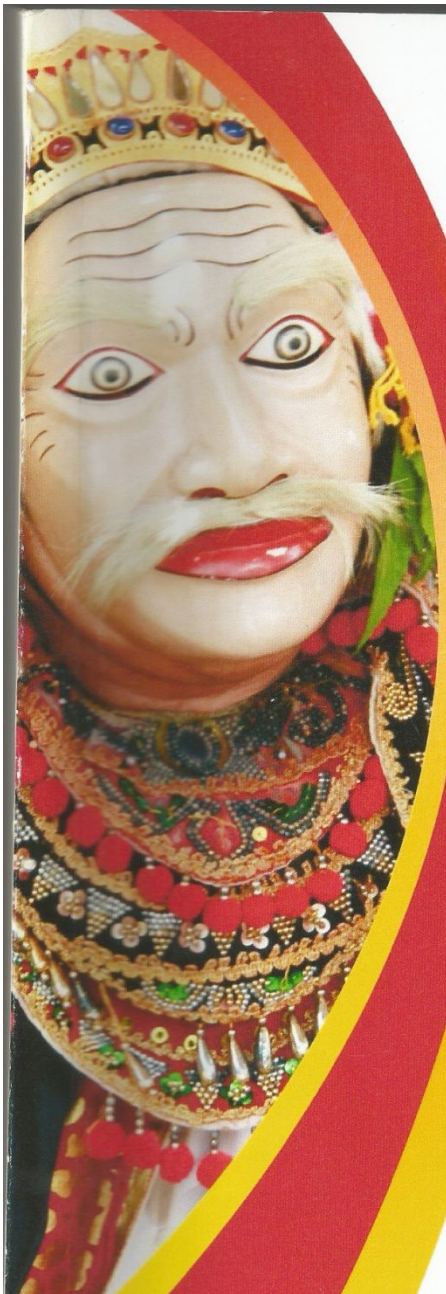
ISSN 2087-2658



PROSIDING

SEMINAR NASIONAL PENDIDIKAN TEKNIK INFORMATIKA

SENAPATI2014

Seminar Nasional Pendidikan Teknik Informatika

Tema :

***Ubiquitous Learning*:**
Teknologi Pendukung Pendidikan

Pembicara :

Onno W. Purbo
(Pakar Teknologi Informasi Indonesia)

Hotel Nikki, Denpasar
08 September 2014

Penyelenggara :
Jurusan Pendidikan Teknik Informatika, Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha
Jalan Udayana, Kampus Tengah, Singaraja Bali
Telp : +62-362-27213 , http://pti.undiksha.ac.id/senapati/
e-mail : senapati@undiksha.ac.id

PERANCANGAN DAN IMPLEMENTASI SISTEM KEAMANAN BERBASIS IDS DI JARINGAN INTERNET UNIVERSITAS BINA DARMA

Maria Ulfa [1)], Megawaty [2)]
Universitas Bina Darma
Jalan Jenderal Ahmad Yani No.12 Palembang
Mariakurniawan2009@gmail.com [1)], Megawaty.UBD@gmail.com [2)]

Abstract— Sistem keamanan komputer, dalam beberapa tahun ini telah menjadi fokus utama dalam dunia Jaringan Komputer, hal ini disebabkan tingginya ancaman yang mencurigakan (Suspicious Threat) dan serangan dari Internet. Universitas Bina Darma merupakan salah satu instansi yang aktivitasnya menggunakan layanan jaringan internet, mulai dari mengolah data yang ada, diantaranya adalah sistem KRS online, mail server dan web portal di tiap unit dan lain-lain. Pengelolah jaringan Universitas Bina Darma selama ini membangun sistem keamanan jaringan dengan menerapkan sistem firewall dan proxy sever pada tiap unit server di jaringannya. Untuk lebih mengoptimalkan sistem keamanan jaringan di universitas Bina Darma maka Pada penelitian ini penulis akan mengimplementasikan Intrusion Detection System pada jaringan Universitas Bina Darma sebagai solusi untuk keamanan jaringan baik pada jaringan Intranet maupun jaringan Internet Universitas Bina Darma. Dimana penulis akan membangun sebuah IDS (Intrusion Detection System) dengan menggunakan snort.

Keywords— ***Keamanan Jaringan, Firewall, Proxy Server, IDS (Intrusion Detection System), Snort***

LATAR BELAKANG

Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga *validitas* dan *integritas* data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan oleh pihak yang tidak berhak. Menurut Stiawan [4] Sistem keamanan komputer, dalam beberapa tahun ini telah menjadi fokus utama dalam dunia Jaringan Komputer, hal ini disebabkan tingginya ancaman yang mencurigakan (*Suspicious Threat*) dan serangan dari Internet. Keamanan Komputer (*Security*) merupakan salah satu kunci yang dapat mempengaruhi tingkat *Reliability* (keandalan) termasuk *Performance* (kinerja) dan *Availability* (tersedianya) suatu *Internetwork*.

Kerusakan yang terjadi pada suatu jaringan akan mengakibatkan pertukaran data yang terjadi pada jaringan tersebut akan melambat atau bahkan akan merusak suatu sistem jaringan. Insiden keamanan jaringan adalah suatu aktivitas terhadap suatu jaringan komputer yang memberikan dampak terhadap keamanan sistem yang secara langsung atau tidak bertentangan dengan *security policy* sistem tersebut [7].

Universitas Bina Darma merupakan salah satu instansi yang aktivitasnya didukung oleh layanan jaringan internet, mulai dari mengolah data yang ada, diantaranya adalah sistem KRS *online*, *mail server* dan *web portal* di tiap unit dan lain-lain. Pengelolah jaringan Universitas Bina Darma selama ini membangun sistem keamanan jaringan dengan menerapkan sistem *firewall* dan *proxy sever* pada tiap unit *server* di jaringannya.

Oleh karena itu, Penerapan IDS (*Intrusion Detection System*) diusulkan sebagai salah satu solusi yang dapat digunakan untuk membantu pengaturan jaringan dalam memantau kondisi jaringan dan menganalisa paket-paket berbahaya yang terdapat dalam jaringan tersebut, hal ini bertujuan untuk mencegah adanya penyusup yang memasuki sistem tanpa otorisasi atau seorang *user* yang sah tetapi menyalahgunakan *privilege* sumber daya sistem. Ada beberapa alasan untuk menggunakan IDS, diantaranya adalah mencegah resiko keamanan yang terus meningkat, mendeteksi serangan dan pelanggaran keamanan sistem jaringan yang tidak bisa dicegah oleh sistem yang umum dipakai, mendeteksi serangan awal yang mudah dilakukan, Mengamankan file yang keluar dari jaringan, sebagai pengendali untuk security design dan administrator, serta menyediakan informasi yang akurat terhadap gangguan secara langsung, meningkatkan diagnosis, recovery, dan mengoreksi faktor-faktor penyebab serangan [1].

Pada penelitian ini penulis akan merancang dan mengimplementasikan *Intrusion Detection System* pada jaringan Universitas Bina Darma sebagai solusi untuk menambah sistem keamanan jaringan baik pada jaringan *intranet* maupun jaringan internet Universitas Bina Darma. Dimana penulis akan membangun sebuah IDS (*Intrusion Detection System)* dengan menggunakan *snort,* karena *snort* merupakan IDS *open source* dan dinilai cukup bagus kinerjanya.

LANDASAN TEORI

2.1. Metode Penelitian

Metode penelitian yang di gunakan adalah penelitian tindakan atau a***ction research*** **menurut** Davison, Martinsons dan Kock [2]. Penelitian tindakan atau a***ction research*** yaitu mendeskripsikan, menginterpretasi dan menjelaskan suatu situasi atau keadaan pada jaringan VLAN *server* di Universitas Bina Darma dan melakukan analisis terhadap penerapan *Intrusion Detection System.*

Pada penerapan *Intrusion Detection System* yaitu dengan menggunakan beberapa komponen *Intrusion Detection System* yang terdiri dari *snort engine*, *rule database*, dan *alert* dengan menggunakan *software* atau modul tambahan seperti program BASE (*Basic Analysis and Security Engine*) serta sistem operasi linux ubuntu 10.04 server.

Metodologi yang digunakan dalam penelitian ini menggunakan metode penelitian tindakan atau *action research*. Adapun tahapan penelitian yang merupakan siklus dari *action research* ini yaitu :

1. Melakukan diagnosa dengan melakukan identifikasi masalah pokok yang ada pada objek penelitian. Dimana pada penelitian ini penulis melakukan diagnosa terhadap jaringan VLAN server Universitas Bina Darma yaitu dengan mengenal dan mempelajari jenis-jenis serangan yang sering terjadi dalam jaringan.

2. Membuat rencana tindakan yaitu memahami pokok masalah yang ditemukan dan menyusun rencana tindakan yang tepat. Pada tahapan ini penulis melakukan rencana tindakan yang akan dilakukan pada jaringan dengan membuat perancangan dan penerapan *Intrusion Detection System* pada jaringan VLAN server Universitas Bina Darma.

3. Melakukan tindakan disertai dengan perancangan dan implementasi rencana yang telah dibuat dan mengamati kinerja *Intrusion Detection System* pada jaringan VLAN server Universitas Bina Darma yang telah dibangun.

4. Melakukan evaluasi hasil temuan setelah proses implementasi, pada tahapan evaluasi penelitian yang dilakukan adalah hasil implementasi *Intrusion Detection System* terhadap jaringan VLAN server Universitas Bina Darma. Evaluasi ini dilakukan untuk mengetahui kelebihan dan kekurangan *Intrusion Detection System* yang sudah diterapkan pada jaringan VLAN server Universitas Bina Darma dalam meningkatkan keamanan jaringan.

5. Pembelajaran yaitu mengulas tahapan yang telah dilakukan dan mempelajari prinsip kerja *Intrusion Detection System* serta untuk memperbaiki kelemahan dari penerapan *Intrusion Detection System* pada jaringan VLAN server Universitas Bina Darma.

2.2. *Intrusion Detection System* (IDS)

IDS adalah sebuah aplikasi perangkat lunak atau perangkat keras yang bekerja secara otomatis untuk memonitor kejadian pada jarigan komputer dan menganalisis masalah keamanan jaringan. Sasaran *Intrusion Detection System* (IDS) adalah memonitoring aset jaringan untuk mendeteksi perilaku yang tidak lazim, kegiatan yang tidak sesuai, serangan atau menghentikan serangan (penyusupan) dan bahkan menyediakan informasi untuk menelusuri penyerang. Pada umumnya ada dua bentuk dasar IDS yang digunakan yaitu [6] :

1) *Network-based Intrusion Detection System*

(NIDS)

Menempati secara langsung pada jaringan dan melihat semua aliran yang melewati jaringan. NIDS merupakan strategi yang efektif untuk melihat *traffic* masuk / keluar maupun *traffic* di antara *host* atau di antara segmen jaringan lokal. NIDS biasanya dikembangkan di depan dan di belakang *firewall* dan VPN *gateway* untuk mengukur keefektifan peranti - peranti keamanan tersebut dan berinteraksi dengan mereka untuk memperkuat keamanan jaringan.

2) *Host-Based Intrusion Detection System* (HIDS)

HIDS hanya melakukan pemantauan pada perangkat komputer tertentu dalam jaringan. HIDS biasanya akan memantau kejadian seperti kesalahan *login* berkali-kali dan melakukan pengecekan pada *file*.

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

1) *Knowledge-based* atau *misuse detection*

Knowledge-based IDS dapat mengenali adanya penyusupan dengan cara menyadap paket data kemudian membandingkannya dengan *database rule* IDS (berisi *signature-signature* paket serangan). Jika paket data mempunyai pola

yang sama dengan (setidaknya) salah satu pola di *database rule* IDS, maka paket tersebut dianggap sebagai serangan, dan demikian juga sebaliknya, jika paket data tersebut sama sekali tidak mempunyai pola yang sama dengan pola di *database rule* IDS, maka paket data tersebut dianggap bukan serangan.

2) *Behavior based* (*anomaly*)

IDS jenis ini dapat mendeteksi adanya penyusupan dengan mengamati adanya kejanggalan-kejanggalan pada sistem, atau adanya penyimpangan-penyimpangan dari kondisi normal, sebagai contoh ada penggunaan memori yang melonjak secara terus menerus atau ada koneksi parallel dari 1 buah IP dalam jumlah banyak dan dalam waktu yang bersamaan. Kondisi-kondisi diatas dianggap kejanggalan yang kemudian oleh IDS jenis *anomaly based* dianggap sebagai serangan.

2.3. *Snort*

Snort tidak lain sebuah aplikasi atau *tool* sekuriti yang berfungsi untuk mendeteksi intrusi-intrusi jaringan (penyusupan, penyerangan, pemindaian dan beragam bentuk ancaman lainnya), sekaligus juga melakukan pencegahan. Istilah populernya, *snort* merupakan salah satu *tool Network Intrusion Prevention System* (IPS) dan *Network Intrusion Detection System* (NIDS) [3].

Snort bisa dioperasikan dengan tiga mode [1] :

1. Paket *sniffer* : untuk melihat paket yang lewat di jaringan.

2. Paket *logger* : untuk mencatat semua paket yang lewat di jaringan untuk di analisis dikemudian hari.

3. NIDS, deteksi penyusup pada *network* : pada mode ini *snort* akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer.

Snort mempunyai enam komponen dasar yang bekerja saling berhubungan satu dengan yang lain yaitu :

1. *Decoder* : sesuai dengan paket yang di *capture* dalam bentuk struktur data dan melakukan identifikasi *protocol, decode* IP, TCP atau tergantung informasi yang dibutuhkan.

2. *Preprocessors* : merupakan suatu saringan yang mengidetifikasi berbagai hal yang harus diperiksa seperti *detection engine*.

3. *Global Section* : mengizinkan untuk *mapping file* untuk IIS *Unicode, configure alert* untuk *proxy* server dengan *proxy alert*.

4. Server Section : mengizinkan untuk *setting* HTTP server profiles yang berbeda untuk beberapa server yang berbeda.

5. *Rules Files* : merupakan suatu *file teks* yang berisi daftar aturan yang sintaks-nya sudah diketahui.

6. *Detection Engine* : menggunakan *detection plug-in*, jika ditemukan paket yang cocok maka *snort* akan menginisialisasi paket tersebut sebagai suatu serangan.

PERANCANGAN

3.1. Analisis Kinerja *Intrusion Detection System* (IDS)

Pada penelitian ini penulis melakukan analisis dari kinerja yang dilakukan *Intrusion Detection System* (IDS) yaitu untuk meningkatkan keamanan pada sistem seperti, banyak kemungkinan analisis data untuk analisis *engine* dan dalam rangka memahami proses yang terjadi, ketika data dikumpulkan dari sensor *Intrusion Detection System* (IDS) maka data diklasifikasikan dalam beberapa bentuk dimana tergantung pada skema analisis yang digunakan. Pada penelitian ini dengan menggunakan metode *rule-based detection* atau *misuse detection* maka klasifikasi akan melibatkan aturan dan *pattern* (pola) untuk menganalisis apapun yang berasal dari luar jaringan yang tidak dikenal. Dalam mengenali sebuah serangan yang dilakukan oleh *cracker* atau *hacker* dilakukan menggunakan data yang telah diperoleh. Dimana pada penelitian ini penulis melakukan pendekatan dengan menggunakan *misuse detection*, *detektor* melakukan analisis terhadap aktivitas sistem, mencari *event* atau *set event* yang cocok dengan pola perilaku yang dikenali sebagai serangan. Pola perilaku serangan tersebut disebut sebagai *signatures*, sehingga *misuse detection* banyak dikenal sebagai *signatures based detection*. Ada empat tahap proses analisis yang ada pada *misuse detector* [4]:

1. *Preprocessing*, langkah pertama mengumpulkan data tentang pola dari serangan dan meletakkannya pada skema klasifikasi atau *pattern desciptor*. Dari skema klasifikasi, suatu *model* akan dibangun dan kemudian dimasukkan ke dalam bentuk format yang umum seperti :

a) *Signature Name* : nama panggilan dari suatu tandatangan.

b) *Signature ID* : ID yang unik.

c) *Signature Description* : Deskripsi tentang tandatangan.

d) Kemungkinan deskripsi yang palsu.

e) Informasi yang berhubungan dengan *Vulnerability* (kerentanan): *field* yang berisi semua informasi tentang *Vulnerability*.

f) *User Notes* : *field* ini mengijinkan *professional security* untuk menambahkan suatu catatan khusus yang berhubungan dengan jaringan.

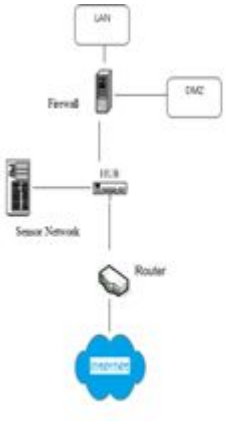
2. *Analysis*, data dan formatnya akan dibandingkan dengan *pattern* yang ada untuk keperluan analisis *engine pattern matching*. Analisis *engine* mencocokkan dengan pola serangan yang sudah dikenalnya.

3. *Response,* jika ada yang *match* (cocok) dengan pola serangan, analisis *engine* akan mengirimkan *alarm* ke *server*.

4. *Refinement* (perbaikan), perbaikan dari analisis *pattern-matching* yang diturunkan untuk memperbarui *signature*, karena *Intrusion Detection System* (IDS) hanya mengijinkan tandatangan yang terakhir yang di-*update.*

3.2 Perancangan Penempatan *Intrusion Detection System* (IDS)

Intrusion Detection System (IDS) pada suatu jaringan akan dapat bekerja dengan baik, tergantung pada peletakannya. Secara prinsip pemahaman penempatan komponen *Intrusion Detection System* (IDS) akan menghasilkan IDS yang benar-benar mudah untuk dikontrol sehingga pengamanan jaringan dari serangan menjadi lebih efisien. Sensor merupakan suatu komponen yang sangat penting dari suatu *Intrusion Detection System* (IDS). Oleh karena itu penempatannya benar-benar harus diperhatikan. *Sensor network* untuk *Intrusion Detection System* (IDS) yang akan dibangun pada jaringan internet universitas bina darma adalah diantara router dan firewall dimana pada penempatan sensor IDS di jaringan Universitas Bina Darma Untuk melindungi jaringan dari serangan *eksternal*, fungsi *sensor network* IDS sangat penting. Yang pertama dilakukan adalah menginstalasi *sensor network* IDS diantara *router* dengan *firewall*. *Sensor* IDS ini akan memberikan akses untuk mengontrol semua lalu lintas jaringan, termasuk lalu lintas pada *Demilitarized Zone.*



Gambar 1. Perancangan Penempatan Sensor Network antara Firewall dan Router

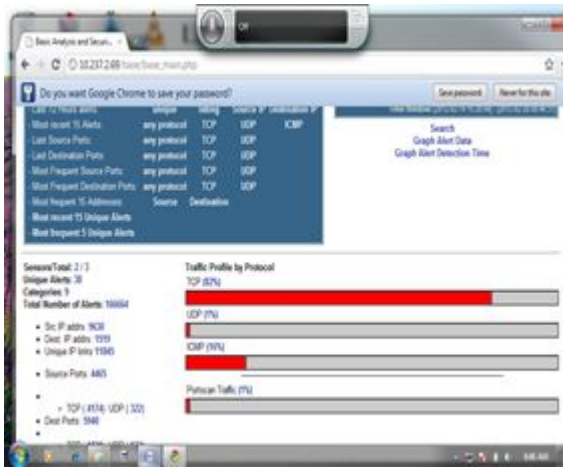
3.2. Hasil Implementasi *Intrusion Detection System* (IDS) di Jaringan Universitas Bina Darma

Hasil implementasi server IDS pada jaringan dapat di analisis jenis atau bentuk alert melalui BASE console pada penelitian ini adalah serangan yang telah dikenali oleh *signature* dan *rule* pada server *Intrusion Detection System* (IDS) pada jaringan internet Universitas Bina Darma diantaranya adalah seperti pada tabel 1 dibawah ini :

Tabel 5.1. Bentuk Serangan

	Bentuk Serangan
	Portscan TCP Portsweep
	http_inspect BARE BYTE UNICODE ENCODING
	http_inspect OVERSIZE REQUEST-URI DIRECTORY
	Portscan ICMP Sweep
	ICMP Destination Unreacheable Communication with Destination Network is Administratively rohibited.
	(portscan) TCP Portscan
	(portscan) TCP Filtered Portscan
	Community SIP TCP/IP message flooding directed to SIP Proxy
	Someone is watching your website
	Community WEB-MISC Proxy Server Access

Dari beberapa bentuk serangan diatas, maka untuk menghindari dari bentuk serangan diatas pada penelitian ini penulis memberikan solusi dengan cara, seperti pada bentuk serangan *flooding* maka di setiap server jaringan Universitas Bina Darma agar pada setiap *server firewall* melakukan proses pencegahan paket *flood syn Attack* dan paket *ping flood attack.* Kemudian untuk bentuk serangan *port scaning* yang terjadi agar melakukan pemblokiran terhadap port-port yang terbuka yang sudah dimasuki oleh penyusup melalui *server firewall*, selain itu juga dapat menggunakan perangkat lunak seperti *portsentry*. Dari bentuk-bentuk serangan yang terjadi pada jaringan internet universitas Bina Darma diatas maka dapat disimpulkan beberapa persen serangan melalui *protocol* TCP (82%), UDP (1%), ICMP (16%) dan Raw IP (1%) dapat dilihat pada gambar 2 berikut ini :



Gambar 2. Traffic Profile by Protocol

KESIMPULAN

Serangan dapat terdeteksi atau tidak tergantung pola serangan tersebut ada didalam *rule* IDS (*Intrusion Detection System)* atau tidak. Oleh karena itu pengelola *Intrusion Detection System* (IDS) harus secara rutin meng-*update rule* terbaru. Untuk mempermudah pengelolaan *rule* pada server IDS maka diperlukan *user interface* (*front end*) yang lebih baik, seperti aplikasi *webmin* yang ditambahkan *plugin snort rule*. Untuk mempermudah analisa terhadap catatan-catatan *Intrusion Detection System* (IDS) atau *security event* perlu ditambahkan program tambahan seperti BASE (*Basic Analysis and Security Engine*) atau ACID (*Analysis Console for Intrusion Databases*).

SARAN

Sebaiknya pengelolah jaringan universitas Bina Darma menggunakan *Intrusion Detection System* (IDS) untuk lebih meningkatkan keamanan jaringan, baik jaringan internet maupun jaringan intranet, sistem keamanan jaringan Universitas Bina Darma dapat memadukan sistem keamanan jaringan yang ada yaitu *firewall* dengan sistem *Intrusion Detection System* (IDS), agar dapat meningkatkan keamanan jaringan yang sudah ada sehingga menjadi lebih baik dan handal, jaringan di Universitas Bina Darma juga menggunakan alat pencegah adanya serangan seperti *honeypot* sebagai pelengkap implementasi *Intrusion Detection System*(IDS).

Daftar Pustaka

[1] Ariyus, Dony. 2007, *Intrusion Detection System, Sistem Pendeteksi Penyusup Pada Jaringan Komputer* :Andi. Yogyakarta; OFFSET

[2] Davison, R. M., Martinsons, M. G., Kock N., 2005, *Journal :* Information Systems *Journal : Principles of Canonical Action Research*

[3] Rafiudin, Rahmat., 2010, *Mengganyang Hacker dengan Snort :*Andi . Yogyakarta; OFFSET

[4] Rebecca Bace and Petter Mell, 2005 "*Intrusion Detection System*", NIST Special Publication on IDS.

[5] Stiawan, Deris., 2009. Intrusion Prevention System (IPS) dan Tantangan dalam Pengembangannya , Deris.unsri.ac.id.[Diakses 2 November 2011].

[6] Thomas, Tom., 2005, *Networking Security First-Step*: Andi. Yogyakarta; OFFSET.

[7] Wiharjito, Tony., 2006, *Keamanan Jaringan Internet* : Jakarta ; PT. Gramedia.