Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort IDS dan Honeypot pada Windows

[1]Usama, [2]F. Yudi Limpraptono, [3]Sotyohadi
Institut Teknologi Nasional, Malang, Indonesia,
[1]usamaassegaf@gmail.com, [2]bryan_130572@yahoo.com, [3]sotyohadi@yahoo.com

Abstrack - Snort sebuah perangkat lunak yang open source yang mendukung semua sistem operasi seperti linux,window maupun solaris, snort merupakan sistem pedeteksi Intrusion Detection System (IDS) yang bisa dikembangkan menjadi sistem pencegah Intrusion Prevention System (IPS) dengan cara mengkombinasikan IDS dan firewall dengan menjalankan snort pada mode inline juga. beberapa administrator jaringan yang menggunakan software ini. snort sangat bermanfaat bagi para administrator jaringan untuk meningkatkan sistem keamanan jaringan karena bisa dikonfigurasi sesuai keinginan. Snort bisa dikonfigurasi untuk meyimpan outputnya ke database log snort yang setiap saat bisa dilihat paket paket yang manakah yang dianggap sebuah serangan. Pada skripsi ini penyusun akan mengkonfigurasi snort pada sistem operasi windows 7, kenapa memilih windows karena pada penelitian sebelumnya kebanyakan menggunakan sistem operasi linux. Disini penulis mengkonfigurasi sebagai sistem pencegahan yang bilamana ada paket paket yang di identifikasi sebuah serangan atau mencurigakan maka akan ditolak. Snort bekerja dengan rule - rulenya yang akan mencocokkan paket yang ada didatabase rules snort itu sendiri. jika berupa sebuah serangan maka sistem akan mengirimkan alert untuk memblocking sehingga paket tersebut tidak diteruskan ke korban namun snort akan mencatat disebuah log databasenya. Ketika Snort NIPS aktif serangan seperti Ping Of death, seranga DOS dan Port Scanning dicegah.

Kata Kunci : Intrusion Detection System, Intrusion Prevention System, Rules Snort.

I. PENDAHULUAN

A. Latar Belakang

Teknologi pada saat ini sangat cepat perkembangannya termasuk perkembangan internet, yang memungkinkan semua pengguna bisa berkomunikasi dan saling bertukar data, namun disamping perkembangan teknologi semakin cepat di sisi lain kejahatan teknologi di dunia maya juga ikut berkembang, keamanan data harus terlindungi dan dijaga, agar validitas dan integritas data terjamin bagi penggunanya. Agar sistem jaringan tidak terganggu bahkan sampai rusak oleh serangan penyusup (*intruder*), maka diperlukan sistem keamanan jaringan yang dapat menanggulangi dan mencegah serangan penyusup tersebut (Dodik,2017).
Untuk mengatasi masalah diatas, dibutuhkan sebuah sistem yang mampu mendeteksi penyusupan dalam jaringan komputer yang dikenal istilah IDS *(Intrusion Detection System)*. IDS *(Intrusion Detection System)* adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. *Snort* IDS merupakan IDS yang *open source* yang secara *defacto* menjadi standar IDS di industri. *Snort* berfungsi untuk mendeteksi serangan dengan cara menghasilkan *alert* (Dodik,2017).

IPS *(Intrusion Prevention System)* adalah sebuah aplikasi yang bekerja untuk *monitoring traffic* jaringan, mendeteksi aktivitas yang mencurigakan, dan melakukan pencegahan dini terhadap serangan. IPS mengkombinasikan teknik *firewall* dan metoda IDS *(Intrusion Detection System)* dengan sangat baik (Agita,2013).

Penelitian sebelumnya sudah pernah dilakukan oleh saudara (Yoga Widya Pradipta,2017). Namun disini konfigurasi pencegahan penyusupan dilakukan pada sistem operasi Linux

Maka pada penelitian ini penulis lebih fokus untuk mengkonfigurasi *snort* pada sistem operasi windows sebagai sistem pendeteksi dan pencegahan penyusupan jaringan dengan snort sebagai *mode inline* yang mana pempunyai dua *interfaces ethernet* sebagai jembatan sebelum paket diteruskan ke server sehingga keamanan pada clientpun juga ikut terjamin akan keamanannya karena setiap paket yang masuk harus melewati komputer *server* terlebih dahulu sebelum dikirim ke alamat yang dituju.

Snort IDS (*Intrusion Detection System*) dan *Honeyd* yang dapat melindungi *server* dari serangan penyusup. Dengan adanya sistem keamanan jaringan ini dapat mempermudah administator melindungi *server* dari serangan penyusup.

B. Rumusan Masalah

Berdasarkan paparan latar belakang di atas maka dapat dirumuskan masalah sebagai berikut :

1. Bagaimana cara merancang dan mengkonfiguasi sistem metode *Snort* dan *Honeyd* untuk mendeteksi dan pencegahan penyusupan pada sistem operasi windows ?
2. Bagaimana menggunakan metode *Snort* sebagai IDS *(Intrusion Detection System)* untuk mendeteksi penyusupan pada sistem operasi windows ?
3. Bagaimana menggunakan metode *Snort* sebagai IPS *(Intrusion Prevention System)* untuk pencegahan penyusupan pada sistem operasi windows ?

C. Tujuan Penelitian

Penelitian dilakukan bertujuan untuk mengimplementasika *Snort* sebagai IDS (*Intrusion Detection System*) dan IPS (*Intrusion Prevention System)* pada sistem operasi windows, agar serangan yang dilakukan peneliti seperti *Ping Of Death*,serangan DOS dan *Port Scanning* bisa terdeteksi dan di cegah, dan untuk menyimpan sebuah serangan yang telah dilakukan untuk dijadikan dokumentasi yang dapat dilihat sewaktu diperlukan

D. Batasan Masalah

Agar analisa ini sesuai dengan konsep awal dan tidak meluas, maka diberikan batasan-batasan sebagai berikut :

1. Menggunakan *Snort* sebagai sistem pendeteksian dan pencegahan penyusupan jaringan .
2. *Snort* hanya mendeteksi dan mencegah paket yang masuk dalam *rule database snort*
3. Menggunakan windows sebagai sistem operasi untuk melakukan konfigurasi *Snort*
4. Pengujian dilakukan dengan dengan beberapa serangan yang umum terjadi saja seperti *ping of death*, serangan DOS, *port scanning* dan *host scanning*
5. Pengujian hanya dilakukan pada jaringan lokal

E. Manfaat Penelitian

Manfaat penelitian yang dilakukan ialah:

1. Bagi panulis bermanfaat untuk menerapkan ilmu yang didapat selama dibangku perkuliahan mengenai ilmu jaringan komputer
2. Bagi penulis bermanfaat agar mengenal lebih jauh *software snort* sebagai pendeteksi dan pencegahan penyusupan jaringan
3. Bagi pembaca bermanfaat menambah wawasan untuk penelitian selanjutnya

II TINJAUAN PUSTAKA

2.1. Pengenalan Jaringan Komputer

2.1.1. Definisi Jaringan

Jaringan Komputer adalah sekelompok komputer otonom yang saling berhubungan antara satu dengan lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, program - program, penggunaan bersama perangkat keras seperti printer, harddisk, dan sebagainya. Selain itu jaringan komputer bisa diartikan sebagai kumpulan sejumlah terminal komunikasi yang berada diberbagai lokasi yang terdiri dari lebih satu komputer yang saling berhubungan (Asep Herman Suyanto,2004).

2.1.2 Jenis Jaringan

Berdasarkan ruang lingkup jangkauannya, maka jenis-jenis jaringan komputer dapat digolongkan menjadi 3 jenis (Diskhams Maulidi Mydza,2011) yaitu:

2.1.2.1 Local Area Network (LAN)

Local Area Network (LAN), merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumberdaya (*resouce*, misalnya printer) dan saling bertukar informasi.

2.1.2.2 Mentropolitan Area Network (MAN)

Metropolitan Area Network (MAN) Merupakan pengembangan dari jaringan LAN yang memiliki kecepatan transfer data yang tinggi, yang menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan dan sebagainya.

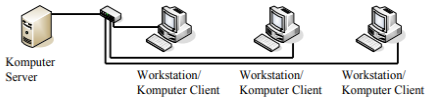
2.1.2.3 Wide Area Network (WAN)

Wide Area Network (WAN) dirancang untuk menghubungkan komputer-komputer yang terletak pada suatu cakupan geografis yang luas, seperti dari satu kota ke kota lain di dalam suatu negara

Berdasarkan cara pengaksesan data, jaringan komputer dibagi menjadi 2 (Diskhams Maulidi Mydza,2011):

2.1.2.4 Client-Server

jenis jaringan yang membagi fungsi komputer menjadi dua, ada komputer yang bertindak sebagai server dan ada komputer yang berperan sebagai *client* (*workstation*). Komputer server dapat mengontrol sepenuhnya komputer *client*.

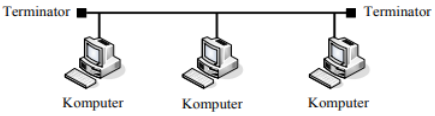


Gambar 2.1 Jaringan client-server

2.1.2.5 Peer to peer (P2P)

jenis jaringan yang tidak membutuhkan server secara khusus karena komputer yang

terhubung pada jaringan dapat berfungsi ganda sebagai server maupun client.



Gambar 2.2 Jaringan peer to peer

2.1.3. Komponen Dasar Jaringan

Dalam membangun sebuah jaringan, anda harus mempersiapkan perangkat-perangkat yang diperlukan yaitu (Andi Supriyadi, 2007):

2.1.3.1 Perangkat Keras

1. Komputer/PC
2. Network Interfaces Card
3. Hub/Switch
4. Repeater
5. Bridge
6. Router
7. Kabel

2.1.3.2 Perangkat Lunak

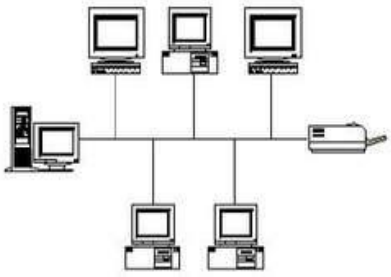
1. Sistem Operasi
2. Protokol Jaringan (TCP/IP)

2.1.4 Topologi Jaringan

Topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Cara yang saat ini banyak digunakan adalah bus, token ring, dan star. Dalam suatu jaringan komputer jenis topologi yang dipilih akan mempengaruhi kecepatan komunikasi. Untuk itu maka perlu dicermati kelebihan/keuntungan dan kekurangan / kerugian dari masing - masing topologi berdasarkan karakteristiknya (Andi Supriyadi,2007).

2.1.4.1 Topologi Bus

Topologi Bus menggunakan metode *unicast*, *multicast* dan *broadcast*. *Unicast* adalah komunikasi antara satu pengirim dengan satu penerima di jaringan. *Multicast* adalah komunikasi antara satu pengirim dengan banyak penerima di jaringan. Sedangkan pada *Broadcast*, setiap titik akan menerima dan menyimpan *frame* yang disalurkan/dihantarkan.



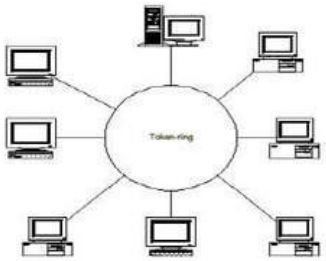
Gambar 2.3 Topologi Bus

Tabel 2.1 Karakteristik Topologi Bus

keuntungan	kerugian
• Hemat kabel • Layout kabel sederhana • Mudah dikembangkan	• Deteksi dan isolasi kesalahan sangat kecil • Kepadatan lalu lintas • Bila salah satu client rusak, maka jaringan tidak bisa berfungsi • Diperlukan repeater untuk jarak jauh

2.1.4.2 Topologi Token Ring

Topologi *Token Ring* (sering disebut ring saja) menghubungkan komputer sehingga berbentuk *ring* (lingkaran). Setiap simpul mempunyai tingkatan yang sama. Jaringan akan disebut sebagai *loop*, data dikirimkan kesetiap simpul dan setiap informasi yang diterima simpul diperiksa alamatnya apakah data itu untuknya atau bukan



Gambar 2.4 Topologi Token Ring

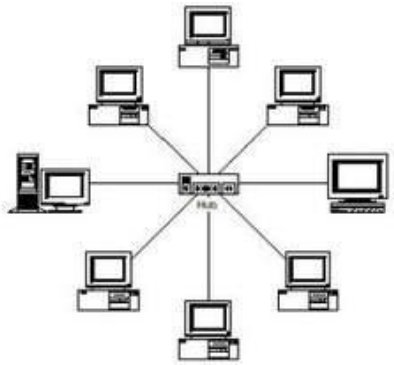
Tabel 2.2 Karakteristik Topologi Token Ring

keuntungan	kerugian
• Hemat kabel	• Peka kesalahan • Pengembangan jaringan lebih kaku

2.1.4.3 Topologi Star

Topologi ini merupakan kontrol terpusat, semua link harus melewati pusat yang menyalurkan data tersebut kesemua simpul atau client yang dipilihnya. Simpul pusat dinamakan stasiun primer atau server dan lainnya dinamakan stasiun sekunder atau client server. Setelah hubungan jaringan dimulai oleh server maka setiap client server sewaktu-waktu dapat menggunakan

hubungan jaringan tersebut tanpa menunggu perintah dari server



Gambar 2.5 Topologi Star

Tabel 2.3 Karakteristik Topologi Star

keuntungan	kerugian
• Paling fleksibel •Pemasangan/perubahan stasiun sangat mudah dan tidak mengganggu bagian jaringan lain • Kontrol terpusat • Kemudahan deteksi dan isolasi kesalahan/kerusakan • Kemudahan pengelolaan jaringan	•Boros kabel •Perlu penanganan khusus •Kontrol terpusat (HUB/Switch) jadi elemen kritis

2.2. Ancaman Keamanan Jaringan

Salah satu pusat perhatian dalam keamanan jaringan adalah mengendalikan akses terhadap resources jaringan tersebut. (Diskhams Maulidi Mydza,2011).

2.2.1. Prinsip Keamanan Jaringan

Prinsip keamanan jaringan sering disebut dengan segitiga CIA *(Confidentiality, Integrity, Availability).*

1. *Confidentiality* (Kerahasiaan) : menjaga infrastruktur jaringan agar tidak dapat diakses oleh pihak yang tidak berhak untuk mengaksesnya.

2. *Integrity* (Integritas) : menjaga data agar tetap asli, tidak dimodifikasi dalam perjalanannya dari sumber menuju penerimanya.

3. *Availability* (Ketersediaan) : user yang mempunyai hak akses *(authorized user)* diberi akses tepat waktu dan tidak terkendala apapun.

2.2.2 Jenis Jenis Serangan Terhadap Jaringan

Berikut ini merupakan jenis serangan terhadap keamanan infrastruktur jaringan.

2.2.2.1 Danial Of Services (DoS)

Serangan yang dikenal dengan istilah DoS dan DDoS *(Distributed Denial of Services)* ini pada dasarnya merupakan suatu aktivitas dengan tujuan utama menghentikan atau meniadakan layanan *(services)* sistem atau jaringan komputer - sehingga sang pengguna tidak dapat menikmati fungsionalitas dari layanan tersebut – dengan cara mengganggu ketersediaan komponen sumber daya yang terkait dengannya. Contohnya adalah dengan cara memutus koneksi antar dua sistem, membanjiri kanal akses dengan jutaan paket, menghabiskan memori dengan cara melakukan aktivitas yang tidak perlu, dan lain sebagainya. Dengan kata lain, DOS dan/atau DDoS merupakan serangan untuk melumpuhkan sebuah layanan dengan cara menghabiskan sumber daya yang diperlukan sistem komputer untuk melakukan kegiatan normalnya. Adapun sumber daya yang biasa diserang misalnya: kanal komunikasi (*bandwidth*), *kernel tables, swap space, RA M, cache memories,* dan lain sebagainya.(Richardus Eko Indrajit,2014).

Berikut adalah sejumlah contoh tipe serangan DoS/DDoS:

1. *SYN-Flooding*: merupakan serangan yang memanfaatkan lubang kerawanan pada saat koneksi TCP/IP terbentuk. 2.
2. Pentium 'FOOF' Bug: merupakan serangan terhadap prosessor yang menyebabkan sistem senantiasa melakukan *"re-booting".* Hal ini tidak bergantung terhadap jenis sistem operasi yang digunakan tetapi lebih spesifik lagi terhadap prosessor yang digunakan.

3. *Ping Flooding*: merupakan aktivitas *"brute force"* sederhana, dilakukan oleh penyerang dengan bandwidth yang lebih baik dari korban, sehingga mesin korban tidak dapat mengirimkan paket data ke dalam jaringan *(network).* Hal ini terjadi karena mesin korban dibanjiri *(flood)* oleh peket-paket ICMP.

4. *Ping Of Death* merupakan serangan 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.*

5. *Smurf Attack* merupakan serangan dimana Server digunakan untuk membanjiri korban dengan data sampah yangtidak berguna. Server atau jaringan yang dipakai menghasilkan respon paket yang banyak seperti ICMP ECHO paket atau UDP paket dari satu paket yang dikirim.

2.2.2.2 Scanning

Scanning terbagi atas tiga jenis, yaitu: (Diskhams Maulidi Mydza,2011).

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

2.3 Intrusion Detection System (IDS)

IDS *(Intrution Detection System)* adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan mencurigakan berhubungan dengan *traffic* jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Dalam banyak kasus IDS juga merespon terhadap traffic yang tidak normal/anomali melalui aksi pemblokiran seorang user atau alamat IP (*Internet Protocol)* sumber dari usaha pengaksesan jaringan. Ada beberapa cara bagaimana IDS bekerja. Cara yang paling populer adalah dengan menggunakan pendeteksian berbasis *signature* (seperti halnya yang dilakukan oleh beberapa antivirus), yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap basis data signature IDS yang bersangkutan. (Arpenta, 2015).

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

2.3.1 Host Based Intrusion Detection System

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. (Diskhams Maulidi Mydza,2011).

2.3.2 Network Based 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. (Diskhams Maulidi Mydza,2011).

2.4 Intrusion Prevention System

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 bertindak seperti layaknya firewall yang akan mengizinkan atau menghalang paket data.(Yoga Widya Pradipta, 2017).

2.5 Sistem Operasi

Sistem operasi merupakan sebuah penghubung antara pengguna komputer dengan perangkat keras komputer. Sebelum ada sistem operasi, orang hanya menggunakan komputer dengan menggunakan sinyal analog dan sinyal digital. Seiring dengan berkembangnya pengetahuan dan teknologi, saat ini telah ada beberapa sistem operasi dengan keunggulan masing-masing. Untuk lebih memahami sistem operasi maka sebaiknya perlu diketahui terlebih dahulu beberapa konsep dasar mengenai sistem operasi itu sendiri. Pengertian sistem operasi secara umum adalah pengelola seluruh sumber daya yang terdapat pada sistem komputer dan menyediakan sekumplan layanan ke pemakai sehingga mempermudah penggunaan serta pemanfaatan sumber daya sistem komputer. (Edy Victor Haryanto,2012).

Dalam ilmu komputer, sistem operasi atau dalam bahasa inggris disebut dengan *operating system* (OS) adalah perangkat lunak sistem yang bertugas melakukan kontrol dan manajemen terhadapa perangkat keras komputer, serta operasi-operasi dasar sistem, termasuk menjalankan aplikasi serta program-program pengolah kata, *desain*, *database* dan *browser web*. (Edy Victor Haryanto,2012).

Secara umum, Sistem operasi terdiri dari beberapa bagian:

1. Mekasnisme *boot*, yaitu melakukan *kernel* ke dalam memori
2. *Kernel*, yaitu inti dari sebuah sistem operasi
3. *Command interpreter* atau *shell*, yaitu bertugas membaca input dari pengguna
4. Pustaka pustaka, yaitu yang menyediakan kumpulan fungsi dasar dan standar yang dapat dipanggil oleh aplikasi lain.

2.5.1 Disk Operating System (DOS)

DOS merupakan *software* sistem operasi untuk pc yang dikembangkan pada awal tahun 1980 oleh *microsoft corporation*. Sistem operasi DOS dijalankan melalui disket sehingga kita harus memasukkan disket DOS ini ke dalam disk drive komputer ketika akan menghidupkan komputer. Karena modelnya *command line interface* maka saat ini sistem operasi DOS mulai ditinggalkan walaupun beberapa pengguna komputer masih menggunakan DOS ini. Pada masa kepopuleranya, diperkirakan DOS pernah dipakai lebih dari 70 juta pengguna komputer di dunia. (Edy Victor Haryanto,2012).

2.5.2 Sistem Operasi Windows 7

Windows 7 sebelumnya dikenal dengan sebutan *Blackcomb* dan *Vienna*. Saat pertama kali dirilis, Windows memiliki kernel NT versi 6.1 build 7600, yaitu perbaikan dari windows vista dimana saat dirilis pertama memiliki kernal NT 6.0 build 6000. Windows 7 dirilis pada tanggal 22 Oktober 2009 memiliki keamanan dan fitur yang baru, diantaranya adalah jump list, Taskbar yang membuka program dengan tampilan kecil, *windows media player*, *internet explorer* 8, dan lain-lain. Beberapa fitur yang unik adalah *Sidebar* yang berganti nama *Gadget* dan bebas ditaruh dimanapun pada *dekstop*. Fitur ini membuat Windows 7 menjadi lebih menarik. (Edy Victor Haryanto,2012).

2.6 Snort

Snort merupakan sebuah perangkat lunak atau tool sekuriti yang berfungsi untuk mendeteksi intrusi-intrusi jaringan (penyuspan, penyerangan dan berbagai bentuk ancaman lainnya), sekaligus juga melakukan pencegahan. Istilah populernya, Snort merupakan salah satu tool *Network Intrusion Prevention System* (NIPS) dan *Network Intrusion Detection System* (NIDS). Dalam praktiknya , *Snort* sangat andal untuk membentuk logging paket-paket dan analisis trafik-trafik secara *real-time* dalam jaringan berbasis TCP/IP.(Rahmat Rafiudin,2010).

2.7 Firewall

Firewall adalah istilah yang biasa digunakan untuk menunjuk pada suatu komponen atau sekumpulan komponen jaringan, yang berfungsi membatasi akses antara dua jaringan, lebih khusus lagi, antara jaringan *internal* dengan jaringan *global Internet*. *Firewall* mempunyai beberapa tugas: (Eueung Mulyana,2016).

2.7.1 Pertama dan yang terpenting adalah: harus dapat mengimplementasikan kebijakan security di jaringan *(site security policy*). Jika aksi tertentu tidak diperbolehkan oleh kebijakan ini, maka *firewall* harus meyakinkan bahwa semua usaha yang mewakili operasi tersebut harus gagal atau digagalkan. Dengan demikian, semua akses *illegal* antar jaringan (tidak diotorisasikan) akan ditolak

2.7.2 Melakukan filtering: mewajibkan semua traffik yang ada untuk dilewatkan melalui *firewall* bagi semua proses pemberian dan pemanfaatan layanan informasi. Dalam konteks ini, aliran paket data dari/menuju *firewall*, diseleksi berdasarkan *IP-address*, nomor port, atau arahnya, dan disesuaikan dengan kebijakan *security*.

2.7.3 *Firewall* juga harus dapat merekam/mencatat even-even mencurigakan serta memberitahu administrator terhadap segala usaha-usaha menembus kebijakan *security*.

III Perancangan Sistem

Pada bab ini penulis akan membahas perancangan dan sistem yang akan dibangun serta beberapa tahapan yang akan dilakukan dan pemilihan komponen – komponen yang akan digunakan dalam membangun sebuah sistem pendeteksi dan pencegahan penyusupan dalam sebuah jaringan lokal, pada bab ini pula penulis menganalisa sistem yang dikembangkan serta melakukan beberapa konfigurasi dan instalasi baik dari sistem operasi maupun aplikasi yang akan digunakan, pada penelitian kali ini sistem operasi yang digunakan windows 7 sebagai snort

3.1 Diagram Secara Umum

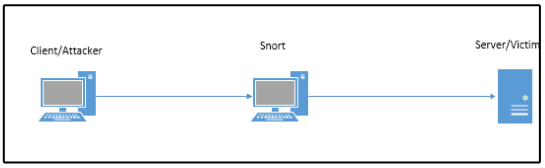
Digram sistem secara umum adalah suatu gambaran yang bertujuan untuk memperlihatkan bahkan menerangkan suatu data yang disajikan, pada dasarnya snort digunakan sebagai ids saja, seiring dengan perkembangan dari *developer snort* sehingga saat ini bisa digunakan sebagai ips, *snort* disini diistlahkan sebagai jembatan dari dua *adapter ethernet*, bisa dibilang sebagai *router* dan *snort* disini di posisikan diantara pc client dan pc server, dikarenakan lebih mudah dalam melakukan instalasi dan konfigurasi.

3.1.1 Client Melakukan Penyerangan

Client mencoba melakukan penyerangan terhadap server namun sebelum masuk ke server ada *firewall* yang berfungsi melakukan penyaringan paket yang masuk ke server, jika paket tersebut terdeteksi sebagai serangan maka *firewall* akan mengirimkan *alert* peringatan ke server, sehingga pc *snort* yang sudah dibangun dengan sistem nips ini akan mencegah paket tersebut. Jika serangan client tidak dicegah sedini mungkin maka akan berhasil menyerang server, sehingga server tidak akan bekerja secara maksimal.

3.1.2 Sistem Melakukan Pencegahan

Sistem yang akan dibangun oleh peneliti adalah client ataupun paket-paket yang harus melewati *snort network intrusion prevention system* terlebih dahulu agar nantinya sistem akan meneruskan paket tersebut apabila paket tidak teridentifikasi sebagai serangan atau penyusup dan sebaliknya jika *snort* nips ini mendefinisikan paket tersebut sebagai serangan maka sistem ini akan mencegahnya.



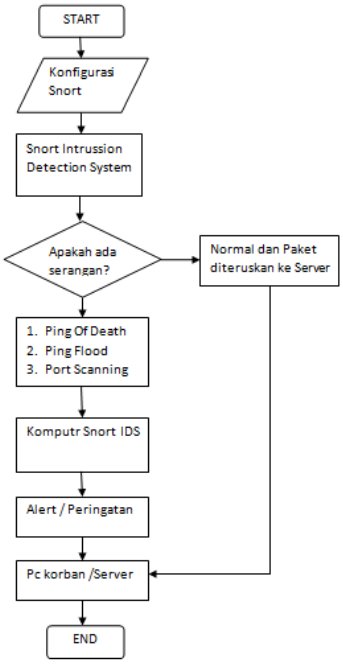
Gambar 3.1 Skema System

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

1. *Attacker* berada pada satu jaringan bersama dengan pc sebagai *snort* dan server
2. *Attacker* melakukan penyerangan terhadap server yang berada dalam satu jaringan dimana penyerang akan melewati komputer *snort* terlebih dahulu sebagai sistem pencegahan.

3. Komputer *snort* merupakan suatu sistem yang memonitoring trafic jaringan secara *real time*
4. Jika terdapat aktifitas yang mecurigakan pada jaringan dan didefinisikan sebagai serangan penyusupan, maka komputer snort *Intrusion Prevention System* akan melakukan pemblockingan.

3.2 Flowchart Sistem



Gambar 3.2 Flowchart Sistem

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

1. Konfigurasi *snort*
2. Konfigurasi *rules snort*
3. Konfigurasi *snort* sebagai *Intrusion Detection System*

3.3 Pemilihan Komponen Yang Digunakan oleh Sistem

Tahapan selanjutnya ialah melakukan pemilihan komponen utama dan komponen pendukung yang akan digunakan dalam mengkonfigurasi sistem. Adapun kompnen-komponen yang dibutuhkan sebagai berikut:

1. Komponen utama
   a. Snort versi 2.9.12
   b. Snort rules versi 2.9.12 snapshot
   c. Vmware worktation versi 12
2. Komponen pendukung
   a. Firewall
   b. MySQL
   c. Winpcap 4.1.3
   d. Notepad ++

3.4 Konfigurasi Sistem

Pada tahapan ini, komponen-komponen yang dibutuhkan akan dikonfigurasi menurut kesimpulan dan analisa kebutuhan sistem. Adapun tahapan konfigurasinya adalah:

1. Tahap konfigurasi snort dan komponen pendukung
   a. Men-download snort
   b. Men-download komponen pendukung
   c. Mengekstrak snort dan komponen pendukung
   d. Menginstal dan mengkonfigurasi snort dan komponen pendukung
2. Tahap konfigurasi snort
   a. Men-download rules snort
   b. Mengekstrak dan menginstal snort
   c. Mengkonfigurasi snort dengan rules snort yang digunakan
3. Tahap konfigurasi rules snort
   a. Mendownload rules snort
   b. Mengekstrak dan mengkonfigurasi rules snort
4. Tahap konfigurasi firewall
   a. Mengaktifkan firewall
   b. Mengkonfigurasikan firewall dengan snort

3.5 Konfigurasi Database Snort

Setelah selesai instalasi *snort*, selanjutnya dengan membuat dan mengkonfigurasi database untuk *snort*, yang nantinya akan digunakan untuk menyimpan *log* dari setiap paket serangan yang dibaca oleh *snort* NIPS. Sehingga peneliti dapat mendokumentasikan serangan-serangan yang dilancarkan oleh penyerang.

3.6 Mengkonfigurasi Snort dan Rules Snort

Agar *snort* dapat berjalan dengan maksimal perlu mengkonfigurasikannya baik itu peletakan *rules snort*, *firewall* kita perlu masuk ke etc/snort/snort.conf dan akan menampilkan banyak aturan seperti yang sudah penulis konfigurasi dibawah ini dimana *mode inline* yang digunakan adalah *mode inline afpacket* dan pada white_list_path dan black_list_path yang sebelumnya kosong penulis menambahkan rules snort etc/snort/rules dan iplist untuk mengaktifkan *firewall* yang nantinya berfungsi sebagai blocking atau pencegahan.

```
# Setup the network addresses you are protecting
  Ipvar HOME_NET 192.168.116.130

# Setup the external network addresses. Leave as
“any” in most situations
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/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists

config daq: afpacket
config daq_dir: /usr/local/lib/snort_dynamicrules
config daq_mode: inline
config policy_mode: inline
config daq_var: queue=0

# path to dyanmic preprocessor libraries
```

```
dynamicpreprocessor dictory
c:\snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine
c:\snort\lib\snort_dynamicengine\sf.engine.dll

# path to dynamic rules libraries
# dynamicdetection directory
/usr/local/lib/snort_dynamicrles
```

1. Rule snort untuk mendeteksi serangan Ping Of Death sebagai berikut :

   Alert ICMP any any -> any any (msg: " PING OF DEATH "; sid:1000005;)

2. Rule snort untuk mendeteksi serangan Ping Flood sebagai berikut :

   Alert ICMP $HOME_NET any -> any any (msg: " PING FLOOD "; sid:1000006;)

3. Rule snort untuk mendeteksi serangan Port Scanning sebagai berikut :

   Alert TCP $HOME_NET any -> any any (msg: " PORT SCANNING "; sid:1000006;)

3.7 Analisa Sistem Snort *Intrusion Detection System*

Intrusion Detection System adalah sebuah metode yang dapat mendeteksi aktifitas yang mencurigakan pada level personal *(host)* dan jaringan *(network)*. Salah satu perangkat lunak *open source* yang banyak digunakan sebagai perangkat *Intrusion Detection System* pada jaringan adalah *snort*. *Snor* selain dapat memonitoring dan menganalisa paket data pada jaringan juga dapat mendeteksi aktifitas yang mencurigakan dapa jaringan. Hasil deteksi tersebut disimpan dalam *log database.*

3.8 Analisa Sistem Snort *Intrusion Prevention System*

Seperti yang sudah dijelaskan sebelumnya, bahwasanya pada skripsi ini akan mengkonfigurasi sebuah sistem yang mempunyai kemampuan untuk mendeteksi adanya aktifitas yang mencurigakan di dalam jaringan yang terdeteksi sebagai serangan penyusupan dan akan melakukan pencegahan terhadap serangan penyusupan tersebut. Sistem yang akan dikonfigurasikan merupakan pengembangan dari sistem yang sudah ada sebelumnya.

Meskipun *Snort* mempunyai banyak fitur dengan berbagai kelebihan, tetapi masih mempunyai keterbatasan dalam fungsi yang disediakannya, diantaranya yaitu Snort belum mampu untuk mencegah serangan secara langsung, *Snort* dapat memberikan alert pemberitahuan kepada *network administrator* ketika terjadi serangan tapi belum menyediakan fasilitas untuk mencegah serangan secara otomatis.

3.9 Perangkat Lunak dan Perangkat Keras yang digunakan

Tahap ini merupakan konfigurasi sistem yang dilakukan, melingkupi dari kebutuhan perangkat keras *(hardware)* dan perangkat lunak *(software)* berdasarkan studi pustaka yang sudah dilakukan sebelumnya dan melihat kecocokan komponen sistem yang dibutuhkan oleh perangkat keras dan perangkat lunak. Lingkungan implementasi untuk mengkonfigurasi *Snort* sebagai pendeteksi dan pencegahan penyusupan terdiri dari:

1. Perangkat Keras

   Perangkat keras yang digunakan memiliki spesifikasi sebagai berikut:

   a. Processor : Intel (R) Core (TM) i3 2.40 GHz
   b. Memory : 4 GB
   c. Harddisk : 500 GB

2. Perangkat Lunak

   Perangkat lunak yang digunakan memiliki spesifikasi sebagai berikut:

   a. Virtual Mesin : Vmware Worktation 12
   b. Sistem Operasi : Windows 7 Professional
   c. Editor Text : Notepad ++
   d. Snort : Snort versi 2.9.12
   e. Rules Snort : Snortrules-snapshot-2.9.12
   e. Plugin : Winpcap 4.1.3
   f. Firewall : Bawaan Windows 7

Selanjutnya adalah pengujian (testing). Pada tahapan ini menggambarkan kondisi-kondisi yang terjadi apabila sistem dijalankan, pengujian dilakukan dengan cara mengetes serangan penyusupan diantara lain:

1. Pengujian Ping Of Death
2. Pengujian Ping Flood
3. Port Scanning

IV. IMPLEMENTASI DAN PENGUJIAN

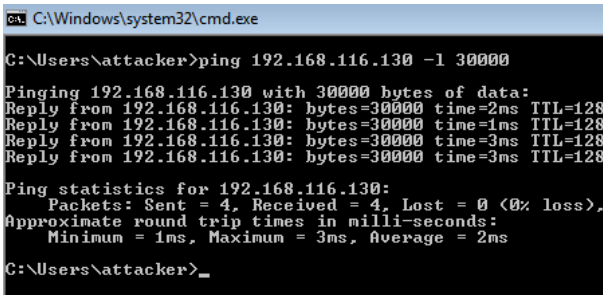
3.1 Pendahuluan

Tahapan selanjutnya adalah tahap implementasi dan pengujian. Pada tahap ini, hasil analisa dan perancangan sistem yang dibuat akan diimplementasikan ke dalam bentuk nyata dan kemudian akan dilakukan pengujian untuk mengetahui hasil dari analisa dan perancangan yang telah dilakukan.

3.2 Pengujian Ping of Death

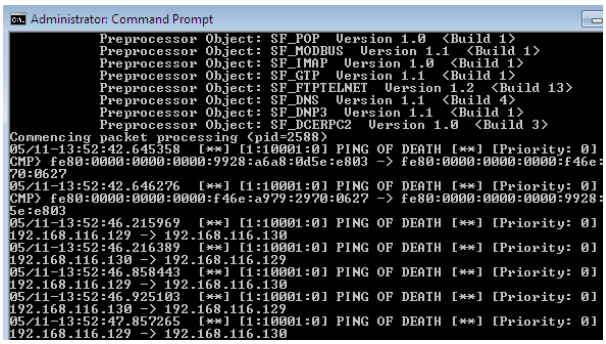
Pada pengujian ini, pc sebagai penyerang akan mencoba melakukan serangan Denial Of Service (DoS) berupa Ping Of Death, yaitu dengan cara mengirimkan ICMP dalam jumlah besar ke server.

1. Komputer sebagai penyerang melakukan serangan Ping Of Death



Gambar 4.1 Serangan Ping Of Death

2. Komputer Snort berhasil mendeteksi sebuah serangan penyusup



Gambar 4.2 Snort mendeteksi Ping Of Death

Dari pengamatan diatas bahwasanya paket berupa *Ping Of Death* dapat di deteksi dengan baik oleh komputer snort ids melalui terminalnya, pada gambar 4.1 paket berhasil menyerang sebanyak 30.000 bytes ke 1p 192.168.116.130 pc korban, pada gambar 4.2 paket serangan berhasil di deteksi oleh snort ids.

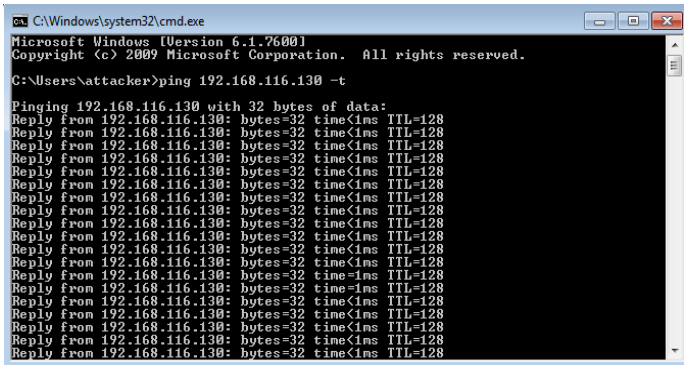
Tabel 4.1 Pengujian Ping Of Death

Deskripsi dan kondisi	Tool dan IP address penyusup	Percobaan dan pengujian	Keluaran	Hasil dan kesimpulan
Snort Intrussion Detection System aktif	Terminal Ip address 192.168.116.129	Penyusup melakukan serangan Ping Of Death pada pc sebagai korban	Tampil ip address penyusup dan korban dalam bentuk alert dan sistem melakukan pendeteksian	Tampil ip address penyusup dan korban dalam bentuk alert pada terminal Dan pengujian pendeteksian berhasil

3.3 Pengujian Ping Flood

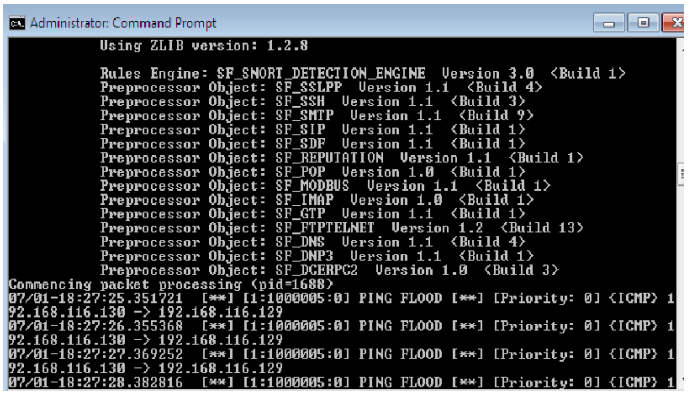
Pada pengujian kali ini, pc sebagai penyerang akan mencoba melakukan serangan Ping Flood, yaitu penyerang mengirim sejumlah besar permintaan Echo ICMP

1. Komputer sebagai penyerang melakukan serangan Ping Flood



Gambar 4.3 Serangan Ping Flood

2. Komputer Snort berhasil mendeteksi sebuah serangan penyusup



Gambar 4.4 Snort mendeteksi Ping Flood

Dari pengamatan diatas bahwasanya paket berupa *Ping Flood* dapat di deteksi dengan baik oleh komputer snort ids melalui terminalnya, pada gambar 4.3 paket berhasil menyerang pc korban, pada gambar 4.4 paket serangan berhasil di deteksi oleh snort ids yang aktif.

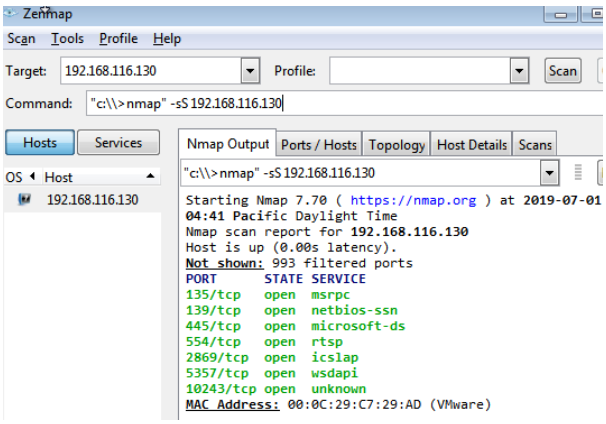
Tabel 4.2 Pengujian Ping Flood

Deskripsi dan kondisi	Tool dan IP address penyusup	Percobaan dan pengujian	Keluaran	Hasil dan kesimpulan
Snort Intrussion Detection System aktif	Terminal Ip address 192.168.116.129	Penyusup melakukan serangan Ping Flood	Tampil ip address penyusup dan korban dalam bentuk alert dan sistem melakukan pendeteksian	Tampil ip address penyusup dan korban dalam bentuk alert pada terminal Dan pengujian pendeteksian berhasil

3.4 Pengujian Port Scanning

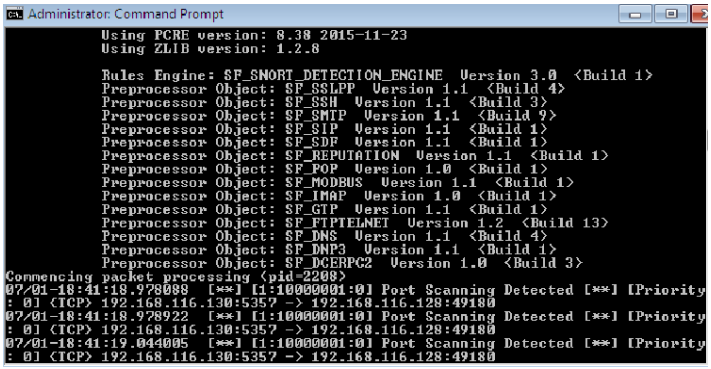
Pada pengujian kali ini, pc sebagai penyerang akan mencoba melakukan serangan Port Scanning, yaitu dimana penyerang akan melakukan pemeriksaan status port TCP dan UDP yang terbuka pada mesin, untuk melancarkan serangan Port Scanning, peneliti menggunakan aplikasi tambahan yakni NMAP.

1. Komputer sebagai penyerang melakukan serangan Port Scanning



Gambar 4.5 Serangan Port Scanning

2. Komputer Snort berhasil mendeteksi sebuah serangan penyusup



Gambar 4.6 Snort mendeteksi Port Scanning

Pada percobaan port scanning ini bisa dilihat di gambar 4.5 bahwasanya port 135/tcp open msrpc, port 139/tcp open netbios-ssn, port 445/tcp open microsoft-ds, port 554/tcp open rtsp, port2869/tcp open icslap dan port 5357/tcp open wsdapi. Pada gambar terlihat port – port yang disebut diatas adalah port yang terbuka semua dengan mengunakan NMAP. Pada gambar 4.6 bisa dilihat hasil tangkapan atau monitoring snort yang nantinya juga disimpan di log.

Tabel 4.3 Pengujian Port Scanning

Deskripsi dan kondisi	Tool dan IP address penyusup	Percobaan dan pengujian	Keluaran	Hasil dan kesimpulan
Snort Intrussion Detection System aktif	Terminal Ip address 192.168.116.129	Penyusup mencoba melakukan serangan Port Scanning	Tampil ip address penyusup dalam bentuk alert dan sistem melakukan pendeteksian	Tampil ip address penyusup dan dalam bentuk alert Berhasil

IV PENUTUP

Pada tahap akhir penulisan laporan ini adalah penutup, tahap ini berisi kesimpulan dan saran setelah melakukan semua konfigurasi dengan baik apa yang didapat dari hasil penelitian tersebut.

1. Kesimpulan

Berdasarkan hasil konfigurasi snort pada windows 7 dapat disimpulkan sebagai berikut :

1. Snort versi terbaru saat ini 2.9.12 sebagai sistem pendeteksi cocok dikonfigurasikan pada windows 7.
2. Snort IDS dapat bekerja dengan baik yang mampu mendeteksi paket paket serangan seperti Ping Of Death dan Ping Flood
3. Snort IPS sebagai sistem pecegahan tidak dapat berjalan dengan baik pada sistem operasi Windows, dikarenakan rules Snort tidak mendukung untuk firewall bawaan windows

2. Saran

Berdasarkan penelitian yang telah peyusun lakukan masih belum sempurna maka diharapkan pada penelitian selanjutnya dapat membangun sebuah sistem Snort yang lebih handal lagi jadi saran dari penulis sebagai berikut :

1. Diharapkan pada penelitian selanjutnya dapat mengkonfigurasi snort yang mampu melakukan pencegahan meskipun dalam rule snort tidak tersedia
2. Diharapkan pula pada penelitian selanjutnya bisa mendeteksi lebih banyak lagi serangan.
3. Pada penelitian selanjutnya bisa mengintregrasikan snort dengan sms server sehingga dapat administrator jaringan tidak harus selalu stanby didepan komputer serta lebih cepat dan tanggap pula untuk mengetahui adanya serangan.

DAFTAR PUSTAKA

Agita Syaimi, Perancangan dan Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort IDS , Jurusan Teknik Elektro Institut Teknologi Nasional Bandung, 2013

Andi Supriyadi, Dhani Gartina, Memilih Topologi Jaringan dan Hardware dalam Desain Sebuah Jaringan Komputer, 2007

Arpenta L.T. Ginting, Sistem Monitoring Pendeteksian Penyusup Menggunakan Snort pada Jaringan Komputer Fakultas Ekonomi Universitas Methodist Indonesia, Program Studi D-III Manajemen Informatika, Universitas Methodist Indonesia, 2015

Asep Herman Suyanto, Pengenalan Jaringan Komputer, Universitas Gadjah Mada Yogyajarta, 2004

Diskkhams Maulidi, Mydza, Analisa dan Konfigurasi Network Intrusion Prevention System (NIPS) pada Linux Ubuntu 10.04 LTS, 2011

Dodik, Analisis Pendeteksian Dan Pencegahan Penyusup Jaringan Dengan Menggunakan Konfigurasi NIPS Snort, 2017

Edy Victor Haryanto, Sistem Operasi Konsep dan Teori, Yogyakarta, 2012

Eueung Mulyana, Onno W, Firewall Sekuriti Internet, Purbo Computer Network Research Group ITB

Rahmat Rafiudin, Mengganyang Hacker dengan Snort, Yogyakarta, 2012

Richardus Eko Indrajit, Aneka Ragam Serangan di Dunia Maya,

Sritrusta Sukaridhoto, ST. Ph.D. Buku Jaringan Komputer I, Politeknik Elektronika Negeri Surabaya, 2014

Yoga Widya Pradipta, Implementasi Intrusion Prevention System (IPS) Menggunakan Snort dan Ip Tables Berbasis Linux, Jurusan Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya, 2017

BIODATA PENULIS

Penulis merupakan anak pertama dari 3 bersaudara dari pasangan Bapak Abd.Hamid Mansur dan Ibu Sunarsih yang lahir di Probolinggo pada 18 Maret 1996. Penulis mulai mengenyam pendidikan dasar SDN 1 Gerongan, kemudian pada tahun 2008 melanjutkan pendidikan di SMPN 3 Gading, kemudian pada tahun 2011 melanjutkan pendidikan di SMK Zainul Hasan Genggong, dan pada tahun 2014 penulis kursus bahasa inggris di kampung inggris Pare Kediri selama 6 bulan, setelah itu penulis melanjutkan pendidikan di ITN Malang dengan mengambil jurusan Teknik Elektro dengan peminatan yang dipilih Teknik Komputer S1.

Email : usamaassegaf@gmail.com