ANALISIS PERBANDINGAN KINERJA SNORT DAN SURICATA SEBAGAI INTRUSION DETECTION SYSTEM DALAM MENDETEKSI SERANGAN SYN FLOOD PADA WEB SERVER APACHE

SKRIPSI

disusun oleh

Melati Suci

16.11.0525

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

2020

ANALISIS PERBANDINGAN KINERJA SNORT DAN SURICATA SEBAGAI INTRUSION DETECTION SYSTEM DALAM MENDETEKSI SERANGAN SYN FLOOD PADA WEB SERVER APACHE

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika

disusun oleh

Melati Suci

16.11.0525

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

PERSETUJUAN

SKRIPSI

ANALISIS PERBANDINGAN KINERJA SNORT DAN SURICATA SEBAGAI INTRUSION DETECTION SYSTEM DALAM MENDETEKSI SERANGAN SYN FLODD PADA WEB SERVER APACHE

yang dipersiapkan dan disusun oleh

Melati Suci
16.11.0525

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 27 September 2019

Dosen Pembimbing,

Lukman, M.Kom
NIK. 190302151

PENGESAHAN

SKRIPSI

ANALISIS PERBANDINGAN KINERJA SNORT DAN SURICATA SEBAGAI INTRUSION DETECTION SYSTEM DALAM MENDETEKSI SERANGAN SYN FLODD PADA WEB SERVER APACHE

yang dipersiapkan dan disusun oleh
Melati Suci
16.11.0525

telah dipertahankan di depan Dewan Penguji
pada tanggal 17 Januari 2020

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Lukman, M.Kom **NIK. 190302151**	
Agung Pambudi, S.T, M.A **NIK. 190302012**	
Ike Verawati, M.Kom **NIK. 190302237**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 17 Januari 2020

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertanda tangan di bawah ini menyatakan, skripsi ini merupakan karya saya sendiri (ASLI) dan isi didalam skripsi tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Instansi Pendidikan dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis / 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 tanggung jawab saya pribadi.

Yogyakarta, 21 Januari 2020

Melati Suci
NIM 16.11.0525

MOTTO

"Every journey begins with a single step. And you'll never finish if you don't start."

HALAMAN PERSEMBAHAN

Tak henti – hentinya saya mengucapkan syukur kepada Allah SWT yang telah memberikan saya kenikmatan, kesehatan, kesempurnaan, serta dapat menyelesaikan skripsi ini, dan skripsi ini saya persembahkan untuk:

1. Allah SWT yang telah mengabulkan semua do'a - do'a saya termasuk doa dalam menyelesaikan skripsi ini dengan lancar.
2. Untuk kedua orangtua saya yaitu Papa dan Mama yang selalu memberikan dorongan baik itu moril maupun materil, terimakasih selalu mendoakan yang terbaik dan mengasihiku sepenuh hati.
3. Untuk Kakak saya dan Adik saya, A Galih dan Dek Agung yang selalu memberikan dukungan dan semangatnya.
4. Untuk Bapak Lukman, M.Kom selaku dosen pembimbing sekaligus dosen wali, terimakasih banyak atas bimbingannya sehingga skripsi ini dapat terselesaikan.
5. Untuk Dian Lesmana sebagai support system yang selalu ada dan membantu dalam proses skripsi ini sehingga mendapatkan hasil yang terbaik. Terimkasih selalu sabar dan selalu mendoakanku.
6. Terimakasih untuk sister by heart a.k.a geng sobat ngegas yaitu Alifa, Anggita, Hesty,Dw,Ozka,Revi, telah bersamaku selama satu dekade, yang selalu memberikan semangat dan menghiburku sehingga memperlancar skripsiku.
7. Terimakasih untuk geng Kecehbong yaitu, Mayang yang selalu menjadi teman sepernasiban mungkin nasib kita memang berjodoh, Winda yang siap sedia

dalam bidang revisi penulisanku, Fafa yang menjadi mentor jaringanku, Anes yang selalu menyemangatiku.

8. Untuk keluarga besar Informatika-08 terimakasih sudah hadir di pendadaranku meskipun hanya sebagian.
9. Untuk asdosku mas bekti terimakasih sudah menjadi mentor skripsi ini.
10. Seluruh pihak yang tidak dapat disebutkan satu per satu, terimakasih atas segala bantuannya dan do'anya sehingga terselesaikan skripsi ini.

KATA PENGANTAR

Puji dan syukur senantiasa peneliti panjatkan kepada ALLAH SWT, karena berkat pertolongan-Nya Alhamdulillah peneliti dapat menyelesaikan laporan skripsi ini dengan baik. Laporan skripsi yang dibuat untuk memenuhi syarat memperoleh gelar kesarjanaan Strata-1 (S1) jurusan Informatika Universitas AMIKOM Yogyakarta diharapkan bisa menjadi salah satu referensi pembuatan skripsi di Universitas AMIKOM Yogyakarta serta dapat memberikan penambahan ide yang dapat dikembangkan dimasa depan.

Skripsi ini disusun sebagai salah satu syarat kelulusan perguruan tinggi Program Studi Strata-1 Informatika di Universitas AMIKOM Yogyakarta. Selain itu skripsi ini bertujuan agar pembaca dapat menambah ilmu pengetahuan dan wawasannya.

Pada kesempatan ini dengan segala ketulusan, keikhlasan serta kerendahan hati penulis ingin mengucapkan banyak berterima kasih yang sebesar-besarnya dan penghargaan setinggi-tingginya kepada semua pihak yang telah membantu penulis dalam menyelesaikan skripsi ini**.** Dalam penulisan laporan skripsi ini, peneliti banyak mendapatkan bantuan serta semangat dari berbagai pihak. Untuk itu peneliti menyampaikan rasa hormat, dan terimakasih kepada:

1. Papa saya Edia Herdis, S.Pd, Ibu saya tercinta Hernaningsih, S.Pd, Kakak saya Galih CS, dan Adik saya Agung Gumilang.
2. Bapak M. Suyanto, Prof. Dr, M.M., selaku rektor Universitas AMIKOM Yogyakarta.

3. Bapak Sudarmawan, M.T selaku ketua program studi Informatika
4. Bapak Lukman, M.Kom selaku dosen pembimbing.
5. Tim penguji, segenap dosen dan karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu pengetahuan dan dukungan moral.
6. Keluarga sobat ngegas.
7. Keluarga besar kecehbong.
8. Keluarga besar Informatika-08

Peneliti juga memohon maaf kepada semua pihak jika dalam pelaksanaan dan penulisan laporan skripsi ini terdapat kesalahan atau hal yang kurang berkenan, semua tidak lepas karena keterbatasan peneliti.

Akhirnya, hanya dengan berdoa kepada ALLAH SWT, peneliti berharap semoga laporan skripsi ini dapat bermanfaat bagi kita semua. Amin.

Yogyakarta, 21 Januari 2020

Melati Suci

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Keamanan jaringan pada *web server* merupakan bagian yang paling penting untuk menjamin integritas dan layanan bagi pengguna. *Web server* sering kali menjadi target serangan yang mengakibatkan kerusakan data. Salah satunya serangan *SYN Flood* merupakan jenis serangan *Denial of Service* (DOS) yang memberikan permintaan *SYN* secara besar-besaran kepada web server.

Untuk memperkuat keamanan jaringan web server penerapan *Intrusion Detection System* (IDS) digunakan untuk mendeteksi serangan, memantau dan menganalisa serangan pada *web server*. *Software* IDS yang sering digunakan yaitu IDS *Snort* dan IDS *Suricata* yang memiliki kelebihan dan kekurangannya masing-masing.

Tujuan penelitian kali ini untuk membandingkan kedua IDS menggunakan sistem operasi linux dengan pengujian serangan menggunakan *SYN Flood* yang akan menyerang *web server* kemudian IDS *Snort* dan *Suricata* yang telah terpasang pada web server akan memberikan peringatan jika terjadi serangan. Dalam menentukan hasil perbandingan, digunakan parameter-parameter yang akan menjadi acuan yaitu jumlah serangan yang terdeteksi dan efektivitas deteksi serangan dari kedua IDS tersebut.

Kata kunci : *Intrusion Detection System*, keamanan jaringan, *Web Server, Snort, Suricata*

.

ABSTRACT

Network security on the web server is the most important part to guarantee the integrity and service for users. Web servers are often the target of attacks that result in data damage. One of them is the SYN Flood attack which is a type of Denial of Service (DOS) attack that gives a massive SYN request to the web server.

To strengthen the web server network security the application of Intrusion Detection System (IDS) is used to detect attacks, monitor and analyze attacks on web servers. IDS applications that are often used are IDS Snort and Suricata IDS which have their respective advantages and disadvantages.

The purpose of this study is to compare the two IDS using the Linux operating system with testing the attack using SYN Flood which will attack the web server then IDS Snort and Suricata that have been installed on the web server will give a warning if an attack occurs. In determining the results of the comparison, the parameters used will be the reference, namely the number of attacks detected and the effectiveness of attack detection from the two IDS.

KeyWords : *Intrusionn Detection System, Network Security, Web Server, Snort, Suricata*