ANALISIS PERBANDINGAN PERFORMA INTRUSION DETECTION SYSTEM BERBASIS SNORT, SURICATA DAN OSSEC

SKRIPSI

disusun oleh

Kurniawan Sumargo

15.11.8999

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020

ANALISIS PERBANDINGAN PERFORMA INTRUSION DETECTION SYSTEM BERBASIS SNORT, SURICATA DAN OSSEC

Skripsi

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana
pada Program Studi Informatika

Disusun Oleh

Kurniawan Sumargo

15.11.8999

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020

PERSETUJUAN

SKRIPSI

ANALISIS PERBANDINGAN PERFORMA INTRUSION DETECTION SYSTEM BERBASIS SNORT, SURICATA DAN OSSEC

yang dipersiapkan dan disusun oleh

Kurniawan Sumargo

15.11.9035

telah disetujui oleh Dosen Pembimbing Skripsi

Pada tanggal 21 Juni 2019

Dosen Pembimbing,

Rum Mohamad Andri Kr, Ir, M.Kom

NIK. 190302011

PENGESAHAN

SKRIPSI

ANALISIS PERBANDINGAN PERFORMA INTRUSION DETECTION SYSTEM BERBASIS SNORT, SURICATA DAN OSSEC

Yang dipersiapkan dan disusun oleh

Kurniawan Sumargo

15.11.9035

telah dipertahankan di depan Dewan Penguji

Pada tanggal 21 Agustus 2020

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Rum Mohamad Andri Kr, Ir, M.Kom. **NIK. 190302011**	
Erni Seniwati, S.Kom., M.Cs. **NIK : 190302231**	
Hendra Kurniawan, M.Kom. **NIK : 190302244**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal Agustus 2020

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.

NIK. 190302038

PERNYATAAN

Saya yang bertandatangan 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, 11 Agustus 2020

Kurniawan Sumargo
NIM. 15.11.9035

MOTTO

- Tidak ada kesuksesan melainkan dengan pertolongan Allah. Q.S. Huud: 88
- Ridho Allah, Ridho orang tua.
- Man Jadda Wa Jadda, Barang siapa yang bersungguh-sungguh pasti akan mendapatkan hasil.
- La Tahzan Innallaha Ma'ana, janganlah bersedih sesungguhnya Allah bersama kita.
- Bekerjalah 2 bahakan 3 kali lebih keras dari orang lain, karna usaha tidak pernah menghianti hasil.
- Indonesia tidak kekurangan orang pintar tapi kekurangan orang jujur.
- Everyday is a chance to be better than the day before.
- Jika kamu tidak sanggup menahan lelahnya belajar, maka kamu harus sanggup menahan perihnya kebodohan. – Imam Syafi'i Rahimahullah.
- Bersyukur dan berterima kasih pada Allah atas bantuannya dan atas apa yang sudah didapatkan.

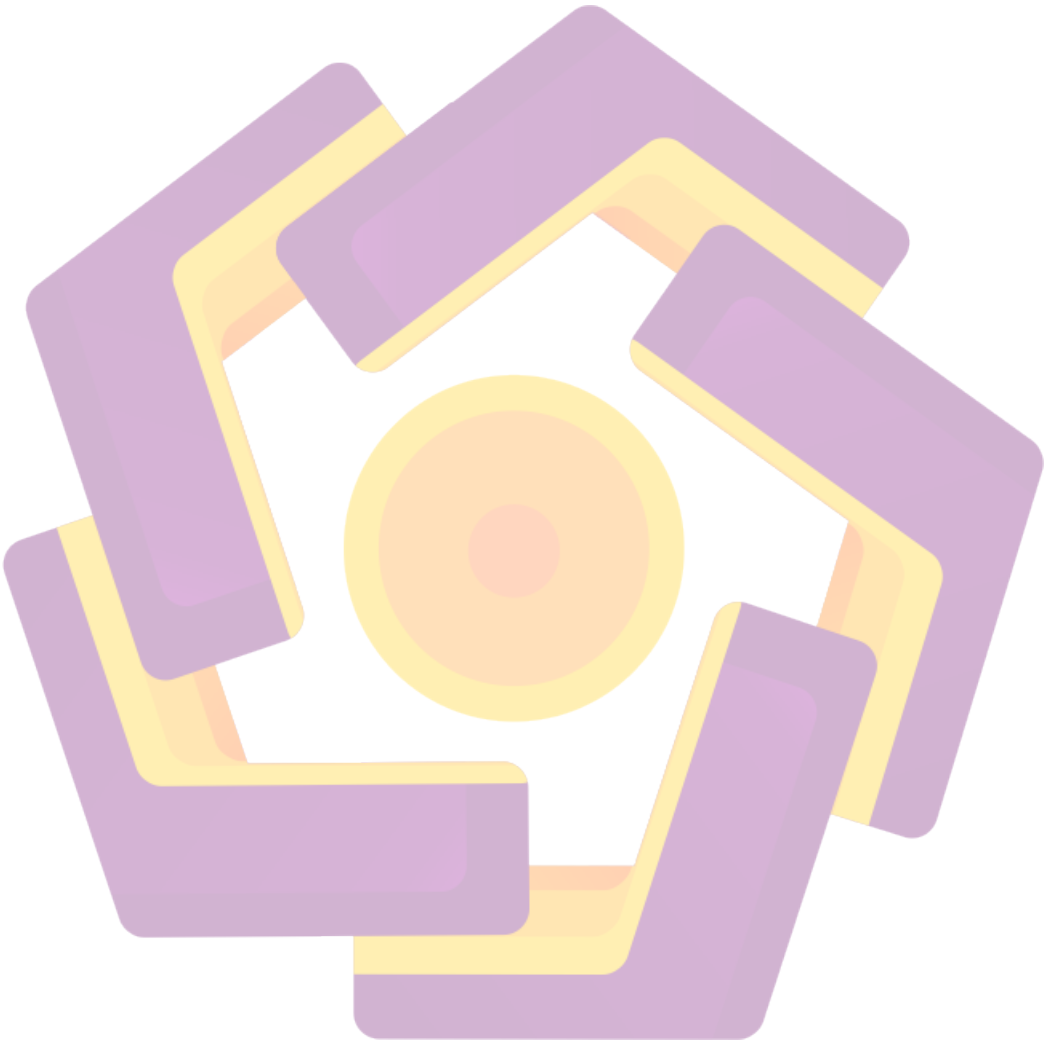
PERSEMBAHAN

Alhamdulillah, segala puji bagi Allah SWT atas segala limpahan ridho, hidayah dan inayah-Nya sehingga Skripsi dengan judul "Analisis Perbandingan Performa *Intrusion Detection System* Berbasis *Snort*, *Suricata* dan *OSSEC* pada *Mail Server*" telah selesai dikerjakan denga baik dan lancar.

Skripsi ini saya persembahkan untuk:

1. Bapak Sumargo, Ibu Kartini D.J Sidik, Adik laki-laki Hamdani Sumargo, Adik Perempuan Aulia Putri Sumargo dan segenap keluarga besar tercinta yang tidak henti-hentinya mendukungku, baik moril maupun materil serta memberikan doa restu dan semangat sehingga Saya dapat menyelesaikan kuliah di Fakultas Ilmu Komputer Jurusan Informatika Universitas Amikom Yogyakarta.
2. Bapak Rum Mohamad Andri Kr, Ir, M.Kom. selaku dosen pembimbing yang telah mengarahkan dan memberikan motivasi dalam penyelesaian skripsi Saya.
3. Bapak Rico Agung Firmansyah, S.Kom. dan Mba Septiana Saraswati, Saya ucapkan terima kasih sudah memberikan Saya dukungan, saran, motivasi, arahan dan menemani Saya.
4. Sahabat-sahabat serta teman-teman saya Septiana Saraswati, Junior Mamuntu, Rizky Adi Saputra, Farhan Sodik Albana, Fandi Ahmad, Fikri Sasikome,Rizki Masalah, dan yang tidak tersebutkan dalam lembar ini saya ucapkan terima kasih telah memberikan semangat, dukungan, bantuan, saring, motivasi dan menemani dikala sedang tidak percaya diri.
5. Teman-teman Universitas Amikom Yogyakarta kelas S1-TI 08 angkatan 2015 yang telah berjuang bersama selama perkuliahan.
6. Teman-teman Universitas Amikom Yogyakarta konsentrasi Jaringan 2015 yang telah menemani berjuang dalam hal baru yang Saya pelajari.
7. Dan tak lupa Saya persembahkan skripsi ini untuk yang selalu bertanya: "kapan skripsimu selesai?". Terlambat lulus atau lulus tidak tepat wwaktu bukan sebuah kejahatan, bukan sebuah aib. Alangkah kerdilnya jika

mengukur kepintaran seseorang hanya dari siapa yang paling cepat lulus. Bukankah sebaik-baik skripsi adalah skripsi yang selesai? Baik itu selesai tepat waktu maupun tidak tepat waktu.



KATA PENGANTAR

Bismillahirrahmanirrahiim

Puji syukur penulis ucapkan kepada Allah SWT, karena berkat rahmat dan hidayah-Nya penulis dapat menyelesaikan laporan skripsi yang berjudul "Analisis Perbandingan Performa Intrusion Detection System Berbasis *Snort*, *Suricata* dan *OSSEC* pada *Mail Server*".

Selanjutnya, penilis ingin menyampaikan rasa terima kasih yang tak terhingga kepada semua pihak yang membantu kelancaran pembuatan laporan skripsi ini, baik berupa dorongan moril maupun materiil. Karena penulis yakin tanpa bantuan dan dukungan tersebut, sulit rasanya bagi penulis untuk menyelesaikan penulisan skripsi ini. Disamping itu, izinkan penulis untuk menyampaikan ucapan terima kasih dan penghargaan yang setinggi-tinggina kepada:

1. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor dan Ketua Yayasan Universitas Amikom Yogyakarta.
2. Ibu Krisnawati, S.Si., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta beserta seluruh staffnya.
3. Bapak Sudarmawan, S.T.,M.T. selaku Ketua Jurusan Informatika Universitas Amikom Yogyakarta beserta seluruh staffnya.
4. Bapak Rum Mohamad Andri Kr, Ir, M.Kom. selaku dosen pembimbing skripsi yang telah memberikan pengarahan, bimbingan dan motivasi kepada penulis selama proses penyusunan skripsi hingga selesai.
5. Bapak Joko Dwi Santoso, M.Kom. selaku dosen wali selama menempuh perkuliahan di Universitas Amikom Yogyakarta.
6. Segenap Bapak dan Ibu Dosen serta Karyawan Universitas Amikom Yogyakarta yang telah memberikan ilmu pengetahuan dan pengalamannya kepada penulis. Semoga Bapak dan Ibu dosen selalu dalam rahmat dan lindungan Allah SWT. Sehingga ilmu yang telah diajarkan dapat bermanfaat dikemudian hari.
7. Ungkapan terima kasih dan penghargaan yang sangat spesial penulis haturkan dengan rendah hati dan asa hormat kepada kedua orang tua penulis

Bapak Sumargo dan Ibu Kartini D.J Sidik yang telah mengasihi, membesarkan, mendidik dan selalu memberikan dukungan serta doa restu untuk bekal dalam perjalanan hidup penulis kelak.

8. Bapak Rico gung Firmansyah, S.Kom dosen konsentrasi jaringan yang sudah memberikan saya saran, arahan, dan motivasi.
9. Pimpinan beserta para staff Perpustakaan Resource Center Universitas Amikom Yogyakarta atas segala kemudahan yang diberikan kepada penulis untuk mendapatkan referensi yang mendukung penyelesaian skripsi ini.
10. Segenap teman-teman Universitas Amikom Yogyakarta angkatan 2015 khususnya kelas 15 S1-TI 08 yang telah berjuang bersama.
11. Teman-teman Universitas Amikom Yogyakarta konsentrasi jaringan angkatan 2015 yang telah berbagi ilmu bersama.
12. Seseorang terdekat dan terkasih yang selalu mendukung penyelesaian skripsi ini.

Akhirnya penulis berharap semoga amal baik dari semua pihak yang telah membantu penulis dalam menyelesaikan skripsi ini mendapatkan balasan pahala dari rahmat Allah SWT. Penulis menyadari sepenuhnya bahwa laporan skripsi ini masih sangat jauh dari kesempurnaan, itu semua tidak lepas dari keterbatasan pengetahuan dan kemmpuan dari penulis sendiri. Untuk itu penulis mengharapkan kritik dan saran yang bersifat membangun guna mencapai kesempurnaan yang selalu penulis harapkan sehingga dapat bermanfaat bagi penulis serta pihak-pihak yang membutuhkan.

Yogyakarta, 11 Agustus 2020

Kurniawan Sumargo

DAFTAR ISI

DAFTAR TABLE

DAFTAR GAMBAR

INTISARI

Platform *email* merupakan salah satu jenis *platform* pertukaran data di jaringan. *Mail application server* atau sering disingkat *mail server* adalah perangkat lunak program yang mendistribusikan *file* atau informasi sebagai respons atas permintaan yang dikirim via *elektronik*. Berkat sentralnya pemanfaatan teknologi *email* sebagai penunjang layanan jaringan, maka tak heran jika sering ditemukan serangan terhadap *mail server*. Seperti diantaranya *Denial of Services* terhadap mail *server*. penggunaan IDS/IPS Server untuk membendung serangan dari sisi jaringan. *IDS (Intrusion Detection System)* merupakan sebuah sistem yang digunakan untuk melakukan pendeteksian aktivitas yang mencurigakan terhadap *server* suatu jaringan secara *real-time.*

Perancangan sistem dilakukan menggunakan beberapa langkah untuk memperoleh hasil yang diinginkan. Instalasi dan konfigurasi Sistem Operasi pada *Virtual Machine* untuk masing-maing sistem IDS dengan *resources cpu, ram* dan *storage* yang sama untuk keakuratan pengujian. Instalasi dan konfigurasi *Virtualmin Server Administration Manager* pada setiap sistem *IDS Server* sebagai sarana memepermudah pengaturan mail server. Instalasi dan konfigurasi *Web Mail Server* pada setiap sistem *IDS Server.* Instalasi dan konfigurasi aplikasi *IDS Server.* Pengujian interkoneksi antara satu mesin Attacker dan satu mesin IDS. Pengujian DoS yang dilakukan di mesin Attacker dengan menggunakan LOIC terhadap port 80 *Web Mail* dengan menggunakan parameter pengujian seperti jumlah tread attack packet dan/atau lamanya pengujian. Proses analisa sumberdaya masing-masing server IDS Snort, Suricata dan OSSEC. Analisa serangan terdeteksi dan analisa penggunaan sumberdaya akan dijadikan parameter pengujian efektivitas dan efisiensi sistem.

Hasil penelitian ini menunjukan perhitungan pendeteksian serangan dengan menggunakan parameter jumlah rata-rata, persentase serangan terdeteksi (*captured packets*) dan serangan yang tidak terdeteksi(*uncaptured packets*) dan standar Deviasi dari ketiga IDS. Yang akan menunjukan IDS mana yang paling Efisien dan IDS mana yang paling Efektif.

Kata Kunci: *IDS, Snort, Suricata, Ossec, Mail server*

ABSTRACT

The email platform is one type of data exchange platform on the network. Mail application servers or often abbreviated as mail servers are software programs that distribute files or information in response to requests sent via electronics. Thanks to the central use of email technology to support network services, it's no wonder that attacks on mail servers are often found. Such as Denial of Services to mail servers. use of IDS / IPS Server to stem attacks from the network side. IDS (Intrusion Detection System) is a system used to detect suspicious activity against a network server in real-time.

The system design is carried out using several steps to obtain the desired results. Installing and configuring the Operating System on a Virtual Machine for each IDS system with the same cpu, ram and storage resources for testing accuracy. Installing and configuring Virtualmin Server Administration Manager on each IDS Server system as a means of simplifying mail server settings. Installing and configuring a Web Mail Server on each IDS Server system. IDS Server application installation and configuration. Testing the interconnection between one Attacker machine and one IDS machine. DoS testing performed on the Attacker machine using LOIC against port 80 Web Mail using test parameters such as the number of tread attack packets and / or the length of the test. The process of analyzing the resources of each server's IDS Snort, Suricata and OSSEC. Analysis of detected attacks and analysis of resource use will be used as parameters for testing the effectiveness and efficiency of the system.

The results of this study indicate the calculation of attack detection using the parameters of the average number, the percentage of detected attacks (captured packets) and undetected attacks (uncaptured packets) and the standard deviation of the three IDS. Which will show which IDS is the most Efficient and which IDS is the most Effective.

Keyword: *IDS, Snort, Suricata, Ossec, Mail server*