

ANALISIS PERBANDINGAN KINERJA *INTRUSION DETECTION SYSTEM* (IDS) SNORT DAN SURICATA DALAM MENDETEKSI SERANGAN *DENIAL OF SERVICE* PADA SERVER LINUX

Tugas Akhir

Disusun sebagai salah satu syarat untuk kelulusan
Program Strata 1, Program Studi Teknik Informatika,
Universitas Pasundan Bandung

Oleh :

Raiman Hirrandi
11.304.0067



**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG
DESEMBER 2016**

DAFTAR ISI

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR	i
ABSTRAK	ii
ABSTRACT	iii
KATA PENGANTAR.....	iv
DAFTAR ISI	v
DAFTAR GAMBAR	vii
DAFTAR TABEL	ix
DAFTAR SIMBOL.....	x
BAB 1 PENDAHULUAN.....	1-1
1.1 Latar Belakang	1-1
1.2 Identifikasi Masalah	1-1
1.3 Tujuan Tugas Akhir.....	1-1
1.4 Lingkup Tugas Akhir	1-2
1.5 Metodologi Tugas Akhir	1-2
1.6 Sistematika Penulisan Tugas Akhir.....	1-3
BAB 2 LANDASAN TEORI.....	2-1
2.1 Keamanan Informasi	2-1
2.2 <i>Internet Protocol (IP)</i>	2-2
2.3 <i>Transmission Control Protocol (TCP)</i>	2-2
2.4 <i>Intrusion Detection System (IDS)</i>	2-2
2.5 Snort	2-3
2.6 Snort Base.....	2-3
2.7 Suricata.....	2-3
2.8 Hping3	2-4
2.9 <i>Denial Of Service (DOS)</i>	2-5
2.9.1 Macam-macam serangan <i>Denial Of Service (DOS)</i>	2-5
2.9.2 Cara mengetahui Serangan <i>Denial Of Service (DOS)</i>	2-8
2.10 <i>Anatomy Of Hack</i>	2-9
2.11 Kali Linux.....	2-10
2.12 Zenmap	2-10
2.13 Linux	2-10
2.14 Server.....	2-11
2.15 Web Server Apache.....	2-11
BAB 3 SKEMA PENELITIAN.....	3-1
3.1 Alur Penyelesaian Tugas Akhir.....	3-1

3.2 Peta Analisis.....	3-3
3.2.1 Langkah-langkah Analisis.....	3-3
3.3 Analisis Kondisi Server	3-4
3.3.1 Kesiapan Perangkat.....	3-4
3.3.2 Kondisi Awal Server.....	3-5
3.3.3 Topologi Dan Kondisi Pengujian.....	3-7
3.4 Rancangan Kesiapan Uji <i>Intrusion Detection System</i> (IDS).....	3-8
3.5 Skenario Pengujian	3-9
3.5.1 Uji Aktifitas Normal	3-9
3.5.2 Uji Aktifitas Simulasi Serangan.....	3-9
3.5.3 Gambaran Skenario Uji.....	3-12
3.5.4 Persiapan Data Uji	3-13
3.6 Persiapan Uji.....	3-14
3.6.1 Instalasi IDS Snort	3-14
3.6.2 Instalasi IDS Suricata.....	3-14
BAB 4 PENGUJIAN	4-1
4.1 Pengujian.....	4-1
4.1.1 Pengujian IDS Snort.....	4-1
4.1.2 Pengujian IDS Suricata	4-2
4.2 Hasil Pengujian	4-4
4.2.1 Hasil Pengujian IDS Snort	4-4
4.2.2 Hasil Pengujian IDS Suricata.....	4-5
4.3 Perbandingan Hasil Pengujian	4-7
4.3.1 Berdasarkan Penggunaan Sumber Daya	4-7
4.3.2 Berdasarkan Uji Serangan Port Scanning	4-8
4.3.3 Berdasarkan Uji Serangan Hping.....	4-9
BAB 5 KESIMPULAN DAN SARAN	5-1
5.1 Kesimpulan	5-1
5.2 Saran	5-1

DAFTAR GAMBAR

Gambar 1-1 Metodologi Tugas Akhir	1-2
Gambar 2-1 The Security Trinity [CAN01]	2-1
Gambar 2-2 Skema Program Utility Ping dan Serangan Ping Of Death [NUR04].....	2-6
Gambar 2-3 Skema Serangan SYN [NUR04]	2-7
Gambar 2-4 Skema Serangan LAND [NUR04].....	2-8
Gambar 2-5 Skema Serangan Smurf Attack [NUR04]	2-8
Gambar 3-1 Kerangka Tugas Akhir	3-2
Gambar 3-2 Skema Analisis	3-3
Gambar 3-3 Keadaan Awal Server	3-6
Gambar 3-4 Firewall Pada Server	3-6
Gambar 3-5 Spesifikasi Laptop Pada Server	3-7
Gambar 3-6 Topologi Pengujian IDS.....	3-7
Gambar 3-7 Diagram Alir Sistem IDS	3-9
Gambar 3-8 Tahapan Skenario Pengujian	3-10
Gambar 3-9 Analisis Host Yang Aktif Pada Jaringan	3-10
Gambar 3-10 Topology Host Yang Aktif Pada Jaringan	3-11
Gambar 3-11 Port Scanning Menggunakan Nmap	3-12
Gambar 3-12 Skenario Simulasi Uji Serangan.....	3-12
Gambar 4-1 Pengujian IDS Snort Menggunakan Port Scanning.....	4-1
Gambar 4-2 Alert Serangan Port Scanning	4-2
Gambar 4-3 Serangan Hping3	4-2
Gambar 4-4 Pengujian IDS Suricata Menggunakan Port Scanning	4-3
Gambar 4-5 Serangan Hping3	4-3
Gambar 4-6 Pengujian Aktifitas Normal.....	4-4
Gambar 4-7 Hasil Serangan Hping3 Pada IDS Snort.....	4-5
Gambar 4-8 Pengujian Aktifitas Normal.....	4-6
Gambar 4-9 Hasil Simulasi Serangan Hping3 Pada IDS Suricata	4-7
Gambar A - 1 Konfigurasi snort-mysql 1	A-2
Gambar A - 2 Konfigurasi snort-mysql 2.....	A-2
Gambar A - 3 Konfigurasi snort-mysql 3.....	A-3
Gambar A - 4 Konfigurasi snort-mysql 4.....	A-3
Gambar A - 5 Konfigurasi snort-mysql 5	A-3
Gambar A - 6 Konfigurasi snort-mysql 6.....	A-4
Gambar A - 7 Konfigurasi snort-mysql 7.....	A-4
Gambar A - 8 Konfigurasi snort-mysql 8.....	A-4


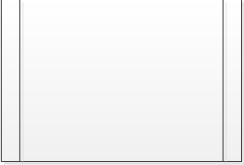
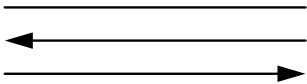
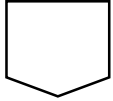
Gambar A - 9 File snort.conf 1	A-5
Gambar A - 10 File snort.conf 2	A-6
Gambar A - 11 Test Snort	A-6
Gambar B - 1 Test IDS Suricata	B-2

DAFTAR TABEL

Tabel 3-1 Langkah-langkah Analisis.....	3-4
Tabel 3-3 Kesiapan Perangkat Keras	3-4
Tabel 3-4 Spesifikasi Laptop.....	3-4
Tabel 3-5 Kesiapan Perangkat Lunak.....	3-5
Tabel 3-6 Keterangan Host Aktif	3-11
Tabel 3-7 Perbandingan Penggunaan Sumber Daya	3-13
Tabel 3-8 Parameter Data Uji Akurasi	3-13
Tabel 3-9 Parameter Perbandingan Respon Waktu Deteksi.....	3-13
Tabel 4-1 Waktu Deteksi Port Scanning Pada IDS Snort	4-5
Tabel 4-2 Waktu Respon Deteksi Serangan Pada IDS Snort	4-5
Tabel 4-3 Waktu Deteksi Port Scanning Pada IDS Suricata	4-6
Tabel 4-4 Waktu Respon Deteksi Serangan Pada IDS Suricata.....	4-7
Tabel 4-5 Perbandingan Penggunaan Sumber Daya	4-8
Tabel 4-6 Perbandingan Hasil Simulasi Serangan	4-8
Tabel 4-7 Kecepatan Deteksi.....	4-8
Tabel 4-8 Perbandingan Hasil Simulasi Serangan	4-9
Tabel 4-9 Kecepatan Deteksi.....	4-9

DAFTAR SIMBOL

Berikut ini merupakan symbol-simbol yang digunakan dalam laporan tugas akhir ini, simbol-simbol tersebut diuraikan pada table dibawah ini.

No	Gambar	Nama Gambar	Keterangan
1		<i>Process</i>	Simbol yang digunakan untuk menunjukan aktivitas pengolahan informasi atau menyatakan suatu posisi.
2		<i>Sub Process</i>	Simbol yang digunakan untuk menunjukan atribut atribut yang berkontribusi untuk mencapai tujuan dari proses
3		Arus/Flow	Simbol yang menyatakan proses dari suatu proses.
4		Off-Page Reference	Simbo yang digunakan jika gambar yang akan dihubungkan berada pada halaman yang berbeda.