ANALISIS PERBANDINGAN INTRUSION DETECTION SYSTEM PADA WEB SERVER MENGGUNAKAN SURICATA DAN OSSEC

SKRIPSI

disusun oleh

Fahrozi Ridwan Joutulis

15.11.8866

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM
YOGYAKARTA
2019

ANALISIS PERBANDINGAN INTRUSION DETECTION SYSTEM PADA WEB SERVER MENGGUNAKAN SURICATA DAN OSSEC

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika

disusun oleh

Fahrozi Ridwan Joutulis

15.11.8866

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM
YOGYAKARTA
2019

PERSETUJUAN

SKRIPSI

ANALISIS PERBANDINGAN INTRUSION DETECTION SYSTEM PADA WEB SERVER MENGGUNAKAN SURICATA DAN OSSEC

yang dipersiapkan dan disusun oleh

Fahrozi Ridwan Joutulis

15.11.8866

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 31 Oktober 2018

Dosen Pembimbing,

Nila Feby Puspitasari, S.Kom, M.Cs

NIK. 190302161

PENGESAHAN

SKRIPSI

ANALISIS PERBANDINGAN INTRUSION DETECTION SYSTEM PADA WEB SERVER MENGGUNAKAN SURICATA DAN OSSEC

yang dipersiapkan dan disusun oleh

Fahrozi Ridwan Joutulis

15.11.8866

telah dipertahankan di depan Dewan Penguji
pada tanggal 26 Agustus 2019

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Agung Nugroho, M.Kom **NIK. 190302242**	
Ike Verawati, M.Kom **NIK. 190302237**	
Nila Feby Puspitasari, S.Kom, M.Cs **NIK. 190302012**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 06 September 2019

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, 26 Agustus 2019

Fahrozi Ridwan Joutulis

NIM. 15.11.8866

MOTTO

"*Karena sesungguhnya sesudah kesulitan itu ada kemudahan*."

(**QS. Alam Nasyroh: 5**)

"*Jika kamu tidak kuat menahan lelahnya belajar,*

maka kamu harus kuat untuk menahan perihnya kebodohan"

(Imam Syafi'i)

"*Sukses itu tidak diukur oleh posisi yang telah diraih seseorang dalam kehidupan,*

tapi hambatan yang telah ia atasi saat berusaha untuk sukses."

(**Booker T. Washington**)

"*Tindakan adalah kunci dasar untuk semua kesuksesan*"

(**Pablo Picasso**)

"*Hanya mereka yang berani gagal yang bisa mendapatkan yang terbaik*"

(**Robert F. Kennedy**)

PERSEMBAHAN

Pertama dan paling utama, saya ucapkan puji syukur atas kehadirat Allah SWT yang telah memberikan kemudahan dan kelancaran dalam proses pembuatan skripsi ini. Skripsi ini sangat berharga karena upaya berbagai pihak yang turut serta memberikan restu, do'a dan dukungan mereka. Untuk itu semua saya ingin mempersembahkan skripsi ini dan berterimakasih kepada :

1. Kedua orang tua saya Bapak H.Murid Joutulis dan Ibu Hj.Siti Aminah yang senantiasa memberikan semangat,do'a,dan uang bulananku (hehehe) semoga selalu dalam lindungan dan kasih sayang-Nya (amin)
2. Ibu Nila Feby Puspitasari, S.Kom, M.Cs., selaku dosen pembimbing yang telah memberikan bimbingan aktif selama proses penyusunan skripsi ini, semoga mendapatkan keberkahan dan kelancaran dalam segala urusannya.
3. Spesial buat seseorang yang masih menjadi rahasia illahi, yang pernah singgah (*Firda Angriyani*), terimkasih untuk semua-semuanya yang pernah tercurah untukku. Untuk seseorang di relung hati percayalah bahwa hanya ada satu namamu yang selalu kusebut-sebut dalam benih-benih doaku, semoga keyakinan dan takdir ini terwujud, insyaallah jodohnya kita bertemu atas ridho dan izin Allah S.W.T.
4. Teman-teman 15-S1IF-06, yang selalu bersama dari awal kuliah sampai akhir kuliah, terimakasih telah memberikan banyak cerita dan pengalaman

kepada saya serta mohon maaf jika selama ini banyak kesalahan, sukses selalu untuk kita semua.

5. Arfan Fachmi, Christanto Triputra Munthe, Indra Setiawan, Raihan Adly Baskara, Reva Arbi, Siti Maulida, Agneli Jolana Putri, Vivi Dwi Oktavian, yang memberikan banyak cerita selama kuliah ini dan menjadi teman untuk berbagi.
6. Serta semua teman-teman dan pihak-pihak yang tidak bisa saya sebutkan satu per satu yang telah mendo'akan, mendukung dan memotivasi saya selama ini.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Puji syukur penulis panjatkan kehadirat Allah SWT karena atas limpahan rahmat, hidayah serta inayah-Nya, penulis masih diberikan kesempatan dan kemudahan untuk menyelesaikan skripsi ini.

Skripsi ini disusun dalam rangka memenuhi salah satu syarat kelulusan perguruan tinggi Program Studi Strata 1 Informatika di Univeristas AMIKOM Yogyakarta dan meraih gelar Sarjana Komputer (S.Kom). Selain itu skripsi ini juga bertujuan untuk menambah pengetahuan tentang sistem keamanan yang dibuat menggunakan metode *IDS/IPS* dengan berbasis *Snort*.

Pembuatan skripsi ini tidak lepas dari berbagai pihak yang telah membantu baik dari segi material dan spiritual. Penulis juga mengucapkan terimakasih yang sebesar-besarnya kepada :

1. Bapak Prof. Dr. Suyanto, M.M., selaku rektor Universitas AMIKOM Yogyakarta.
2. Ibu Nila Feby Puspitasari, S.Kom, M.Cs selaku dosen pembimbing yang telah memberikan masukan, saran, bantuan dan bimbingan dalam menyelesaikan naskah skripsi ini.
3. Ibu Krisnawati, S.Si., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
4. Bapak Sudarmawan, M.T., selaku Ketua Program Studi S1 Informatika Universitas AMIKOM Yogyakarta.

5. Dosen Universitas AMIKOM Yogyakarta yang telah memberikan ilmu dan pengalaman, terimakasih atas semua jasa Bapak dan Ibu sekalian.
6. Orang tua yang tidak pernah lelah dalam memberikan dukungan, restu dan do'anya.
7. Teman-teman dan sahabat yang telah memberikan semangat, motivasi dan bantuan dalam pengerjaan skripsi ini.
8. Seluruh staff dan karyawan Universitas AMIKOM Yogyakarta yang banyak membantu kelancaran segala aktivitas dan administrasi dalam penyusunan skripsi ini.
9. Terima kasih untuk kakak terbaikku selama ini (Faridha Joutulis) yang telah memberi semangat selama ini, hingga terselesaikannya skripsi ini.
10. Semua pihak yang telah membantu sampai terselesaikannya penyusunan skripsi ini yang tentunya sangat berharga dan tidak bisa disebutkan satu per satu.

Penulis menyadari sepenuhnya, bahwa skripsi ini masih jauh dari sempurna, baik dalam hal ini maupun cara penyajian materi. Untuk itu dengan rendah hati penulis mohon saran dan kritik yang membangun dari pembaca.

Semoga skripsi ini dapat bermanfaat bagi penulis pada khusunya dan bagi pembaca pada umumnya serta dapat digunakan sebagai referensi untuk penelitian yang lain.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Yogyakarta, 26 Agustus 2019

Fahrozi Ridwan Joutulis
NIM. 15.11.8866

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Keamanan jaringan *web server* tergantung pada kecepatan pengaturan jaringan dalam menindaklanjuti sistem saat terjadi gangguan. Untuk memperkuat keamanan jaringan *web server* dapat diterapkan sistem pendeteksi serangan dalam jaringan atau *intrusion detection system* (IDS). IDS (*intrusion detection system)* merupakan perangkat keras atau lunak yang mempunyai kemampuan untuk mendeteksi sebuah serangan jaringan

Program *Intrusion Detection System* (IDS) yang sering digunakan untuk menjaga keamanan jaringan yaitu IDS *Ossec* dan *Suricata*. IDS *Ossec* memiliki kelebihan dapat mendeteksi pola pada paket yang lewat dan mengirimkan notifikasi jika pola terdeteksi. Suricata dapat mendeteksi dan mencegah gangguan seperti *Port Scanning* atau aktivitas untuk mendapatkan informasi yang menyeluruh mengenai status port pada sebuah host.

Penelitian dengan membandingkan kedua IDS ini menggunakan sistem operasi Linux dan menggunakan satu jenis serangan yang akan diuji yaitu *Distributed Denial of Service* (DDoS). Skenario serangan yang akan dilakukan pada penelitian ini yaitu DDoS akan menyerang *web server* kemudian IDS *Suricata* dan *Ossec* yang telah terpasang pada *web server* akan memberikan peringatan jika telah terjadi serangan. Dalam menentukan hasil perbandingan, digunakan parameter-parameter yang akan menjadi acuan yaitu Jumlah Serangan Terdeteksi dan Efektivitas Deteksi Serangan kedua IDS.

Kata Kunci: keamanan jaringan, web server, IDS, Ossec, Suricata, DDoS

ABSTRACT

Web server network security depends on the speed of the network settings in following up on the system when an interruption occurs. To strengthen the security of the web server network, an intrusion detection system (IDS) can be applied. IDS (intrusion detection system) is hardware or software that has the ability to detect a network attack

Intrusion Detection System (IDS) programs that are often used to maintain network security are Ossec and Suricata IDS. Ossec IDS has the advantage of being able to detect patterns in passing packets and send notifications if patterns are detected. Suricata can detect and prevent interruptions such as Port Scanning or activities to get comprehensive information about the port status on a host.

Research by comparing the two IDS uses the Linux operating system and uses one type of attack to be tested, namely Distributed Denial of Service (DDoS). The attack scenario that will be carried out in this research is DDoS will attack the web server then IDS Suricata and Ossec which have been installed on the web server will give a warning if an attack has occurred. In determining the results of the comparison, parameters that will be used as reference are the number of attacks detected and the effectiveness of the second IDS attack detection.

Keyword: *network security, web server, IDS, Ossec, Suricata, DDoS*