadi proses yg selalu berfungsi buat membaca paket data serta lalu dibandingkan menggunakan *rule snort*.
3. *Alert* adalah catatan serangan pada deteksi serangan, jika *snort engine* menghukum paket data yang lewat sebagai serangan, maka *snort engine* akan mengirimkan infromasi dalam alert berupa *log file*, untuk kebutuhan analisia, dan dapat disimpan didalam data base.
4. *Preprocessors* adalah jaringan yang mengidentifikasi berbagai hal yang harus di periksa

2.2 Tools

Dalam penelitian ini, terdapat beberapa perangkat yg akan digunakan buat membangun sistem *snort* buat bisa terhubung pada jaringan tadi. Berikut artinya perangkat yang digunakan:

2.3.1 Komputer

Komputer adalah sebuah perangkat yang dapat memuat informasi atau data, dan kelebihan dari komputer ini juga mampu menyimpan, mengambil dan mengolaj data. Komputer yang digunakan pada penelitian ini dengan menggunakan sistem operasi ubuntu 16.04.

2.3.2 Router

Router adalah sebuah perankat jaingan yg berfungsi untuk menentukan jalur pengiriman data sekuensial yang cepat berasal pengirim ke tujuan. Jalur pengiriman ini bisa dilakukan secara statis (untuk jaringan yang sporadis berubah) serta dinamis(Maslan & Wangdra, 2012). Router pula dapat digunakan buat menghubungkan sejumlah LAN, sehingga trafik yang dibangkitkan sang suatu LAN terisolasikan dengan baik router berfungsi sebagai sebuah alat penghubung di antara rangkaian yang berlainan(Operasi & Redhat, 2013).

2.4 Penelitian Terdahulu

Pada penelitian terdahulu ini akan menjadi referensi penulisan sehingga mendapat teori yang akan digunakan dalam penelitian. Maka peneliti akan memuat tentang beberapa penelitian yang sudah dilakukan oleh peneliti. Berikut dibawah ini merupakan beberapa jurnal terkait dengan penelitian yang digunakan sebagai dasar dalam penelitian ini.

Penelitian terdahulu pertama adalah penelitian berjudul *"*Implementasi IDS *(Intrusion Detection System)* pada sistem keamanan jaringan sman 1 cikeusal*"* pada tahun 2018 (ISSN 2406-773). Penelitian ini ditulis oleh Sutarti, Adi Putranto Pancaro dan Fembi Isnanto Saputra. berdasarkan penelitian yg dilakukan terdapat konklusi yaitu berasal akibat implementasi tadi dilakukan simulasi penyerangan dengan hasil IDS *snort* mampu mendeteksi adanya agresi mirip *Ping Of Death* serta *Port Scan, log* yang didapatkan bisa membaca suatu agresi den penyalahgunaan jaringan sesuai menggunakan metode pengujiaannya dengan menyeting bagian bagian *rule* berasal *snort*. *Snort* tidak bisa menindak lanjuti *alert* yang terdeteksi menjadi serangan atau penyalahgunaan jaringan karena sifatnya hanya mendeteksi.

Penelitian terdahulu kedua adalah penelitian yang berjudul "Perancangan sistem pendeteksi serangan pada server jaringan komputer menggunkan *snort* berbasis sms *gateway*" pada tahun 2019 (ISSN 2085-0859, e-ISSN 2620-4770). Penelitian ini ditulis oleh Tria Apriliantom, Sunu Jatmika, Ihsan Wicaksono. Berdasarkan penelitian yang dilakukan terdapat kesimpulan sistem telah di implemensikan rule sebanyak 6 rule serangan yang terdiri dari deteksi Remote SSH, Remote Telnet, Login FTP, Akses web-PHP, Ping of Death dan Scan Port UDP, sistem snort dapat bekerja dengan baik, seluruh serangan dapat terlihat pada sistem pencatatan log serangan yang dicatat oleh BASE, namun pencatatan web server kadang ada beberapa catatan yang ditidak ditampilkan oleh web server. Web login telah di implementasi mampu melindungi web server yang ada, seorang admin tidak dapat melewati web login jika tidak ingin melihat catatan serangan, dari hasil pengujian yang dilakukan, dari 75 serangan yang seharusnya ditampilkan hanya 80%

notifikasi yang dapat ditampilkan di web server hanya 77.3% notifikasi dapat dikirimkan oleh sistem. Sistem registrasi user admin dapat berfungsi dengan0baik, hal ini bisa dilihat dari tingkat kesuksesan pembuatan user yang tersimpan pada database web server.

Penelitian terdahulu ketiga adalah "Efficient Working of Signature Based Intrusion Detection Technique in Computer Networks" pada tahun 2019 (ISSN 2456-3307). Penelitian ini ditilus oleh Dr. Abid Hussain dan Dr. Praveen Kumar Sharma Berdasarkan penelitian ini yang dilakukan terdapat kesimpulan sistem ini mengusulkan proses kerja Signature sistem deteksi intrusi berbasis di Jaringan. Sistem SIDS ini menunjukkan bahwa ia dapat mendeteksi dan menganalisis intrusi dalam lalu lintas jaringan waktu nyata. Kita juga telah membahas tentang alat IDS Jaringan seperti *snort*. Snort dibangun untuk mendeteksi berbagai jenis peretasan dan menggunakan bahasa aturan yang fleksibel untuk menentukan jenis lalu lintas jaringan yang harus dikumpulkan. Itu pekerjaan masa depan adalah mengembangkan kerangka kerja baru untuk disaring, menghapus dan memvalidasi serangan intrusi secara otomatis dalam jaringan komputer.

Penelitian terdahulu keempat adalah "Monitoring keamanan jaringan komputer menggunakan *Network Intrussion Detection System* (NIDS)" pada tahun 2016 (ISBN 978-602-14917-3-7). berdasarkan penelitian yg dilakukan ada kesimpulan snort memudahkan seseorang administrator jaringan pada memantau keamanan jaringan personal komputer , Baseiyang terhubung dengan *Mysql database* memudahkan *administrator* dalam mendapatkan informasi ihwal *snort*. Konfigurasi *snort* pada melakukan monitoring keamanan jaringan komputer

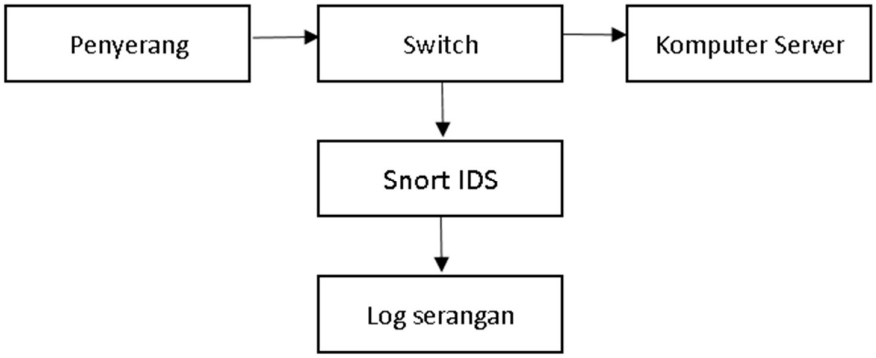
berhasil menggunakan baik pada lingkungan sistem operasi *linux ubuntu server* 14.04 LTS.

Penelitian terdahulu kelima adalah " *The Implementation and Assessment of Snort Capabilities* " pada tahun 2017 (IJCA 0975-8887) Volume 167 No.13. Penelitian ini ditulus oleh Aaruni Goel dan Ashok Vasishtha Phd. Berdasarkan penelitian yang dilakukan terdapat kesimpulan proyek ini dijalankan di Ubuntu 14.04 LTS, membutuhkan waktu hampir tiga jam untuk instalasi lengka p termasuk *sendmail, swatch, snort* dan beberapa paket pendukung, fungis *snort* yang lengkap dan teknologi IDSP berjalan dengan baik, akan tetapi terdapa sedikit menghambat tugas mengfungsikan NAS, hal lain secara umum ada lebih dari 23000 *signature* ditemukan dalam aturan snort yang telah di sedikan oleh snort.org. Selain itu NAS juga membuat banyak aturan demi kebijakan organisasi dari waktu ke waktu, karena tujuan tersebut sangat sulit bekerja pada aplikasi lain yang tidak diketahui tetapi asli pada komputer yang berada di snort. Hasil akhir dapat dikatakan bahwa dalam waktu dekat dan dengan alat fleksibel masalah yang terkait dalam snort akan lebih mudah diperiksa.

2.5 Kerangka pemikiran

di kerangka pemikiran ini akan menjelasan sementara dari tanda-tanda yg akan menjadi objek persoalan, serta akan di jelaskan bagaimana teori berhubungan menggunakan banyak sekali faktor. serta disarankan artinya kerangka kerja yang diekspresikan dalam bentuk diagram sebagai akibatnya pembaca dapat memahami paradigma yang pada maksud.

Berdasarkan teori yang dibahas sebelumnya, maka kerangka berpikir yang dibuat dalam penelitian ini adalah sebagai berikut:



Gambar 2. 8 Kerangka Pemikiran

Pada kerangka pemikiran diatas, sistem *snort* IDS akan terhubung kedalam jaringan lokal. Dimana salah satu komputer akan melakukan penyerangan ke komputer server. Dalam jaringan tersebut terdapat akan terdapat sebuah komputer yang berperan sebagai *snort* yang akan bertugas untuk memantau jaringan pada komputer *server.* Setelah adanya terjadi aktivitas yang terdeteksi oleh *snort*, maka *snort* akan menyimpan dalam bentuk log, maka dengan komputer *snort* tersebut bisa diakses buat melihat *log* agresi Bila terdapat terjadi agresi di jaringan personal komputer *server.*

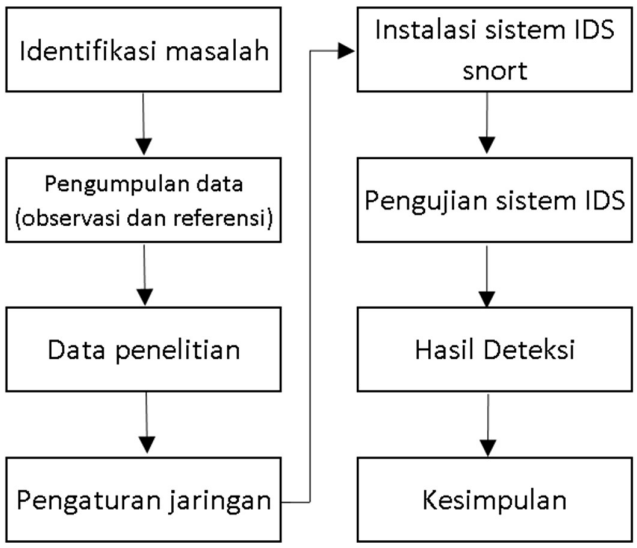
BAB III
PENDAHULUAN

3.1 Desain Penelitian

Pada desain penelitian ini akan di jelaskan hal yang akan dilakukan oleh peneliti secara teknis dan desain ini harus bisa meliputi tahapan yg dilakukan sang peneliti, menggunakan bagaimana cara peneliti melakukan pengumpulan data serta metodenya beserta indera atau perangkat yang digunakan dalam penelitian ini.

Metode penelitian yang akan dilakukan memakai metode observasi, wawancara, literatur, dan teknik *knowleadge based* berasal metode peneliti melakukan analisa terhadap permasalahan jaringan dan dibuat perancangan jaringan yang dibutuhkan kemudian dilakukan pengujian terhadap hasil rancangan yang baru yg kemudian diimplementasikan.

Berikut adalah desain penelitian dari implementasi sistem IDS *snort* :

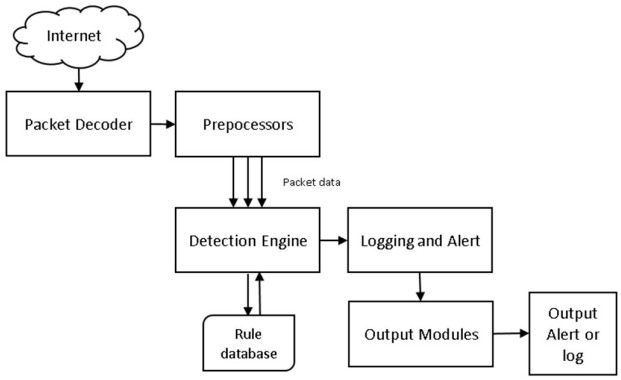


Gambar 3. 1 Desain penelitian

Berikut adalah pembahasan dari gambar diatas :

1. Pada tahap awal identifikasi persoalan ini ialah dasar asal penelitian ini yg sudah diceritakan pada awal pada bab 1.
2. Pada Pengumpulan data ini akan mengumpulkan materi atau berita yg didapatkan dari observasi dan referensi berupa jurnal dan studi pustaka. Pengumpulan data pula akan membantu peneliti buat memilih perangkat apa saja yang akan dibutuhkan..
3. Pada data penelitian ini adalah bagian dari kumpulan data-data yang diperoleh dari pengumpulan data dan hasil referensi berupa jurnal."
4. Pengaturan jaringan ini yang akan dilakukan untuk menghubungkan komputer IDS *snort* kedalam jaringan."
5. Instalisasi sistem IDS snort merupakan implementasi IDS *snort* pada perangkat komputer.
6. Hasil deteksi yang didapatkan dari pengujian sistem berupa serangan ini akan tersimpan bentuk log , dan dapat di baca dengan *snort.*
7. Pada tahap akhir artinya konklusi kompendium berasal metode serta hasil penelitian yg telah dilakukan. Saran akan ditulis dibagian konklusi Bila hasil penelitian dinilai kurang puas maka memungkinkan adanya penelitian yang dilanjut.

3.2 Arsitektur Snort Dalam mendeteksi serangan



Berikut adalah beberapa komponen yang berada pada *snort:*

1. Paket *decoder* bertugas sebagai pengambilan paket dari berbagai macam jenis jaringan *interface* danmempersiapkan paket tersebut ke *prepocessors.*
2. *Prepocessors* ini adalah sebuah komponen atau *plug-in*0yang digunakan oleh *snort* untuk memodifikasi paket data sebelum *detection egine* untuk mengetahui paket yang digunakan oleh penyusup. Prepocessors sangat penting untuk setiap IDS agar dapat menganalisa paket data berdasarkan aturan dalam *detection engine.*
3. *Detection engine* adalah salah satu komponen yang terpenting pada snort, yg akan digunakan buat mendeteksi adanya aktivitas intrusi pada sebuah paket. *Detection engine* ini mendeteksi berdasarkan *rule snort*. Jika ada paket tersebut yang cocok dengan *rule*, maka akan dilakukan tindakan, komponen bisa mendeteksi menggunakan baik atau tidak tergantung dari Seberapa bertenaga mesin dan berapa banyak aturan yg ditetapkan,

mungkin dibutuhkan saat buat merespon paket Jika lalulintas jaringan terlalu tinggi.

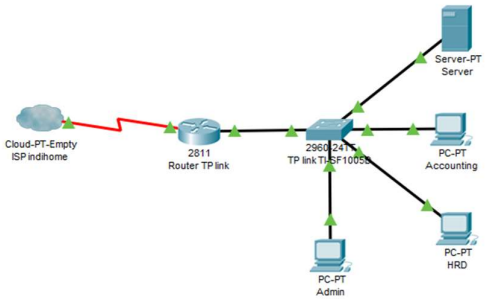
4. *Logging and alert* bertugas untuk mencatat aktivitas dan hasil peringatan kedalam bentuk file, tergantung dari apa yang *detection engine* telah temukan dalam sebuah paket.
5. *Output Modules* dapat melakukan operasi yang berbeda tergantung dari pengguna dalam menyimpan output yang dihasilkan *logging dan alert* dari snort.

3.3 Analisis Jaringan Lama/yang Sedang Berjalan

Analisis jaringan lama adalah tahapan pada melakukan penelitian supaya bisa mengetahui profil jaringan yg digunakan sebelumnya. Berikut alur jaringan yg di pakai pada perusahaan:

3.2.1 Topologi jaringan

Berikut adalah topologi jaringan lama yang digunakan :



Gambar 3. 2 Topologi jaringan yang sedang berjalan

Pada jaringan lama , *router* yang terhubung dengan ISP dan disambungkan ke *switch*, semua PC client dan *server* dihubungkan oleh *switch* agar semua perangkat dapat berkomunikasi . setiap perangkat memiliki ip yang berbeda-beda, dan *server* dapat diakses melalui alamat IP 192.168.100.10, sedangkan *router* dapat diakses melalui IP 192.168.100.1.

3.2.2 *Hardware* Jaringan

Ada bagian ini akan menjelaskan perangkat keras yang dibutuhkan untuk server PC IDS. Adapun perangkat yang dibutuhkan adalah sebagai berikut :

Tabel 3. 1 Perangkat Keras yang Sedang Berjalan

Nama Perangkat	Fungsi
Desktop *Switch D-LINK DES-1016C, 16 port*	Sebuah komponen jaringan yang bertugas untuk menghubungkan beberapa perangkat komputer kedalam sebuah jaringan komputer.
Router	Menentukan jalur yang akan dilewati paket dari pengirim ke penerima atau sebaliknya yang berada dalam satu jaringan.

3.2.3 Software

Perangkat lunak yang beperan sebagai aplikasi dimana aplikasi tersebut digunakan pada jaringan yang sedang berjalan yaitu :

Tabel 3. 2 Perangkat lunak yang sedang berjalan

Software	Keterangan
OS windows 10	OS *microsoft corporation* 2018 64-bit
Browser	Sebuah aplikasi yang digunakan untuk browsing dengan protokol http dan sebagainya

3.2.4 Policy/Kebijakan Bidang Jaringan yang Sedang Berjalan

Kebijakan pada jaringan digunakan sebagai manajemen keamanan di perusahaan agar mendapatkan alur kerja yang baik, aman, dan tentram. Kebijakan pada perusahaan yang diteliti mencakup hal-hal berikut ini :

1. Konfigurasi *router* bisa diakses dengan alamat IP 192.168.100.1
2. Jumlah akses yang terhubung ke *router* tidak dibatas.
3. Tidak menggangu kecepatan akses dalam sistem yang sedang berjalan.

3.2.5 Table IP Topologi Fisik

Berikut adalah informasi *IP Address* pada perangkat komputer yang ada.

Tabel 3. 3 Table IP sedang berjalan

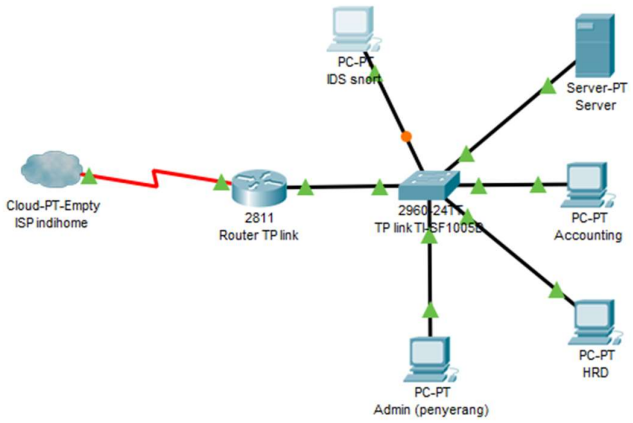
NO	Device	IP Address	Subnet Mask	Gate way
1.	Router	192.168.100.1/24	255.255.255.0	-
2.	Server	192.168.100.10/24	255.255.255.0	192.168.100.1
3.	HRD	192.168.100.13/24	255.255.255.0	192.168.100.1
4.	Accounting	192.168.100.33/24	255.255.255.0	192.168.100.1
5.	Admin	192.168.100.20/24	255.255.255.0	192.168.100.1

3.3 Rancangan Jaringan yang Dibangun/Diusulkan

Rancangan jaringan baru tadi didesain buat membantu mencapai tujuan berasal penelitian ini. Berikut adalah rancangan jaringan baru yang akan dibangun:

3.3.1 Topologi jaringan

Berikut adalah topologi jaringan baru yang akan dirancang dalam penelitian ini :



Gambar 3. 3 Topologi jaringan baru

Pada rancangan jaringan yang baru, terdapat penambahan sistem pada PC IDS snort sistem operasi yang digunakan adalah Linux Ubuntu Dekstop 16.04 LTS. Sedangkan client tetap menggunakan sistem operasi yang ada. Ketika terdapat jaringan yang dianggap mencurigakan maka akan ada notifikasi pada PC IDS *snort*, sehingga membantu administrator untuk melakukan tindak lanjut pada serangan terserbut, Terdapat sebuah laptop sementara dalam jaringan digunakan untuk simulasi / pengujian hasil implementasi sistem IDS,

3.3.2 *Hardware* pada Jaringan

Berikut adalah perangkat keras jaringan yang akan digunakan pada hasil rancangan jaringan baru:

Tabel 3. 4 Perangkat keras pada jaringan baru

Nama Perangkat	Fungsi
Desktop Switch D-LINK DES-1016C, 16 port	Sebuah komponen jaringan yang bertugas untuk menghubungkan beberapa perangkat komputer kedalam sebuah jaringan komputer.
Router	Menentukan jalur yang akan dilewati paket dari pengirim ke penerima atau sebaliknya yang berada dalam satu jaringan.

3.3.3 Software

Perangkat lunak yang beperan sebagai aplikasi dimana aplikasi tersebut digunakan pada jaringan yang sedang berjalan yaitu :

Tabel 3. 5 Perangkat lunak Jaringan baru

Software	Keterangan
OS *Ubuntu Desktop* 16.04 LTS	Sebagai OS dari yang akan di gunakan pada komputer *snort*
Snort	Sebagai program pendukung dari sistem IDS
Windows 10	OS microsoft corporation 2018 64-bit
Browser	Sebuah aplikasi yang digunakan untuk browsing dengan protokol http dan sebagainya

3.3.4 Table IP Topologi Fisik

Berikut adalah informasi *IP Address* pada perangkat komputer yang ada.

Tabel 3. 6 Tabel IP Jaringan baru

NO	Device	IP Address	Subnet Mask	Gate way

1.	Router	192.168.100.1/24	255.255.255.0	-
2.	Mesin IDS	192.168.100.9/24	255.255.255.0	192.168.100.1
3.	Server	192.168.100.10/24	255.255.255.0	192.168.100.1
4.	HRD	192.168.100.13/24	255.255.255.0	192.168.100.1
5.	Accounting	192.168.100.33/24	255.255.255.0	192.168.100.1
6.	Penyerang	192.168.100.20/24	255.255.255.0	192.168.100.1

3.3.5 Tahapan Rencana Implementasi

Pada implementasi, sebuah rencana diperlukan buat membuat akibat implementasi lebih terstruktur. buat membentuk urutan dan implementasi *snort* pada jaringan yg terdapat, sebuah rencana dikembangkan dengan tujuan menjaga konektivitas jaringan buat mempertahankan operasi serta menaikkan *security* jaringan dengan menambahkan sistem *snort* tanpa menghambat jalur pada jaringan. Tahapan rencana buat menerapkan sistem *snort* kedalam jaringan perusahaan:

1. Perencanaan

   Sebelum mengimpementasikan perencanaan, perlu buat perancangan desain jaringan dan implementasinya secara teratur. Jaringan baru yan direncanakan terfokus di keamanan jaringan tanpa mengganggu ketenangan pengguna lain. *Server* bisa diserang sang perangkat lain di jaringan yang sama, maka keamanan sangat krusial, sehingga perangkat yang dibutuhkan tidak diserang dan diprioritaskan ketika perancangan.

2. Perancangan jaringan

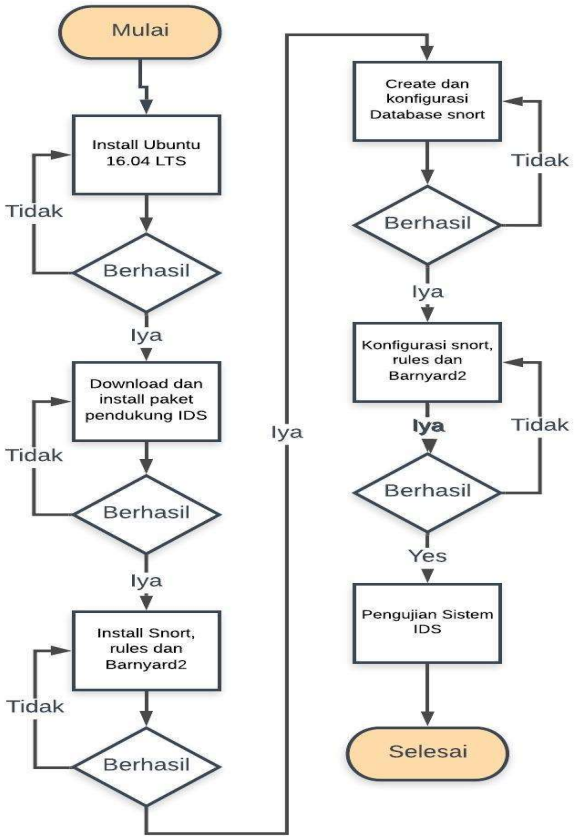
Pada perencangan ini yg dimaksud artinya lebih jelasnya rapikan letak jaringan teknis. Jaringan baru untuk menerapkan snort pada pemantauan jaringan. Topologi jaringan bergantung di surat keterangan penelitian sebelumnya, sesuai dengan batasan biaya serta fasilitas perangkat keras jaringan yang terdapat.

3. Implementasi jaringan

   Pada tahap implementasi ini akan membuat atau memasang jaringan konkret berdasarkan perencanaan yang telah tersusun. berikut adalah ialah beberapa hal yg dilakukan ketika implementasi jaringan baru::

   a. Melakukan install sistem operasi pada PC. Sitem operasi yang digunakan pada PC adalah Linux Ubuntu Dekstop 16.04 LTS.
   b. Download dan instal paket pendukung IDS tersebut.
   c. Install *snort* dan *barnyard2* sebagai inti dari sistem yang akan kita bangun.
   d. Melakukan konfigurasi data base dari snort agar nantinya semua log dan sistem yang kita bangun bisa menyimpan semua kejadian kedalam database
   e. Melakukan konfigurasi *snort* dan barnyard2
   f. Setelah selesai semua dilakukan, maka di jalan kan sistem *snort*
   g. Dan melakukan simulasi serangan untuk menguji sistem *snort* yang sudah dibuat.

Berikut adalah diagaram *flowchart* yang akan menjelaskan proses perencanaan implementasi sistem IDS *snort* dengan simulasi serangannya.



Gambar 3. 4 Flowchart Implementasi snort

3.3.6 Cara snort mendeteksi paket yang mengandung serangan

Pada penelitian ini untuk mendeteksi paket-paket yang termasuk serangan DoS dapat dideteksi berdasarkan pola pola atribut atau feature sebagai berikut:

Tabel 3. 7 Tabel Rules Snort

	Atribut	**Keterangan**	***Type***

Rule Header	Action	Alert	*Text*
	Protokol	ICMP, UDP, TCP	*Number*
	Source Address	Alamat IP asal paket	*Decimal*
	Source Port	Alamat port asal paket	*Decimal*
	Direction operator	Menunjukan orientasi lalu lintas.	*Symbol*
	Destination Address	Alamat IP yang di pantau	*Decimal*
	Destination Port	Alamat Port yang di pantau	*Decimal*
Rule Options	Msg	Pesan *alert* yang ditampilkan	*Text*
	Reference	Memasukan referensi ke sistem identifikasi serangan	*Text*
	Gid	Untuk identifikasi bagian snort event ketika aturan dijalankan	
	Sid	Snort *Rules* Id, sebagai identifikasi	*Number*
	Rev	Identifikasi revisi dari rule snort	*Number*
	Classtype	Membagikan kategori serangan	*Text*
	Priority	memberikan nilai hasil deteksi pada aturan.	*Decimal*
	Metadata	Untuk membuat informasi tambahan tentang aturan	*Text*

Dari beberapa atribut yang di sebutkan diatas, maka snort akan mendeteksi berdasarkan pola-pola seperti action, protokol, *source address*, *source port*, *direction,destination address, destination port* dalam aturan yang dibuat dalam *snort.conf* , cara kerja *snort* menggunakan teknik *Knowledge-based* dengan menyadap paket data kemudian membandingkannya dengan *rules snort* IDS. *Signature ID* atau sid digunakan untuk mengidentifikasi secara khusus dalam *snort rules*. Informasi ini memungkinkan *plugin output* untuk mengindentifikasi *rule* dengan mudah dan harus digunakan dengan *rev*(revisi) kata kunci. Jika paket data mempunyai pola dengan salah satu pola dalam database rules IDS, maka data tersebut dianggap sebagai serangan.

3.4 Lokasi dan jadwal penelitian

Lokasi penelitian akan dilakukan di Pt Sumber Inovasi Sejati, jadwal penelitian akan dilakukan seperti tabel berikut :

Tabel 3. 8 Jadwal Penelitian

Tahap	Uraian	Bulan															
		April 2019				Mei 2019				Juni 2019				Juli 2019			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Pengajuan judul penelitian																
2	Studi kepustakaan																
3	Penulisan Bab I																
4	Penulisan Bab II																
5	Penulisan Bab III																

6	Penulisan Bab IV																
7	Penulisan Bab V																
8	Pengumpulan skripsi																