MONITORING JARINGAN MENGGUNAKAN SNORT

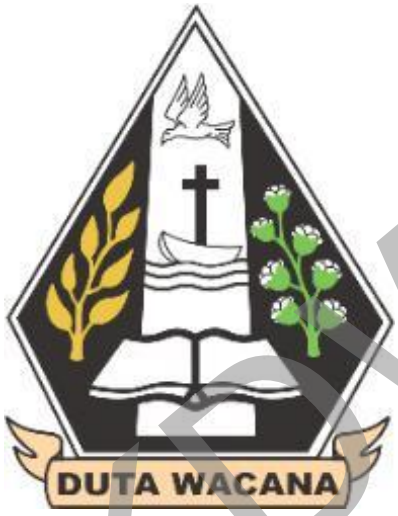
Skripsi

oleh
DODI FERDAUS
71140103

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

MONITORING JARINGAN MENGGUNAKAN SNORT

Skripsi



Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

DODI FERDAUS
71140103

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

PERNYATAAN KEASLIAN SKRIPSI

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

MONITORING JARINGAN MENGGUNAKAN SNORT

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, 14 Agustus 2017

DODI FERDAUS
71140103

HALAMAN PERSETUJUAN

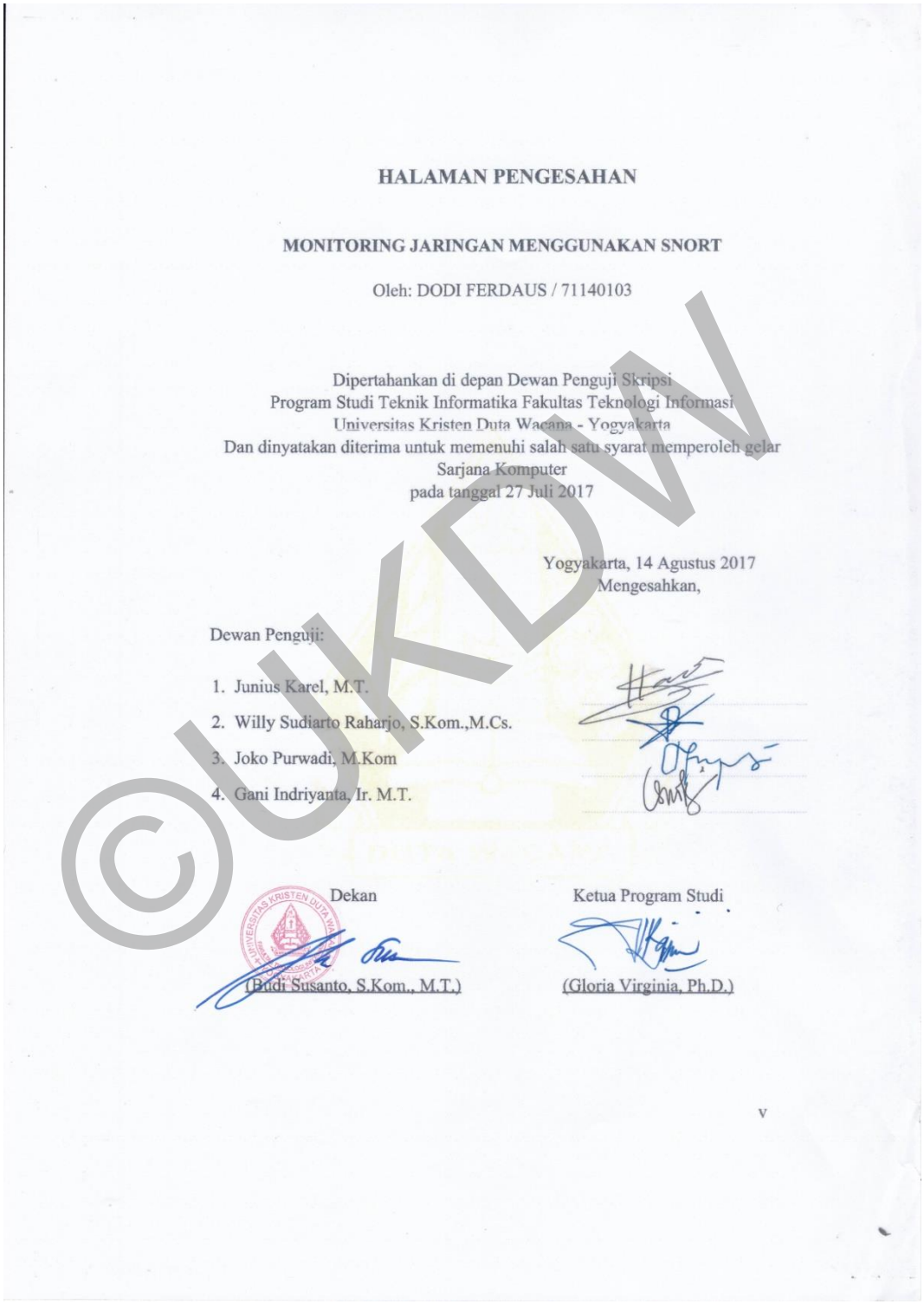
HALAMAN PERSETUJUAN

Judul Skripsi	:	MONITORING JARINGAN MENGGUNAKAN SNORT
Nama Mahasiswa	:	DODI FERDAUS
N I M	:	71140103
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Genap
Tahun Akademik	:	2016/2017

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 14 Agustus 2017

Dosen Pembimbing I	Dosen Pembimbing II
Junius Karel, M.T.	Willy Sudiarto Raharjo, S.Kom.,M.Cs.

HALAMAN PENGESAHAN



HALAMAN PENGESAHAN

MONITORING JARINGAN MENGGUNAKAN SNORT

Oleh: DODI FERDAUS / 71140103

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 27 Juli 2017

Yogyakarta, 14 Agustus 2017
Mengesahkan,

Dewan Penguji:

1. Junius Karel, M.T.
2. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
3. Joko Purwadi, M.Kom
4. Gani Indriyanta, Ir. M.T.

Dekan

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

Ketua Program Studi

(Gloria Virginia, Ph.D.)

v

UCAPAN TERIMAKASIH

Puji syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa yang telah melimpahkan rahmat dan anugerah, sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul "Monitoring Jaringan Menggunakan Snort".

Penulisan laporan Tugas Akhir ini merupakan kelengkapan dan pemenuhan dari salah satu syarat dalam memperoleh gelar Sarjana Komputer. Selain itu bertujuan melatih mahasiswa untuk dapat menghasilkan suatu karya yang dapat dipertanggungjawabkan secara ilmiah, sehingga dapat bermanfaat bagi penggunanya.

Dalam menyelesaikan pembuatan program dan laporan Tugas Akhir ini, penulis telah banyak menerima bimbingan, saran dan masukan dari berbagai pihak baik secara langsung maupun secara tidak langsung. Untuk itu, pada kesempatan ini, penulis ingin menyampaikan rasa terimakasih terhadap semua pihak yang telah berperan serta dalam pengerjaan Tugas Akhir ini, yaitu :

1. Tuhan Yesus Kristus yang telah memberikan hikmat, jalan keluar, pertolongan-pertolongan pada waktu-NYA dan semangat serta kekuatan baru dalam mengerjakan Tugas Akhir ini hingga selesai.
2. Bapak Junius Karel, M.T. selaku dosen pembimbing I yang telah banyak memberikan ide, masukan, kritik dan saran dalam penulisan laporan dan pembuatan program tugas akhir ini.
3. Bapak Willy Sudiarto Raharjo, S.Kom., M.Cs selaku dosen pembimbing II yang telah banyak memberikan ide, masukan, kritik dan saran dalam penulisan laporan dan pembuatan tugas akhir ini.
4. Keluarga tercinta yang telah memberikan dukungan baik doa maupun moral serta semangat.
5. Semua pihak yang tidak dapat penulis sebutkan satu per satu, sehingga tugas akhir ini dapat terselesaikan dengan baik. Terimakasih atas doa dan dukungannya.

Penulis menyadari bahea laporan tugas akhir ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca sekalian, sehingga suatu saat penulis dapat memberikan karya yang lebih baik lagi.

Akhir kata penulis ingin meminta maaf bila ada kesalahan baik dalam penulisan laporan yang pernah penulis lakukan, dan semoga Tugas Akhir ini dapat membantu, serta memberikan inspirasi untuk menghasilkan karya yang lebih baik lagi.

KATA PENGANTAR

Puji syukur Penulis Panjatkan ke Hadirat Tuhan Yang Maha Esa karena atas Rahmat dan Karunia-Nya, sehingga penulis dapat menyelesaikan tugas akhir ini.

Dengan selesainya tugas akhir ini tidak lepas dari bantuan banyak pihak yang telah memberikan masukan-masukan kepada penulis.Untuk itu penulis mengucapkan banyak terimakasih.

Penulis menyadari bahwa laporan tugas akhir ini masih jauh dari kesempurnaan baik dari bentuk penyusunan maupun materinya. Oleh karena itu segala kritikan dan saran yang membangun akan penulis terima dengan baik. Akhir kata semoga laporan tugas akhir ini dapat memberikan manfaat kepada kita sekalian.

Yogyakarta, Juli 2017

Penulis

INTISARI

MONITORING JARINGAN MENGGUNAKAN SNORT

Monitoring jaringan komputer merupakan bagian yang sangat penting dalam menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus diawasi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. *Intrusion Detection System* (IDS) merupakan salah satu bentuk usaha dalam meningkatkan sistem keamanan. Kemampuan sistem ini dalam mendeteksi setiap pola paket data dan memberikan peringatan semakin meningkatkan sistem keamanan yang sudah ada dan juga memudahkan seorang administrator dalam mengawasi setiap proses pertukaran informasi salam sebuah jaringan komputer.

Penelitian akan mengulas tentang monitoring jaringan dengan menggunakan Snort yang berfungsi untuk mendeteksi intrusi-intrusi jaringan seperti penyusupan, penyerangan, dan pemindaian, sekaligus juga melakukan pencegahan. Ulasan yang dibahas didasarkan pada tinjauan pustaka dari berbagai karya ilmiah yang telah dipublikasikan serta simulasi sederhana penerapan Snort dalam sebuah jaringan.

Kata Kunci : Monitoring Jaringan, Intrusion Detection System (IDS), Snort.

DAFTAR ISI

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan teknologi informasi memiliki banyak keuntungan, namun sisi negatifnya juga banyak terjadi, seperti kejahatan komputer yang meliputi pencurian, penipuan, pemerasan, dan banyak lagi yang lainnya. Ketika suatu komputer terkoneksi ke internet, tidak saja dapat mengakses ke server suatu web tertentu, akan tetapi komputer tersebut juga sangat mungkin untuk diakses oleh komputer lain yang juga terkoneksi ke internet. Kondisi tersebut dapat menjadi suatu celah untuk terjadinya kejahatan di dunia maya (digital), sehingga sangat perlu untuk memberikan pemahaman tentang berbagai hal yang dapat setidaknya mencegah terjadinya ancaman kejahatan yang dapat masuk ke dalam suatu jaringan.

Terdapat banyak alternatif teknologi baik hardware atau software yang dapat digunakan untuk mendeteksi, memonitor, bahkan melakukan tindakan tertentu terhadap ancaman kejahatan, seperti penyusupan ataupun pencurian. Teknologi tersebut antara lain *Firewall*, *Anti Virus Software*, serta *tools* keamanan jaringan seperti *Firestrom*, *Prelude*, dan *Dragon*.

Dalam studi literatur ini, peneliti akan mengulas tentang monitoring jaringan dengan menggunakan snort. Snort merupakan aplikasi keamanan atau *security tool* yang berfungsi untuk mendeteksi intrusi-intrusi jaringan seperti penyusupan, penyerangan, dan pemindaian, sekaligus juga melakukan pencegahan. Ulasan yang dibahas didasarkan pada tinjauan pustaka dari berbagai karya ilmiah yang telah dipublikasikan.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dikemukakan di atas, pada studi literatur ini peneliti akan meninjau kembali bagaimana penerapan Snort dalam monitoring jaringan.

1.3 Batasan Masalah

Adapun batasan masalah dari penulisan ini adalah :

1. Hanya membahas sistem Snort sebagai Intrusion Detection System (IDS) untuk mendeteksi ancaman keamanan.
2. Simulasi sistem Snort IDS diterapkan dalam Sistem Operasi Windows.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penulisan studi literatur ini adalah :

1. Mengetahui penerapan Snort IDS dan ancaman keamanan yang dapat dideteksi.
2. Dapat digunakan sebagai acuan bagi perusahaan atau instansi yang menerapkan Snort sebagai sistem keamanan jaringan serta mahasiswa yang ingin membahas tentang Snort secara detail.

1.5 Metode Penelitian

Metode pendekatan dalam penulisan studi literatur ini adalah dengan melakukan studi pustaka untuk mencari informasi mengenai monitoring jaringan menggunakan Snort dan simulasi penerapan Snort pada sebuah jaringan.

1.6 Sistematika Penulisan

Laporan studi literatur tugas akhir ini disusun menjadi 5 bab, yaitu : Pendahuluan, Studi Literatur, Pembahasan, Simulasi dan Kesimpulan.

BAB I PENDAHULUAN yang berisi latar belakang masalah dilakukan penulisan, perumusan masalah, batasan masalah, tujuan penelitian, metode serta sistematika penulisan.

BAB II STUDI LITERATUR yang berisi tentang teori keamanan jaringan, *Intrusion Detection System* (IDS), dan Snort dari beberapa jurnal sebagai dasar penulisan tugas akhir yang terdiri dari tinjauan pustaka dan landasan teori.

BAB III PERANCANGAN SIMULASI SNORT yang berisi tentang penjelasan topologi, perangkat keras, dan perangkat yang digunakan dalam simulasi Snort.

BAB IV PENGUJIAN DAN ANALISIS SIMULASI SNORT yang berisi tentang penerapan simulasi serangan terhadap sistem Snort dan analisa hasil simulasi.

BAB V KESIMPULAN yang berisi rangkuman kesimpulan keseluruhan dari penelitian-penelitian ilmiah yang ada dan juga dari simulasi penerapan, beserta kelebihan dan kekurangan sistem Snort.

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan studi literatur dan analisa hasil simulasi keamanan jaringan Snort yang telah dilakukan dapat diambil kesimpulan :

1. Sistem Snort dapat berjalan baik dalam sistem operasi Windows dan dapat diterapkan dalam jaringan lokal maupun jaringan yang terkoneksi Internet.
2. Sistem Snort mampu mendeteksi semua jenis serangan yang disimulasikan. Hal ini menunjukkan bahwa Snort masih handal untuk digunakan sebagai sistem pendeteksi penyusupan IDS.

5.2. Saran

Untuk mendapatkan hasil yang lebih baik lagi, maka ada beberapa hal yang bisa dijadikan saran sebagai perkembangan kedepannya, antara lain :

1. Mengembangkan penggunaan Snort tidak hanya sebatas sebagai sistem pendeteksi penyusup (IDS) tetapi juga sebagai sistem pencegahan penyusupan (IPS).
2. Mengembangkan pengaturan rules Snort untuk meningkatkan kinerja sistem Snort.

DAFTAR PUSTAKA

Aickelin, U., Twycross, J., & Hesketh-Roberts, T. (2007). Rule Generalisation in Intrusion Detection Systems Using Snort. *International Journal Electronic Security and Digital Forensics, 1*, 101-116. doi:10.1504/IJESDF.2007.013596,

Alsafasfeh, M. H., & Alshbatat, A. I. (2011). Configuring Snort as a Firewall on Windows 7 Environment. *Journal of Ubiquitos Systems & Pervasive Networks, 3*(2), 73-77. Retrieved from http://www.iasks.org/sites/default/files/JUSPN2011030207377.pdf

Ariyus, D. (2007). *Computer Security.* Yogyakarta: Penerbit ANDI.

Ariyus, D. (2007). *Intrusion Detection System : Sistem Pendeteksi penyusupan Pada Jaringan Komputer.* Yogyakarta: Penerbit ANDI.

Boyce, C. A., & Zincir-Heywood, A. N. (2003). A Comparison of Four Intrusion Detection Systems for Secure E-Business. *Proceedings of the International Conference on Electronic Commerce Research*, 302-314. Retrieved from http://www.cs.dal.ca/~zincir/bildiri/ieeer03-cn.pdf

Dhak, B. S., & Lade, S. (2012). An Evolutionary Approach to Intrusion Detection System using Genetic Algorithm. International Journal of Emerging Technology and Advanced Engineering, 2(12). Retrieved from www.ijetae.com/files/Volume2Issue12/IJETAE_1212_111.pdf

Gupta, S., & Sharma, L. (2010). Performance Analysis of Internal vs. External Security Mechanism in Web Applications. *Int. J. of Advanced Networking and Applications, 01*(05), 314-317. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.419.7323

Kacha, C. C., Shevade, K. A., & Raghuwanshi, K. S. (2013). Improved Snort Intrusion Detection System Using Modified Pattern Matching Technique. *International Journal of Emerging Technology and Advanced Engineering*, *3*(7), 81-88. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.413.5935

Koziol, J. (2003). *Intrusion detection with Snort*. Indianapolis, Ind: Sams.

Kumar, S., & Kaur, R. (2013). IPv6 Network Security using Snort. *Journal Of Engineering, Computer & Applied Sciences, 2*, 17-22. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.402.4905

Kumar, V., & Sangwan, O. P. (2012). Signature Based Intrusion Detection System Using SNORT. *International Journal of Computer Applications & Information Technology*, *1*(3), 35-41. Retrieved from http://www.ijcait.com/IJCAIT/index.php/www-ijcs/article/download/171/81

Kurundkar, G.D., Naik, N. A., & Khamitkar, S.D. (2012). Network Intrusion Detection using SNORT. *International Journal of Engineering Research and Applications (IJERA), 2*(2), 1288-1296. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.417.1282

Lawal, O.B., Ibitola, A., & Longe, O. B. (2013). Analysis and Evaluation of Network-Based Intrusion Detection and Prevention System in an Enterprise Network Using Snort Freeware. *African Journal Of Computing & ICT, 6,* 169-184. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.411.4688

McClure, S., Shah, S., & Shah, S. (2003). *Web Hacking: Serangan dan Pertahanannya* (E.Philipus, Trans.). Yogyakarta: Penerbit ANDI.

Odom, W. (2008). *Computer Networking First-Step*. Yogyakarta: Penerbit ANDI.

Rafiudin, R. (2010). *Mengganyang Hacker dengan Snort*. Yogyakarta: Penerbit ANDI.

Rani, S., & Singh, V. (2012). SNORT: An Open Source Network Security Tool for Intrusion Detection in Campus Environment. *International Journal of Computer Technology and Electronics Engineering (IJCTEE), 2*(1). Retrieved from http://www.ijctee.org/files/VOLUME2ISSUE1/IJCTEE_0212_24.pdf

Rehman, R. U. (2003). *Intrusion detection systems with Snort: Advanced IDS techniques using Snort, Apache, MySQL, PHP and ACID*. Upper Saddle River: Prentice Hall.

Roesch, M. (1999). Snort: Lightweight Intrusion Detection for Networks. *Proceedings of LISA '99: 13th Systems Administration Conference*, 229-238. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.105.6212

Tiwari, R., & Jain, A. (2012). Design and Analysis of Distributed Honeypot System. *International Journal of Computer Applications, 55*(13). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.244.8772

Tuteja, A., & Shanker, R. (2012). Optimization of Snort for Extrusion and Intrusion Detection and Prevention. *International Journal of Engineering Research and Applications (IJERA), 2*(3), 1768-1774. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.416.6308