NARATIF(Jurnal Ilmiah Nasional Riset Aplikasi dan Teknik Informatika)
Vol. 03 No. 02 Desember 2021
P-ISSN: 2656-7377 || E-ISSN: 2714-8467

PERANCANGAN DAN IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN *SNORT* SEBAGAI *INTRUSION PREVENTION SYSTEM (IPS)* PADA JARINGAN INTERNET STEI ITB

Hendi Suhendi[1], Wahyu Dwi Cahyo[2]
Program Studi Teknik Informatika[1,2]
ARS University[1,2]
hendi2708@ars.ac.id[1], dwicahyo1429@gmail.com[2]

Abstrak

Snort merupakan salah satu sistem pendeteksi penyusupan (*Intrusion Detection System/IDS*) yang *open source* dan banyak digunakan oleh administrator jaringan sebagai sistem untuk memonitor jaringan serta sebagai pendeteksi adanya serangan penyusupan pada pada jaringan. Fungsi *Snort* sebagai sistem pendeteksi penyusupan dapat dikembangkan menjadi sebuah sistem pencegah penyusupan (*Intrusion Prevention System/IPS*) dengan mengaktifkan snort pada mode inline dengan *Data Aquisition* (DAQ). *Data Aquitsition* (DAQ) adalah sebuah modul yang di dalamnya terdapat skema penangkapan paket dari suatu *interface*. *Snort* mengidentifikasi paket data tersebut sebagai sebuah penyusupan karena pola paket data tersebut sama dengan pola rule Snort yang mendefinisikan sebagai sebuah penyusupan. Log dari pendeteksian penyusupan tersebut disimpan sebagai alert. Dalam tugas akhir ini, penulis akan mengkonfigurasi sistem pencegah penyusupan (*Intrusion Prevention System/IPS*) dengan menjalankan *Snort* pada mode *inline* menggunakan *DAQ AFPACKET* pada sistem operasi Linux Ubuntu. Alasan pemilihan Linux Ubuntu sebagai sistem operasi pada konfigurasi sistem pencegah penyusupan ini karena Ubuntu merupakan sistem operasi Linux yang mudah digunakan dan dikembangkan sesuai dari keinginan penggunanya.
Kata Kunci: *Intrusion Detection System, Intrusion Prevention System, Linux, Ubuntu, Snort*.

Abstract

Snort is an intrusion detection system (Intrusion Detection System / IDS) is open source and widely used by the network as a system administrator to monitor the network as well as the detection of incursions on the network. The function of Snort as an intrusion detection system can be developed into an intrusion prevention system (Intrusion Prevention System / IPS) to enable Snort in inline mode with Data Aquisition (DAQ). Data Aquitsition (DAQ) is a module in which there are schemes arrest of an interface package. Snort identify the data packet as an intrusion because of the pattern of the data packets similar to the pattern that defines the Snort rule as an intrusion. Logs from the intrusion detection saved as alerts. In this thesis, the author will configure intrusion prevention system (Intrusion Prevention System / IPS) by running Snort in inline mode using the DAQ AFPACKET on Ubuntu Linux operating system. The reason of choosing Ubuntu Linux as the operating system on intrusion prevention system configuration is because Ubuntu is a Linux operating system that is easy to use and developed in accordance of the wishes of its users
Keywords : Intrusion Detection System, Intrusion Prevention System, Linux, Ubuntu, Snort.

I. PENDAHULUAN

Perkembangan teknologi pada era globalisasi telah berkembang begitu pesat. Hal ini bisa di rasakan dengan semakin banyaknya penemuan sistem baru yang berbasiskan teknologi informasi. Selain kinerja suatu sistem dapat meningkat, teknologi informasi juga menawarkan suatu kemudahan dalam mengelola dan menjalankan sistem tersebut. Berkembangnya teknologi informasi saat ini berdampak pada penggunaan koneksi *internet* yang semakin luas. Koneksi internet menjadi hal yang wajib ada dalam kegiatan sehari-hari. Tanpa adanya koneksi *internet*, bagi suatu lembaga atau instansi yang bergerak dalam bidang teknologi informasi, seolah tertinggal dengan kemajuan yang ada saat ini. Dunia *internet* sudah menjadi dunia bagi setiap kalangan untuk mencari sumber ilmu, selain ilmu yang di dapatkan dalam lembaga pendidikan.

Dengan penggunaan *internet* yang semakin luas, isu-isu mengenai keamanan jaringan internet bermunculan dan menjadi masalah baru yang semakin mengkhawatirkan. Hal ini menyebabkan keresahan para pengguna *internet* pada umumnya dan juga meresahkan perusahaan, dan lembaga-lembaga yang bergerak dalam bidang teknologi informasi, karena bisa sewaktu-waktu data yang penting bisa di retas oleh pihak-pihak yang tidak bertanggung jawab. Untuk menjaga kelancaran pengaksesan *internet* suatu perusahaan atau lembaga harus memberikan perhatian khusus pada sistem jaringan *internet* dan keamanannya. Suatu keamanan jaringalotrn internal yang terhubung ke *internet* harus dapat di percaya dan handal untuk melindungi jaringan dan data internal. Masalahnya adalah kebebasan mengakses *internet* membuat seseorang tidak dapat mengontrol diri dan lupa akana apa yang harusnya dikerjakan. Contoh pada jaringan computer sebuah perusahaan itu memungkinkan setiap *client* bebas mengakses situs-situs yang seharusnya tidak boleh diakses pada jam-jam tertentu atau bahkan tidak boleh diakses sama sekali, karena dapat mengganggu proses bisnis dan kinerja karyawan dalam perusahaan tersebut. Dan juga pada jaringan sebesar internet banyak *hacker* / *cracker* yang kita tidak ketahui dari mana datangnya yang dapat mengganggu atau bahkan merusak jaringan, Oleh karena itu di perlukan pemantauan jaringan oleh seorang *administrator* untuk memantau aktifitas jaringan, serta akses data dalam jaringan. Hal ini berguna untuk mencegah adanya ancaman dari luar, dan dapat di antisipasi dan di tangani dengan cepat oleh *administrator*.

Lembaga pendidikan Sekolah Tinggi Elektro dan Informatika (STEI) ITB adalah lembaga pendidikan yang bergerak dalam bidang teknologi informasi dan menggunakan *internet* dalam melakukan kegiatan pendidikan seperti penggunaan email internal, *e-learning*, *FTP (file transfer protocol),* system penilaian, forum mahasiswa dan sebagainya. Akan tetapi ada kalanya terjadi suatu masalah pada jaringan komputer khususnya internet seperti : jaringan *internet* lambat atau *server down* yang di sebabkan oleh hal-hal tidak terduga. Berdasarkan latar belakang tersebut, untuk menangani permasalahan yang ada maka di buatlah suatu sistem keamanan pada jaringan komputer di gedung STEI ITB dengan memasang pendeteksi gangguan jaringan menggunakan *Snort* yang di pasang pada OS *Linux Ubuntu Server 14-04*. Di harapkan dengan adanya sistem keamanan jaringan, proses penyampaian informasi dapat perangkat – perangkat di dalamnya terjaga keamanan dan kerahasiannya serta tetap berjalan sesuai fungsinya masing – masing.

II. TINJAUAN PUSTAKA

1. *Brute Force*

Serangan ini adalah upaya untuk masuk ke dalam jaringan dengan menyerang database password atau menyerang login prompt yang sedang aktif. *Brute force* menggunakan cara yang sistematis dengan mencoba berbagai kombinasi angka, huruf, simbol dan kamus data yang telah didefenisikan terlebih dahulu untuk menemukan password dari account *user*. Pendapat lain mengatakan Serangan brute-force adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin[4]

2. *Denial of Service (DoS)*

DoS adalah salah satu ancaman keamanan jaringan yang membuat suatu layanan jaringan jadi tersendat, serangan yang membuat jaringan tidak bisa diakses atau serangan yang membuat sistem tidak bisa memproses atau merespon permintaan layanan terhadap object dan resource jaringan. Bentuk umum dari serangan DoS ini adalah dengan cara mengirim paket data dalam jumlah yang sangat bersar terhadap suatu server dimana server tersebut tidak bisa memproses semuanya. Bentuk lain dari serangan DoS ini adalah memanfaatkan port-port yang rentan dari sistem operasi. Tidak semua DoS merupakan akibat dari serangan keamanan jaringan. Kesalahan dalam *coding* suatu program juga bisa mengakibatkan kondisi seperti serangan DoS. Ada beberapa jenis dari DoS, antara lain:

a. *Distributed Denial of Service* (DDoS); Terjadi saat penyerang berhasil menggabungkan beberapa layanan sistem dan menggunakannya sebagai pusat untuk menyebarkan serangan terhadap korban.
b. *Distributed Reflective Denial of Service* (DRDoS); Memanfaatkan operasi normal dari layanan internet seperti *protocol-protocol* update DNS dan router. DRDoS ini menyerang fungsi dengan mengirim *update* dalam jumlah yang sangat besar kepada berbagai macam layanan *server* atau *router* dengan menggunakan *address spoofing* kepada target korban.
c. SYN *flooding;* Upaya untuk membanjiri sinyal SYN kepada sistem yang menggunakan *protocol* TCP/IP dalam melakukan inisiasi sesi komunikasi.
d. *Smurf Attack; Server* digunakan untuk membanjiri korban dengan data sampah yang tidak berguna. *Server* atau jaringan yang dipakai menghasilkan *respon* paket yang banyak seperti ICMP ECHO paket atau UDP paket dari satu paket yang dikirim.
e. *Ping of Death;* Dengan menggunakan tool khusus, penyerang dapat mengirimkan paket ping yang *oversize* yang banyak kepada korban. *Ping of death* tidak lebih dari semacam serangan *buffer overflow*. Serangan ini dapat menyebabkan *crash sistem, freeze* atau *reboot*.
f. *Stream Attack;* Serangan ini terjadi saat banyak jumlah paket yang besar dikirim menuju ke *port* pada sistem korban menggunakan sumber nomor yang *random*.

3. Man-in-The-Middle (MiTM) attacking

Serangan ini terjadi saat *attacker* bertindak sebagai perantara diantara dua *node* yang saling berkomunikasi.

4. *Sniffer*

Merupakan kegiatan untuk mendapatkan informasi tentang *traffic* jaringan. Suatu *sniffer* sering merupakan program penagkap paket yang bisa menduplikasikan isi paket yang lewat pada media jaringan ke dalam file. Serangan ini sering difokuskan pada koneksi awal antara *client* dan *server* untuk mendapatkan *account user* dan lainnya.

5. *Spamming*

Spam pada umumnya bukan merupakan serangan keamanan jaringan akan tetapi hampir mirip dengan DoS. *Spam* bisa berupa iklan atau *trojan*. Pendapat lain mengatakan bahwa *spamming* merupakan pengiriman informasi dan komunikasi elektronik untuk menampilkan berita iklan dan keperluan lainnya yang mengakibatkan ketidaknyamanan bagi para pengguna[5].

6. *Scanning*

Scanning terbagi atas tiga jenis, yaitu:

a. *Port Scanning* : merupakan kegiatan scanning yang bertujuan menemukan port-port yang terbuka dari suatu host.
b. *Network Scanning* : merupakan kegiatan *scanning* yang bertujuan menemukan *host* atau komputer yang aktif pada suatu jaringan.
c. *Vulnerability Scanning* : merupakan kegiatan scanning yang bertujuan menemukan kelemahan dari sebuah sistem.

7. *Intrusion Detection System (IDS)*

Intrusion Detection System (IDS) merupakan suatu perangkat lunak atau sistem perangkat keras yang bekerja secara otomatis untuk memonitor kejadian pada jaringan computer dan dapat menganalisa masalah keamanan jaringan. Suatu IDS dapat didefenisikan sebagai *tool*, metode atau sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan komputer. IDS sebenarnya tidak mendeteksi penyusup tetapi hanya mendeteksi aktivitas *traffic* jaringan yang tidak layak terjadi sehingga awal dari langkah kerja penyerang(bisa diketahui. Dengan demikian *network administrator* dapat melakukan tindakan pencegahan dan bersiap atas kemungkinan serangan yang akan terjadi. [1]

Ada 2 jenis IDS, yaitu *Host Based Intrusion Detection System (HIDS)* dan *Network Based Intrusion Detection System (NIDS).*

a. *Host Intrusion Detection System (HIDS);* HIDS bekerja pada host yang akan dilindungi. IDS jenis ini dappat melakukan berbagai macam tugas untuk mendeteksi serangan yang dilakukan pada host tersebut. Keunggulan HIDS adalah tugas-tugas yang berhubungan dengan keamanan file. Misalnya ada tidaknya file yang telah diubah atau ada usaha untuk mendapatkan akses ke file-file yang sensitif.
b. *Network Intrusion Detection System (NIDS);* Digunakan untuk melakukan monitoring di seluruh segmen jaringan. NIDS akan mengumpulkan paket-paket data yang terdapat pada jaringan kemudian menganalisanya serta menentukan apakah paket-paket tersebut berupa suatu paket yang normal atau suatu aktivitas yang mencurigakan.

8. *Intrusion Prevention System (IPS)*

Intrusion Prevention System (IPS) adalah sebuah perangkat lunak atau perangkat keras yang bekerja untuk monitoring *trafik* jaringan, mendeteksi aktivitas yang mencurigakan dan melakukan pencegahan dini terhadap penyusupan atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti sebagaimana mestinya. IPS merupakan pendekatan yang sering digunakan untuk membangun sistem keamanan komputer, IPS mengombinasikan teknik *firewall* dan metode *intrusion detection system* (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor saat seragan teridentifikasi. Jadi IPS bertidak seperti layaknya *firewall* yang akan mengizinkan atau menghalang paket data [1].

9. Sistem Operasi

Sistem operasi adalah sebuah layer atau software yang bertugas untuk mengontrol *device* dan memberikan user program dengan *interface* sederhana terhadap *hardware*. Defenisi lain dari sistem operasi adalah sistem yang mampu melakukan pengontrolan yang bersifat *hardware oriented* yaitu pendekatan secara perangkat keras.

a. Ubuntu; Ubuntu merupakan distributor linux (distro) turunan dari debian. Tujuan dari distro Ubuntu adalah membawa semangat yang terkandung di dalam Ubuntu ke dalam dunia perangkat lunak. Ubuntu adalah sistem operasi lengkap berbasis Linux, tersedia secara bebas dan mempunyai dukungan baik yang berasal dari komunitas maupun tenaga ahli profesional. Ubuntu berkembang sangat cepat karena dukungan yang baik dan menyediakan berbagai kebutuhan aplikasi hampir di seluruh bidang computer[2].

Sistem operasi GNU Linux terdiri dari tiga bagian kode penting, yaitu:

a. *Kernell Linux; Kernell* merupakan inti dari suatu sistem operasi yang bertugas sebagai pengendali dan mengontrol kinerja dari semua yang ada pada sistem, mulai dari peralatan, penggunaan memori untuk aplikasi yang sedang berjalan, mengatur peletakan file, mengenali *driver* dan hal lainnya.
b. *Library System; Library System* menyediakan banyak tipe fungsi. Pada level paling rendah, mengizinkan aplikasi untuk melakukan permintaan pada *service* sistem *kernell*.
c. *Utility System;* Sistem linux mengandung banyak program-program user-mode, *utilitity* sistem dan *utility user*. *Utilitity* sistem termasuk semua program yang diperlukan untuk menginisialisasi sistem, seperti program untuk konfigurasi alat jaringan (*network device*) atau untuk load modul *kernel*.

10. *Snort*

Snort merupakan perangkat lunak untuk mendeteksi penyusup dan mampu menganalisa paket yang melintasi jaringan secara *real-time traffic* dan *logging* ke dalam *database* serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan [3].

Snort bisa dioperasikan dengan tiga mode, yaitu:

a. Paket *Sniffer Mode*; *Snort* bertindak sebagai *software sniffer* yang dapat melihat semua paket yang lewat dalam jaringan komputer dimana *Snort* dipasang. Dalam mode ini, berbagai paket ditampilkan hanya dalam bentuk layar monitor secara *real-time*.
b. Paket *Logger Mode*; Dalam mode ini, selain dapat melihat semua paket yang lewat dalam jaringan komputer, *Snort* juga dapat mencatat atau melakukan *logging* terhadap berbagai paket tersebut ke dalam *database*. Dengan kata lain, *Snort* mampu membuat *copy* dari paket-paket yang lewat dan menyimpan *copy* tersebut ke dalam *database* sehingga *network administrator* dapat melakukan analisa terhadap paket data atau *traffic* jaringan tersebut.

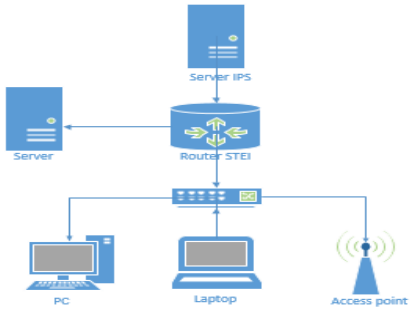
11. *Network Intrusion Detection System* (NIDS)

Dalam mode ini, Snort dapat melakukan monitoring dan menganalisa paket data, mendeteksi adanya paket data yang didefinisikan sebagai sebuah serangan penyusupan dan melakukan logging terhadap serangan penyusupan yang terjadi pada jaringan komputer berdasarkan *rule* yang telah ditetapkan oleh *network administrator*.

III. ANALISIS DAN PERANCANGAN SISTEM JARINGAN

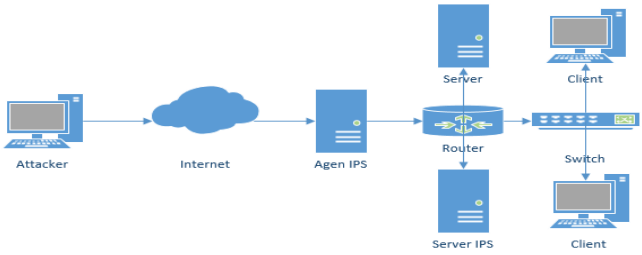
1. Topologi Jaringan

Topologi yang digunakan untuk pengimplementasian Intrusion Prevention System ini cukup sederhana, hanya menambahakan 1 *server* untuk penempatan aplikasi IPS (*Intrusion Prevention System*). Berikut adalah gambar topologi jaringan tersebut.



Gambar. 1 Topologi Jaringan Usulan

2. Skema Jaringan



Gambar. 2 Skema jaringan IPS (Intrusion Prevention System)

Rincian penjelasan skema sistem pencegah penyusupan pada jaringan dapat dilihat pada uraian dibawah ini:

a. *Attacker* berada pada satu jaringan bersama dengan *user/client* dan *server Intrusion Prevention System.*
b. *Attacker* melakukan serangan terhadap *server* maupun *user/client* yang berada pada jaringan.
c. *Server Intrusion Prevention System* merupakan suatu sistem yang memonitor *traffic* jaringan secara *real time*, tidak hanya pada *server Intrusion Prevention System* sendiri tapi juga memonitor aktifitas *traffic* jaringan pada *user/client*.
d. Jika terdapat aktifitas yang mencurigakan pada jaringan yang didefiniskan sebagai sebuah serangan penyusupan, agen *server Intrusion Prevention System* akan memberikan alert adanya gangguan pada jaringan dan secara otomatis serangan penyusupan tersebut akan di-block oleh firewall. Tujuan dari agen server tersebut adalah mengantisipasi serangan agar tidak langsung menyerang ke server *Intrusion Prevention System* utama.

Untuk itu komponen-komponen yang harus ada pada sistem pencegahan penyusupan pada jaringan meliputi:

a. *Intrusion Detection System* (IDS)

Dilihat dari cara kerja dalam menganalisa apakah paket dianggap sebagai penyusupan atau bukan, IDS dibagi menjadi 2 yaitu :

a. *Knowledge-based* atau *misuse detection* yaitu mendeteksi adanya penyusupan dengan cara me-monitoring paket data kemudian membandingkannya dengan rule IDS yang berisi signature paket

serangan. Jika paket data mempunyai pola yang sama dengan rule maka paket tersebut dianggap sebagai sebuah serangan.

b. *Behavior-based* atau *anomaly* yaitu dapat mendeteksi adanya penyusupan dengan mengamati adanya kejanggalan-kejanggalan pada sistem atau adanya penyimpangan-penyimpangan dari kondisi normal.

b. *Packet Filtering Firewall*

Packet Filtering Firewall dapat membatasi akses koneksi berdasarkan parameter-parameter seperti protocol, IP asal, IP tujuan, port asal, port tujuan, dan aliran data (*chain*) sehingga dapat diatur hanya akses yang sesuai dengan *policy* saja yang dapat mengakses sistem. *Packet Filtering Firewall* ini bersifat statik sehingga fungsi untuk membatasi akses pun bersifat statik. Untuk itulah *Packet Filtering Firewall* tidak dapat mengatasi gangguan yang bersifat dinamik sehingga harus dikombinasikan dengan IDS untuk membentuk sistem yang maksimal.

c. *Engine System*

Engine ini bertugas untuk membaca *alert* dari IDS (dapat berupa jenis serangan dan IP *address* penyusup) untuk kemudian memerintahkan *firewall* untuk mem-*block* akses koneksi penyusup ke sistem.

3. Keamanan Jaringan

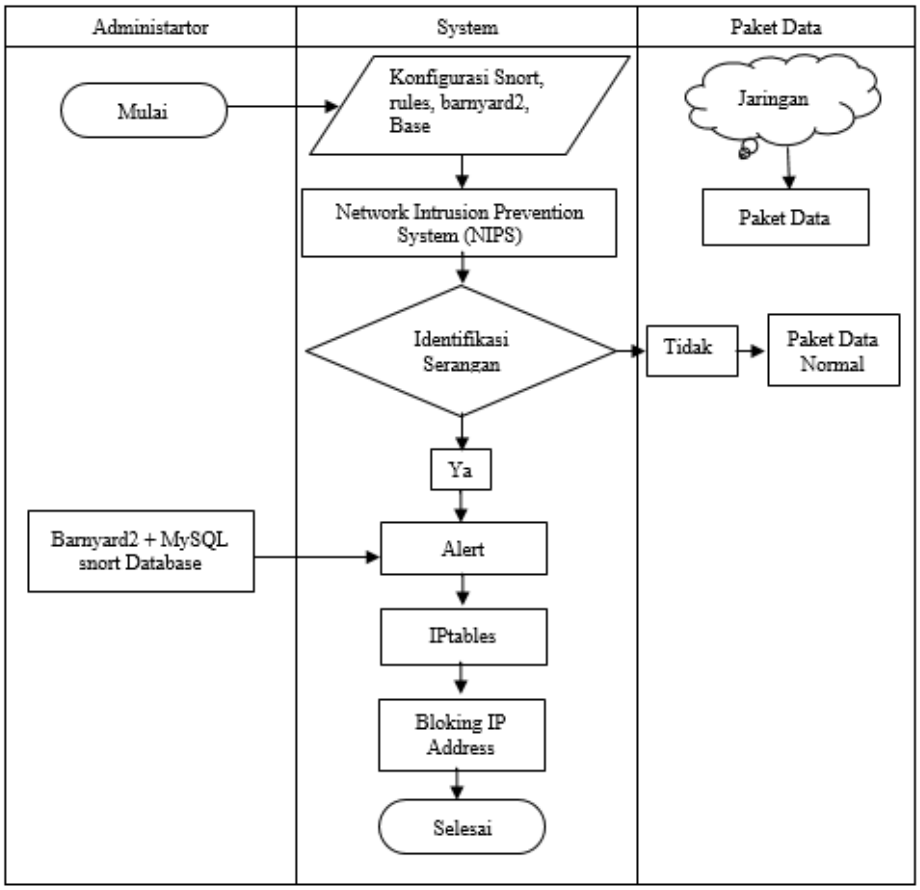
Keamanan jaringan dalam jaringan usulan menggunakan sistem operasi *Ubuntu Server* 14-04 untuk nantinya di pasang aplikasi snort sebagai software IPS (*Intrusion Prevention System*). Setelah terpasang dan di konfigurasi aplikasi *Snort* akan mendeteksi penyusup, menganalisa paket yang melintasi jaringan secara real-*time traffic* dan logging ke dalam *database* serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan.

4. Perancangan Aplikasi

Untuk memenuhi kebutuhan fungsional sistem pencegahan penyusup pada jaringan (*Network Intrusion Prevention System*), dibutuhkan modul-modul utama untuk mendukung sistem tersebut. Modul utama berupa ,*Snort, Snortrules, Apache, MySQL, Barnyard2, BASE.*

Target implementasi *Intrusion Prevention System* (IPS) yaitu pada sistem operasi *Linux Ubuntu* 14-04. Instalasi sistem operasi *Linux Ubuntu* dan konfigurasi Snort *Intrusion Prevention System* dapat dilihat pada lampiran . *Flowchart Network Intrusion Prevention System* (NIPS) dapat dilihat pada gambar berikut:

TABEL I
FLOWCHART NETWORK INTRUSION PREVENTION SYSTEM



Dari *flowchart* diatas dapat dilihat tahapan kerja *network administrator* dalam membangun *Network Intrusion Prevention System* (NIPS) meliputi:

a. Konfigurasi *Snort*
b. Konfigurasi *Rules Snort*
c. Konfigurasi *Barnyard2*
d. Konfigurasi BASE (*Basic Analis Security Engine*)

Log yang *dihasilkan* dari pendeteksian serangan penyusupan akan disimpan pada *database Snort*.

5. Implementasi Sistem

Implementasi merupakan tahapan lanjutan setelah analisa dan konfigurasi dilakukan. Pada tahapan ini, sistem yang telah selesai, siap untuk dioperasikan dan dilakukan pengujian untuk melihat sejauh mana sistem yang dibuat dapat mencapai tujuan.

Tujuan implementasi yaitu: menyelesaikan konfigurasi system, menguji prosedur-prosedur konfigurasi system dan mempertimbangkan bahwa sistem sesuai dengan harapan yakni menguji sistem secara keseluruhan.

Langkah-langkah yang dibutuhkan dalam pengimplementasian sistem adalah sebagai berikut:

a. Menyelesaikan konfigurasi sistem
b. Memilih komponen pendukung yang cocok dengan IDS yang digunakan
c. Mempersiapkan lingkungan implementasi
d. Menguji sistem

Terdapat tiga bagian utama yang berperan pada proses implementasi *Intrusion Prevention System*. Berikut adalah deskripsi implementasi sistem:

a. Implementasi *Snort engine;* Memonitor *traffik* dan paket data pada jaringan.
b. Implementasi *rules snort;* Mendeteksi dan mengelompokkan paket data yang lewat apakah merupakan sebuah serangan atau hanya paket data biasa.
c. Implementasi *output*; *Snort* dijalankan pada mode *inline* dengan data *aquisition* (daq).

6. Ruang Lingkup Implementasi

Lingkungan implementasi yang digunakan untuk mengkonfigurasikan *Snort* sebagai sistem pencegahan penyusupan pada jaringan (*Network Intrusion Prevention System*/NIPS) terdiri dari:

a. Perangkat Keras
   Perangkat keras yang digunakan memiliki spesifikasi sebagai berikut:
   a. Processor : Intel Core i5 1.8 GHz
   b. Memory : 4 GB
   c. Harddisk : 500 GB
b. Perangkat Lunak
   a. *Virtualbox Version* 5.0.26 r108824
   b. Sistem Operasi : *Ubuntu Server* 14-04
   c. *Kernell* : 3.10.0-327.22.2.el6.x86_64
   d. *Intrusion Detection System* : *Snort* 2.9.8.3
   e. *Rules Snort : Snortrules-Snapshot*-2983
   f. *Firewall* : IPTables
c. Lain-lain
   a. Snort Sensor : eth0 – 192.168.56.101
   b. Range IP address : 192.168.56.0/24
   c. Web Browser Monitoring : BASE, Mozilla

7. Batasan Implementasi

Snort NIPS menguji serangan yang umum terjadi. Pengujian tipe serangan lainnya dapat dikondisikan menurut *rules Snort*.

8. Hasil Implementasi

Hasil implementasi adalah mendeteksi serangan yang terjadi pada sistem kemudian mencegahan penyusupan pada jaringan (Network *Intrusion Prevention System)* dan menampilkan *output monitoring* pada *database*.

9. Pengujian Jaringan

Untuk menguji sistem pencegahan penyusupan, dilakukan dengan cara melancarkan paket serangan ke sistem yang dilindungi oleh sistem pencegahan penyusupan (*Network Intrusion Prevention System*).

10. Ruang Lingkup Pengujian

Lingkungan pengujian yang digunakan untuk menguji sistem pencegahan penyusupan pada jaringan (*Network Intrusion* Prevention *System*/NIPS) terdiri dari:

a. Perangkat Keras
   a. *Processor* : Intel Core i5 CPU 1.80 GHz (4 CPUs)
   b. *Memory* : 4 GB
   c. *Harddisk* : 500 GB
b. Perangkat Lunak
   a. *VirtualBox*
   b. *Server* Menggunakan OS *ubuntu*
   c. IP *address* : 192.168.56.105
   d. *Attacker Linux Backtrack 5 R3*
   e. Aplikasi Pengujian : *Backtrack tools*
   f. IP *address* : 192.168.56.104

11. Identifikasi dan Rencana Pengujian

Identifikasi dan rencana pengujian dapat dilihat pada table IV.2.

TABEL II
IDENTIFIKASI DAN RENCANA PENGUJIAN

Identifikasi	Butir Uji	Tingkat Pengujian	Jenis Pengujian
Percobaan penyusupan dan pengujian mode yang ada pada *snort*.	Ping,SSH, , Drop akses, snort *inline* mode, *snort* mode *sniffer*,	Pengujian *Intrusion Deteksion System* dan *Intrusion Prevention System*	*Blackbox*

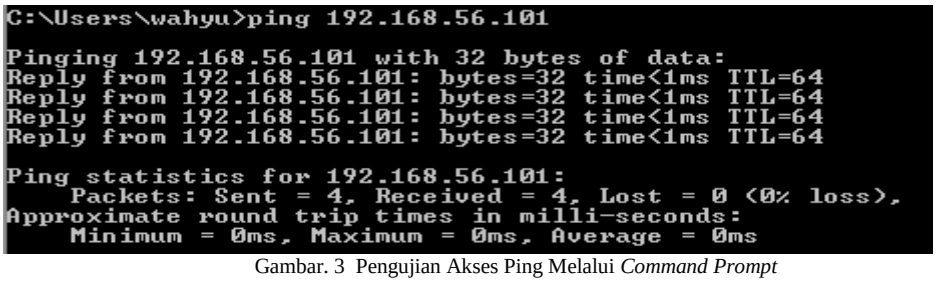
12. Pengujian Akses Ping

Pada pengujian ini, penyerang akan mengakses *Snort* melalui *command prompt* menggunakan *ping*. Dengan konfugurasi *rule* sebagai berikut :

 # alert icmp any any -> any any (msg:"ada orang yang lagi nyoba ngeping";sid:10000001;rev:0;)

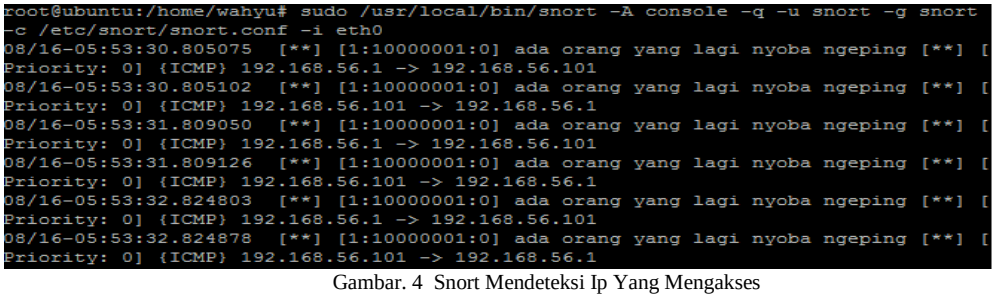
Sid : Digunakan untuk mengenali *rule snort* secara unik.

Rev : Digunakn Untuk mengindentifikasi atas *rules-rules snort.*



Gambar. 3 Pengujian Akses Ping Melalui *Command Prompt*

a. Kondisi *Snort* aktif



Gambar. 4 Snort Mendeteksi Ip Yang Mengakses

b. Tampil di web monitoring BASE

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-74)	[snort] Snort Alert [1:10000001:1]	2016-08-16 03:39:09	192.168.56.1	192.168.56.101	ICMP
#1-(1-73)	[snort] Snort Alert [1:10000001:1]	2016-08-16 03:39:08	192.168.56.1	192.168.56.101	ICMP
#2-(1-72)	[snort] Snort Alert [1:10000001:1]	2016-08-16 03:39:07	192.168.56.1	192.168.56.101	ICMP
#3-(1-71)	[snort] Snort Alert [1:10000001:1]	2016-08-16 03:39:06	192.168.56.1	192.168.56.101	ICMP
#4-(1-70)	[snort] Snort Alert [1:10000001:1]	2016-08-16 03:39:05	192.168.56.1	192.168.56.101	ICMP

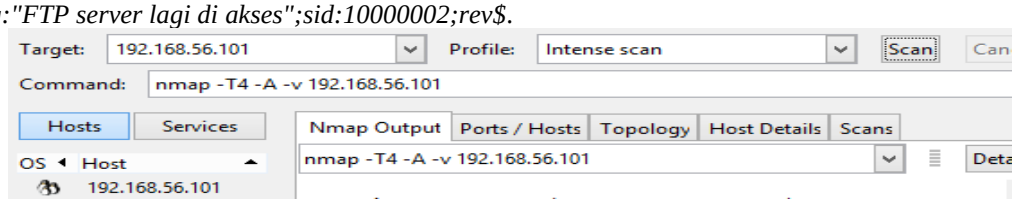
Gambar. 5 Pengujian Monitoring Base

TABEL III
BUTIR UJI MODUL PENGUJIAN PENDETEKSIAN PENYUSUP

Deskripsi	Tools	Prosedur Uji	Output	Hasil
Snort) dalam keadaan aktif	Commad Prompt	Penyusup melakukan Ping	Tampil IP Address penyusup dalam bentuk alert	Tampil IP address penyusup dalam bentuk alert pada terminal dan Base Kesimpulan : Berhasil

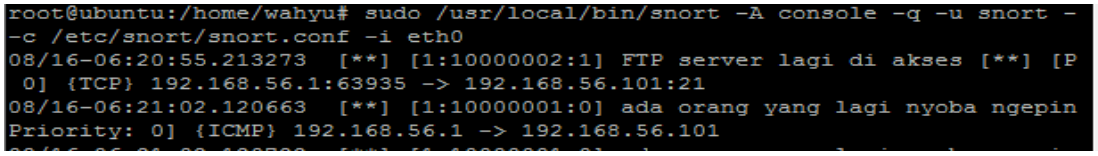
13. Pengujian akses FTP

Pada pengujian ini, penyerang akan melakukan *remot login* dan untuk mendeteksinya *alert tcp any any -> any 21 (msg:"FTP server lagi di akses";sid:10000002;rev$*.



Gambar. 6 Tes FTP menggunakan Zenmap

a. Snort aktif



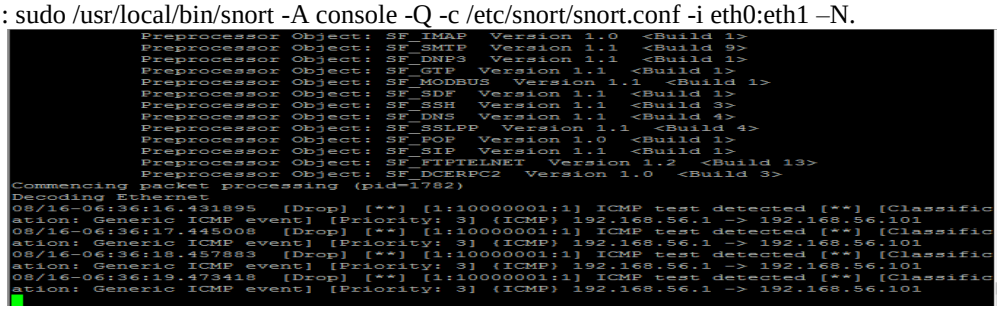
Gambar. 7 Akses FTP ke Server

TABEL IV
BUTIR UJI MODUL PENGUJIAN FTP PADA *SERVER SNORT*

Deskripsi	Tools	Prosedur Uji	Output	Hasil
Snort aktif	Zenmap	Penyusup melakukan akses ke *server*	Tampil IP Address penyusup dalam bentuk alert	Tampil IP address penyusup dalam bentuk alert pada terminal Kesimpulan : Berhasil

14. Pengujian Snort Menggunakan Mode *Inline*

Pada pengujian ini *Snort* di jalankan pada mode yang berbeda yaitu menggunakan menggunakn *afpacket* sebagai *tool* pendeteksinya. Untuk rule menggunakan : *drop icmp any any -> $HOME_NET any (msg:"ICMP test detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event*;). Dan untuk melihat report menggunakan perintah : sudo /usr/local/bin/snort -A console -Q -c /etc/snort/snort.conf -i eth0:eth1 –N.



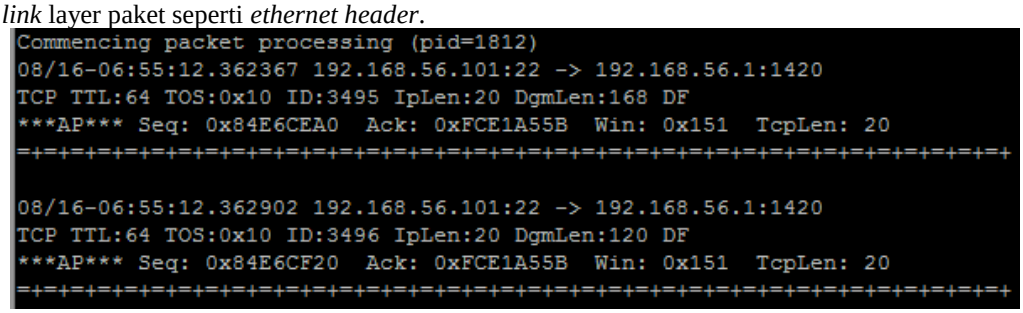
Gambar. 8 Pengujian *Snor Inline Mode*

TABEL V
BUTIR UJI MODUL PENGUJIAN *SNORT INLINE*

Deskripsi	Tools	Prosedur Uji	Output	Hasil
Snort aktif	Command prompt	Penyusup melakukan akses ke *server*	Tampil IP Address penyusup dalam bentuk drop alert	Tampil IP address penyusup pada terminal (Berhasi)

15. Pengujian Snort Mode Sniffer

Pengujian ini dengan menambahkan beberapa switch –v, -d, -e akan menghasilkan beberapa keluaran yang berbeda, yaitu : -v, untuk melihat header TCP/IP paket yang lewat, -d, untuk melihat isi paket, -e, untuk melihat *header link* layer paket seperti *ethernet header*.



Gambar. 9 Pengujian Snort Mode *Sniffer*

Tampak bahwa antar paket selalu di batasi tanda =+=+=+=+=+. Karena sniffer di aktifkan hanya menggunakan *switch –v*, maka hanya *header network & transport protocol* yang diperlihatkan.

TABEL VI
BUTIR UJI MODUL PENGUJIAN *SNORT SIFFER*

Deskripsi	Tools	Prosedur Uji	Output	Hasil
Snort aktif	Terminal	Malakukan perintah snort -v	Tampil header TCP/IP paket	Tampil informasi header TCP/IP

16. Analisa Hasil Pengujian

Analisa hasil pengujian *Snort Intrusion Detection system (IDS)* dan *Network Intrusion Prevention System* (NIPS) dapat dilihat pada Tabel VII

TABEL VII
HASIL PENGUJIAN

Implementasi	Identifikasi	Hasil	Deskripsi
Perancangan dan implementsi snort dan mode snort	Percobaan serangan dan , mode snort	Berhasil	Menghasilkan analisa yang sesuai dengan metode yang digunakan dan konfigurasi yang dilakukan

IV. KESIMPULAN

Berdasarkan penelitian pada tahap konfigurasi dan implementasi diatas, dapat diambil beberapa kesimpulan, yakni:

1. *Snort Network Intrusion Prevention System* (NIPS) bisa di implementasikan pada sistem operasi *Linux Ubuntu* karena kemudahan dalam penggunaan dan kecocokan komponen utama dan komponen pendukung untuk mengkonfigurasikan *Snort* NIDS atau NIPS.
2. Suatu serangan dapat terdeteksi atau tidak oleh *snort engine* tergantung pada pola serangan yang ada pada *rule database snort*. Jika pola serangan tidak terdefinisi pada *rule database*, maka serangan akan dianggap sebagai paket data biasa.
3. *Snort Network Intrusion Prevention System* (NIPS) yang di konfigurasi mengunakn *mode inline*, yang di pasang di OS *Ubuntu Server* 14-04, dapat berjalan dengan baik jika paket-paket yang mendukung *software Snort* telah di konfigurasi dengan baik.

REFERENSI

[1] Budiman, S. A., Iswahyudi, C., & Sholeh, M. (2014). IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) PADA SERVER DEBIAN. *Jurnal JARKOM Vol. 2 No. 1 ISSN:2338-6313*, 36-40.
[2] Homenta, J. I., & Efendi, R. (2015). MENGANALISA SISTEM KEAMANAN JARINGAN BERBASIS INTRUSION PREVENTION SYSTEM DAN HONEYPOT SEBAGAI PENDETEKSI DAN PENCEGAH MALWARE. Jurnal Teknologi Informasi dan Komunikasi, 1-8.
[3] Wiyanto, P., Hamzah, A., & Sholeh, M. (2014). APLIKASI MONITORING KEAMANAN JARINGAN DENGAN MENGGUNAKAN IDS DAN. *Jurnal JARKOM Vol. 2 No. 1 ISSN:2338-6313*, 89-91.
[4] Gunawan, Indra. "Penggunaan Brute Force Attack Dalam Penerapannya Pada Crypt8 Dan CSA-Rainbow Tool Untuk Mencari BISS." InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan 1.1 (2016): 52-55.
[5] Rahmatullah, Tansah. "PERLINDUNGAN HUKUM TERHADAP PRIVACY DARI SPAMMING BERDASARKAN UNDANG-UNDANG NO. 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK." JURNAL HUKUM MEDIA JUSTITIA NUSANTARA 4.2 (2019).