ANALISIS *COMPARISON SNORT* DAN *SURICATA* SEBAGAI *NETWORK INTRUSION DETECTION SYSTEM* (NIDS)

Skripsi

untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Teknik Informatika

disusun oleh:

Muhammad Naufal Bahreisy

10651038

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2015

ANALISIS *COMPARISON SNORT* DAN *SURICATA* SEBAGAI *NETWORK INTRUSION DETECTION SYSTEM* (NIDS)

Skripsi

untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Teknik Informatika

disusun oleh:

Muhammad Naufal Bahreisy

10651038

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2015

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-07/R0

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/1756/2015

Skripsi/Tugas Akhir dengan judul : Analisis *Comparison Snort* dan *Suricata* Sebagai *Network Intrusion Detection System* (NIDS)

Yang dipersiapkan dan disusun oleh :
Nama : Muhammad Naufal Bahreisy
NIM : 10651038
Telah dimunaqasyahkan pada : Selasa, 26 Mei 2015
Nilai Munaqasyah : A / B
Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

Dr. Imam Riadi, M.Kom
NIY. 60020397

Penguji I

Bambang Sugiantoro, M.T
NIP.19751024 200912 1 002

Penguji II

Nurochman, M.Kom
NIP. 19801223 200901 1 007

Yogyakarta, 22 Juni 2015
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

Dr. Maizer Said Nahdi, M.Si.
NIP. 19550427 198403 2 001

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Permohonan
Lamp : -

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Muhammad Naufal Bahreisy
NIM : 10651038
Judul Skripsi : Analisis *Comparison Snort* dan *Suricata* Sebagai *Network Intrusion Detection System (NIDS)*

sudah dapat diajukan kembali kepada Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Teknik Informatika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 18 Mei 2015
Pembimbing

Dr. Imam Riadi, M.Kom
NIY.60020397

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama	: Muhammad Naufal Bahreisy
NIM	: 10651038
Program Studi	: Teknik Informatika
Fakultas	: Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul **Analisis *Comparison Snort* dan *Suricata* Sebagai *Network Intrusion Detection System* (NIDS)** tidak terdapat pada karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi, dan sepengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 18 Mei 2015

Yang Menyatakan,

Muhammad Naufal Bahreisy

NIM : 10651038

iv

MOTTO

ترجو النجاة ولم تسلك مسالكها ان السفينة لاتجري علي اليبس

Engkau mengharapkan kesuksesan dan jalannya tidak kau tempuh

Sesungguhnya perahu tidak akan berlayar ditempat yang kering.

(Ibnu athaillah al-sakandari)

Anglaras ilining banyu, angeli nanging ora keli.

(Sunan Kalijogo)

Do the best and get the best. Just do it. (Me)

KATA PENGANTAR

Alhamdulillahi Robbil 'Alamin. Puji syukur kehadirat Allah SWT yang telah melimpahkan rahmat, hidayah, serta bimbingan-Nya. Shalawat dan salam semoga tercurah kepada Nabi Muhammad SAW. Akhirnya, penulis dapat menyelesaikan penelitian tugas akhir yang berjudul "Analisis *Comparison Snort* dan *Suricata* Sebagai *Network Intrusion Detection System* (NIDS)*"* sebagai salah satu syarat untuk mencapai selar kesarjanaan pada program studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta.

Penulis mengucapkan terima kasih kepada semua pihak yang telah ikut membantu memberikan sumbangan dan sarannya baik secara moril maupun materil, sehingga tugas akhir ini dapat terselesaikan dengan baik. Penyusun tidak lupa untuk menghaturkan banyak terimakasih kepada semua pihak atas segala bimbingan dan bantuan dalam penyusunan skripsi ini, semoga amal baik tersebut mendapatkan balasan dan limpahan karunia dari Allah SWT. Sebagai rasa hormat dan ucapan terimakasih penyusun sampaikan kepada :

1. Bapak Prof. Drs. H. Akh. Minhaji, M.A, Ph.D., selaku Rektor UIN Sunan Kalijaga Yogyakarta.
2. Dr. Maizer Said Nahdi, M.si. Selaku Dekan Fakultas Sains dan Teknonogi.
3. Bapak Sumarsono, S.T, M.Kom. Selaku Ketua Program Studi Teknik Informatika.
4. Bapak Nurochman, S.Kom, M.Kom, Selaku Sekretaris Program Studi Teknik Informatika UIN Sunan Kalijaga.

5. Bapak Dr. H. Imam Riadi, M.Kom, Selaku Dosen Pembimbing yang telah dengan sabar membimbing penulis dalam penyusunan skripsi, dan terima kasih pula karena telah memberikan arahan, saran, waktu serta masukan kepada penulis dalam menyusun skripsi.
6. Bapak Mustakim, M.T, selaku Dosen Pembimbing Akademik dan juga sudah memberikan saran terbaik mengenai penelitian saya.
7. Bapak dan Ibu Dosen Program Studi Informatika UIN Sunan Kalijaga yang telah memberikan banyak bekal ilmu kepada penulis.
8. Bapak dan Ibu di rumah yang senantiasa mendoakan saya.
9. Teman-teman TIF UIN SUKA umumnya dan khususnya INFUS-K 2010 yang telah mengisi hari-hari selama perkulihaan.
10. Teman-teman Teknik Informatika angkatan 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013 yang tidak dapat disebutkan satu persatu yang telah sedikit banyak memberikan bantuan, dukungan, serta motivasi kepada penulis.
11. Sahabat-sahabat seperbimbingan Bapak Imam Riadi Angkatan 2010, Fafa, Hanan, Arya, Feri, Faizal dan Fajar yang telah berjuang bersama-sama, sampai setiap hari menginap di Lab. Terpadu bersama-sama. Semoga kebersamaan ini senantiasa dieratkan.
12. Semua pihak yang tidak bisa disebutkan satu per satu, terima kasih atas segala bantuannya.

Akhir kata, semoga Allah SWT memberikan balasan pahala kebaikan atas segala bantuan yang telah diberikan kepada penysun, serta mendapatkan

kebahagiaan dunia dan akhirat kelak. Amin. Penyusun menyadari sepenuhnya masih bangyak kesalahan dan kekurangan dalam skripsi ini, maka sebagai saran dan kritik yang sifatnya membangun dari semua pihak demi kesempurnaan dimasa mendatang. Semoga skripsi ini dapat bermafaat bagi penyusun sendiri pada hususnya dan bagi para pembaca pada umumnya. Terima Kasih.

Yogyakarta, 16 Mei 2015

Penyusun

Muhammad Naufal Bahreisy

NIM.10651038

HALAMAN PERSEMBAHAN

Karya ini kupersembahkan untuk :

Allah SWT, yang selalu melimpahkan banyak karunia dan kenikmatan sehingga skripsi ini dapat terselesaikan dengan lancar

Nabi besar Muhammad SAW, semoga shalawat senantiasa terhatur kepadamu.

Ayah dan Ibu, terimakasih atas bimbingan moral dan spiritualnya selama ini. Semoga kalian berdua selalu dijunjung tinggi haknya di dunia maupun di akhirat.

Adik-adik ku, Naufi dan Nayiel yang senantiasa menyemangati untuk terus berkarya.

Mg Evi, Bi Shopy, Kg Ayat, Kg Iki, Nang Fahmi, Nok Ai, tante Gina dan Habibi terimakasih untuk semuanya yang selalu membatu baik susah maupun senang.

Keluarga KKY (Keluarga Karawang Yogyakarta) teman seperjuangan dalam perantauan.

Teman-teman Kos Pak-Gito Imam, Taha, Nur, Mbah adi, Sahir, Adam, kg Prio, Kg Mus, Kg iki dan Nang Fahmi yang selalu memberikan warna pada hari-hari.

Teman-teman seperjuangan, INFUS-K 2010 yang selalu memberikan motivasi, inspirasi, semangat, tangis, dan tawa.

Almamater tercinta Teknik Informatika UIN Sunan Kalijaga Yogyakarta. Inilah Goresan yang bisa aku torehkan sebagai kenang-kenangan hasil pembelajaranku.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LIST

ANALISIS *COMPARISON SNORT* DAN *SURICATA* SEBAGAI *NETWORK INTRUSION DETECTION SYSTEM* (NIDS)

Muhammad Naufal Bahreisy
10651038

INTISARI

Keamanan sebuah jaringan merupakan kebutuhan yang kadang dilupakan. Keamanan sebuah jaringan dalam mengamankan aliran data yang terhubung antara satu komputer dan komputer lainnya sangat diperlukan, sistem jaringan yang tidak mempunyai sistem keamanan berpotensi kehilangan data dan informasi yang dimiliki. Namun tidak sedikit yang mengabaikan keamanan pada suatu jaringan komputer. Salah satu solusi dari permasalahan dalam mengamankan sebuah jaringan komputer adalah memasang *Network Intrusion Detection System* (NIDS). NIDS merupakan sistem yang dapat mengawasi aliran data yang masuk pada jaringan komputer, contoh aplikasi *Network Intrusion Detection System* (NIDS) yaitu *Snort* dan *Suricata.*

Penelitian ini menekankan perbandingan dua aplikasi *open source* yang dijadikan *Network Intrusion Detection System* (NIDS) yaitu *Snort* dan *Suricata* sebagai aplikasi *open source* yang diujikan meliputi analisis kinerja jaringan dan sistem pada *server Snort* dan *Suricata* meliputi *delay* pada pengujian jaringan dan analisis tingkat akurasi dan kecepatan deteksi pada sistem terhadap serangan. Penelitian ini menggunakan metode komparatif yang bersifat eksperimental. Tahapan penelitian ini terbagi dalam beberapa langkah yakni perancangan sistem dan jaringan, implementasi rancangan, konfigurasi jaringan serta pengujian sistem menggunakan *stress test*.

Berdasarkan hasil penelitian, menunjukan *Snort* memiliki kinerja lebih efisien dari *Suricata,* berdasarkan hasil pengujian jaringan dan aktivitas serangan. Pada pengujian jaringan *(delay)* rata-rata keseluruhan 5.52 *ms* pada *Snort* dan *Suricata* menghasilkan nilai rata-rata dengan nilai *delay* 5.60 *ms*. Pada pengujian *port-scanning Snort* lebih unggul dengan nilai total rata-rata akurasi per waktu adalah 1 *alert/s* pada *Snort* dan 1.27 *alert/s* Pada *Suricata,* pada serangan *DDoS Snort* lebih unggul karena dapan mendeteksi serangan *DDoS,* dan pada serangan *brute-force Snort* lebih unggul dengan nilai total rata-rata akurasi per waktu 0.65 *alert/s* dan 21.69 *alert/s* pada *Suricata* dalam merespon serangan. Selanjutnya dapat disimpulakan *Snort* lebih efisien untuk dijadikan *Network Intrusion Detection System* (NIDS).

Kata kunci: *Comparison,* Keamanan, Jaringan, *Snort, Suricata*

ANALISIS *COMPARISON SNORT* DAN *SURICATA* SEBAGAI *NETWORK INTRUSION DETECTION SYSTEM* (NIDS)

Muhammad Naufal Bahreisy
10651038

ABSTRACT

The security of a network is a requirement that is sometimes forgotten. The security of a network in securing the data stream that is connected between the computer and other computers is indispensable, network systems that do not have a security system could potentially lose a data and a held information. One solution to the problems in securing a computer network is to install the *Network Intrusion Detection System* (NIDS). This study emphasizes the analysis of the accuracy and speed of detection on the *server Snort* and *Suricata* against activities attack on the server in the form of *Port-Scanning, DDoS* and *Brute-force*, and the network analysis in the form of delay values.

This study uses comparative method is experimental. Stages of this research is divided into several steps that the system design and network, at this stage, the design of the system is used as the system under test. The operating system used in this study using Ubuntu linux 12:04 which serve as *Snort* and *Suricata servers* and network topology used in this study using by LAN cable as a link between the attacker and the *servers*. Implementation of the draft, at this stage, the application or implementation of designs that have been created to be tested by comparing the *Snort* and *Suricata*. And testing the system using a stress test.

Based on the results of the study, showed *Snort* has a more efficient performance of *Suricata*, based on the results of testing the network and attack activity. On testing the network *(delay)* the overall average 5:52 *ms* on *Snort* and *Suricata* result an average value with a value of *delay* 5.60 *ms*. On testing *port-scanning Snort* is superior to the total value of the average accuracy in time is 1 *alert/s* on *Snort* and 1.27 *alerts/s* on *Suricata*, on *DDoS* attack *Snort* is superior because it can detect *DDoS* attack, and *brute-force* attack *Snort* is superior to the total value of the average accuracy in time 0.65 *alerts/s* and 21.69 *alerts/s* on *Suricata* in response to the attack. Based on test results concluded *Snort* is more efficient to be used as *Network Intrusion Detection System* (NIDS).

Keywords: Comparison, Network, Security, *Snort, Suricata*

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi komunikasi yang cenderung meningkat dan sangat pesat biasanya tidak didukung dengan sistem keamanan yang kurang memadai, sangatlah penting bagi suatu sistem jaringan komputer yang terhubung dengan jaringan luar atau *internet* hendaknya meningkatkan sistem keamanan pada jaringan tersebut. Karena *internet* merupakan sebuah jaringan komputer yang sangat terbuka di dunia, konsekuensi yang harus ditanggung adalah bagaimana jaminan sebuah keamanan bagi jaringan yang terhubung dengan *Internet*. Keamanan jaringan merupakan bagian dari sebuah sistem yang sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya.

Banyak masalah yang sering terjadi pada keamanan jaringan dikarenakan sering terjadi *Backdoor, Port-Scanning, Virus dan Malware, Hacker/Cracker, Denial of Servis (DoS/DDoS)*. Akibat dari kelemahan sistem keamanan jaringan.

Untuk mengatasi masalah keamanan jaringan dan sistem pada jaringan komputer perlu adanya penerapan pengawasan dalam sebuah jaringan komputer, *Snort* dan *Suricata* merupakan contoh aplikasi *Network Intrusion Detection System* (NIDS), dua aplikasi berbasis *open source* yang digunakan sebagai *Network Intrusion Detection System* (NIDS) yang dapat membantu memonitoring paket data yang masuk dalam jaringan sehingga memudahkan admin dalam menganalisis paket data yang masuk dalam jaringan komputer. Penelitian ini

membahas perbandingan kinerja 2 buah IDS *opensource* yang berbasis *network* yaitu *Snort* dan *Suricata* dengan indikator perbandingan akurasi dan kecepatan deteksi berdasarkan aktivitas normal dan pengujian serangan (*Port-Scaning*, *DDoS* dan *Brute-force*).

Deteksi *event* atau *alert* pada NIDS dengan waktu terlama yang terdeteksi sampai hasil dari deteksi *event* atau *alert* NIDS dengan waktu tercepat untuk mengetahui perbandingan kedua NIDS tersebut.

1.2 Rumusan Masalah

Dari latar belakang diatas dapat disimpulkan beberapa pokok permasalahan, diantaranya :

1. Bagaimana analisis faktor efisiensi aplikasi *Snort* sebagai *Network Intrusion Detection System* (NIDS) terhadap keamanan jaringan *networking*.
2. Bagaimana analisis faktor efisiensi aplikasi *Suricata* sebagai *Network Intrusion Detection System* (NIDS) terhadap keamanan jaringan *networking.*
3. Bagaimana membandingkan kinerja dari 2 buah aplikasi *Network Intrusion Detection System* (NIDS) yaitu *Snort* dan *Suricata* agar dapat diketahui aplikasi mana yang lebih efisien, berdasarkan akurasi dan kecepatan deteksi dalam memonitor aktivitas jaringan komputer.

1.3 Batasan Masalah

Batasan masalah penelitian yang dilakuakan adalah :

1. Objek penelitian yang dipilih adalah *Snort* dan *Suricata* sebagai *Network Intrusion Detection System* (NIDS).
2. Simulasi pengujian serangan yang digunakan *Port-Scanning, DDoS* dan *Brute-Force.*
3. Melakukan analisa kemampuan deteksi yang digunakan meliputi tingkat akurasi dan kecepatan deteksi dengan tidak menggunakan funsi *firewall.*

1.4 Tujuan Penelitian

Sesuai dengan masalah yang telah dirumuskan, maka tujuan dari penelitian ini unutuk :

1. Membandingkan kinerja dari 2 buah aplikasi *Network Intrusion Detection System* (NIDS) yaitu *Snort* dan *Suricata*.
2. Untuk mengetahui kinerja aplikasi *Snort* dan *Suricata* sebagai *Network Intrusion Detection System* (NIDS) terhadap serangan *Port-Scanning, DDoS* dan *Brute-Force* pada jaringan computer.
3. Menganalisis faktor efisiensi aplikasi *Snort* dan *Suricata* sebagai *Network Intrusion Detection System* (NIDS) terhadap keamanan jaringan berdasarkan akurasi dan kecepatan deteksi tanpa menggunakan fungsi *firewall*.

1.5 Manfaat Penelitian

1.5.1 Bagi Penulis

1. Dapat mengimplementasikan ilmu-ilmu yang diperoleh selama belajar di bangku kuliah.
2. Dapat membandingkan antara teori dan praktek dalam pembuatan karya ilmiah.
3. Mengembangkan pengetahuan yang telah dipelajari.

1.5.2 Bagi Intitusi Perguruan Tinggi

1. Sebagai sarana pembelajaran ilmu pengetahuan dan teknologi khususnya jurusan Teknik Informatika yang berkonsentrasi pada bidang *Networking* di Universitas Islam Negri Sunan Kalijaga Yogyakarta.
2. Sebagai bahan evaluasi dan masukan program studi Teknik Informatika di Universitas Islam Negri Sunan Kalijaga.

1.6 Keaslian Penelitian

Penelitian yang berhubungan dengan analisis perbandingan *Network Intrusion Detection System* (NIDS) yang membandingkan dua buah aplikasi NIDS yaitu *Snort* dan *Suricata* IDS blum banyak dilakukan. Untuk penelitian analisis perbandingan *Network Intrusion Detection System* (NIDS) sama sekali belum pernah ada maupun belum pernah dilakukan di Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian yang dilakukan, maka dapat diambil kesimpulan sebagai berikut :

1. *Intrusion Detection System* (IDS) yang dijadikan sebagai *Network Intrusion Detection System* (NIDS) yang terbaik dapat dilakukan analisis perbandingan antara dua *Intrusion Detection System* (IDS) untuk mengetahui kinerja yang terbaik antara *Snort* dan *Suricata*.
2. Pada pengujian jaringan menggunakan teknik *flooding server Snort* mempunyai nilai *delay* dengan rata-rata keseluruhan 5.52 *ms* sedangkan *server Suricata* menghasilkan nilai rata-rata keseluruhan lebih besar 0.8 dengan nilai *delay* 5.60 *ms*. Pada pengujian serangan menggunakan *port-scanning* terhadap *server Snort* dan *server Suricata* membuktikan *server Snort* lebih unggul dibandingkan dengan *server Suricata* dengan nilai total rata-rata akurasi per waktu adalah 1 *alert/s* pada *Snort* sedangkan 1.27 *alert/s* Pada *Suricata*. Dan pada pengujian serangan *Ddos Snort* lebih unggul karena dapat mendeteksi serangan *Ddos*. Pada serangan *brute-force server Snort* lebih unggul dengan nilai total rata-rata akurasi per waktu 0.65 *alert/s* sedangkan 21.69 *alert/s* terhadap *server Suricata*.
3. Berdasarkan hasil pengujian terhadap analisis perbandingan kinerja *Snort* dan *Suricata* sebagai *Network Intrusion Detection System* (NIDS) pada *local Area Network* (LAN) dengan parameter *delay, port-scanning, Ddos*

dan *Brute-force* dengan melakukan aktifitas serangan dari *client* ke *server* dengan jumlah parameter 5 yang diujikan menghasilkan *Snort* lebih efisien dijadikan *Network Intrusion Detection System* (NIDS).

5.2 Saran

Berdasarkan penelitian yang telah dilakukan, masih membutuhkan saran-saran untuk mendukung kesempatan dalam penelitian ini, saran tersebut diantaranya sebagai berikut :

1. Peneliti kedepan diharapakan mampu meneliti *Snort* dan *Suricata* dalam mencangkup jaringan yang lebih luas.
2. Peneliti diharapakan menganalisa *Snort* dan *Suricata* versi terbaru dan mengimplementasi secara meluas dengan media nirkabel yaitu *Wireless*, sehingga penggunaannya tidak terbatas dengan jarak serta mengembangkan sistem yang dapat memonitor secata *real time.*

DAFTAR PUSTAKA

Bradley, T. (2014). *Introduction to Intrusion Detection Systems (IDS)*. Retrieved from About Technology: http://netsecurity.about.com/cs/hackertools/a/aa030504_2.htm

Dony Ariyus, M. (2007). *Intrusion Detection System.* yogyakarta: ANDI OFFSET.

Gondohanindijo, J. (2011). Sistem Untuk Mendeteksi Adanya Penyusup (IDS : Intrusion Detection System). *Majalah Ilmiah Informatika Vol.2*, 49.

Ira Vaoliya Shafitri, R. Rumani M, Yudha Purwanto. (2012). Analisis Dan Implementasi Intrusion Detection System (IDS) untuk Pemberitahuan Serangan Pada Keamanan Sistem Jaringan Komputer Melalui Email. *IT Telkom Journal on ICT*, 105.

Kadir, Abdul, Terra Ch, Triwahyuni, (2003) Pengenalan Teknologi Inform asi (Sofiana, 2012), Yogyakarta: Penerbit Andi.

Mehra, P. (2012). A brief study and comparison of Snort and Bro Open Source Network Intrusion Detection Systems. *International Journal of Advanced Research in Computer and Communication Engineering*, 383.

Niswati, L. N. (2007). *BERBAGAI MACAM SERANGAN TERHADAP JARINGAN KOMPUTER*. Retrieved from Ilmukomputer.com: http://ilmukomputer.org/wp-content/uploads/2013/01/BERBAGAI-MACAM-SERANGAN-TERHADAP-JARINGAN-KOMPUTER.pdf

Northcutt, S. (2007). *Snort IDS and IPS Toolkit.* Burlington: Syngress Publishing.

Oetomo, Budi Sutedjo Dharma (2003) *Konsep dan Perancangan Jaringan Komputer***,** Yogyakarta: Penerbit Andi.

Oktavia, L. (2013, Oktober 15). *Laila Oktavia Dalimunthe*. Retrieved from DESAIN RISET DAN METODE PENELITIAN: http://laila-oktavia.blogspot.com/2013/10/desain-riset-dan-metode-penelitian.html

sundaram, A. (1996). An Introduction to Intrusion Detection. *USA:Whitepaper*, 4.

Susanto, I. (2010). penerapan easy intrusion detection system (EASYIDS) sebagai pemberi peringatan dini pada administrator sistem jaringan. *Skripsi*, 13.

Syafrizal, M. (2005). *Pengantar Jaringan Komputer.* Yogyakarta: Andi.

http://ilmukomputer.org/wp-content/uploads/2013/01/BERBAGAI-MACAM-SERANGAN-TERHADAP-JARINGAN-KOMPUTER.pdf diakses pada 25/08/2014 11:34

http://netsecurity.about.com/cs/hackertools/a/aa030504_2.htm diakses pada 15/08/2014 14:23

LAMPIRAN 1

Rules Snort Dan Rules Suricata

LAMPIRAN 2

Konfigurasi Barnyard dan Acidbase

Rules snort

attack-responses.rules
community-web-dos.rules
policy.rules
backdoor.rules
community-web-iis.rules pop2.rules
bad-traffic.rules
community-web-misc.rules
pop3.rules
chat.rules
community-web-php.rules porn.rules
community-bot.rules
ddos.rules
rpc.rules
community-deleted.rules
deleted.rules
rservices.rules
community-dos.rules
dns.rules
scan.rules
community-exploit.rules
dos.rules
shellcode.rules
community-ftp.rules
experimental.rules
smtp.rules
community-game.rules
exploit.rules
snmp.rules
community-icmp.rules
finger.rules
sql.rules
community-imap.rules
ftp.rules
telnet.rules
community-inappropriate.rules
icmp-info.rules
tftp.rules
community-mail-client.rules
icmp.rules
virus.rules
community-misc.rules
imap.rules
web-attacks.rules
community-nntp.rules
info.rules
web-cgi.rules
community-oracle.rules
local.rules
web-client.rules
community-policy.rules
misc.rules
web-coldfusion.rules
community-sip.rules
multimedia.rules
web-frontpage.rules
community-smtp.rules
mysql.rules
web-iis.rules
community-sql-injection.rules
netbios.rules
web-misc.rules
community-virus.rules
nntp.rules
web-php.rules
community-web-attacks.rules
oracle.rules
x11.rules
community-web-cgi.rules other-ids.rules
community-web-client.rules
p2p.rules

Rules Suricata

botcc.portgrouped.rules
emerging-rpc.rules
botcc.rules
emerging-scada.rules
BSD-License.txt
emerging-scan.rules
ciarmy.rules
emerging-shellcode.rules
classification.config
emerging-smtp.rules
compromised-ips.txt
emerging-snmp.rules
compromised.rules
emerging-sql.rules
decoder-events.rules
emerging-telnet.rules
drop.rules
emerging-tftp.rules
dshield.rules
emerging-trojan.rules
emerging-activex.rules
emerging-user_agents.rules
emerging-attack_response.rules
emerging-voip.rules
emerging-chat.rules
emerging-web_client.rules
emerging.conf
emerging-web_server.rules
emerging
current_events.rules
emerging-web_specific_apps.rules
emerging-deleted.rules
emerging-worm.rules
emerging-dns.rules
files.rules
emerging-dos.rules
gen-msg.map
emerging-exploit.rules
gpl-2.0.txt
emerging-ftp.rules
http-events.rules
emerging-games.rules
LICENSE
emerging-icmp_info.rules
rbn-malvertisers.rules
emerging-icmp.rules
rbn.rules
emerging-imap.rules
reference.config
emerging-inappropriate.rules
sid-msg.map
emerging-info.rules
smtp-events.rules
emerging-malware.rules
stream-events.rules
emerging-misc.rules
suricata-1.2-prior-open.yaml
emerging-mobile_malware.rules
suricata-open.txt
emerging-netbios.rules
tls-events.rules
emerging-p2p.rules
tor.rules
emerging-policy.rules
unicode.map
emerging-pop3.rules

Snort

Configurasi barnyard.conf sebagai penghubung *log* snort.conf ke *database mysql*

/etc/snort/barnyard.conf

output database: log, mysql, user=snort password=snort dbname=snort host=localhost

output database: alert, mysql, user=snort password=snort dbname=snort host=localhost

Configurasi database.conf pada acidbase sebagai GUI *Snort* yang akan ditampilkan di browser

/etc/acidbase/database.php

$alert_user='snort';

$alert_password='snort';

$basepath='/acidbase';

$alert_dbname='snort';

$alert_host='localhost';

$alert_port='';

$DBtype='mysql';;

Suricata

Configurasi barnyard.conf sebagai penghubung *log* suricatat.yaml ke *database mysql*

/etc/suricata/barnyard.conf

output database: log, mysql, user=suricata password=suricata dbname=suricata host=localhost

output database: alert, mysql, user=suricata password=suricata dbname=suricata host=localhost

Configurasi database.conf pada acidbase sebagai GUI *Suricata* yang akan ditampilkan di browser

/etc/acidbase/database.php

$alert_user='suricata';

$alert_password='suricata';

$basepath='/acidbase';

$alert_dbname='suricata';

$alert_host='localhost';

$alert_port='';

$DBtype='mysql';