



**IMPLEMENTASI DAN ANALISIS PENGAMANAN
JARINGAN MENGGUNAKAN SNORT *INTRUSION*
*DETECTION SYSTEM (IDS) DAN HONEYPOT***

SKRIPSI

FAJAR DWI SAPUTRA

1110511069

**UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI TEKNIK INFORMATIKA
2016**



**IMPLEMENTASI DAN ANALISIS PENGAMANAN
JARINGAN MENGGUNAKAN SNORT *INTRUSION*
*DETECTION SYSTEM (IDS) DAN HONEYPOT***

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar
Sarjana Komputer**

FAJAR DWI SAPUTRA

1110511069

**UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI TEKNIK INFORMATIKA
2016**

Pernyataan Orisinalitas

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Fajar Dwi Saputra

NRP : 1110511069

Tanggal : 22 Januari 2015

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 22 Januari 2016

Yang Menyatakan,



(Fajar Dwi Saputra)

Lembar Pengesahan

Skripsi diajukan oleh :

Nama : Fajar Dwi Saputra

NRP : 1110511069

Program Studi : S1 Teknik Informatika

Judul Skripsi : Implementasi dan Analisis Pengamanan Jaringan
Menggunakan Snort *Intrusion Detection System* (IDS) dan
Honeypot

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Strata 1 Teknik Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional “Veteran” Jakarta.



Titin Pramiyati, S.Kom., M.Si.

Ketua Penguji



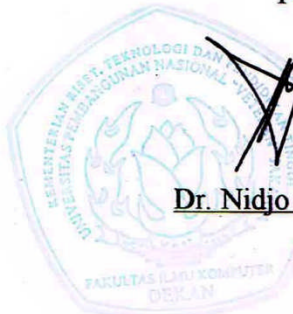
Anita Muliawati, S.Kom., M.TI.

Penguji I



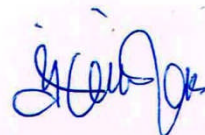
Henki Bayu Seta, S.Kom., M.TI.

Penguji II (Pembimbing)



Dr. Nidjo Sandjojo., M.Sc

Dekan



Yuni Widiastiwi, S.Kom., M.Si.

Ka. Prodi

Ditetapkan di : Jakarta

Tanggal Ujian : 22 Januari 2016

Pernyataan Persetujuan Publikasi Skripsi Untuk Kepentingan Akademis

Sebagai civitas akademik Universitas Pembangunan Nasional “Veteran” Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Fajar Dwi Saputra
NRP : 1110511069
Fakultas : Ilmu Komputer
Program Studi : Teknik Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional “Veteran” Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

Implementasi dan Analisis Pengamanan Jaringan Menggunakan Snort Intrusion Detection System (IDS) dan Honeypot

Beserta yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional “Veteran” Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencatumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 22 Januari 2016

Yang Menyatakan,



(Fajar Dwi Saputra)

IMPLEMENTASI DAN ANALISIS PENGAMANAN JARINGAN MENGGUNAKAN SNORT *INTRUSION DETECTION SYSTEM (IDS)* DAN *HONEYPOT*

Fajar Dwi Saputra

Abstrak

Penelitian ini dilakukan untuk membuat sistem yang dapat digunakan untuk mendeteksi gangguan pada sisi sistem kinerja server yang bekerja secara otomatis untuk memonitor kejadian pada jaringan komputer dan menganalisis masalah keamanan jaringan. Snort menggunakan dua metode yaitu *knowledge based* atau *misusedetection* yaitu mengenali adanya penyusupan atau serangan dengan cara menyadap paket data kemudian membandingkannya dengan *database rule* yang berisi *signature-signature* serangan dan *behavior based* atau *anomaly based*. Snort IDS ini bekerja dengan cara mendeteksi serangan yang telah dilakukan oleh penyusup (*intruder*). Setelah serangan berhasil terdeteksi, maka serangan tersebut akan dibelokkan ke server palsu (Honeypot). Akibat dari serangan penyusup adalah terjadinya gangguan pada sisi sistem kinerja server. Begitupula pada pemakaian CPU *history* adanya peningkatan kapasitas server 47,5% ketika terjadi serangan. Akan tetapi setelah terjadinya pembelokan, kapasitas server menurun menjadi 13,7%. Setelah dilakukan proses pendeteksian dan pembelokan maka sistem sudah bekerja dengan baik untuk mengamankan suatu jaringan komputer. Serangan dapat terdeteksi atau tidak tergantung pola serangan tersebut ada di dalam *rule* IDS atau tidak. Oleh karena itu, pengelola IDS harus secara rutin memperbaharui *rule*.

Kata Kunci : Snort IDS, CPU History, Honeyd, Kinerja Sistem, penyusup.

IMPLEMENTATION AND ANALYSIS OF NETWORK SECURITY USING SNORT INTRUSION DETECTION SYSTEM (IDS) AND HONEYPOT

Fajar Dwi Saputra

Abstract

This study was conducted to create system that can be used to detect intruder on the server performance system that works automatically to monitor events on computer networks and analyze network security issues. Snort uses two methods of knowledge based or misusedetection that recognize their intrusion or attack by way of intercepting data packets and then compares it with a database rule that contains an attack signature and signature-based or behavior-based anomaly. IDS Snort works by detecting attacks that have been carried out by the intruder. After a successful attack is detected, then the attack will be diverted to a fake server (Honeypot). As a result of the attack the intruder is interference with the performance of server side system. Likewise, CPU usage history to an increase of 47.5% server capacity when the attack occurred. But after the deflection, server capacity decreased to 13.7%. After the detection process and the deflection of the system is already working well to secure a computer network. The attack can be detected or not depending on the pattern of the attacks in the IDS rule or not. Therefore, managers should regularly update the IDS rule.

Keywords : Snort IDS, CPU History, Honeyd, System Performance, Intuder.

Kata Pengantar

Puji dan syukur penulis panjatkan kehadiran Allah SWT atas segala karunia-Nya sehingga skripsi ini berhasil diselesaikan. Judul yang dipilih dalam penelitian ini yang dilaksanakan sejak Maret 2015 ini adalah Implementasi dan Analisis Pengamanan Jaringan Menggunakan Snort *Intrusion Detection System* (IDS) dan Honeypot. Terima kasih penulis ucapkan kepada :

1. Bapak Dr. Nidjo Sandjojo. M.Sc selaku Dekan Fakultas Ilmu Komputer.
2. Bapak Henki Bayu Seta, S.Kom., M.TI. selaku dosen pembimbing yang telah banyak memberikan saran yang sangat bermanfaat.
3. Ibu Yuni Widiastiwi, S.Kom., M.Si. sebagai Kepala Program Studi Teknik Informatika.
4. Disamping itu, ucapan terima kasih juga disampaikan kepada Ayahanda Suroto dan Ibunda Nur Suprihatin serta seluruh keluarga yang tidak henti-hentinya memberikan penulis semangat dan doa.
5. Penulis juga sampaikan terima kasih kepada Adiya Mugi Raharja, Sarah Triwulan, dan Nasya Ramadhana yang telah telah membantu dalam penulisan skripsi ini.

Penulis menyadari sepenuhnya bahwa dalam laporan skripsi ini masih banyak kekurangan dan jauh dari kata sempurna. Penulis berharap semoga apa yang menurut Allah benar dalam penulisan ini bisa bermanfaat bagi pembaca.

Jakarta, 22 Januari 2016

Penulis

DAFTAR ISI

Halaman Judul	
Halaman Pernyataan Orisinalitas	
Halaman Pengesahan	
Halaman Pernyataan Persetujuan Publikasi	
Abstrak	
Abstract	
Kata Pengantar	i
DAFTAR ISI	ii
DAFTAR GAMBAR	iv
DAFTAR TABEL	v
DAFTAR LAMPIRAN	vi
 BAB I PENDAHULUAN	 1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Ruang Lingkup Penelitian	2
1.4 Tujuan Dan Manfaat Penelitian	2
1.5 Luaran Yang Diharapkan	3
1.6 Sistematika Penulisan	3
 BAB II LANDASAN TEORI	 4
2.1 Keamanan Jaringan	4
2.2 Kebijakan Keamanan	6
2.3 Intrusion Detection System (IDS)	7
2.4 IDS Mengenali Adanya Intruder	9
2.5 Melindungi IDS	10
2.6 Snort	11
2.7 Support Platforms	14
2.8 Jenis Serangan	15
2.9 Honeypot	18
2.10 Pengertian Algoritme	21
2.11 Algoritme Boyer Moore	22
2.12 Penelitian Yang Sesuai	22
 BAB III METODOLOGI PENELITIAN	 27
3.1 Tahapan Penelitian	27
3.2 Flowchart Perancangan Sistem Dan Uji Coba	30
3.3 Analisis Kebutuhan	31
3.4 Waktu Dan Tempat	31
3.5 Jadwal Kegiatan	31
 BAB IV HASIL DAN PEMBAHASAN	 33
4.1 Analisis	33
4.2 Bahan Penelitian	36
4.3 Tujuan Pengujian	37

4.4 Tahap Pengujian	37
4.5 Tahap Pengujian Server.....	37
4.6 Dampak Serangan Terhadap Sistem.....	57
4.7 Pemantauan Serangan.....	59
4.8 Hasil Analisis Pengujian.....	60
BAB V PENUTUP	62
5.1 Simpulan.....	62
5.2 Saran	62
DAFTAR PUSTAKA	63
DAFTAR RIWAYAT HIDUP	
LAMPIRAN	

DAFTAR GAMBAR

Gambar 1	Komponen-komponen Snort	13
Gambar 2	Klasifikasi Honeyd Berdasarkan Level Interaksinya	20
Gambar 3	Grafik Insiden Penyusupan Keamanan Jaringan.....	23
Gambar 4	Tahapan Penelitian	27
Gambar 5	Flowchart Perancangan	30
Gambar 6	Topologi Sebelum Menggunakan Snort IDS	33
Gambar 7	Suhu Pada Saat Terjadi Serangan.....	34
Gambar 8	Traffic Serangan.....	34
Gambar 9	Topologi Setelah Menggunakan Snort IDS	35
Gambar 10	Suhu Setelah Serangan Di Alihkan	35
Gambar 11	Traffic Serangan Yang Menurun.....	36
Gambar 12	Tampilan Snort Apabila Sedang Dijalankan.....	38
Gambar 13	Tampilan IP Scanner	38
Gambar 14	Keadaan Server Sebelum Ada Serangan.....	39
Gambar 15	Port Scanning Dari Client Ke Server	39
Gambar 16	Alert Snort Berupa Serangan Port Scanner	40
Gambar 17	Keadaan Server setelah terjadi penyerangan.....	40
Gambar 18	Log File Serangan Pada Snort.....	41
Gambar 19	Tampilan Honeyd Ketika Mendapatkan IP DHCP	42
Gambar 20	Tampilan PING Dari Client Ke Honeyd	42
Gambar 21	Reaksi Honeyd Dari Serangan PING Dari Client	42
Gambar 22	Keadaan Server Saat Intruder Masuk Ke Honeyd	43
Gambar 23	Port Scanning	44
Gambar 24	Pola Serangan Port Scanner	45
Gambar 25	Log Snort Pada Serangan Port Scanner	45
Gambar 26	Statik Port Scanner Pada IPTraf.....	46
Gambar 27	Pengiriman Paket UDP.....	47
Gambar 28	Serangan Syn Attack Dari Client Ke Server	49
Gambar 29	Log IPTraf Terhadap Serangan Syn Attack	49
Gambar 30	Alert Syn Attack Dari Client Ke Server.....	50
Gambar 31	PING Attack.....	51
Gambar 32	Alert PING Attack.....	52
Gambar 33	Penyerangan Brute Force	52
Gambar 34	Alert serangan PING Attack Dan Brute Force.....	53
Gambar 35	Tampilan Program LOIC	54
Gambar 36	Tampilan Reaksi Honeyd Ketika Di Atack.....	55
Gambar 37	Tampilan Alert Snort Yang Mendeteksi DoS	56
Gambar 38	Tampilan Paket Snort Yang Masuk	56
Gambar 39	Trafik Pada Iptraf Saat Ada Serangan.....	57
Gambar 40	Sebelum Adanya Penyerangan.....	58
Gambar 41	Setelah TERJADINYA PENYERANGAN	58
Gambar 42	Monitoring IPTraf	59

DAFTAR TABEL

Tabel 1	Jadwal Kegiatan ..	32
Tabel 2	Statik Eth0 Pada IPTraf.....	46
Tabel 3	Alert Pada IPTraf Terhadap Serangan Syn Attack	50
Tabel 4	Tabel Trafik Serangan Pada Iptraf	57
Tabel 5	Monitoring IPTraf	60
Tabel 6	Serangan Yang Telah Di Uji Coba	61

DAFTAR LAMPIRAN

- Lampiran 1 Instalasi Dan Konfigurasi Snort
- Lampiran 2 Surat Keterangan Telah Melaksanakan Riset
- Lampiran 3 Lembar Kehadiran Riset