Vol.1 No.2 Juni-Desember 2015
JESIK
JURNAL ELEKRONIK SISTEM INFORMASI DAN KOMPUTER
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER (STMIK) BINA MULIA

# PENERAPAN NETWORK INTRUSION DETECTION SYSTEM MENGGUNAKAN SNORT BERBASIS DATABASE MYSQL PADA HOTSPOT KOTA

[1] Fitriyanti A.Masse,[2] Andi Nurul Hidayat,[3] Badrianto
*Ilmu Komputer*
*Stmik Bina Mulia Palu*
*Website kampus:stmik-binamulia.ac.id*

**ABSTRAK**

Gangguan keamanan dapat dibagi menjadi dua kategori, gangguan internal dan gangguan eksternal atau keamanan dari luar dan keamana dai luar jaringan. Gangguan dari dalam jaringan terjadi dari pihak yang sudah mengetahui kondisi jaringan, dan gangguan dari luar jaringan terjadi dari pihak yang sengaja ingin melakukan percobaan terhadap sistem keamanan jaringan dari luar. Gangguan keamanan terjadi pada tempat yang menjadi studi kasus ini terjadi dari dalam jaringan yang ini mencoba mengambil alih sistem atau sekedar mengetes kemanan jaringan pada tempat tesebut. Dengan menggunakan IDS (*Intrusion Detection System*) hal tersebut dapat diatasi dengan cara mengenali setiap pola serangan yang di lalui oleh penyerang. Untuk mendeteksi setiap gejala serangan tersebut, sistem menggunakan pengenalan terhadapa source yang didapat dari pihak yang dianggap sebagai ancaman dalam sistem jaringan komputer. Metode pengembangan sistem yang digunakan dalam penelitian ini adalah *Netework Development Life Cycle.* Penulis menggunakan snort yang di implementasikan pada mesin sensor berbasis *Open Source.* Hasil penelitian ini menyimpulkan bahwa setiap tindakan yang dilakukan oleh peyerang terhadap jaringan dapat diketahui oleh mesin sensor, sehingga dapat dilakukan pencegahan sebelum terjadi kerusakan pada jaringan yang lebih luas.

**Kata Kunci :** Network, Intrusion, Detection, System, Snort, *Netework Development Life Cycle*.

## 1. Pendahuluan

Gangguan pada dasarnya dapat dibagi atas dua bagian, yaitu gangguan dari dalam dan gangguan dari luar jaringan. Gangguan dari dalam merupakan gangguan yang berasal dari lingkup dalam jaringan tersebut, dalam hal ini adalah pihak-pihak yang telah mengetahui kondisi keamanan dan kelemahan dari jaringan tersebut. Gangguan dari luar jaringan adalah gangguan yang berasal dari pihak luar yang ingin mencoba atau dengan sengaja ingin mengetes/menguji keamanan dari luar. Pada tempat yang menjadi studi kasus penulis, terdapat ganguan jaringan dari dalam yantu seorang pengguna yang ingin menjatuhkan kinerja dari jaringan dan melakukan dan melakukan pengujian ketahanan terhadap sistem keamanan yang terdapat pada tempat penelitian penulis. Sistem dapat mendeteksi gangguan dari yang telah dipaparkan diatas memang telah banyak dibuat, tetapi sistem yang mampu melakukan pendeteksi layaknya manusia serta mempelajari kondisi yang ada. Keamanan jaringan bergantung pada kecepatan pengaturan jaringan atau koneksi yang cepat, dalam menindak lanjuti sistem pada saat terjadi gangguan. Salah satu komponen dari jaringan komputer yang perlu dikelolah dengan menggunakan manejemen jaringan adalah *Intrusion Detection System* (IDS). Penerapan IDS diusulkan sebagai salah satu solusi yang dapat digunakan untuk membanti pengaturan jaringan untuk memantau kondisi jaringan dan menganalisa paket-paket berbahaya yang terdapat dalam

jaringan tersebut. IDS diterapkan karena mampu mendeteksi paket-paket berbahaya pada pada jaringan pada jaringan dan langsung memberikan peringatan kepada administrator jaringan tentang kondisi jaringan saat itu. Sudah terdapat banyak software IDS seperti snort yang merupakan *open source* IDS yang juga di gunakan dalam penelitian khususnya untuk mendeteksi serangan ataupun penyusupan. Oleh karena itu pada hotspotkota diusulkan untuk membuat sistem IDS yang diharapkan dapat membantu administrator dalam memonitoring kondisi jaringannya serta meningkatkan kinerja jaringan tersebut [1].

### 1.1 Rumusan Masalah

Dengan didasari oleh latar belakang permasalahan di atas, maka permasalahan penelitian yang akan dibahas pada jaringan Hotspotkota dapat dirumuskan sebagai berikut:

1. Bagaimana cara kerja snort?
2. Intrusion seperti apa yang ditampilkan snort?

### 1.2 Tujuan Penelitian

Tujuan penelitian yang ingin dicapai dari peneliatian ini adalah sebagai berikut :

1. Membantu para *administrator* dalam pengawasan jaringan komputer.
2. Memberikan informasi yang akurat tentang intrusion yang dideteksi.

### 2. Penelitian terkait

Dalam melakukan penelitian ini, peneliti juga mempelajari penelitian-penelitian terdahulu yang dapat dijadikan sebagai bahan acuan penelitian serta perbandingan dengan sistem yang akan dibangun. Adapun penelitian yang terkait atara lain:

1. Penerapan *Aesy Intrusion Detection Systen* (Easyids) Sebagai Pemberi Peringatan Dini Kepada Administrator Sistem Jaringan Tujuan dari penelitian ini adalah untuk memberikan peringatan dini kepada administrator sistem jaringan dalam mengetahui adanya suatu kekeliruan dalam jaringan, adapun Intrusion detection system yang digunakan adalah snort. Kemudian metode pengumpulan data didapat dari bergai sumber dan menggunakan NDLC (Network Development Life Cycle) sebagai metode pengembangan sistem.

2. *Implementasi Intrusion Detection System* (IDS) menggunakan *Snort* pada jaringan Wireless. Tujuan penelitian ini adalah untuk menerapkan keamanan jaringan pada hotspotkota khususnya, memonitoring keamanan, jaringan internet di pada object penelitian khususnya pada hotspot kota memahami kelebihan dan kekurangan IDS pada wireless serta mengetahui serangan yang terjadi didalam jaringan sehingga dapat dilakukan pendeteksian.

Adapun metodelogi data yang di gunakan dalam penelitian ini adalah dengan cara melakukan pengambilan data-data traffic jaringan hotspotkota serta membaca sumber-sumber ilmiah dari buku dan internet sebagai referensi, melakukan observasi langsung serta studi literatur dengan mempelajari dan membaca hasil laporan penelitian yang behubungan dengan topik penelitian. jenis penelitian ini adalah penelitian ekperimental dalam keamanan jaringan. Metode mengembangan sistem yang digunakan dalam penelitian ini adalah SDLC (Security Policy Development Life Cycle.

1. Implementasi *Intrusion Detection System* Untuk *filtering* Paket Data adapun tujuan dari penelitian ini adalah menerapkan konsep yang digunakan dalam *experiment*) dan penelitian lapangan (*field experiment*).
2. Melakukan analisis dan mencari bukti dari percobaan intrusion deteksi sistem pada jaringan hotspotkota, menemukan usaha-usaha tidak sah untuk mengakses resource komputer seseorang dan untuk mengetahui serangan yang terjadi didalam jaringan sehingga dapat melakukan pendeteksian. Metode pengembangan sistem yang dugunakan dalam penelitian adalah NDLC (*Network Development Life Cycle*).
3. Penerapan *Network Intrusion Detection System* yang akan Menggunakan Snort pada Hotspotkota. Tujuan penelitian yang ingin dicapai dari peneliatian ini adalah untuk membantu *administrator* dalam pengawasan jaringan, memberikan informasi yang tepat dan cepat mengenai serangan dan ancaman kepada administrator. Manfaat yang diperoleh dari penelitian ini, administrator akan terbantu oleh sistem dalam pengawasan jaringan, sehingga tidak akan timbul masalah administrator sedang berada di luar kota. Informasi yang diterima oleh administrator dapat menjadi bahan pertimbangan dalam melakukan perbaikan keamanan jaringan, adapun metode

Tabel1 Penelitian Terkait

| No | Judul | Metode | Teknik simulation |
|---|---|---|---|
| 1 | Penerapan *Aesy Intrusion Detection System* (easyids) Sebagai Pemberi Peringatan Dini Kepada Administrator Sistem Jaringa. Imam Susanto, 2011. | 1. Metode pengembangan sistem<br>2. Pembuatan IDS | 1. Simulasi *prototype* |
| 2 | *Implementasi Intrusion Detection System* (IDS) menggunakan *Snort* pada jaringan Wireless. Lidia Putri, 2011. | 1. Jenis penelitian<br>2. Pembuatan IDS | 1. Metode Pengembangan sistem |
| 3 | Implementasi Intrusion Detection System Untukfiltering Paket Data | 1. Teknik Pengumpulan data<br>2. Metode pengembangan sistem | 1. Simulasi jaringan |
| 4 | Penerapan Network Intrusion Detection System Menggunakan Snort pada Hotspotkota | Sistem pendeteksi | Tidak menggunakan simulasi |

pengembangan system yang digunakan adalah

NDSC (Network Development Security Cycle).[2]

**3.1 Intrusion Detection System (IDS)**

Menurut Juntono Gondohandijo IDS (*Intrusion Detection System*) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. *Intrusion detection system* (IDS) secara khusus berfungsi sebagai proteksi secara keseluruhan dari sistem yang telah diinstall *intrusion detection system* (IDS) yang berfungsi untuk memberikan peringatan dini kepada administrator jaringan bahwa terjadi kejanggalan dalam lalulintas jaringan yang tidak sesuai dengan aturan[3].

**3.2 Fungsi Intrusion Detection System (IDS)**

Menurut Ariyus (2007:31) Beberapa alasan untuk memperoleh dan menggunakan *intrusion detection system* (IDS) diantaranya:

1. Mencegah resiko keamanan yang terus meningkat, karena banyak ditemukan kegiatan ilegal yang diperbuat oleh orang-orang yang tidak bertanggung jawab dan hukuman yang diberikan atas kegiatan tersebut.
2. Mendeteksi serangan dan pelanggaran keamanan sistem jaringan yang tidak bisa dicegah oleh sistem, seperti *firewall.*
3. Mendeteksi serangan awal, penyerang akan menyerang suatu sistem yang biasaya melakukan langkah-langkah awal yang mudah diketahui yaitu dengan melakukan penyelidikan atau menguji sistem jaringan yang akan menjadi target, untuk mendapatkan titik-titik dimana mereka akan masuk.
4. Mengamankan file yang keluar dari jaringan.
5. Sebagai pengendali untuk merancang keamanan terutama bagi perusahaan yang besar.
6. Menyediakan informasi yang akurat tehadap gangguan seracara langsung, meningkatkan diagnosis, recovery, dan mengoreksi faktor-faktor penyebab suatu serangan yang ada pada jaringan tersebut.

**2.2.1 Peranan *Intrusion Detection System* (IDS)**

Menurut Ariyus (2007:34) *Intrusion detection system* juga memiliki peranan penting untuk mendapatkan arsitektur *defence-in-depth* (pertahanan yang mendalam) dengan melindungi akses

jaringan internal, sebagai tambahan dari *paramete defence*, hal yang dilakukan *intrusion detection system* (IDS) pada jaringan *internal* adalah sebagai berikut:

Memonitoring akses *database*, ketika mempertimbangkan pemilihan kandidat untuk menyimpan data, suatu perusahaan akan memilih database sebagai solusi untuk menyimpan data-data yang berharga.

1. Melindungi *e-mail server*, *intrusion detection system* (IDS) juga befungsi untuk mendeteksi virus *e-mail* seperti QAZ, *Wom, NAVIDAD Worm*, dan versi terbaru dari *ExploreZip*.
2. Memonitor policy system, jika ada pelanggaran terhadap *policy security* maka *intrusion detection system* (IDS) akan memberi tahukan bahwa telah terjadi sesuatu yang tidak sesuai dengan aturan yang ada.

### 2.2.2 Jenis-Jenis *Intrusion Detection System* (IDS)

Menurut Ariyus (2007:36) Pada dasarnya terdapat tiga macam intrusion detection system (IDS), yaitu:

1. *Network based Intrusion Detection System* (NIDS). Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. NIDS umumnya terletak di dalam segmen jaringan penting di mana server berada atau terdapat pada "pintu masuk" jaringan. Kelemahan NIDS adalah bahwa NIDS agak rumit diimplementasikan dalam sebuah jaringan yang menggunakan *switch Ethernet*, meskipun beberapa vendor *switch Ethernet* sekarang telah menerapkan fungsi IDS di dalam *switch* buatannya untuk memonitor *port* atau koneksi.
2. *Host based Intrusion Detection System* (HIDS): Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya firewall, web server, atau server yang terkoneksi ke Internet.
3. *Distributed Intrusion Detection System* (DIDS). Sekumpulan sensor IDS yang saling terhubung satu sama lain dan berfungsi sebagai remotet sensor (sensor jarak jauh) yang memberikann informasi pelaporan-pelaporan pada suatu jaringan *Distributed Intrusion Detection System* yang di gunakan pada manajemen sistem

terpusat. Dari jenis-jenis IDS tersebut, sistem IDS yang digunakan adalah yang berbasis pada jaringan (*Network-Based*) untuk memantau paket-paket data yang berjalan didalam jaringan. Snort merupakan aplikasi yang dapat digunakan pada tingkat network, karena cara kerja snort hampir sama dengan alarm yaitu memberitahukan adanya penyusup yang akan masuk kejaringan[6].

**2.2.3 Transmission Control Protocol/Internet Protocol (TCP/IP)**

Menurut S'to (2014:41) TCP/IP merupakan singkatan dari *Transmission Control Protocol/Internet Protocol* merupakan protokol utama yang digunakan dalam jaringan internet dan juga didalam jaringan Local Area Network (LAN) saat ini.[5]

Pada awalnya TCP/IP diciptakan khusus untuk komunikasi jaringan DARPA. TCP/IP kemudian digunakan sebagai protokol jaringan yang digunakan oleh distribusi Berkeley Software yaitu UNIX. Tetapi sekarang TCP/IP menjadi standart de facto untuk komunikasi internetwork, server, dan protokol transportasi bagi internet yang menjadikan jutaan komputer dapat berkomunikasi secara global.

Pada dasarnya, komunikasi data merupakan proses mengirimkan dara dari satu komputer ke komputer lain. Unutk mengirimkan data, pada komputer harus ditambahkan alat khusus, yang dikenala sebagai *network interface*. Untuk dapat mengirimkan data, ada hal yang harus diperhatikan untuk sampainya data ketujuan, salah satunya dengan menggunakan TCP/IP sebagai protokol yang menjadi identitas pada setiap komputer. (Purbo, 1998:21)

**2.5 Snort**

**2.5.1 Definisi dan Konsep Snort**

Menurut Zico Sweatly Ekel (ASWB:129) *Snort* adalah *open source network intrusion detection system* (NIDS) yang memiliki kemampuan untuk memonitoring paket-paket sekaligus menjadi *security tools* yang berguna untuk mendeteksi berbagai serangan, sebagai contoh ddos, MITM *attack* dll.[4] *Snort* dapat di operasikan dengan tiga mode (Ariyus,2007:146) yaitu:

1. Paket *Sniffer*: untuk melihat paket yang lewat di jaringan.
2. Paket *Logger*: untuk mencatat semua paket yang lewat di jaringan untuk di analisis di kemudian hari.

3. NIDS: pada mode ini snort akan berfungsi untu mendeteksi serangan yang dilakukan melalui jaringan komputer.

**2.5.2 Komponen-Komponen Snort**

Menurut Slameto (2007:7) komponen-komponen snort meliputi:

1. *Rule Snort*

Merupakan *database* yang berisi pola-pola serangan berupa s*ignature* jenis-jenis serangan. *Rule snort* IDS ini, harus di*update* secara rutin agar ketika ada suatu teknik serangan yang baru.

2. *Snort Engine*

Merupakan program yang berjalan sebagian proses yang selalu bekerja untuk membaca paket data dan kemudian membandingkannya dengan *rule snort*.

3. *Alert*

Merupakan catatan serangan pada deteksi penyusupan. Untuk kebutuhan analisa, alert dapat disimpan dalam database, sebagai contoh ACID (*Analysis Console for Intrusion Database*) sebagai modul tambahan pada *snort.*

## 2.6 MySql

Menurut Diar Puji Oktavian (2010:63) MySql adalah sebuah program *database client-server* yang berbasikan *console,* berupa kode-kode/teks.

MySQL adalah *Relational Database Management System* (RDBMS) yang di distribusikan secara gratis dibawah lisensi GPL (*General Public License*). Dimana setiap orang bebas untuk menggunakan MySQL, namun tidak boleh dijadikan produk turunan yang bersifat komersial. MySQL sebenarnya merupakan turunan salah satu konsep utama dalam database sejak lama, yaitu SQL (*Structured Query Language*). SQL adalah sebuah konsep pengoperasian database, terutama untuk pemilihan atau seleksi dan pemasukan data, yang memungkinkan pengoperasian data dikerjakan dengan mudah secara otomatis.

## 2.7 Keamanan Jaringan

Definisi keamanan jaringan menurut Cheng Min yaitu “Keamanan jaringan berarti data-data yang berada pada perangkat keras dan perangkat lunak dalam sistem jaringan dilindungi dari tindakan-tindakan yang bersifat jahat atau kerusakan akibat ecelakaan, modifikasi dan hal-hal yang bersifat membocorkan data tersebut ke pihak lain, untuk memastikan sistem akan berjalan secara konsisten dan handal dan tanpa adanya gangguan pada sistem tersebut .

### 2.7.1 Ancaman Keamanan Jaringan

Beberapa ancaman dalam dunia jaringa komputer :

1. *Leakage* (Kebocoran)

   Pengambilan informasi oleh penerima yang tidak berhak

2. *Tampering*

   Pengubahan informasi yang tidak legal

3. *Vandalisme* (perusakan)

Gangguan operasi sistem tertentu. Pelaku tidak mengharap keuntungan apapun.

4. Serangan pada sistem terdistribusi tergantung pada pengaksesan kesaluran komunikasi yang ada atau membuat saluran baru yang menyamarkan (masquerade) sebagai koneksi legal.
5. Penyerangan pasif yang hanya mengamati komunikasi atau aliran data.
6. Penyerangan Aktif yang secara aktif memodifikasi komunikasi atau data.
7. Pemalsuan atau pengubahan Email
8. TCP/IP *Spoofin*

### 2.7.2 Jenis-jenis Serangan

Terdapat beberapa jenis serang yang sering dilakukan oleh hacker pada jaringan komputer, diantaranya:

1. *Password attack*

   Serangan berbentuk pembobolan password sering dilakukan oleh para peretas jaringan demi mengetahui informasi yang tersembunyi dibalik password tersebut.

2. *Malicious Code*

   Biasanya berupa virus, trojan ataupun worm, yang bentuknya berupa kode-kode instruksi yang berfungsi untuk memberatkan sebuah sistem agar performansi dari sistem tersebut berangsur-angsur menurun.

3. *Sniffer*

   Adalah sebuah perangkat (baik perangkat keras maupun perangkat lunak) yang berfungsi untuk melakukan penyadapan data-data pada komunikasi di jaringan komputer dengan memanfaatkan mode premicious pada ethernet card.

4. *Scanner*

Merupakan suatu program yang didesain untuk menemukan layanan-layanan (*services*) apa saja yang berjalan pada *host* di suatu jaringan komputer. atau bisa juga disebut sebagai perangkat yang berfungsi untuk memberikan informasi-informasi penting mengenai sasaran (target) yang dituju, misalnya sistem operasi yang dipergunakan, IP *host* tersebut, layanan jaringan yang aktif, jenis mesin yang terhubung kejaringan, serta konfigurasi jaringannya.

5. *Spoofing*

Adalah suatu teknik untuk melakukan penyamaran agar terdeteksi sebagai dentitas asli dari host yang benar-benar sudah terdaftar pada sistem tersebut padahal sebenarnya dia tidak terdaftar.

6. *Denial of Service*

Merupakan sebuah serangan dengan cara membanjiri saluran pada jaringan komputer dengan banyaknya permintaan (*request*) sebuah pesan tertentu agar menggagalkan pengguna lain untuk mengakses sistem dijaringan komputer tersebut. biasanya serangan ini dapat dijalankan ketika mesin penyerang lebih kuat di bandingkan dengan targetnya.

**2.7.3 Analisis Sistem**

Metode analisa yang digunakan dalam penelitian ini adalah metode analisa komperatif. Metode komperatif adalah medote penelitian yang sifatnya membadingkan dua hal yang berbeda, misalnya sistem lama yang diteliti dengan sistem baru yang akan dirancang. Dua hal yang berbeda yang akan dibandingkan adalah sistem lama yang diteliti dan sistem baru yang dibuat oleh peneliti. Dalam penelitian ini peneliti berusaha mencocokkan masalah dengan menerapkan sistem deteksi pada jaringan internal menggunakan snort.

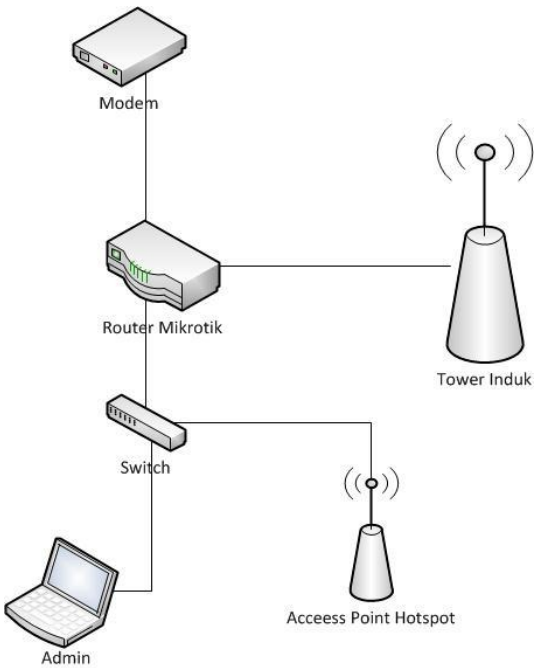
Penerapan snort dilakukan berdasarkan data yang akan diperoleh peneliti dari admin Hotspotkota untuk menemukan solusi dari permasalahan yang ada, kemudian akan dibandingkan dengan toeri lain yang diproleh dari studi pustaka dan berbagai literature kemudian ditarik kesimpulan. Langkah-langkah teknik analisa yang digunakan pada penelitian ini adalah sebagai berikut:

1. Mengidentifikasi dan merumuskan permasalahan yang ada pada jaringan Hotspotkota.
2. Mengumpulkan data yang berhubungan dengan snort dan metode deteksi.
3. Mengevaluasi sebuah sistem deteksi menggunakan snort yang diproleh dari studi pustaka.

**2.7.3 Jaringan yang ada**

Analisa jaringan yang ada bertujuan untuk menjelaskan sistem yang ada secara lengkap. Pada tahap ini penulis dapat melakukan identifikasi terhadap jaringan yang tealah berjalan dan diperoleh beberapa gambaran bahwa sistem yang ada saat ini masih di temukan kekurangannya[9].

dalam sebuah analisa jaringan yang ada bertujuan untuk menjelaskan sistem yang ada secara lengkap. Pada tahap ini penulis dapat melakukan identifikasi terhadap jaringan yang tealah berjalan dan diperoleh beberapa gambaran bahwa sistem yang ada saat ini masih di temukan kekurangan seperti yang telah di jabarkan pada latar belakang penulisan. Berdasarkan uraian tersebut maka penulis dapat menggambarkan jaringan yang ada sebagai berikut:




Gambar 1 Topologi jaringan yang ada

**3. Metode Yang Di Usulkan**

Metode Pengembangan Sistem menggunakan NDLC (*Network Development Life Cycle*) Menurut (Goldman et all, 2001), NDLC adalah kunci dibalik proses perancangan jaringan komputer. Salah satu metode NDLC merupakan model mendefinisikan siklus proses pembangunan atau pengembangan sistem jaringan komputer. kata *cycle* (siklus) adalah kata kunci deskriptif dari siklus hidup pengembangan sistem jaringan yang menggambarkan secara eksplisit seluruh proses dan tahapan pengembangan sistem jaringan yang berkesinambungan. Dalam hal ini metode pengembangan sistem yang digunakan adalah *Network Development Life Cycle* (NDLC). Berikut penerapanya dari setiap tahap NDLC adalah sebagai berikut :

1. Analysis : Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan seorang *user*, dan analisa topologi/jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya :
   a. Wawancara, dilakukan dengan pihak terkait melibatkan dari struktur manajemen atas sampai ke *level* bawah/*operator* agar mendapatkan data yang konkrit dan lengkap. Pada kasus di *Computer Engineering* biasanya juga melakukan *brainstorming* juga dari pihak vendor untuk solusi yang ditawarkan dari vendor tersebut karena setiap mempunyai karakteristik yang berbeda.
   b. *Survey* langsung kelapangan, pada tahap analisis juga biasanya dilakukan *survey* langsung kelapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya

sebelum masuk ke tahap *design, survey* biasa dilengkapi dengan alat ukur seperti GPS dan alat lain sesuai kebutuhan untuk mengetahui detail yang dilakukan.

c. Membaca *manual* atau *blueprint* dokumentasi, pada *analysis* awal ini juga dilakukan dengan mencari informasi dari *manual-manual* atau *blueprint* dokumentasi yang mungkin pernah dibuat sebelumnya. Sudah menjadi keharusan dalam setiap pengembangan suatu sistem dokumentasi menjadi pendukung akhir dari pengembangan tersebut, begitu juga pada *project network*, dokumentasi menjadi syarat mutlak setelah sistem selesai dibangun.

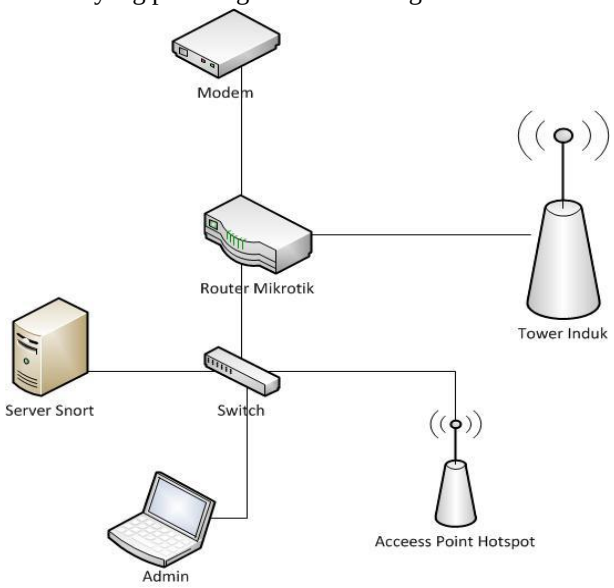
d. berdasarkan setiap data yang didapatkan dari sumber data-data sebelumnya, maka perlu dilakukan analisa data tersebut untuk masuk ke tahap berikutnya. Adapun yang bisa menjadi pedoman dalam mencari data pada tahap *analysis* ini adalah :

1. *User/ people* : jumlah *user,* kegiatan yang sering dilakukan, peta politik yang ada, *level* teknis *user*.
2. Media H/W & S/W : peralatan yang ada, status jaringan, ketersedian data yang dapat diakses dari peralatan, aplikasi s/w yang digunakan.
3. Data : jumlah pelanggan, jumlah inventaris sistem, sistem keamanan yang sudah ada dalam mengamankan data.
4. *Network* : konfigurasi jaringan, *volume* trafik jaringan, *protocol*, *monitoring network* yang ada saat ini, harapan dan rencana pengembangan kedepan.
5. Perencanaan fisik : masalah listrik, tata letak, ruang khusus, sistem keamanan yang ada, dan kemungkinan akan pengembangan kedepan.

2. Design : dari data-data yang didapatkan sebelumnya, tahap *Design* ini akan membuat gambar *design topology* jaringan interkoneksi yang akan dibangun, diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. *Design* bisa berupa *design struktur topology, design* akses data*, design tata layout* perkabelan*,* serta dapat memberikan gambaran jelas tentang *project* yang akan dibangun. Biasanya hasil dari *design* berupa

a. gambar-gambar *topology (server farm, firewall, datacenter, storages, lastmiles*, perkabelan, titik akses dan sebagainya).
b. gambar-gambar *detailed* estimasi kebutuhan data yang ada.

dengan menggunakan sebuah server yang telah diinstal aplikasi snort untuk mendeteksi intrusion yang dianggap mengganggu keamanan dan kinerja jaringan, yang diharapkan mampu mengatasi permasalahan yang ada, berikut ini adalah topologi jaringan yang penulis gambarkan sebagai usulan:

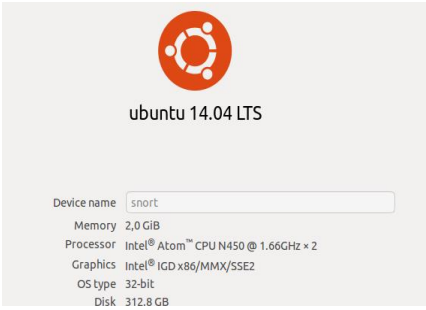



Gambar 2 Topologi jaringan yang diusulka**n**

**4.0 Kebutuhan Hardware**

Hardware atau perangkat keras yang dibutuhakan dalam merancang dan menerapkan sistem deteksi dengan snort adalah sebagai berikut:

1. PC (Personal Computer)
2. Kabel UTP (Unshielded Twisted Pair)



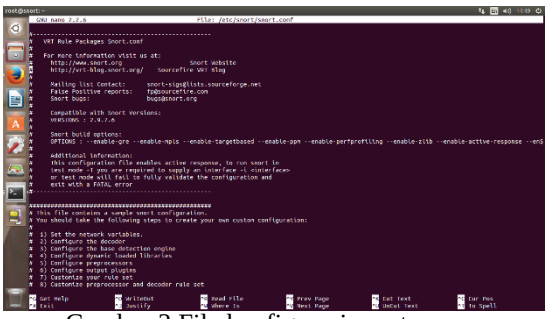

Gambar 4. Spesifikasi komputer yang digunakan untuk menginstal snort

Software atau perangkat lunak yang dibutuhakan untuk menjalankan snort sebagai pedeteksi adalah sebagai berikut:

1. Ubuntu 14.04 LTS
2. Snort
3. Putty
4. Browser
5. Ping

### 4.4.2 Konfigurasi Snort

Pada tahap ini penulis menampilkan file yang dimana file snort.conf yang merupakan file konfigurasi snort, yang mana merupakan suatu tempat untuk mengaktifkan snort sebagai NIDS (*Network Intrusion detection system*) berikut tampilan filenya menggunakan editor *nano*:



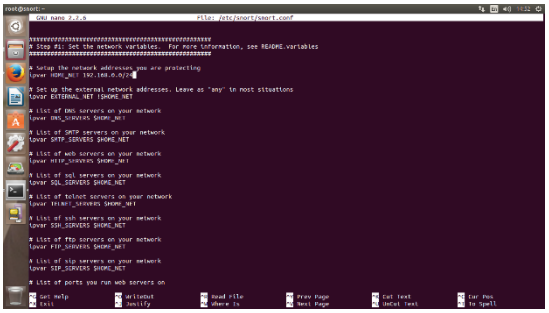
Gambar 3 File konfigurasi snort.

Pada tahap ini penulis melakukan konfigurasi ip address network pada server snort agar dapat medeteksi lalulintas data di lalu pada address tersebut[7].

ipvar HOME_NET 10.0.0.0/24
ipvar EXTERNAL_NET !$HOME_NET

var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules

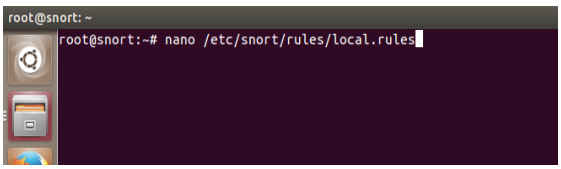


Gambar 5 konfigurasi ip address network

Pada tahap ini penulis telah selesai melakukan konfigurasi pada server snort dan mencoba menjalankan snort dengan printah snort –V[8]:


Gambar 6 Menampilkan versi snort Ver. 2.9.7.6

Agar server snort dapat mendeteksi jenis intrusi tertentu maka penulis menambahkan sebuah rules yang di letak di direktory /etc/snort/rules/:

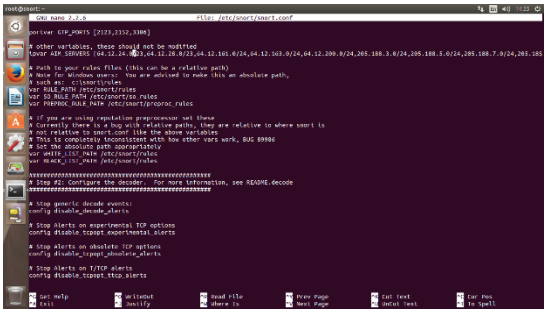



Gambar 8 Konfigurasi rules local snort

Pada tahap ini penulis mengambil sampel rules ping yang nantinya semua user/client yang melakukan perintah ping ke server snort akan terdeteksi. Berikut ini sampel rulesnya:

alert icmp any any -> any any (msg:"Sedang terjadi percobaan ICMP"; sid: 10001;)
alert tcp any any <> any 22 (msg: "seseorang melakukan remot ssh dari port 22"; sid: 1000000;)
alert tcp any any <> any 80 (msg: "Sedang terjadi aktifitas yang berjalan di port 80"; sid:1000002;)
alert icmp any any -> any any (msg:"Warning! terjadi percobaan Ping of Death"; dsize:>1500;sid:3000003;rev:1;)

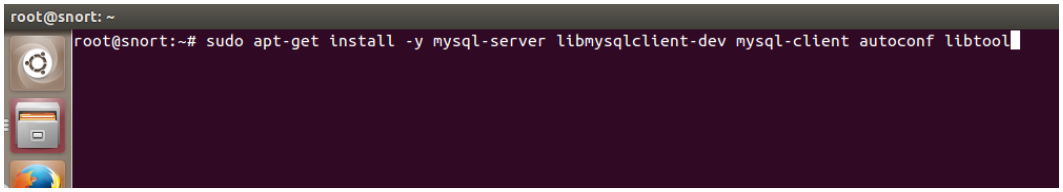
Pada tahap ini penulis mengaktifkan rules yang telah di konfigurasi agar dapat membaca intrusi sesuai dengan rules yang telah di set.



Gambar 7 Mengaktifkan snort

### 4.4.3 Konfigurasi BASE/Mysql

Untuk menitoring snort via web dan melihat data log yg tersimpan di database penulis menambahkan aplikasi mysql seperti pada gambar berikut:




Gambar 9 install base dan mysql

Pada tahap ini penulis mengkoneksikan base ke mysql seperi pada gambar berikut ini:

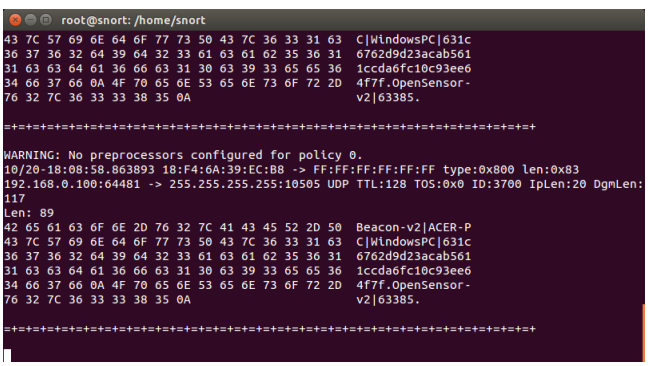
```
$BASE_urlpath = '/base';
$DBlib_path = '/var/adodb/';
$alert_dbname   = 'snort';
$alert_host     = 'localhost';
$alert_port     = '';
$alert_user     = 'snort';
$alert_password = 'rahasia';
```

### 4.4.4 Hasil Pengujian

Untuk pengujian dilakukan dari sisi attacker dan server snort. Dalam pengujian pertama attacker akan mencoba melakukan manufer tarhadap jaringan dan kemudian di deteksi oleh server snort dan snort akan menampilkan informasi hasil deteksi [10].

### 4.4.1 Percobaan *Snort*

Berikut ini adalah tampilan snort yang telah mendeteksi traffic jaringan dengan mode sniffer.




Gambar 10 Testing snort mode sniffer

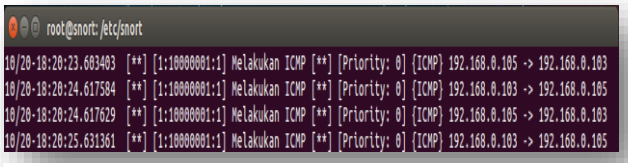
Tabel 2 Daftar Hasil Pengujian Mode Sniffer

| Waktu | Ip Address | Hasil |
|---|---|---|
| 18:08 | 192.168.0.105 | Breacon-v2\|ACER-PC\|WindowsPC\|631c6762d9d23acab561iccda6f10c93ee64f7f-Opensensorv2\|63385 |

### 4.4.2 Percobaan *Ping*

Pada tahap ini penulis mencoba melakukan testing ping ke komputer server dan secara otomatis snort menampilakan suatu pesan bahwa terdapat percobaan ICMP dari 192.168.0.103 sampai dengan ip address 192.168.0.105. berikut hasilnya:

Berikut ini adalah sampel pesan yang ditampilkan




Gambar 9 sampel pesan yg di tampilkan oleh snort

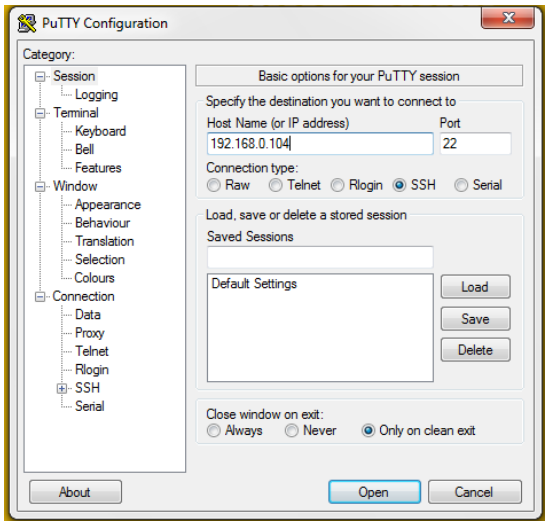
oleh snort yang penulis sederhanakan melalui table 3 pengujian ping.

Tabel 3 Hasil pengujian *ping*

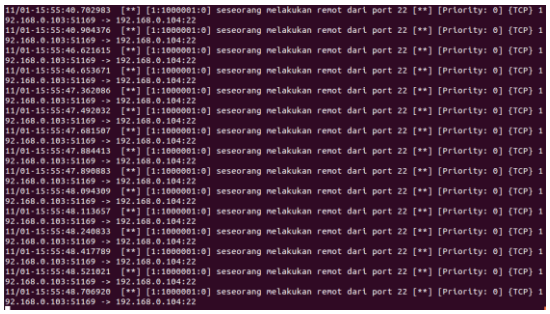
| Waktu | Ip User | Attacker | Intrusi |
|---|---|---|---|
| 18:20 | 192.168.0.103 | 192.168.0.105 | Melakukan ping |
| 18:20 | 192.168.0.103 | 192.168.0.105 | Merespon Ping |

### 4.4.3 Percobaan Remot SSH

Pada tahap ini penulis pada tahap ini penulis melakukan pengujian dengan mencoba melakukan remot ssh menggunakan aplikasi *putty*.




Gambar 11 Menggunakan Aplikasi Putty



Gambar 12 Hasil intrusion remot ssh

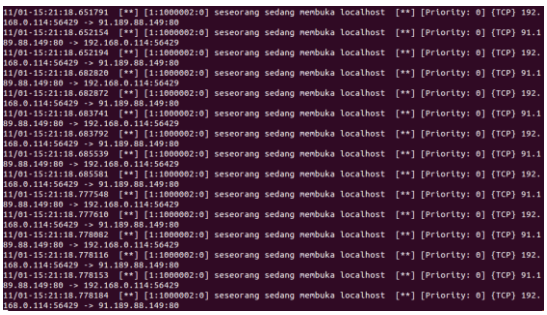
Tabel 5 Hasil pengujian remot ssh

| Waktu | Ip User | Attacker | Intrusi |
|---|---|---|---|
| 15:55 | 192.168.0.103 | 192.168.0.104 | Sesesorang melakukan remot dari port 22 |
| 18:20 | 192.168.0.103 | 192.168.0.104 | Sesesorang melakukan remot dari port 22 |

Berdasarkan pada tabel 5 hasil pengujian Ssh diatas menunjukan proses estimasi waktu, ip, attacker penyerangan serta intrusi port-port apa yang melakukan remot akses pada komputer target[11].

### 4.4.3 Percobaan Port 80

Pada tahap ini penulis melakukan pengujian mengakses localhost yang terinstall pada pc server.



Gambar 4.9 Intrusi pengujian port 80

Tabel 4 Hasil pengujian port 80

| Waktu | Ip User | Attacker | Intrusi |
|---|---|---|---|
| 15:21 | 192.168.0.103 | 192.168.0.104 | Sesesorang sedang membuka localhost |
| 18:21 | 192.168.0.103 | 192.168.0.104 | Sesesorang sedang membuka localhost |

## 4. Kesimpulan

Berdasarkan hasil evaluasi implementasi sistem pada jaringan internal hotspotkota, maka dapat ditarik beberapa kesimpulan sebagai berikut:

1.Sistem NIDS (Network Detection System) yang diterapkan telah berhasil dibangun dengan baik dan keseluruhan sistem NIDS dapat bekerja dengan baik sebagai sistem pendeteksi intrusion pada jaringan.

2.Mekanisme sistem kerja snort dan Base yang telah diimplementasikan dengan baik. Dalam pengujian sistem snort ping attack dan remot ssh.

3.Kelebihan dalam menggunakan NIDS ini adalah suatu jaringan komputer dapat di pantau hanya dengan sebuah mesin yang dapat memonitoring jaringan secara real time dan suatu saat dapat di analisa.

## Reference

[1] Ariyus, Dony. 2007. *Intrusion detection system*, Yogyakarta:ANDI.

[2] Dietrich, Noah. 2015. *Snort 2.9.7.x on Ubuntu 12 and 14 with Barnyard2, PulledPork, and BASE*.http://sublimerobots.com/2014/12/instali

ng-snort-part-1/(diakses pada tanggal 20 Oktober 2015.

[3] http://www.securityarchitecture.com/learning/intrusion-detection-systems-learningwith snort/creating-a-linux-virtual-machine/ (diakses pada tanggal 19 Oktober 2015)

[4] *(manual.snort.org/node15.html (diakses pada tanggal 19 oktober 2015)*

[5] Purbo, W. Ono 2006. *Buku Pinter Internet TCP/IP*. PT. Elex Media Komputindo. Jakarta

[6] Putri, Lidia. 2011. *Implementasi Intrusion Detection System*. Universitas Islam Negeri Starif Hidayatullah Jakarta.

[7] Satria. Muhammad Nugraha. 2010. *Implementasi Intrusion Detection System Untuk Filtering Paket Data*. Universitas Islam Negeri Starif Hidayatullah Jakarta.

[8] S'To 2014. *Network+ 100% Illegal*. Jasakom.

[9] S'To 2013. *Backtrack 5 R3.100% Attack*. Jasakom

[10] S'To 2009. *Certified Ethical Hacker (CEH) 100% illegal*. Jasakom

[11] S'To 2009. *Certified Ethical Hacker (CEH) 200% illegal*. Jasakom