

**RANCANG BANGUN *INTRUSION DETECTION SYSTEM*
MENGUNAKAN SURICATA
PADA UBUNTU 14.10**

SKRIPSI



disusun oleh

Rahmat Yani Hidayat

12.11.6570

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2015**

**RANCANG BANGUN *INTRUSION DETECTION SYSTEM*
MENGUNAKAN SURICATA
PADA UBUNTU 14.10**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Sistem Informasi



disusun oleh

Rahmat Yani Hidayat

12.11.6570

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2015**

PERSETUJUAN

SKRIPSI

**RANCANG BANGUN *INTRUSION DETECTION SYSTEM*
MENGUNAKAN SURICATA
PADA UBUNTU 14.10**


yang disusun oleh

Rahmat Yani Hidayat

12.11.6570

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 14 Mei 2015

Dosen Pembimbing,


Robert Marco, MT
NIK. 190302228

PENGESAHAN
SKRIPSI
RANCANG BANGUN *INTRUSION DETECTION SYSTEM*
MENGGUNAKAN SURICATA
PADA UBUNTU 14.10

yang disusun oleh
Rahmat Yani Hidayat
12.11.6570

telah dipertahankan di depan Dewan Penguji
pada tanggal 1 September 2015

Susunan Dewan Penguji

Nama Penguji

Krisnawati, S.Si, MT
NIK. 190302038

Robert Marco, MT
NIK. 190302228

Windha Mega Pradnya D, M.Kom
NIK. 190302185

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 1 September 2015

KETUA STMIK AMIKOM YOGYAKARTA



Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau 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 tanggungjawab saya pribadi.

Yogyakarta, 11 September 2015



Rahmat Yani Hidayat

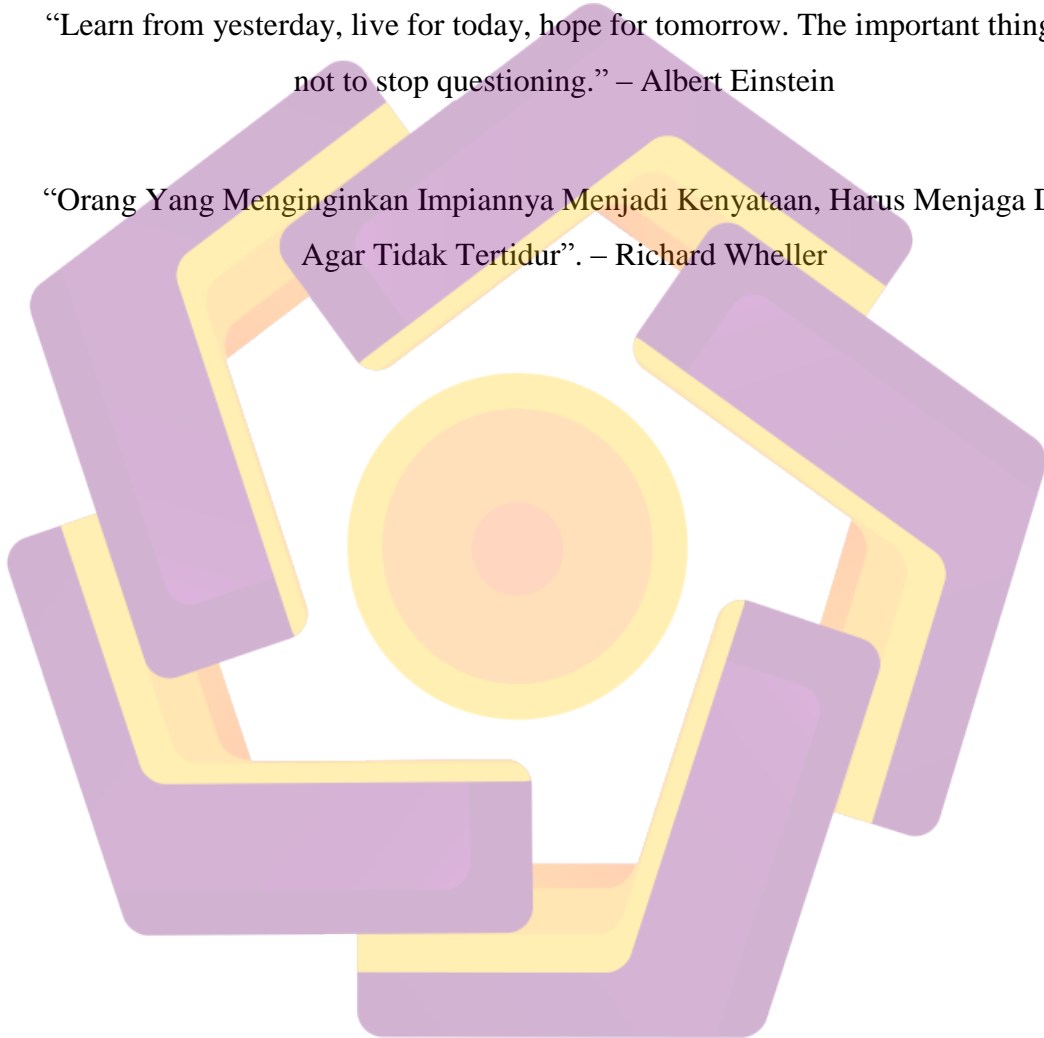
NIM. 12.11.6570

MOTTO

“Maka sesungguhnya bersama kesulitan itu ada kemudahan. Sesungguhnya bersama kesulitan itu ada kemudahan.” (Q.S. Al-Insyirah: 5-6)

“Learn from yesterday, live for today, hope for tomorrow. The important thing is not to stop questioning.” – Albert Einstein

“Orang Yang Menginginkan Impiannya Menjadi Kenyataan, Harus Menjaga Diri Agar Tidak Tertidur”. – Richard Wheller



PERSEMBAHAN

- Dengan Rahmat Allah Yang Maha Pengasih Lagi Maha Penyayang Saya Dapat Menyelesaikan Karya Skripsi Ini.
- Terima Kasih Kepada Kedua Orang Tuaku Ayah (Alm) Dan Ibu Yang Sudah Memberikan Segalanya Sehingga Saya Dapat Menjadi Seperti Sekarang.
- Terima Kasih Kepada Adikku M Rizki Syahri Ramadhan Dan Virgie Nurul Fadhillah Atas Semua Semangat Dan Dukungannya.
- Terima Kasih Untuk Semua Keluargaku Yang Sudah Memberikan Motivasi Dan Semangat Serta Dukungannya
- Untuk Anak-Anak Kontrakan (Bony, Hamdi, Tamma) Terima Kasih Bro-Bro Semua, Berkat Dukungan Semangat dan Motivasi Kalianlah Saya Dapat Menyelesaikan Skripsi Ini. Salam Satu Nasib Satu Perjuangan !
- Terima Kasih Buat Kamu Kurniawati yang Disana telah Memberikanku Semangat, Motivasi, dan Dukungannya. Tetap Kompak Ya !
- Untuk Semua teman – teman satu angkatan, khususnya kelas 12-TI-12 teman satu perjuangan satu penanggung, Terima Kasih untuk semua canda tawa yang sudah kalian berikan sehingga hari hari kuliah terasa sangat berarti dan untuk semua teman – teman ku yang sudah memberikan dukungan dan semangatnya yang mungkin namanya tidak dapat saya sebutkan satu persatu saya ucapkan Terima Kasih.
- Semoga Allah SWT membalas semua kebaikan kalian dikemudian hari dan diberikan segala kemudahan dalam segala hal, aamiin..

KATA PENGANTAR

Segala puji hanya milik Allah SWT serta Shalawat dan salam selalu tercurahkan untuk Rasulullah SAW. Berkat limpahan dan rahmat-Nya lah penulis mampu menyelesaikan penulisan tugas akhir yaitu Skripsi ini guna untuk memenuhi syarat kelulusan untuk jenjang Strata 1 di STMIK Amikom Yogyakarta

Dalam penyusunan Skripsi ini, tidak sedikit hambatan yang penulis hadapi. Namun penulis menyadari bahwa kelancaran dalam penyusunan Skripsi ini tidak lain karena bantuan bimbingan, dan dorongan dari Orang Tua, keluarga, serta orang-orang terdekat, sehingga kendala – kendala dapat teratasi.

Skripsi ini disajikan berdasarkan pengamatan dari berbagai macam sumber informasi dan referensi. Semoga dengan Skripsi ini dapat menambah wawasan yang lebih luas dan menjadi sumbangan pemikiran serta referensi bagi para pembacanya, khususnya bagi mahasiswa STMIK AMIKOM Yogyakarta. Penulis menyadari bahwa Skripsi ini masih banyak kekurangan dan jauh dari kata sempurna. Maka diharapkan kepada pembaca untuk memberikan kritik dan saran demi perbaikan untuk Skripsi ini dimasa yang akan datang.

Yogyakarta, Agustus 2015

Rahmat Yani Hidayat

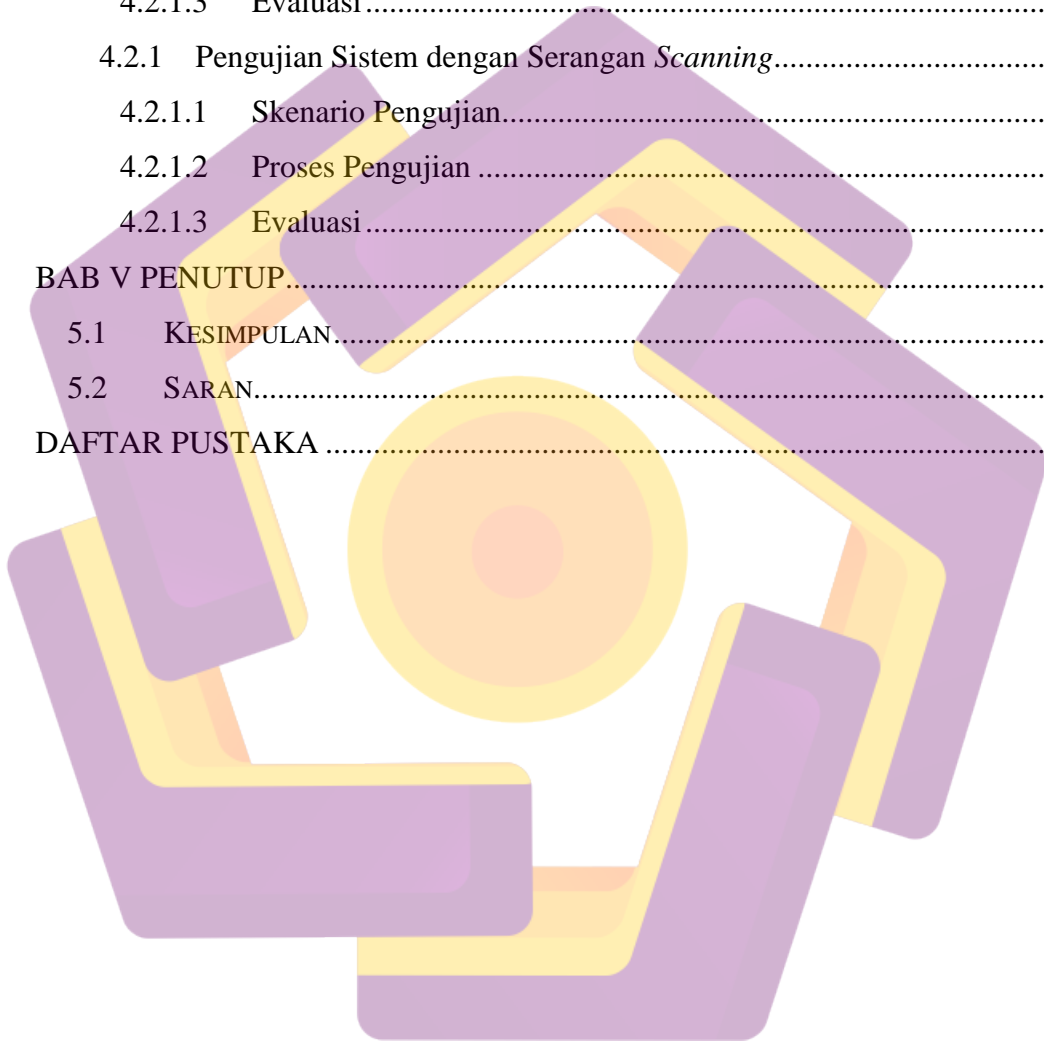
DAFTAR ISI

| | |
|--|----------|
| JUDUL..... | I |
| PERSETUJUAN | II |
| PENGESAHAN | III |
| PERNYATAAN..... | IV |
| MOTTO | V |
| PERSEMBAHAN..... | VI |
| KATA PENGANTAR | VII |
| DAFTAR ISI..... | VIII |
| DAFTAR TABEL..... | XII |
| DAFTAR GAMBAR | XIII |
| INTISARI..... | XV |
| ABSTRACT..... | XVI |
| BAB I PENDAHULUAN..... | 1 |
| 1.1 LATAR BELAKANG MASALAH..... | 1 |
| 1.2 RUMUSAN MASALAH | 3 |
| 1.3 BATASAN MASALAH..... | 3 |
| 1.4 TUJUAN PENELITIAN | 4 |
| 1.5 MANFAAT PENELITIAN..... | 5 |
| 1.6 METODE PENELITIAN | 5 |
| 1.7 SISTEMATIKA PENULISAN | 7 |
| BAB II LANDASAN TEORI..... | 9 |
| 2.1 TINJAUAN PUSTAKA..... | 9 |
| 2.2 PENGERTIAN JARINGAN KOMPUTER..... | 10 |
| 2.3 JENIS JARINGAN KOMPUTER | 11 |
| 2.3.1 Personal Area Network | 11 |
| 2.3.2 Local Area Network..... | 11 |
| 2.3.3 Metropolitan Area Network | 11 |
| 2.3.4 Wide Area Network | 12 |
| 2.4 DEFINISI KEAMANAN JARINGAN | 12 |

| | | |
|---|---|----|
| 2.5 | KONSEP DASAR KEAMANAN JARINGAN | 13 |
| 2.6 | PENGERTIAN PENYUSUP (<i>INTRUDER</i>) JARINGAN KOMPUTER | 14 |
| 2.7 | ANCAMAN JARINGAN KOMPUTER | 15 |
| 2.7.1 | <i>Intrusion</i> | 15 |
| 2.7.2 | <i>Denial of Service</i> | 15 |
| 2.7.3 | <i>Ping Scan</i> | 16 |
| 2.7.4 | <i>Sniffer</i> | 16 |
| 2.7.5 | <i>Port Scan</i> | 16 |
| 2.7.6 | <i>Malicious Code</i> | 16 |
| 2.8 | DEFENISI DAN KONSEP IDS | 17 |
| 2.9 | JENIS – JENIS IDS..... | 17 |
| 2.9.1 | Network Intrusion Detection System | 17 |
| 2.9.2 | Host Intrusion Detection System | 19 |
| 2.10 | METODE PENDEKATAN IDS | 20 |
| 2.10.1 | <i>Rule Based Detection</i> | 20 |
| 2.10.2 | <i>Adaptive Detection System</i> | 21 |
| 2.11 | CARA KERJA IDS | 22 |
| 2.12 | PERANGKAT LUNAK YANG DIGUNAKAN | 23 |
| 2.12.1 | Ubuntu Linux | 23 |
| 2.12.2 | Suricata..... | 23 |
| 2.12.3 | Logstash | 24 |
| 2.12.4 | Elasticsearch..... | 24 |
| 2.12.5 | Kibana | 25 |
| 2.12.6 | Java..... | 25 |
| 2.12.7 | Nginx..... | 25 |
| 2.12.8 | NMap | 26 |
| 2.12.9 | <i>Low Orbit Ion Cannon</i> | 26 |
| BAB III ANALISIS DAN PERANCANGAN SISTEM | | 28 |
| 3.1 | ANALISIS MASALAH | 28 |
| 3.2 | ANALISIS KELEMAHAN SISTEM..... | 30 |
| 3.2.1 | Kelemahan Sistem Keamanan Jaringan yang Digunakan..... | 30 |

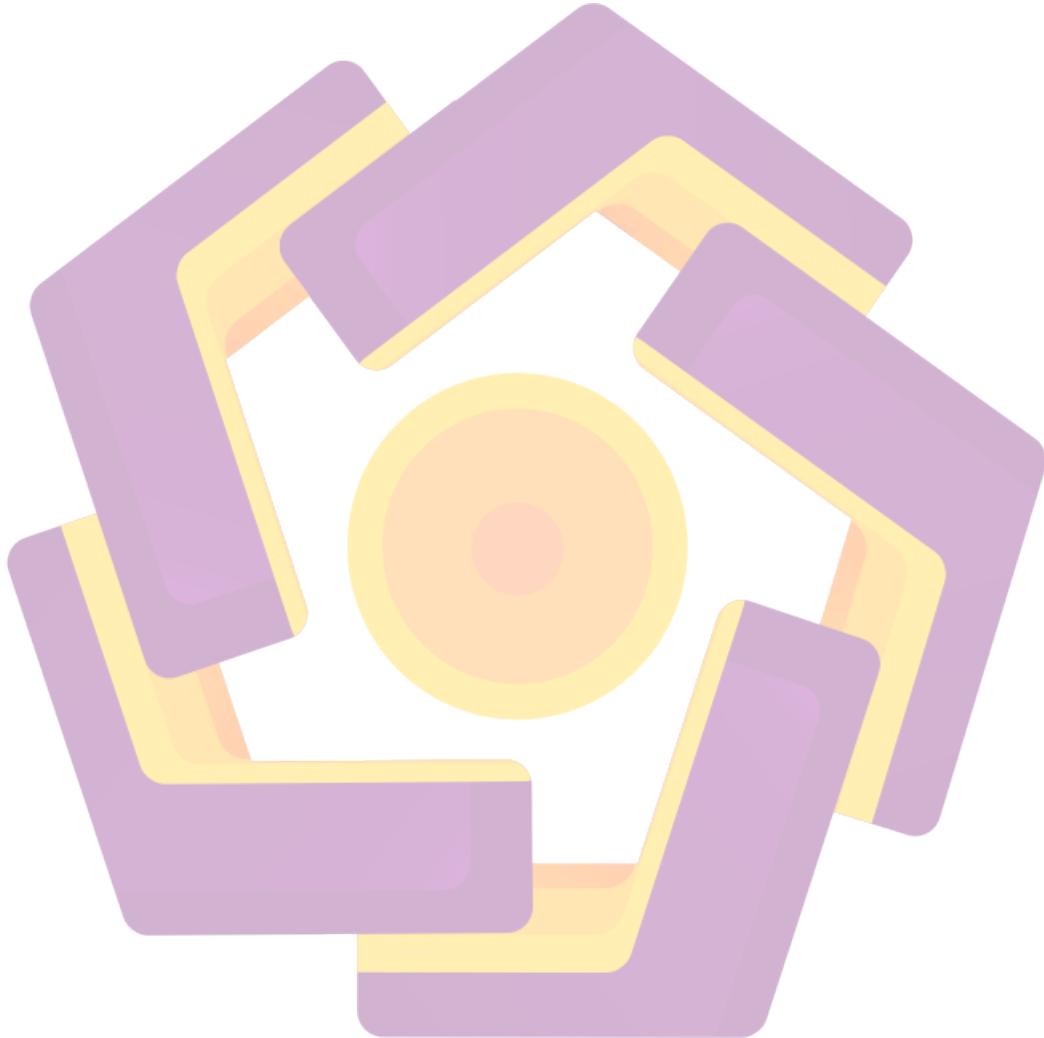
| | | |
|---|--|-----------|
| 3.2.2 | Tindak Penanganan Masalah | 32 |
| 3.2.3 | Rancang Bangun IDS dan Monitoring..... | 32 |
| 3.3 | ANALISIS KELEMAHAN SISTEM..... | 33 |
| 3.3.1 | Identifikasi Sistem..... | 33 |
| 3.3.2 | Pemahaman Kerja Sistem | 34 |
| 3.4 | ANALISIS KEBUTUHAN SISTEM | 35 |
| 3.4.1 | Kebutuhan Sistem Fungsional | 35 |
| 3.4.2 | Kebutuhan Sistem Non-Fungsional | 36 |
| 3.4.2.1 | Kebutuhan Perangkat Keras (<i>Hardware</i>)..... | 36 |
| 3.4.2.2 | Kebutuhan Perangkat Lunak (<i>Software</i>)..... | 37 |
| 3.5 | ANALISIS PERANCANGAN SISTEM..... | 38 |
| 3.5.1 | Perancangan Topologi untuk IDS | 38 |
| 3.5.2 | Perancangan Hubungan Modul Sistem | 39 |
| 3.5.2.1 | Penjelasan Komponen Modul | 39 |
| 3.5.3 | Flowchart IDS | 41 |
| 3.5.3.1 | Kebutuhan Perangkat Lunak (<i>Software</i>)..... | 42 |
| 3.6 | RANCANGAN ANTAR MUKA (<i>INTERFACE</i>)..... | 43 |
| BAB IV IMPLEMENTASI DAN PEMBAHASAN | | 44 |
| 4.1 | IMPLEMENTASI SISTEM | 44 |
| 4.1.1 | Persiapan Sistem | 44 |
| 4.1.1.1 | Menambahkan Repository | 44 |
| 4.1.1.2 | Instalasi Suricata | 45 |
| 4.1.1.3 | Instalasi Oracle Java..... | 46 |
| 4.1.1.4 | Instalasi Logstash | 48 |
| 4.1.1.5 | Instalasi Elasticsearch | 48 |
| 4.1.1.6 | Instalasi Nginx | 51 |
| 4.1.1.7 | Instalasi Kibana..... | 51 |
| 4.1.2 | Konfigurasi Suricata..... | 54 |
| 4.1.3 | Konfigurasi Rule Suricata..... | 58 |
| 4.1.4 | Konfigurasi Logstash | 61 |
| 4.1.5 | Mengkonfigurasi Nginx sebagai Reverse Proxy..... | 64 |

| | | |
|----------------------|---|----|
| 4.1.6 | Menggunakan Kibana | 66 |
| 4.2 | PENGUJIAN SISTEM | 68 |
| 4.2.1 | Pengujian Sistem dengan Serangan <i>Denial of Service</i> | 68 |
| 4.2.1.1 | Skenario Pengujian..... | 68 |
| 4.2.1.2 | Proses Pengujian | 69 |
| 4.2.1.3 | Evaluasi | 71 |
| 4.2.1 | Pengujian Sistem dengan Serangan <i>Scanning</i> | 73 |
| 4.2.1.1 | Skenario Pengujian..... | 73 |
| 4.2.1.2 | Proses Pengujian | 74 |
| 4.2.1.3 | Evaluasi | 76 |
| BAB V PENUTUP..... | | 78 |
| 5.1 | KESIMPULAN..... | 78 |
| 5.2 | SARAN..... | 79 |
| DAFTAR PUSTAKA | | 80 |



DAFTAR TABEL

| | | |
|------------------|---|-----------|
| Tabel 3.1 | Spesifikasi Server IDS | 36 |
| Tabel 3.2 | Spesifikasi Komputer Penyerang (Attacker)..... | 37 |



DAFTAR GAMBAR

| | | |
|-------------|---|----|
| Gambar 2.1 | Network Intrusion Detection System | 18 |
| Gambar 2.2 | Host Intrusion Detection System | 19 |
| Gambar 2.3 | Alur Kerja IDS | 22 |
| Gambar 3.1 | Grafik Serangan pada Januari 2015 | 28 |
| Gambar 3.2 | Grafik Target Serangan Januari 2015 | 29 |
| Gambar 3.3 | Uji Coba dengan LOIC..... | 31 |
| Gambar 3.4 | Uji Coba dengan NMap..... | 31 |
| Gambar 3.5 | Grafik Kerja Sistem..... | 35 |
| Gambar 3.6 | Rancangan Topologi yang Digunakan | 38 |
| Gambar 3.7 | Hubungan Modul Sistem..... | 39 |
| Gambar 3.8 | Flowchart IDS | 41 |
| Gambar 3.9 | Rancangan Antar Muka..... | 43 |
| Gambar 4.1 | Update Repository..... | 45 |
| Gambar 4.2 | Instansi Suricata..... | 45 |
| Gambar 4.3 | Uninstall OpenJDK..... | 46 |
| Gambar 4.4 | Instalasi Oracle Java..... | 47 |
| Gambar 4.5 | License Agreement Oracle Java | 47 |
| Gambar 4.6 | Instalasi Logstash..... | 48 |
| Gambar 4.7 | Instalasi Elasticsearch..... | 49 |
| Gambar 4.8 | Instalasi Plugin Elasticsearch | 50 |
| Gambar 4.9 | Elasticsearch HQ Plugin..... | 50 |
| Gambar 4.10 | Instalasi Nginx..... | 51 |
| Gambar 4.11 | Instalasi Kibana..... | 52 |
| Gambar 4.12 | Konfigurasi Kibana..... | 52 |
| Gambar 4.13 | Membuat Direktory Kibana..... | 53 |
| Gambar 4.14 | Menjalankan Kibana sebagai Service | 54 |
| Gambar 4.15 | Konfigurasi Output JSON Suricata | 56 |
| Gambar 4.16 | Salah satu isi file Rule Suricata | 61 |

| | |
|--|----|
| Gambar 4.17 Struktur Dasar Logstash | 62 |
| Gambar 4.18 Menggunakan htpasswd | 65 |
| Gambar 4.19 Konfigurasi Nginx sebagai Reverse Proxy | 66 |
| Gambar 4.20 Sistem Autentikasi Kibana | 67 |
| Gambar 4.21 Web Interface Kibana | 67 |
| Gambar 4.22 Alamat IP komputer penyerang | 69 |
| Gambar 4.23 Alamat IP komputer target | 70 |
| Gambar 4.24 Memasukkan Data Target | 70 |
| Gambar 4.25 Memulai Proses Penyerangan | 71 |
| Gambar 4.26 Pengujian Latency sebelum penyerangan | 72 |
| Gambar 4.27 Pengujian Latency setelah penyerangan | 72 |
| Gambar 4.28 Screenshot hasil Log Suricata pada Terminal | 72 |
| Gambar 4.29 Screenshot hasil Log Suricata pada Kibana | 73 |
| Gambar 4.30 Memindahkan Direktori Aktif | 75 |
| Gambar 4.31 Melakukan Scanning | 75 |
| Gambar 4.32 Screenshot hasil Log Suricata pada Terminal | 76 |
| Gambar 4.33 Screenshot hasil Log Suricata pada Kibana | 76 |

INTISARI

Seiring berkembangannya teknologi informasi terutama pada jaringan komputer membuat semua orang dapat mengakses informasi darimana saja melalui internet. Dengan semakin banyaknya perangkat yang terhubung ke internet maka akan berpengaruh pada penurunan performa pada jaringan dan tidak menutup kemungkinan jika akan ada paket berbahaya yang masuk ke dalam jaringan tanpa sepengetahuan user. Hal ini dapat mengancam keamanan informasi yang tersimpan didalamnya.

Dengan menganalisis permasalahan yang ada, maka penulis memberikan solusi untuk mengurangi dampak hal yang dapat mengurangi keamanan informasi yaitu dengan mengimplementasikan Sistem *Intrusion Detection System* menggunakan Suricata yang akan diimplementasikan pada Sistem Operasi Ubuntu 14.10 dengan menggunakan metode Analisis, metode Perancangan dan Evaluasi Sistem

Setelah Mengimplementasikan IDS Suricata pada Sistem Operasi Ubuntu 14.10, dihasilkan sebuah sistem yang dapat membantu dalam mengawasi lalu lintas jaringan. Sistem ini dapat memeriksa setiap paket yang lewat serta mendeteksi setiap ancaman yang masuk kedalam jaringan lalu melaporkan setiap Log ke dalam bentuk yang mudah dipahami.

Kata Kunci: *Intrusion Detection System*, Keamanan Jaringan, Suricata

ABSTRACT

As the information technology develop especially in computer networks make everyone can access the information from anywhere via the internet. With the growing number of devices that are connected to the internet then it will affect performance on the decline on the network and does not cover the possibility if there will be a dangerous package that goes into the network without the knowledge of the user. This can threaten the security of information.

By analyzing the existing problems, then the author provides solutions to mitigate the impact of the things that can reduce the security of information that is to Implements an Intrusion Detection System using Suricata which will be implemented on the Ubuntu operating system using the 14 methods of analysis, methods of design and Evaluation System

After implementing the IDS Suricata on Ubuntu 14.10 Operating System, produced a system that can help in keeping an eye on network traffic. The system can check any package that passes as well as detect any threats to the network and then report any Logs into a form that is easily understood.

Keywords: *Intrusion Detection System, Network Security, Suricata*