SISTEM PENDETEKSI SERANGAN FLOODING PACKET BERBASIS OPEN SOURCE MENGGUNAKAN SNORT IDS

ARTIKEL SKRIPSI

Diajukan Untuk Memenuhi Sebagian Syarat Guna
Memperoleh Gelar Sarjana Komputer (S.Kom)
Pada Program Studi Teknik Informatika

OLEH :

DZANIAL MUBAROK

NPM: 11.1.03.02.0426

FAKULTAS TEKNIK
UNIVERSITAS NUSANTARA PGRI KEDIRI
2015

ii

Skripsi Oleh:

DZANIAL MUBAROK

NPM: 11.1.03.02.0426P

Judul:

SISTEM PENDETEKSI SERANGAN FLOODING PACKET BERBASIS OPEN SOURCE MENGGUNAKAN SNORT IDS

Telah disetujui untuk diajukan Kepada
Panitia Ujian/Sidang SKRIPSI Program Studi Teknik Informatika
Fakultas Teknik UNP Kediri

Tanggal : 03 Agustus 2015

Pembimbing I	Pembimbing II
SURATMAN,S.H,M .Pd.	M.KHAYAT SUBHKAN,M .Pd,M.Kom.
NIDN.0719036102	NIDN.

iii

Skripsi Oleh:

DZANIAL MUBAROK

NPM: 11.1.03.02.0426P

Judul:

SISTEM PENDETEKSI SERANGAN FLOODING PACKET BERBASIS OPEN SOURCE MENGGUNAKAN SNORT IDS

Telah dipertahankan di depan Panitia Ujian/Sidang Skripsi
Program Studi Teknik Informatika Fakultas Teknik UNP Kediri
Pada tanggal: 06 Agustus 2015

Dan Dinyatakan Telah Memenuhi Persyaratan

Panitia Penguji :

1. Ketua : Dr. SURYO WIDODO, M.Pd
2. Penguji I : RINI INDRIATI, M.Kom
3. Penguji II : MARGO RIDHO L. M.Kom

Mengetahui,
Dekan FT

Dr. SURYO WIDODO, M.Pd
NIP.19640202 199103 1 002

SISTEM PENDETEKSI SERANGAN FLOODING PACKET BERBASIS OPEN SOURCE MENGGUNAKAN SNORT IDS

DZANIAL MUBAROK

NPM: 11.1.03.02.0426P

Fakultas Teknik - Prodi Teknik Informatika
dpredator@rocketmail.com
Pembimbing I SURATMAN, S.H., M.Pd. dan Pembimbing 2 M.KHAYAT SUBKHAN, M.Pd.,M.Kom.
UNIVERSITAS NUSANTARA PGRI KEDIRI

Abstrak

Dzanial Mubarok : Sistem Pendeteksi Serangan Packet Flooding Berbasis Open Source Menggunakan SNORT IDS, Skripsi, Teknik Informatika, FT UNP Kediri, 2015.

Kata Kunci: Keamanan, Jaringan, Intrusion, Deteksi

Penelitian ini dilatar belakangi hasil pengamatan dan pengalaman peneliti, bahwa sistem keamanan jaringan dalam beberapa tahun terakhir ini manjadi fokus utama dalam dunia jaringan komputer, hal ini dikarenakan tingginya kebutuhan akan informasi dan keingintahuan dari pihak-pihak tertentu yang dilakukan melalui cara apapun termasuk dengan serangan dan tindakan kriminal lainya untuk memperoleh suatu informasi yang diinginkan. Hal tersebut tentunya dapat mengancam dan mempengaruhi realibilitas, performa pada suatu.

Permasalahan yang dihadapi adalah (1)Bagaimana cara mengamankan jaringan dan aset informasi yang kita miliki? (2) Bagaimana proses instalasi dan konfigurasi snort beserta software pendukungnya?(3) Apa saja fitur yang dimiliki snort ?

Penelitian ini menggunakan pendekatan Rekayasa Teknologi Informasi dengan format untuk topik acuan Jaringan. Kesimpulan hasil penelitian ini adalah melalui proses Rancang Bangun Sistem Pendeteksi Serangan Berbasis Open Source Menggunakan SNORT IDS dapat ditemukan (1) Cara mengamankan jaringan dan aset informasi yang kita miliki (2)Tahapan proses instalasi dan konfigurasi snort beserta software pendukungnya (3) Fitur-fitur yang dimiliki oleh snort IDS.

Berdasarkan simpulan hasil penelitian ini, untuk pengembangan penelitian di masa mendatang direkomendasikan untuk mengoptimalkan kinerja serta fitur-fitur yang dimiliki oleh snort IDS agar sesuai dengan meningkatnya ancaman serangan di masa mendatang.

I. Latar Belakang

Jaringan komputer terus mengalami kemajuan dan perkembangan yang pesat. Faktor keamanan merupakan suatu hal yang diperlukan dalam membangun suatu jaringan agar dapat melindungi sumber daya dan investasi yang ada.. Untuk mencegah terjadinya kejahatan komputer perlu dilakukan pengamanan yang berlapis-lapis pada suatu jaringan komputer, seperti firewall yang berfungsi mengatur TCP/IP dan port-port mana yang diizinkan atau tidak untuk melewati jaringan. Keamanan yang ada pada sistem operasi juga berfungsi untuk menghalangi dan memperlambat suatu serangan untuk mendapatkan akses layaknya sebagai administrator. System keamanan tersebut tidaklah cukup untuk meminimalisir terjadinya serangan terhadap suatu jaringan komputer.

Banyak serangan yang terjadi pada jaringan komputer baru dapat diketahui setelah adanya kejadian-kejadian yang tidak wajar pada jaringan. Administrator tidak bisa langsung mengetahui secara pasti apa yang terjadi, sehingga dibutuhkan waktu yang cukup lama untuk mengaudit dan mengidentifikasi sistem guna mencari permasalahan yang telah terjadi. Keterbatasan *administrator* dalam memonitor menjadi kendala untuk mengawasi aktifitas jaringannya jika muncul adanya penyusup atau ancaman.

Belum adanya sistem yang mampu merekam segala aktivitas yang terjadi di server mengakibatkan integritas sistem bergantung pada *administrator*.

A.Rumusan Masalah

Berdasarkan uraian batasan masalah yang ada, maka dapat dirumuskan beberapa masalah sebagi berikut:

1 Bagaimana implementasi snort pada jaringan ?
2 Bagaimana proses instalasi Snort dan software pendukungnya ?
3 Apa fitur yang dimiliki oleh Snort dan bagaimana konfigurasinya ?
4 Bagaimana pengujian sistem yang telah diterapkan?

II. Metode

1. Penelitian ini menggunakan pendekatan dan teknik penelitian Rekayasa Teknologi Informasi dengan format untuk topik acuan Jaringan.

2. Prosedur penelitian dimulai dari pencarian tempat penelitian, wawancara, analisa sistem, perancangan sistem, implementasi hingga pengujian sistem.
3. Waktu penelitian selama 6 bulan, seperti yang telah ditetapkan lembaga sesuai SK Rektor / Dekan.
4. Pengujian dilakukan dengan menguji sistem sebelum dan sesudah diterapkannya IDS yang terbukti cukup efektif mendeteksi serangan.

A. Implementasi Sistem

Tahap ini merupakan kegiatan untuk mengimplemen- tasikan rancangan sistem yang telah disusun agar dapat diwujudkan. Agar sistem dapat berjalan dengan optimal dibutuhkan komponen perangkat keras (hardware) dan perangkat lunak (software) dengan spesifikasi tertentu.

1. Kebutuhan perangkat keras

Spesifikasi perangkat keras minimal yang digunakan dalam implementasi IDS agar dapat berjalan optimal adalah :

a. Personal computer/Note-book dual core processor atau lebih
b. Memory ram 2 gb
c. Hard disk dengan space yang cukup
d. Acces Point wireless/ switch

2. Kebutuhan perangkat lunak (software)

Hardware tidak dapat dapat bekerja tanpa adanya software. Software merupa-kan komponen di dalam sistem berupa program atau instruksi untuk mengontrol suatu sistem hardware.Perangkat lunak yang diperlukan untuk menjalan-kan IDS adalah :

a. Sistem Operasi Windows 7
b. Web Browser (Google Chrome)
c. Aplikasi IDS dan software pendukungnya *Download*

B. Evaluasi Sistem

Setelah sitem mampu berjalan normal lakukan pengujian dengan bermacam-macam teknik serangan ke komputer target. Sistem akan mengenali jenis serangan yang terjadi meskipun tidak mampu menangkalnya dan akan disimpan dalam bentuk log.

III. Kesimpulan dan Saran

Berdasarkan kegiatan yang telah penulis lakukan dalam Rancang Bangun Sistem Pendeteksi Serangan Berbasis Open Source Menggunakan SNORT IDS, maka

dapat diambil beberapa kesimpulan sebagai berikut :

1. Implementasi sistem pada sistem operasi windows memerlukan banyak tambahan software pendukung agar IDS dapat bekerja optimal
2. Sistem ini telah mampu berjalan guna mendeteksi serangan yang ada khususnya flooding paket
3. File config pada SNORT adalah otak dari IDS karena semua komponen kinerja dan variable didefenisikan di file ini.
4. Perlu peneambahan rule yang spesifik untuk serangan tertentu.

Dengan keterbatasan kemampuan, waktu dan peralatan yang tersedia, maka penulis hanya membahas Rancang Bangun Sistem Pendeteksi Serangan flooding packet Berbasis Open Source Menggunakan SNORT IDS dan melakukan konfigurasi agar mampu mendeteksi adanya serangan pada server. Agar sistem ini dapat bekerja optimal, maka penulis menyarankan beberapa hal antara lain :

1. Instalasi IDS dan komponen pendukung harus selalu mengunakan versi yang kompatibel agar ids dapat berjalan optimal.
2. Aktif dalam mencari informasi terbaru seputar perkembangan keamanan jaringan.
3. Mempelajari teknik serangan agar dapat menguji coba sistem yang dibangun.
4. Untuk pengembangan penelitian di masa mendatang direkomendasikan untuk mengoptimalkan kinerja serta fitur-fitur yang dimiliki oleh snort IDS agar sesuai dengan meningkatnya ancaman serangan di masa mendatang.

DAFTAR PUSTAKA

Jae K. Shim, Ph.D.and Anique A. Qureshi, Ph.D., CPA, CIA, 2002, The International Handbook of Komputer Security, The GlenlakePublishing Company, Ltd, Unite State of America

Arifianto,Fadel, 2010, e-paper topologi jaringan

Amruta, Inamdar, 2003," Intrusion Detection Systems and a Case Study of SNORT", University of Minnesota

Andry, Haidar, 2004," e-paper Studi Kasus Mengenai Aplikasi Multilayer Perceptron Neural Network Pada Sistem Pendeteksi Gangguan (IDS) Berdasarkan Anomali Suatu Jaringan" Teknologi Informasi Program Pasca Sarjana Teknik Elektro Institut Teknologi Bandung

Jacob Babbin, Simon Biles, Angela D. Orebaugh, 2005," Snort Cookbook" O'Reilly United States of America.

Kusumawati, Monika, 2010, e-paper Keamanan Jaringan,

Pranata,Gilang 2010," Materi Jaringan Komputer

Kerry J.Cox, Christopher Gerg, 2004," Managing Security with Snort and IDS Tools" O'Reilly, United States of America

Rowton, Mitchell, 2005, Introduction to Network Security – Intrusion Detection, URL: http://www.securitydocs.com/library/3009

SnortTM Users Manual 2.4.0RC1 The Snort Project 16th September 2005 URL: www. Snort.org\

Subianto, Hedi ,2012 Mengupas Isi Paket Data Jaringan Komputer, URL : http://www.kompasiana.com/omhedy/mengupas-isi-paket-data-jaringan-komputer_551b4d10a33311e621b65e92