

# **INTRUSION PREVENTION SYSTEM BERBASIS FWSNORT DAN PSAD**

Skripsi



oleh  
**ENDRA DWI PRASETIA**  
**22074315**

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI  
UNIVERSITAS KRISTEN DUTA WACANA  
2012

# **INTRUSION PREVENTION SYSTEM BERBASIS FWSNORT DAN PSAD**

Skripsi



Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi  
Universitas Kristen Duta Wacana  
Sebagai Salah Satu Syarat dalam Memperoleh Gelar  
Sarjana Komputer

Disusun oleh

**ENDRA DWI PRASETIA**  
**22074315**

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI  
UNIVERSITAS KRISTEN DUTA WACANA  
2012

## PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

### **Intrusion Prevention System Berbasis Fwsnort dan PSAD**

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 28 September 2012



ENDRA DWI PRASETIA

22074315

## HALAMAN PERSETUJUAN

Judul Skripsi : Instrusion Prevention System Berbasis Fwsnort dan PSAD  
Nama Mahasiswa : ENDRA DWI PRASETIA  
N I M : 22074315  
Matakuliah : Skripsi (Tugas Akhir)  
Kode : TIW276  
Semester : Gasal  
Tahun Akademik : 2012/2013



Telah diperiksa dan disetujui di  
Yogyakarta,  
Pada tanggal 28 September 2012

Dosen Pembimbing I

Willy Sudiarto Raharjo, SKom.,M.Cs

Dosen Pembimbing II

Joko Purwadi, M.Kom

## HALAMAN PENGESAHAN

### INTRUSION PREVENTION SYSTEM BERBASIS FWSNORT DAN PSAD

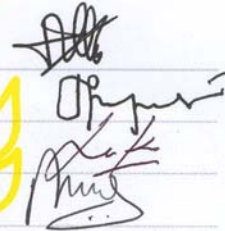
Oleh: ENDRA DWI PRASETIA / 22074315

Dipertahankan di depan Dewan Penguji Skripsi  
Program Studi Teknik Informatika Fakultas Teknologi Informasi  
Universitas Kristen Duta Wacana - Yogyakarta  
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar  
Sarjana Komputer  
pada tanggal 19 September 2012


Yogyakarta, 28 September 2012  
Mengesahkan,

Dewan Penguji:

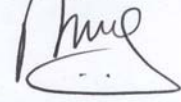
1. Willy Sudiarto Raharjo, SKom., M.Cs
2. Joko Purwadi, M.Kom
3. Lukas Chrisantyo, M.Eng.
4. Nugroho Agus Haryono, M.Si



Dekan

  
(Drs. Wimmie Handiwidjojo, MIT.)

Ketua Program Studi

  
(Nugroho Agus Haryono, M.Si)

## UCAPAN TERIMA KASIH

Segala puji dan syukur penulis naikkan bagi Tuhan Yesus Kristus yang telah melimpahkan segala berkat, rahmat, bimbingan, dan perlindungan-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul “Instution Prevention System Berbasis Fwsnort dan PSAD” dengan baik dalam semester ini.

Penulisan laporan Tugas Akhir ini merupakan kelengkapan dan pemenuhan dari salah satu syarat untuk memperoleh gelar Sarjana Komputer. Selain itu bertujuan melatih mahasiswa untuk dapat menghasilkan suatu karya yang dapat dipertanggungjawabkan secara ilmiah, sehingga dapat bermanfaat bagi penggunaanya.

Dalam menyelesaikan pembuatan analisis penelitian dan laporan Tugas Akhir ini, penulis telah banyak menerima bimbingan, saran dan masukan dari berbagai pihak, baik secara langsung maupun secara tidak langsung. Untuk itu dengan segala kerendahan hati, pada kesempatan ini penulis menyampaikan ucapan terimakasih kepada :

1. Bapak **Willy Sudiarto Raharjo, S. Kom, M. Cs**, selaku dosen pembimbing I yang telah banyak memberikan ide, masukan kritik dan saran dalam penulisan laporan dan pembuatan Tugas Akhir ini.
2. Bapak **Joko Purwadi S.Kom, M.Kom**, selaku pembimbing II yang telah banyak memberikan masukan dan saran selama penulisan laporan Tugas Akhir ini.
3. **PPUKDW dan PUSPINDIKA UNIVERSITAS KRISTEN DUTA WACANA** yang mengizinkan penulis untuk melakukan implementasi di lab, peminjaman peralatan dan IP publik yang tidak ternilai harganya, sehingga penulis mendapatkan banyak pengalaman baru.
4. Ayah dan Ibu tercinta, Laurentius Agus Mahendra Wibowo dan Chatarina Endang Kuswantini, kakak dan adik tercinta Agatha Intania Riza Febrianti dan Theresia Ria Anjani Kurniawati yang dengan segala kasih sayang dan

perhatian serta dukungan doa kepada penulis, sehingga penulis mampu menyelesaikan Tugas Akhir ini.

5. Teman-teman DWTC angkatan 2007 dan 2008, Unyil, Celeng, Roy, Bogi, Ori, Cane, Roy, Celna, Riris, dll. yang senantiasa memberi semangat, masukan, dan menghibur dalam mengerjakan Tugas Akhir ini.
6. Rekan-rekan dan pihak-pihak yang tidak dapat penulis sebutkan satu persatu yang secara langsung maupun tidak langsung yang telah mendukung penyelesaian Tugas Akhir ini. Terimakasih atas dukungan dan doanya.

Penulis menyadari bahwa penelitian dan laporan Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca, sehingga suatu saat penulis dapat memberikan karya lebih baik lagi.

Akhir kata, penulis ingin meminta maaf apabila terjadi kesalahan baik dalam penyusunan laporan maupun yang pernah penulis lakukan selama membuat Tugas Akhir.

Yogyakarta, 5 September 2012

Penulis



MOTTO

*KEGAGALAN ADALAH SEBUAH  
PROSES UNTUK MENCAPAI  
KESUKSESAN*

© UKDW



## INTISARI

### Institution Prevention System Berbasis Fwsnort dan PSAD

Perkembangan jaringan internet saat ini memiliki masalah yang cukup serius yaitu terdapat celah serangan pada jaringan internet. Banyak kasus serangan yang terjadi karena beberapa orang tidak menyadari pentingnya keamanan jaringan untuk diterapkan pada sistem yang ada.

IPS (Intrusion Prevention System) merupakan solusi untuk masalah tersebut, IPS berfungsi sebagai sebuah sistem yang bekerja dengan memantau lalu lintas jaringan. Agar dapat bekerja secara optimal, IPS satu dengan yang lain bisa saling digabungkan. Fwsnort dan PSAD merupakan IPS berbasis *log* yang mampu menangkap, memeriksa, dan membuang setiap paket yang masuk dalam jaringan berdasarkan *rules* yang dimilikinya melalui IPtables. IPS juga mampu melakukan DROP paket terhadap IP yang sudah melakukan penyusupan agar tidak mampu lagi melakukan serangan pada sistem. Sistem alert yang dimiliki IPS Fwsnort dan PSAD mampu memudahkan administrator untuk mengetahui kejadian yang ada melalui email.

Hasil penelitian menunjukkan bahwa kemampuan IPS Fwnort dan PSAD cukup baik dalam mendeteksi serangan jaringan yang ada. IPS sulit mendeteksi serangan pada layer aplikasi, karena serangan-serangan tersebut memanfaatkan protokol yang sah dan diijinkan oleh IPS Fwsnort dan PSAD. Sistem alert yang dimiliki oleh IPS PSAD dan Fwsnort ini cukup baik karena false alarm yang dimunculkan IPS ini mampu diminimalkan dengan konfigurasi yang benar.

## DAFTAR ISI

PERNYATAAN KEASLIAN SKRIPSI.....	iii
HALAMAN PERSETUJUAN.....	iv
HALAMAN PENGESAHAN.....	v
<b>MOTTO.....</b>	<b>viii</b>
<b>INTISARI.....</b>	<b>ix</b>
<b>DAFTAR ISI.....</b>	<b>x</b>
<b>DAFTAR GAMBAR.....</b>	<b>xiii</b>
<b>DAFTAR TABEL.....</b>	<b>xiv</b>
<b>BAB 1.....</b>	<b>1</b>
<b>PENDAHULUAN.....</b>	<b>1</b>
1.1. Latar Belakang Masalah.....	1
1.2. Rumusan Masalah.....	2
1.3. Batasan Masalah.....	2
1.4. Hipotesis.....	3
1.5. Tujuan Penelitian.....	3
1.6. Metode Penelitian.....	3
1.7. Sistematika Penulisan.....	3
<b>BAB 2.....</b>	<b>5</b>
<b>LANDASAN TEORI.....</b>	<b>5</b>
2.1. Tinjauan Pustaka.....	5
2.2. Landasan Teori.....	6
2.2.1. Intrusion Detection System (IDS).....	6

2.2.2.	Intrusion Prevention System (IPS).....	10
2.2.3.	Fwsnort.....	12
2.2.4.	Port Scan Attack Detector (PSAD).....	13
2.2.5.	Iptables.....	13
2.2.6.	DoS ( <i>Denial of Service</i> ).....	15
2.2.7.	<i>Metasploit Framework</i> .....	15
2.2.8.	<i>SQL Injection</i> .....	15
2.2.9.	Port Scan.....	16
BAB 3.	.....	19
PERANCANGAN DAN PENELITIAN	.....	19
3.1.	Kebutuhan <i>Hardware</i> dan <i>Software</i> .....	19
3.1.1.	Kebutuhan <i>Hardware</i> .....	19
3.1.2.	Kebutuhan <i>Software</i> .....	20
3.2.	Rancangan Penelitian dan Desain <i>Topologi</i> .....	24
3.3.	Perancangan Skenario Penelitian.....	25
3.3.1.	Perancangan Skenario Pengujian Penyusupan.....	25
BAB 4.	.....	27
IMPLEMENTASI DAN ANALISIS SISTEM	.....	27
4.1.	Pemasangan Intrusion Prevention System pada <i>Topologi</i> Penelitian.....	27
4.2.	Pengujian Skenario Port Scanning.....	37
4.2.1.	Pengujian Port Scanning.....	37
4.2.2.	Analisis Pengujian Port Scanning.....	41
4.3.	Pengujian Skenario Menggunakan <i>Metasploit Framework</i> .....	42
4.3.1.	Pengujian menggunakan <i>Metasploit Framework</i> .....	42

4.3.2.	Analisis Pengujian menggunakan <i>Metasploit Framework</i> .....	47
4.4.	Pengujian Skenario <i>Denial of Service (DoS)</i> .....	48
4.4.1.	Pengujian <i>Denial of Service (DoS)</i> .....	48
4.4.2.	Analisis Pengujian <i>Denial of Service (DoS)</i> .....	51
4.5.	Pengujian Skenario dengan <i>SQL injection</i> .....	51
4.5.1.	Pengujian <i>SQL injection</i> .....	51
4.5.2.	Analisis Pengujian <i>SQL injection</i> .....	59
BAB 5.	.....	61
KESIMPULAN DAN SARAN.	.....	61
5.1.	Kesimpulan.....	61
5.2.	Saran.....	62
DAFTAR PUSTAKA.	.....	63



UKDWN

## DAFTAR GAMBAR

Gambar 2.1 Perbedaan IPS dengan IDS.....	10
Gambar 2.2 IPTables Flow Chart.....	14
Gambar 2.3 TCP three-way handshake.....	16
Gambar 3.1 Aplikasi Zenmap.....	22
Gambar 3.2 Tampilan Squirrelmail.....	23
Gambar 3.3 Aplikasi Putty.....	23
Gambar 3.4 Topologi Penelitian IPS Fwsmort dan PSAD.....	25
Gambar 3.5 Topologi Serangan Pada DMZ Server.....	25
Gambar 4.1 Topologi Penelitian IPS.....	28
Gambar 4.2 Alamat IP Pada Setiap Device.....	30
Gambar 4.3 Hasil Port Scanning Menggunakan Intense Scan.....	38
Gambar 4.4 Hasil Port Scanning Menggunakan Slow comprehensive scan.....	40
Gambar 4.5 Proses serangan menggunakan <i>Metasploit Framework</i> .....	45
Gambar 4.6 Proses Prevention PSAD.....	47
Gambar 4.7 Proses <i>SQL Injection</i> menggunakan Havij.....	53



## DAFTAR TABEL

Tabel 3.1 Spesifikasi IPS.....	19
Tabel 3.2 Spesifikasi DMZ atau dummy server.....	19
Tabel 3.3 Rancangan Alamat IP Penelitian IPS Fwport dan PSAD.....	24
Tabel 4.1 List rules Fwport.....	35

© UKDW

## INTISARI

### Instution Prevention System Berbasis Fwsnort dan PSAD

Perkembangan jaringan internet saat ini memiliki masalah yang cukup serius yaitu terdapat celah serangan pada jaringan internet. Banyak kasus serangan yang terjadi karena beberapa orang tidak menyadari pentingnya keamanan jaringan untuk diterapkan pada sistem yang ada.

IPS (Intrusion Prevention System) merupakan solusi untuk masalah tersebut, IPS berfungsi sebagai sebuah sistem yang bekerja dengan memantau lalu lintas jaringan. Agar dapat bekerja secara optimal, IPS satu dengan yang lain bisa saling digabungkan. Fwsnort dan PSAD merupakan IPS berbasis *log* yang mampu menangkap, memeriksa, dan membuang setiap paket yang masuk dalam jaringan berdasarkan *rules* yang dimilikinya melalui IPTables. IPS juga mampu melakukan DROP paket terhadap IP yang sudah melakukan penyusupan agar tidak mampu lagi melakukan serangan pada sistem. Sistem alert yang dimiliki IPS Fwsnort dan PSAD mampu memudahkan administrator untuk mengetahui kejadian yang ada melalui email.

Hasil penelitian menunjukkan bahwa kemampuan IPS Fwnort dan PSAD cukup baik dalam mendeteksi serangan jaringan yang ada. IPS sulit mendeteksi serangan pada layer aplikasi, karena serangan-serangan tersebut memanfaatkan protokol yang sah dan diijinkan oleh IPS Fwsnort dan PSAD. Sistem alert yang dimiliki oleh IPS PSAD dan Fwsnort ini cukup baik karena false alarm yang dimunculkan IPS ini mampu diminimalkan dengan konfigurasi yang benar.

# BAB 1

## PENDAHULUAN

### 1.1.Latar Belakang Masalah

Keamanan komputer maupun jaringan komputer, terutama yang terhubung ke internet harus direncanakan dan dikoordinasikan dengan baik agar dapat melindungi sumber daya (*resource*) dan investasi di dalamnya. Informasi (*data*) dan *service* (pelayanan) sudah menjadi sebuah komoditi yang sangat penting. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi suatu organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Salah satu contoh keamanan komputer untuk melindungi jaringan komputer yang ada adalah *firewall*.

Teknologi *firewall* yang sudah ada dirasa kurang baik dalam mendeteksi penyusupan yang ada. Karena *firewall* dirancang untuk memblokir suatu aktifitas di mana penyusupan dilakukan secara tegas. Prosedur *firewall* juga dimanfaatkan oleh program-program *exploit* untuk masuk ke sistem tertentu dengan menggunakan sebuah protokol yang diijinkan oleh *firewall*.

Sistem Pendeteksian *Intrusion Detection System (IDS)* memegang peranan penting dalam pengamanan jaringan. Fwsnort merupakan salah satu produk *Open Source* yang menjadi pilihan ideal sebagai pendeteksi intrusi dalam jaringan. Namun perlu diketahui bahwa fungsi dari Fwsnort bisa dikembangkan menjadi sebuah Sistem *Intrusion Prevention System (IPS)*, dengan bantuan *Port Scan Attack Detector (PSAD)*. Dalam pengerjaan Tugas Akhir ini penulis akan merancang dan membuat sistem yang mampu mendeteksi suatu penyusupan dengan menggabungkan Fwsnort dan PSAD. Ketika Fwsnort mendeteksi adanya



intrusi maka alamat IP, *port* asal dan informasi lainnya tentang penyerang akan ditampung sebagai *alert*. Kemudian *alert* akan diterima oleh *Blockit* sehingga nantinya *Blockit* menetapkan suatu tindakan mengkonfigurasi ulang rule *Firewall* untuk menghadang alamat IP penyerang. Setelah jangka waktu tertentu maka *Blockit* akan membuka kembali koneksi IP *address* tersebut.

## 1.2.Rumusan Masalah

Rumusan yang akan dibahas oleh penulis yaitu analisis kualitas data pada Intrusion Prevention System dengan menggunakan PSAD yang dikombinasikan dengan Fwsnort pada saat pengambilan tindakan pada paket yang berbahaya melalui skenario serangan.

## 1.3.Batasan Masalah

Adapun batasan-batasan masalah yang dilakukan dalam penelitian ini :

- a. Penelitian hanya diimplementasikan pada IP publik milik PUSPINDIKA.
- b. Serangan yang akan dideteksi berasal dari jaringan luar jaringan vital, serangan yang berasal dari dalam jaringan vital tidak akan dideteksi.
- c. Pada penulisan ini tidak membahas mengenai source code atau tool yang digunakan untuk uji coba serangan pada sistem.
- d. Pada penulisan tugas akhir ini tidak akan dibahas tentang pembuatan *rulesFwsnort*.
- e. *Rules* yang digunakan menggunakan *rules* snort versi snort-2.9.0, yang diambil dari <http://rules.emergingthreats.net/open/snort-2.9.0/emerging-all.rules>.
- f. Sistem ini dibangun menggunakan Sistem Operasi Ubuntu Server 11.10
- g. Tidak membahas tentang konfigurasi DMZ atau *dummy server*.

#### **1.4.Hipotesis**

Fwsnort dan PSAD dapat mengenali dan menganalisis serangan yang masuk berdasarkan *rules* yang sudah ada pada IPTables. Bila pola serangan tersebut cocok dengan *rules* yang ada, maka dilakukan pencegahan alamat IP dengan menggunakan IPTables agar serangan tidak dapat dilakukan kembali.

#### **1.5.Tujuan Penelitian**

Penelitian ini bertujuan untuk mengembangkan *Intrusion Prevention System* (IPS) yang bekerja untuk melakukan pencegahan aktifitas penyusup terhadap *server* dengan memblokir alamat IP dengan menggunakan PSAD dan Fwsnort untuk mendeteksi dan menghentikan lalu lintas yang berbahaya.

#### **1.6.Metode Penelitian**

Metode yang digunakan dalam melakukan penelitian adalah :

- a. Analisis permasalahan
- b. Melakukan kajian literatur
- c. Merancang prototipe penelitian, dengan pemasangan Fwsnort dan PSAD pada IP publik PUSPINDIKA.
- d. Pengambilan sampel data
- e. Pengolahan data pengamatan
- f. Penarikan kesimpulan

#### **1.7.Sistematika Penulisan**

Bab 1 PENDAHULUAN, membahas tentang latar belakang masalah dari penelitian, rumusan masalah, batasan-batasan masalah, metode penelitian, hipotesis, tujuan serta sistematika penulisan dari penelitian ini.

Bab 2 TINJAUAN PUSTAKA DAN LANDASAN TEORI, berisi bahasan penelitian dan berbagai referensi mengenai penelitian IPS, Fwsnort, dan

PSADserta landasan teori yang menjadi dasar penelitian ini. Pada bab ini akan diterangkan secara detail sesuai informasi yang diperoleh berkaitan dengan keamanan jaringan

Bab 3 ANALISIS DAN PERANCANGAN, berisi rancangan dari IPS yang mengimplementasikan Fwsnort dan PSAD. Kerja sistem, serta spesifikasi kebutuhan *hardware* dan *software* yang dipakai untuk melakukan penelitian, serta langkah-langkah penelitian yang dilakukan.

Bab 4 IMPLEMENTASI SISTEM DAN ANALISIS SISTEM, berisi uraian detail implementasi sistem dan hasil analisis yang didapatkan dari hasil implementasi dari setiap tahap penelitian.

Bab 5 KESIMPULAN DAN SARAN, berisi kesimpulan dari hasil penelitian serta saran berkaitan dengan implementasi Fwsnort dan PSAD.



## BAB 5

### KESIMPULAN DAN SARAN

#### 5.1. Kesimpulan

Berdasarkan hasil implementasi dan analisis sistem, maka diperoleh kesimpulan sebagai berikut :

- a. Konfigurasi PSAD dan Fwsnort harus disesuaikan dengan versi kernel dan jenis sistem operasi yang digunakan, khususnya konfigurasi file untuk penyimpanan pesan *log* agar *log analyzer* yang dimiliki PSAD dapat berjalan dengan baik. Pada konfigurasi PSAD pada ubuntu 11.10 file *log* terdapat pada `/var/log/kern.log`, yang secara default konfigurasi PSAD `/var/log/messages`.
- b. IPS PSAD dan Fwsnort tidak mampu mencegah serangan DoS yang menggunakan tool *slowloris.pl*. Solusi serangan ini hanya bisa dicegah dengan menggunakan *cluster* pada server. Pada pengujian *SQL injection*, IPS dengan menggunakan PSAD dan Fwsnort tidak mampu mendeteksi serangan yang dilakukan oleh tool *sqlmap* dan *Havij*, karena IPS tidak bisa membaca kesalahan pada kode *php*. Pada serangan DoS dan *SQL injection*, serangan ini memanfaatkan kelemahan PSAD dan Fwsnort untuk menembus protokol *http* yang sah yang diijinkan oleh IPS Fwsnort dan PSAD.
- c. Pada serangan port scan tidak semua dapat di deteksi oleh IPS PSAD dan Fwsnort, dikarenakan *rules* yang ada pada Fwsnort tidak sesuai dengan serangan port scan yang digunakan untuk pengujian. Pada serangan yang digunakan *Metasploit Framework* untuk mengeksploit semua port yang aktif, IPS berbasis PSAD dan Fwsnort hanya mendeteksi serangan pada port

*http*. Hal ini disebabkan *rules* ada ada database Fwsnort tidak terupdate, di lain sisi port scanner dan *Metasploit Framework* yang digunakan untuk serangan selalu terupdate. Sehingga metode serangan yang baru tidak semua dapat di deteksi oleh IPS Fwsnort dan PSAD.

- d. IPSPSAD dan Fwsnort mempunyai kemampuan untuk meneliti paket-paket yang masuk ke dalam jaringan internal dan mampu memberikan respon pada serangan yang masuk dengan memblokir alamat IP tersebut dengan waktu akses tertentu sesuai dengan konfigurasi yang diberikan. Hal ini yang merupakan salah satu kelebihan IPS Fsnort yang digabungkan dengan PSAD dibandingkan hanya menggunakan IPS SNORT.
- e. Untuk meningkatkan sistem alert yang dimiliki IPS Fwsnort dan PSAD digunakan konfigurasi *auto\_d* untuk memberikan nilai *danger level* pada alamat IP tertentu. Sehingga false alarm dapat diminimalkan pada sistem IPS ini.

## 5.2.Saran

Saran yang diajukan oleh penulis untuk pengembangan sistem demi mencapai hasil yang lebih baik adalah:

- a. Pengembangan penelitian selanjutnya IPS PSAD dan Fwsnort dapat digabungkan dengan SNORT agar mampu membuat *rules* sesuai dengan serangan-serangan dengan metode yang baru.
- b. Pengembangan penelitian selanjutnya dapat menggunakan DMZ dengan Sistem Operasi Windows agar dapat menambah varian serangan yang dilakukan.
- c. Pengembangan penelitian berikutnya dengan membandingkan performa IPS dengan *topologi* NIPS dengan HIPS pada saat serangan berlangsung.
- d. Pengembangan penelitian selanjutnya agar meningkatkan spesifikasi *hardware* server agar mampu menampung banyak *rules* pada iptables.

## DAFTAR PUSTAKA

- Kristianto, Yohan. (2011). *Intrusion Prevention System Berbasis Snort dan Iptables*. Yogyakarta Universitas Kristen Duta Wacana.
- Nalavade, Kamini. *Generic Network Intrusion Prevention System*. Mumbai: Computer Engineering Department.
- Rash, Michael. (2007). *Linux Firewall*. San Francisco: William Pollock.
- Rash, Michael & Orebaugh, Angela & Clark, Graham & Pinkard, Becky & Babbin, Jake. (2005). *Intrusion Prevention and Active Response: Deploying Network and Host IPS*. Rockland : Syngress Publishing.
- Smith, Mike. (2006). *A Design for Building an IPS Using Open Source Products*. United States: SANS Institute.
- Stanger, James & Lane, Patrick T. (2001). *Hack Proofing Linux: A Guide to Open Source Security*. Rockland: Syngress Publishing.
- Stiawan, Deris & Abdullah, Abdul H & Idris, Mohd Yazid. (2011). *Characterizing Network Intrusion Prevention System*. Malaysia: International Journal of Computer Application
- Wu, T. Max. (2009). *Information Assurance Tools Report – Intrusion Detection Systems*. Fort Belvoir: Defense Technical Information Center.