ANALISIS PERBANDINGAN PERFORMA SNORT DAN SURICATA SEBAGAI INTRUSION PREVENTION SYSTEM PADA UBUNTU 14.04

SKRIPSI

disusun oleh

Soni Setiawan

12.11.6642

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA

2016

ANALISIS PERBANDINGAN PERFORMA SNORT DAN SURICATA SEBAGAI INTRUSION PREVENTION SYSTEM PADA UBUNTU 14.04

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika

disusun oleh

Soni Setiawan

12.11.6642

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA

2016

PERSETUJUAN

SKRIPSI

ANALISIS PERBANDINGAN PERFORMA SNORT DAN SURICATA SEBAGAI INTRUSION PREVENTION SYSTEM PADA UBUNTU 14.04

yang disusun oleh

Soni Setiawan

12.11.6642

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 21 November 2015

Dosen Pembimbing,

Sudarmawan, MT
NIK. 190302035

PENGESAHAN
SKRIPSI

ANALISIS PERBANDINGAN PERFORMA SNORT DAN SURICATA SEBAGAI INTRUSION PREVENTION SYSTEM PADA UBUNTU 14.04

yang disusun oleh

Soni Setiawan

12.11.6642

telah dipertahankan di depan Dewan Penguji
pada tanggal 19 April 2016

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Sudarmawan, MT **NIK. 190302035**	
Heri Sismoro, M.Kom **NIK. 190302057**	
Akhmad Dahlan, M.Kom **NIK. 190302174**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 04 Mei 2016

KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN KEASLIAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 28 April 2016

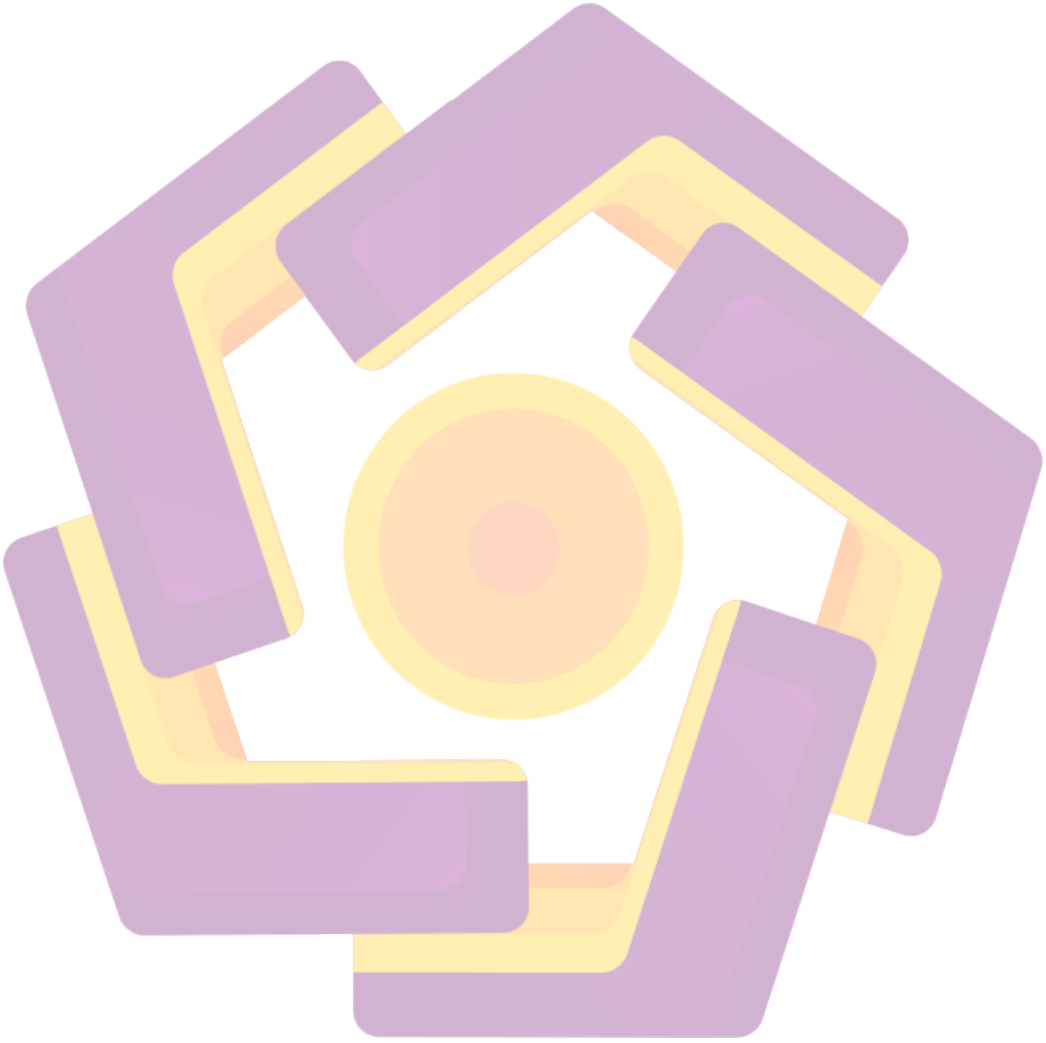
Soni Setiawan
NIM. 12.11.6642

MOTTO

"Ridho Allah SWT, Ridho Orang Tua."

"Man Jadda Wa Jadda"

"Sebaik-baik manusia adalah yang bermanfaat bagi orang lain."



PERSEMBAHAN

Puji syukur kehadirat Allah SWT, atas nikmat, rahmat, dan hidayah-Nya yang telah dianugerahkan sehingga penulis dapat menyelesaikan skripsi ini. Sholawat serta salam senantiasa penulis haturkan kepada Nabi Muhammad SAW sebagai suri tauladan terbaik. Pada kesempatan ini, penulis ingin mengucapkan terima kasih kepada :

1. Kedua orang tua dan juga adik tercinta, Risky Dwi Setyowati yang telah memberikan dukungan baik moral maupun materiil dan juga do'a yang tak pernah terhenti.
2. Bapak Sudarmawan, MT selaku ketua jurusan Strata 1 Teknik Informatika sekaligus dosen pembimbing atas bimbingan dan saran yang diberikan sehingga penulisan skripsi dapat berjalan dengan lancar.
3. Teman-teman dari kelas 12-S1TI-13, terima kasih atas canda dan tawa dalam kebersamaan yang telah dilalui. Tak lupa dukungan dan semangat dari kalian semuanya.
4. Sahabat-sahabat kost Deresan, Bayu, Faisal, Ofani, Robin dan EB 2009 lainnya terima kasih atas dukungan, semangat, canda, tawa, ejekan, nasehat dan ilmu yang kalian berikan.

KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang senantiasa melimpahkan rahmat dan hidayah kepada setiap hamba-Nya. Tugas Akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.

Dengan selesainya Tugas Akhir dengan judul "Analisis Perbandingan Performa Snort dan Suricata sebagai *Intrusion Prevention System* pada Ubuntu 14.04", penyusun ingin mengucapkan terima kasih kepada :

1. Bapak Prof. M. Suyanto, M.M., selaku ketua STMIK AMIKOM Yogyakarta
2. Bapak Sudarmawan, MT, selaku ketua jurusan Strata 1 Teknik Informatika sekaligus dosen pembimbing yang telah memberikan bimbingan dan masukan sehingga dapat menyelesaikan tugas akhir ini.
3. Seluruh Dosen STMIK AMIKOM Yogyakarta yang telah memberikan ilmu yang bermanfaat.
4. Kedua orang tua dan keluarga yang senantiasa memberikan semangat, motivasi dan do'a.
5. Semua pihak yang telah membantu dalam proses pelaksanaan dan penyelesaian tugas akhir.

Penyusun menyadari bahwa laporan tugas akhir ini masih banyak kekurangan. Oleh karena itu diharapkan saran dan kritik yang membangun dari

pembaca untuk yang lebih baik.

Semoga tugas akhir ini dapat bermanfaat bagi pembaca untuk kedepannya.

Yogyakarta, 28 April 2016

Penyusun

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Keamanan menjadi salah satu faktor penting dalam proses pertukaran informasi yang dikirimkan dalam sebuah jaringan komputer. Namun banyak yang mengabaikannya sehingga menyebabkan adanya pencurian dan kehilangan data. Salah satu metode yang diterapkan adalah Intrusion Prevention System. Aplikasi yang mendukung penerapan Intrusion Prevention System adalah snort dan suricata.

Dalam penelitian menekankan analisa dan perbandingan kinerja dari aplikasi open source yaitu snort dan suricata untuk mengukur penggunaan sumber daya, tingkat akurasi dan respon waktu dari masing-masing aplikasi. Sehingga diperoleh informasi yang sesuai dari aplikasi yang akan digunakan.

Setelah implementasi, hasil penelitian menunjukkan bahwa Snort menggunakan 4,5% dari CPU dan 30% dari RAM sedangkan Suricata menggunakan 6,2% CPU dan 30,9% dari RAM. Dalam kasus memblokir paket data antara Snort dan Suricata, Suricata menunjukkan bahwa lebih baik dari Snort. Sementara dalam hal kecepatan deteksi dan blocking menunjukkan bahwa Snort lebih baik dari Suricata.

Kata Kunci: *Intrusion Prevention System*, snort, suricata

ABSTRACT

Security has become an important factor in the process of exchange of information transmitted in a computer network. But many ignore that led to the theft and data loss. One of the methods applied are Intrusion Prevention System. Applications that support the implementation of Intrusion Prevention System is a snort and Suricata.

In the study emphasizes the analysis and comparison of the performance of an open source application that Snort and Suricata to measure resource use power, level of accuracy and response time of each application. So that obtained the appropriate information from the application to be used.

After implementation, the results showed that Snort uses 4.5% of CPU and 30% of RAM while Suricata uses the 6,2 % CPU and 30.9% of RAM. In the case of blocking of data packets between Snort and Suricata, Suricata showed that better than Snort. While in terms of speed of detection and blocking shows that Snort is better than Suricata.

***Keyword**: Intrusion Prevention System, snort, suricata*