ANALISIS PERBANDINGAN *INTRUSTION DETECTION SYSTEM SNORT* DAN *SURICATA*

SKRIPSI

Disusun sebagai salah satu syarat menyelesaikan Program Studi Strata I pada Program Studi Informatika Fakultas Komunikasi dan Informatika Universitas Muhammadiyah Surakarta

Oleh :

Lutfi Nur Hakim

NIM : L200100094

PROGRAM STUDI INFORMATIKA

FAKULTAS KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS MUHAMMADIYAH SURAKARTA

2015

HALAMAN PERSETUJUAN

Skripsi dengan judul

ANALISIS PERBANDINGAN INTRUSTION DETECTION SYSTEM

SNORT DAN SURICATA

telah diperiksa dan disetujui untuk diajukan pada sidang pendadaran pada:

Hari : Jumat

Tanggal : 10 - 7 - 2015

Pembimbing I	Pembimbing II
Prof. Dr. Budi Murtiyasa, M.Kom.	Dr.Ir.Bana Handaga,M.T.
NIK :	NIK: 793

HALAMAN PENGESAHAN

ANALISIS PERBANDINGAN INTRUSTION DETECTION SYSTEM SNORT DAN SURICATA

Dipersiapkan dan disusun oleh

LUTFI NUR HAKIM

NIM : L200100094

Telah dipertahankan di depan dewan penguji

pada tanggal 14 Jul 2015

Susunan Dewan Penguji

Pembimbing I	Pembimbing II
Prof. Dr. Budi Murtiyasa, M.Kom.	Dr. Ir. Bana Handaga, M.T.
NIK :	NIK: 793

Dewan penguji I

Drs. Sudjalwo, M.Kom.
NIK

Skripsi ini telah diterima sebagai salah satu persyaratan untuk memperoleh gelar sarjana

Tanggal.....

Dekan	Ketua Program Studi
Fakultaas Komunikasi dan Informatika	Informatika
Husni thamrin, S.T, M.T, Ph.D	Dr.Heru Supriyono,M.Sc.
NIK : 706	NIK: 970

DAFTAR KONTRIBUSI

Dengan ini saya menyatakan bahwa skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Berikut saya sampaikan daftar kontribusi dalam penyusunan skripsi :

1. Penulis melakukan analisa dan perbandingan intrustion detection system ini dengan bantuan buku dan internet.
2. Software yang penulis gunakan dalam analisa dan perbandingan ini Orcle VirtualBox 4.2.0, Snort 2.9.6.2, Suricata 2.0.4, Barnyard2 2-1.13, Snorby.
3. Penulis menggunakan PC dengan spesifikasi Core i3-2100 CPU 3.10Ghz dan RAM 4GB dalam melakukan penelitian.
4. Sistem operasi yang digunakan penulis adalah Windows 7 ultimate 64 bit dan Linux Ubuntu 12.04 LTS.

Demikian pernyataan dan daftar kontribusi ini saya buat dengan sejujurnya. Saya bertanggung jawab atas isi dan kebenaran daftar di atas.

Surakarta, 03 Agustus 2015

Lutfi Nur Hakim

Mengetahui :

Pembimbing I	Pembimbing II
Prof. Dr. Budi Murtiyasa, M.Kom.	Dr.Ir.Bana Handaga,M.T.
NIK :	NIK:

MOTTO PERSEMBAHAN

"Barang siapa yang bersungguh–sungguh, sesungguhnya kesungguhannya itu adalah untuk dirinya sendiri"

(Q.S. Al-Ankabut: 6)

"Jadikan shalat dan sabarmu sebagai penolongmu, sesungguhnya Allah beserta orang-orang yang sabar"

(Al-Baqoroh : 153)

"Percaya bahwa kecerdasan bukan penentu kesuksesan, akan tetapi usaha dan kerja keras yang maksimal merupakan kunci kesuksesan yang sebenarnya"

(Penulis)

HALAMAN PERSEMBAHAN

Puji syukur Alhamdulillah peneliti ucapkan atas kehadirat Allah SWT yang telah melimpahkan segala Rahmat-NYA yang telah memberikan kesehatan, kelancaran, dan kemudahan dalam menyelesaikan skripsi ini. Dan skripsi ini penulis dedikasikan untuk:

1. Ibu dan alm.Bapak, yang senantiasa memberikan doa, dukungan, dorongan, perhatian yang tiada henti–hentinya selama pembuatan karya megah bagi penulis dan dapat membanggakannya.
2. Keluarga tercinta Kang Agung, Mbak Ninik, Kang Gupron, Mbak Nur, Kang Kabul yang selalu mendoakan menghibur, memberikan dorongan, mendukung, menasehati dan memotivasi agar selalu semangat hingga skripsi selesai dan lulus seperti yang di harapkan.
3. Keponakan akmal, tazkia, dan Alma yang sudah menemani dan selalu bikin rame dalam pengerjaan skripsi setiap saya dirumah.
4. Biro skripsi Bro Ajik yang membantu saya dan memberi semangat dan motivasi.
5. Teman TI seangkatan 2010 khususnya kelas D, Ali, Ahmad, Abdan, Andik, Andrean, Benny, Candra, Dodi, Fenny, Fahrudin Al Ansori (komo), Galih, Hasan, I’in, Lilis, Lutvi, David, Mukhrom, Novita, Pahrudin, Pramanda Hanung, TriBudiyanta (josua), Auliamadina (uli), Wahyu anggoro (Mul), Wahyu Andri.

6. Teman TI angkatan 2010 yang sudah pada lulus dan yang belum lulus.semoga kalian cepet menyusul.
7. Semua pihak yang telah membantu serta mendoakanku untuk kelancaran skripsi ini yang tak dapat disebutkan satu persatu.

Dari kesemuanya tersebut penulis ucapkan terima kasih atas doa dan dukungan, semoga Allah SWT membalas semua kebaikan semuanya, diberikan kesehatan dan mendapatkan perlindungan–NYA.

KATA PENGANTAR

Alhamdulillah, kami panjatkan syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan judul “Analisis Perbandingan Intrustion Detection System Snort Dan Suricata”.

Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan, oleh karena itu kritik saran yang membangun dari berbagai pihak sangat penulis harapkan demi perbaikan-perbaikan ke depan. Skripsi ini dapat terselesaikan berkat bantuan dari berbagai pihak, oleh karena itu pada kesempatan ini penulis menyampaikan terima kasih dan penghargaan kepada :

1. Bapak Husni Thamrin, S.T, MT., Ph.D. selaku Dekan Fakultas Komunikasi dan Informatika yang telah melayani dan memberikan fasilitas bagi kelancaran studi.
2. Bapak Dr. HeruSupriyono, M.Sc. selaku ketua jurusan Informatika.
3. Bapak Prof. Dr. Budi Murtiyasa, M.Kom. selaku pembimbing I yang telah memberikan bimbingan dan arahan sehingga dapat menyelesaikan skripsi ini.
4. Bapak Dr. Ir. BanaHandaga, MT selaku pembimbing II yang telah memberikan arahan judul skripsi serta memberikan saran demi kesempurnaan skripsi ini.
5. Segenap dosen penguji pada seminar proposal, pra pendadaran, dan pendadaran yang telah memberikan saran dan masukan dalam penyusunan skripsi ini.

6. Bapak dan ibu dosen pengampu mata kuliah pada Program Studi Informatika yang telah memberikan bekal ilmu yang sangat bermanfaat bagi penulis..
7. Semua pihak yang tidak bisa disebutkan satu-persatu yang telah membantu hingga terselesainya skripsi ini

Akhirnya penulis berharap semoga skripsi ini berguna bagi semua pihak dan bermanfaat bagi penulis khususnya dan pembaca pada umumnya dalam menambah pengetahuan dan wawasan ilmu. Amiin

Surakarta,

penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

ABSTRAKSI

Pertumbuhan internet dan jaringan komputer yang terjadi pada zaman sekarang ini memberikan keuntungan dan kemudahan kepada pengguna komputer untuk dapat berbagi sumber daya dan informasi. Dibalik kemudahan pengaksesan informasi yang disediakan oleh internet terdapat bahaya besar yang mengintai, yaitu berbagai macam serangan yang berusaha mencari celah dari sistem keamanan jaringan komputer yang digunakan. Serangan – serangan itu dapat mengakibatkan kerusakan data dan bahkan kerusakan pada *hardware.* Penerapan IDS diusulkan sebagai salah satu solusi yang dapat digunakan untuk membantu pengatur jaringan dalam memantau kondisi jaringan dan menganalisa paket-paket berbahaya yang terdapat dalam jaringan tersebut. Akan tetapi sebuah aplikasi IDS tersebut pastilah memiliki kelebihan dan kekurangannya, sehimgga penulis merasa tertarik untuk melakukan penelitian untuk menganalisa dan membandingkan kinerja dari kedua IDS tersebut.

Analisa dan perbandingan IDS Snort dan Suricata untuk mengukur tingkat akurasi, kecepatan deteksi dan penggunaan sumberdaya. Pengukuran dilakukan didalam mesin virtual, simulasi dengan serangan *port scanning, brute force* dan *dos.* Menggunakan Snorby sebagai *font-end* IDS.

Hasil penelitian Suricata lebih unggul dalam hal mendeteksi serangan akan tetapi, dalam kecepatan dan penggunaan sumber daya pada hasil pengukuran Snort selalu lebih unggul.

Kata kunci : IDS, Snort, Suricata