ANALISIS KEEFEKTIFAN SNORT DALAM MENDETEKSI SERANGAN BERDASARKAN JUMLAH ALERT YANG DIHASILKAN

Tugas Akhir

Oleh
GREGORIUS ADVIAN W
71120098

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
YOGYAKARTA
2017

©UKDW

ANALISIS KEEFEKTIFAN SNORT DALAM MENDETEKSI SERANGAN BERDASARKAN JUMLAH ALERT YANG DIHASILKAN

Tugas Akhir

Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi

Universitas Kristen Duta Wacana

Sebagai Salah Satu Syarat dalam Memperoleh Gelar

Sarjana Komputer

Disusun Oleh

Gregorius Advian Widiyanto
71120098

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
YOGYAKARTA
2017

©UKDW

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

ANALISIS KEEFEKTIFAN SNORT DALAM MENDETEKSI SERANGAN PADA JARINGAN BERDASARKAN JUMLAH ALERT YANG DIHASILKAN

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 28 September 2017

GREGORIUS ADVIAN W

71120098

©UKDW

HALAMAN PERSETUJUAN

Judul Skripsi	:	ANALISIS KEEFEKTIFAN SNORT DALAM MENDETEKSI SERANGAN PADA JARINGAN BERDASARKAN JUMLAH ALERT YANG DIHASILKAN
Nama Mahasiswa	:	GREGORIUS ADVIAN W
N I M	:	71120098
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Gasal
Tahun Akademik	:	2017/2018

©UKDW

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 22 Oktober 2017

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, S.Kom.,M.Cs.	Gani Indriyanta, Ir. M.T.

HALAMAN PENGESAHAN

ANALISIS KEEFEKTIFAN SNORT DALAM MENDETEKSI SERANGAN PADA JARINGAN BERDASARKAN JUMLAH ALERT YANG DIHASILKAN

Oleh: GREGORIUS ADVIAN W / 71120098

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 16 Oktober 2017

Yogyakarta, 23 Oktober 2017
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
2. Gani Indriyanta, Ir. M.T.
3. Nugroho Agus Haryono, M.Si
4. Budi Susanto, SKom.,M.T.

Dekan

(Budi Susanto, S.Kom., M.T.)

Ketua Program Studi

(Gloria Virginia, Ph.D.)

©UKDW

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa karena atas berkat dan rahmatNya skripsi yang berjudul ”Analisis Keefektifan Snort Dalam Mendeteksi Serangan Berdasarkan Alert Yang Dihasilkan” dapat terselesaikan dengan baik.

Laporan tugas akhir ini diajukan guna melengkapi sebagai syarat dalam mencapai gelar sarjana strata satu (S1) di Fakultas Teknologi Informasi Studi Teknik Informatika Universitas Kristen Duta Wacana. Penulis menyadari meskipun telah berusaha untuk menyajikan pembahasan sebaik mungkin, namun masih terdapat kekurangan dalam tugas akhir ini. Hal ini terjadi dikarenakan masih terbatasnya kemampuan dan pengetahuan penulis, penulis mengharapkan kritik dan saran yang membangun untuk menyempurnakan tugas akhir ini.

Dalam proses penyusunan tugas akhir ini penulis banyak mengalami kendala, namun berkat bantuan, bimbingan, dan kerjasama dari berbagai pihak serta berkah dari Tuhan Yang Maha Esa sehingga kendala-kendala yang dihadapi tersebut dapat diatasi. Oleh karena itu penulis menyampaikan ucapan terima kasih dan penghargaan kepada Bapak Willy Sudiarto Raharjo, S.Kom.,M.Cs. selaku pembimbing I dan Bapak Ir. Gani Indriyanta, M.T. selaku pembimbing II yang telah bersedia membimbing dengan sabar, tekun, ikhlas dan bersedia meluangkan waktu, tenaga dan pikiran dalam memberikan bimbingan, motivasi, arahan serta saran-saran yang sangat berharga bagi penulis dalam menyusun skripsi.

Selanjutnya ucapan terima kasih penulis sampaikan pula kepada :

1. Bapak Budi Susanto, S.Kom. M.T. selaku Dekan Fakultas Teknologi Informasi Universitas Kristen Duta Wacana.
2. Ibu Gloria Virginia, S.Kom, MAI, Ph.D. Selaku Kepala Program Studi Teknik Informatika Universitas Kristen Duta Wacana.

©UKDW

3. Teristimewa kepada orang tua penulis Y.Sumarno dan Christina Umi Listyantini serta seluruh keluarga yang selalu mendoakan, memberikan motivasi dan pengorbanan baik dari segi moril dan materi kepada penulis sehingga dapat menyelesaikan tugas akhir ini dengan baik.
4. Teman seperjuangan "TimLeng" yang selalu mengerjakan tugas akhir bersama, Bryan Sutisna dan Girindra Wahyuanggriananta dengan saling memberikan dukungan satu sama lain.
5. Jeffie Avando Saputra, Lusius Puput, Cacad, Noel dan Gangga yang selalu membantu dan memberikan hiburan dikala sedang jenuh mengerjakan penelitian .
6. Teman kontrakan Cepit Baru yang selalu menyediakan tempat dan sarana dan prasarana serta selalu mendukung penulis untuk menyelesaikan tugas akhir ini.
7. Semua pihak yang tidak dapat disebutkan satu persatu yang telah ikut memberikan dukungan baik secara langsung maupun tidak langsung.

Penulis menyadari bahwa masih banyak kekurangan, baik dalam penelitian ini maupun dalam penulisan laporan penelitian. Akhir kata penulis mengucapkan terima kasih kepada semua pihak yang telah membantu dan penulis berharap semoga tugas akhir ini dapat bermanfaat bagi kita semua dan menjadi bahan masukan bagi dunia pendidikan.

Yogyakarta, September 2017

Penulis

©UKDW

MOTTO

"You only live once, so make every second divine"

(Mitch Lucker)

©UKDW

INTISARI

Perkembangan teknologi informasi sekarang ini sangatlah pesat terutama dalam dunia Internet, namun yang cukup disayangkan adalah ketidakseimbangan antara perkembangan suatu teknologi dengan perkembangan sistem keamanan itu sendiri. Hadirnya *firewall* telah banyak membantu dalam pengamanan, akan tetapi hanya dengan *firewall* keamanan tersebut belum dapat dijamin sepenuhnya. Sekarang ini telah banyak *tools* atau aplikasi yang digunakan untuk mendeteksi serangan menggunakan *Instrusion Detection System* (IDS) salah satunya yaitu Snort**.**

Instrusion Detection System (IDS) *Snort* memiliki banyak *rule* yang disediakan. Serangan yang dapat dideteksi oleh *Snort* sangat bergantung pada *rule* yang diterapkan pada *Snort* itu sendiri. Snort menyediakan *rule* yang dapat diperoleh secara gratis untuk kemudian diterapkan kedalam Snort. Penerapan *rule* tersebut dapat dilakukan secara otomatis menggunakan Pulledpork. Penelitian ini dilakukan untuk mengetahui sejauh mana akurasi dari Snort yang menggunakan *rule* dari Pulledpork dalam mendeteksi beberapa serangan yang dilakukan selama pengujian.

Kesimpulan yang didapat oleh peneliti dari penelitian ini berupa tingkat *precision rate* dan *recall rate* dari Snort dari beberapa pengujian yang dilakukan. Snort memiliki *precision rate* sebesar 0,842105 dan *recall rate* sebesar 0,72727. Snort mampu mendeteksi sebagian besar serangan yang mengunakan protokol TCP namum memiliki kelemahan dalam mendeteksi serangan yang menggunakan protokol UDP dan *Spoofing*. Dari hasil kesimpulan tersebut dapat digunakan sebagai pertimbangan dalam membangun sebuah sistem keamanan jaringan komputer.

Kata kunci: Snort,*Intrusion Detection System,* Keamanan Jaringan

©UKDW

DAFTAR ISI

©UKDW

©UKDW

DAFTAR GAMBAR

©UKDW

DAFTAR TABEL

©UKDW

BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Perkembangan teknologi informasi sekarang ini sangatlah pesat terutama dalam dunia Internet, hal ini terbukti dengan semakin berkembangnya aplikasi yang berbasis web yang membutuhkan koneksi Internet agar bisa diakses oleh *user*. Sebuah aplikasi yang berbasiskan Internet tidak akan terlepas dari sebuah jaringan komputer dan *server* sebagai tempat penyimpanan data terpusat. Namun yang cukup disayangkan adalah ketidakseimbangan antara perkembangan suatu teknologi dengan perkembangan sistem keamanan itu sendiri. Keamanan jaringan komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga *validitas* dan *integritas* data serta menjamin ketersediaan layanan bagi penggunanya.

Keamanan sebuah jaringan komputer dapat dikelompokkan menjadi dua bagian yaitu keamanan yang bersifat fisik dan bersifat non fisik. Keamanan fisik lebih cenderung terhadap segala sesuatu yang berhubungan dengan fisiknya sedangkan keamanan non fisik adalah keamanan di mana suatu kondisi keamanan yang menitikberatkan pada kepentingan secara sifat, sebagai contoh yaitu pengamanan data, misalnya data sebuah perusahaan yang sangat penting. Keamanan suatu jaringan seringkali terganggu dengan adanya ancaman dari dalam ataupun dari luar. Serangan tersebut berupa serangan *hacker* yang bermaksud merusak jaringan komputer yang terkoneksi pada Internet ataupun mencuri informasi penting yang ada pada jaringan tersebut.

Dalam keamanan jaringan yang bersifat non fisik, hadirnya *firewall* telah banyak membantu dalam pengamanan, akan tetapi seiring berkembang teknologi sekarang ini hanya dengan *firewall* keamanan tersebut belum dapat dijamin sepenuhnya. Oleh karena itu dibutuhkan suatu sistem dalam menangani

©UKDW

gangguan atau ancaman yang akan terjadi secara optimal dalam waktu yang cepat dan otomatis. Sekarang ini telah banyak *tools* yang digunakan untuk mendeteksi serangan dengan menggunakan *Instrusion Detection System* (IDS) salah satunya yaitu *Snort.*

Instrusion Detection System (IDS) *Snort* memiliki banyak *rule* yang disediakan. Serangan yang dapat dideteksi oleh *Snort* sangat bergantung pada *rule* yang diterapkan pada *Snort* itu sendiri. Oleh karena itu pemilihan dan pemasangan *rule* dalam *Snort* sangat penting dalam sistem deteksi ini. Pada penelitian ini akan dilakukan pengujian terhadap *rule Snort* dengan melakukan beberapa serangan untuk menguji serangan apa saja yang dapat di deteksi oleh *Snort* menggunakan *rule* tersebut.

Pengujian dilakukan dengan menggunakan *tool* seperti Metasploit untuk melakukan serangan seperti *IP Scan, Port Scan,* dan *Flooding* sebagai serangan yang diujikan sedangkan untuk menampilkan *alert* dari serangan yang terdeteksi akan ditampilkan menggunakan *Basic Analysis Security Engine* (BASE) .

Dari hasil keluaran atau *alert* yang ditampilkan oleh BASE tersebut akan dilakukan penelitian seberapa akurat Snort dalam mendeteksi serangan berdasarkan jumlah serangan yang dihasilkan dari berbagai serangan yang dilakukan.

©UKDW

1.2. Rumusan Masalah

Berdasarkan penjelasan latar belakang di atas, maka penulis dapat merumuskan pokok masalah yang akan dikaji dalam penelitian ini. Penelitian ini dilakukan untuk mengetahui akurasi dari Snort *Intrusion Detection System* (IDS) dalam mendeteksi beberapa serangan yang dilakukan terhadap suatu sistem jaringan komputer.

1.3. Batasan Sistem

Dalam penelitian ini, penulis memberikan beberapa batasan sistem guna mempermudah dan membatasi ruang lingkup masalah yang akan dikaji, antara lain:

a. *Intrusion Detection System* (IDS) yang digunakan adalah Snort versi 2990.
b. Hasil analisa berdasarkan persentase dari keakuratan alert yang dihasilkan.
c. Rule yang digunakan merupakan rule yang berasal dari PulledPork dengan update pada tanggal 20 September 2017.
d. Simulasi serangan menggunakan : Port Scanning, Sniffing, Flooding, Spoofing, Bruteforce, SQL Injection.

1.4. Tujuan Penelitian

Tujuan penelitian ini adalah menganalisa keakuratan dari *Snort Intrusion Detection System* dalam mendeteksi serangan penyusup (*intruder*) dengan menghitung persentase keberhasilan sistem dalam mendeteksi serangan yang dilakukan.

1.5. Metodologi Penelitian

Metode yang dilakukan penulis dalam melakukan penelitian ini antara lain sebagai berikut :

a. Studi Literatur

Studi literatur digunakan dengan membaca jurnal, buku-buku, dan hasil penelitian (skripsi dan thesis) yang berkaitan dengan keamanan jaringan komputer, *Intrusion Detection System* (IDS), *Snort.*

b. Analisa dan perancangan sistem.

©UKDW

Melakukan perancangan sistem *Snort Intrusion Detection System* (IDS) dengan mengimplementasikan *rule* yang sudah ditentukan.

c. Implementasi Sistem

Menerapkan sistem *Intrusion Detection System* (IDS) dengan *Snort* yang menerapkan rule yang sudah ditentukan ke dalam sebuah jaringan komputer. Memberikan berbagai jenis serangan terhadap *dummy* server dengan *software* yang sudah ditentukan. Jika paket serangan memenuhi kriteria dari *rule* yang diterapkan, maka Snort akan mengirimkan *alert*.

d. Evaluasi dan Kesimpulan

Setelah proses implementasi selesai, penulis dapat menarik kesimpulan dan melakukan evaluasi terhadap sistem yang telah diujikan. Evaluasi meliputi tingkat keakuratan sistem dalam mendeteksi ancaman atau gangguan yang masuk ke dalam jaringan berdasarkan keakuratan *alert* yang dihasilkan.

1.6. Sistematika Penulisan

Sistematika diperlukan untuk memberi dasar-dasar penulisan supaya hasil yang diperoleh dari penulisan akan lebih terarah. Adapun sistematika penulisan yang digunakan kali ini adalah:

BAB 1 Pendahuluan

Bab Pendahuluan berisi tentang bagian awal dari penulisan laporan. Di mana pada bagian ini memuat Latar Belakang Masalah, Perumusan Masalah, Batasan Masalah, Tujuan Penelitian, Metode Penelitian dan Sistematika Penulisan.

BAB 2 Tinjauan Pustaka

©UKDW

Pada bab ini berisi bahasan penelitian dan berbagai referensi mengenai penelitian *Snort IDS* serta landasan teori yang menjadi dasar penelitian ini. Pada bab ini akan diterangkan secara detail sesuai informasi serta studi pustaka yang diperoleh peneliti berkaitan dengan analisis keamanan jaringan.

Pada bab ini memuat mengenai berbagai teori yang didapatkan dari berbagai sumber pustaka yang diperlukan untuk memecahkan masalah. Bab ini terdiri dari dua bagian utama, yaitu Tinjauan Pustaka dan Landasan Teori. Tinjauan Pustaka berisi tentang penelitian-penelitian *Snort IDS* sebelumnya, sedangkan untuk Landasan Teori berisi tentang penjelasan tentang keamanan jaringan komputer khususnya *Intrusion Detection System* (IDS).

BAB 3 Metodologi Penelitian

Bab ini berisikan rancangan dari sistem yang akan mengimplementasikan *Snort IDS*, alur kerja sistem, serta kebutuhan akan *hardware* maupun *software* untuk mendukung penelitian serta langkah-langkah implementasi dalam penelitian yang dilakukan secara lebih jelas.

BAB 4 Hasil dan Pembahasan

Bab ini memuat uraian mengenai hasil analisis yang didapat berdasarkan *alert* yang dihasilkan dari ujicoba yang dilakukan.

Untuk hasil implementasi dan analisis akan disajikan dalam bentuk daftar, tabel, foto, maupun bentuk lainnya.

BAB 5 Kesimpulan dan Saran

Bab ini berisi tentang kesimpulan dari hasil pengujian yang telah dilakukan dan berisi saran untuk mengembangkan penelitian selanjutnya yang berkaitan dengan *Snort IDS.*

©UKDW

BAB V
KESIMPULAN DAN SARAN

Bab ini akan berisi kesimpulan yang diambil setelah pengujian dari Snort IDS yang sebelumnya telah dibuat serta saran mengenai perbaikan dalam pengujian dan kemungkinan penelitian lanjutan.

5.1. Kesimpulan

Setelah penulis melakukan implementasi dan analisis dalam pengujian Snort IDS maka diperoleh hasil penelitian sebagai berikut:

a. Dari berbagai macam percobaan dan serangan yang dilakukan dalam pengujian Snort memiliki *Precision rate* sebesar 0,88461dan *Recall rate* sebesar 0,74193 dengan akurasi sebesar 0.82539.
b. Snort IDS mampu mendeteksi sebagian besar serangan yang dilakukan melalui protokol TCP.
c. Pada pengujian IP *Spoofing*, Snort IDS tidak dapat mendeteksi serangan tersebut.
d. Pada pengujian UDP *Flooding*, Snort IDS tidak dapat mendeteksi serangan tersebut.

5.2. Saran

Beberapa saran penulis untuk penelitian lebih lanjut yaitu :

a. Peneletian lebih lanjut dengan memperbanyak jumlah dan jenis serangan yang dilakukan.
b. Penelitian perbandingan Snort IDS dengan aplikasi IDS yang lain.

©UKDW

DAFTAR PUSTAKA

Airlangga, G., & Mualo, A. (2015). Seminar Nasional Teknologi Informasi dan Komunikasi. *Penggunaan Algoritma Brute Force Dalam Jenis Serangan DDOS Untuk Menguji Pertahanan Website*, 417-423.

Babu, P. R., Bhasari, D. L., & Satyanaranaya, C. (2010). A Comprehensive Analysis of Spoofing. *International Journal of Advanced Computer Science and Applications*, 157-162.

Babys, J. Y., & Kusrini, S. (2013). Analisis Aspek Keamanan Informasi Jaringan Komputer. *Seminar Nasional Informatika*, 7-14.

Baskoro, A. P., Muchammad, H., & Rahajeng, E. (2013). Pendeteksi Serangan SQL Injection Menggunakan Algoritma SQL Injection Free Secure pada Aplikasi Web. *JURNAL TEKNIK POMITS Vol 2 No 1*, 1-6.

Elhamahmy, M. E., Hesham, Elmahdy, & Saroit, I. A. (2010). A New Approach for Evaluating Intrusion Detection System. *CiiT International Journal of Artificial Intelligent Systems and Machine Learning*, 291-298.

Gondohanindijo, & Jutono. (2011). Sistem Untuk Mendeteksi Adanya Penyusup. *Majalah Ilmiah Informatika Vol. 2 No. 2 Mei 2011*, 46-54.

Jabez J, D. (2015). Intrusion Detection System (IDS): Anomaly Detection using Outlier. *Procedia Computer Science*, 338 – 346.

Jannah, M., Hustinawati, & Wildani, R. (2012). Implementasi Intrusion System (IDS) Snort Pada Laboratorium Jaringan Komputer. *UG Jurnal, 6*, 1-4.

Patel, J., & Panchal, M. K. (2015). Effective Intrusion Detection System using Data Mining Technique. *Journal of Emerging Technologies and Innovative Research*, 1869-1878.

Pramudita, K. E. (2010). Krisnaldi Eka Pramudita . *Makalah IF3051 Strategi Algoritma*, 62-68.

Regina, R., Lidyawati, L., & Ramadhan, Z. (2013). Analisis Kinerja Sistem Pengamanan Jaringan dengan Menggunakan Snort IDS Dan Ip-Tables di Area Laboratorium RDNM PT. ”X”. *Jurnal Reka Elkomika*, 186-197.

Utami, A. S., Lidyawati, L., & Ramadhan, Z. (2013). Perancangan dan Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort IDS dan Honeyd. *Jurnal Reka Elkomika*, 317-327.

©UKDW