ANALISIS PERFORMA *NETWORK INTRUSION DETECTION SYSTEM* (NIDS) MENGGUNAKAN METODE *SIGNATURE BASED* DALAM MENDETEKSI SERANGAN *DENIAL OF SERVICE* (DOS) BERBASIS *UDP FLOODING*

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer

MUHAMMAD RIEN SURYATAMA IDRUS

1112001026

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK DAN ILMU KOMPUTER

UNIVERSITAS BAKRIE

JAKARTA

2015

HALAMAN PERNYATAAN ORISINALITAS

Tugas Akhir ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : **Muhammad Rien Suryatama Idrus**

NIM : **1112001026**

Tanda Tangan :

Tanggal : **24 Agustus 2015**

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama	: Muhammad Rien Suryatama Idrus
NIM	: 1112001026
Program Studi	: Informatika
Fakultas	: Teknik dan Ilmu Komputer
Judul Skripsi	: Analisis Performa *Network Intrusion Detection System* (NIDS) Menggunakan Metode *Signature Based* Dalam Mendeteksi Serangan *Denial of Service* (DoS) Berbasis *UDP Flooding*.

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Bakrie.

DEWAN PENGUJI

Pembimbing 1	**: Berkah I. Santoso, S.T., M.TI.**	**(.....)**
Pembimbing 2	**: I Gusti Nyoman Mantra, S.Kom., M.Kom.**	**(.....)**
Penguji 1	**: Irwan P. Gunawan, S.T., M.Eng., Ph.D.**	**(.....)**
Penguji 2	**: Yusuf Lestanto, S.T., M.Sc.**	**(.....)**

Ditetapkan di : Jakarta

Tanggal : 24 Agustus 2015

UNGKAPAN TERIMA KASIH

Puji dan syukur penulis panjatkan kehadirat Allah SWT karena atas rahmat-Nya dan karunia-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan baik. Tugas Akhir dengan judul "Analisis Performa *Network Intrusion Detection System* (NIDS) dalam Mendeteksi Serangan DoS *UDP Flooding*" ini ditulis untuk memenuhi salah satu syarat dalam menyelesaikan perkuliahan pendidikan strata satu (S1) pada Program Studi Informatika, Universitas Bakrie.

Banyak pihak yang telah membantu penulis dalam penelitian dan penulisan Tugas Akhir ini, baik itu berupa bimbingan, ilmu, saran maupun dukungan secara moril dan materil. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan rasa terima kasih dan penghargaan yang setinggi-tingginya kepada:

1. Bapak Berkah I. Santoso dan Bapak I Gusti Nyoman Mantra, selaku Dosen Pembimbing, yang telah meluangkan waktu, tenaga serta memberikan bimbingan, ilmu, motivasi, saran dan perbaikan dalam menyelesaikan penelitian ini;
2. Bapak Irwan Prasetya Gunawan dan Bapak Yusuf Lestanto selaku dosen penguji, selaku dosen penguji yang telah membantu penulis untuk menyempurnakan tugas akhir ini;
3. Seluruh Bapak/Ibu dosen Program Studi Informatika Universitas Bakrie, yang telah memberikan banyak ilmu, pengetahuan dan wawasan kepada penulis selama perkuliahan;
4. Seluruh pihak Universitas Bakrie dan Yayasan Pendidikan Bakrie, yang telah memberikan penulis beasiswa penuh selama 4 tahun untuk dapat melanjutkan pendidikan strata satu di Universitas Bakrie;
5. Keluarga tercinta, yang selalu memberikan penulis dukungan dan doa yang sangat berarti. Kedua Orang Tua penulis (H. Idrus Efendi, S.E, M.Si dan Hj. Nurmin S.KM), adik penulis (Loly Subhiaty Idrus, Rizaldy Fataaya Idrus,

dan Abdullah Ma'rif Ibnu Idrus) serta seluruh keluarga besar di Kendari, Sulawesi Tenggara;

6. *Family*; Rahmad Pratama Dita, Rizky Faisal Akbarie, Chandra Setiawan Gimon, Faiz Faidurrahman, Sawitri Sadanti, Sarah Putri Mardhatillah, Stefanny Uliarta dan Evi Margaretha. Terima kasih telah menjadi sahabat terbaik dan kebersamaan selama ini;
7. Andre Arsyan, Rismunandar Winata, Alif Hariry, Fauzan Al-Agung, Mei Silvana Saputri dan Ana Ainul Syamsi yang turut memberikan bantuan dan masukan terhadap penyelesaian Tugas Akhir penulis;
8. Teman-teman TIF 2011 senasib dan seperjuangan, yang menemani dan bekerja sama selama 4 tahun masa perkuliahan di Universitas Bakrie;
9. Mas Rian Adi Wibowo yang membantu dan memberikan ilmu mengenai teori yang digunakan pada tugas akhir ini;
10. Teman-teman Paduan Suara Mahasiswa Universitas Bakrie, yang selalu memberikan keceriaan dan kedamaian dengan lantunan nada-nada yang indah.

Dengan segala keterbatasan yang ada, penulis menyadari bahwa penyusunan Tugas Akhir ini masih terdapat kekurangan dan kesalahan. Untuk itu, saran dan kritik akan selalu di terima penulis agar dapat memperbaiki setiap kekurangan untuk kesempurnaan dimasa mendatang.

Akhirnya, penulis menyampaikan ucapan terima kasih dan semoga Allah SWT membalas segala kebaikan serta melimpahkan berkat dan rahmat-Nya kepada semua pihak yang telah membantu selama ini. Penulis berharap semoga Tugas Akhir ini berguna dan bermanfaat bagi kita semua.

Jakarta, 24 Agustus 2015

Muhammad Rien Suryatama Idrus

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI

Sebagai sivitas akademik Universitas Bakrie, saya yang bertanda tangan di bawah ini,

Nama : Muhammad Rien Suryatama Idrus

NIM : 1112001026

Program Studi : Informatika

Fakultas : Teknik dan Ilmu Komputer

Jenis Tugas Akhir : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bakrie **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul:

Analisis Performa *Network Intrusion Detection System* (NIDS) Menggunakan Metode *Signature Based* Dalam Mendeteksi Serangan *Denial of Service* (DoS) Berbasis *UDP Flooding*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Bakrie berhak menyimpan, mengalih mediakan/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta untuk kepentingan akademis.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 24 Agustus 2014

Yang menyatakan,

(Muhammad Rien Suryatama Idrus)

Analisis Performa *Network Intrusion Detection System* (NIDS) Menggunakan Metode *Signature Based* Dalam Mendeteksi Serangan *Denial of Service* (DoS) Berbasis *UDP Flooding*

Muhammad Rien Suryatama Idrus

ABSTRAK

Cloud computing telah menjadi tren teknologi yang digunakan oleh berbagai kalangan terutama para pelaku *startup* dan perusahaan besar. Beberapa kelebihan yang ditawarkan *cloud computing* seperti kemudahan untuk membuat layanan *cloud* sendiri, hemat biaya infrastruktur dan fleksibel dalam menambah atau mengurangi kapasitas layanan sesuai dengan kebutuhan. Terlepas dari kelebihan-kelebihan tersebut, aspek keamanan *cloud computing* menjadi salah satu faktor yang harus diperhatikan oleh perusahaan. Penggunaan antivirus dan *firewall* belum menjamin sistem *cloud* sepenuhnya aman. Selain itu keterbatasan administrator dalam memonitor *traffic* dan serangan di seluruh bagian jaringan *cloud* menjadi kendala dalam pengelolaan *cloud computing*. Salah satu solusi untuk meningkatkan keamanan jaringan, memonitor serta mengawasi *traffic* serangan pada *cloud computing* adalah *Network-based Intrusion Detection System* (NIDS). NIDS merupakan salah satu jenis *Intrusion Detection System* (IDS) yang dapat melakukan pemantauan terhadap serangan serta *traffic* pada seluruh bagian jaringan. *Signature based* adalah salah satu metode yang dapat digunakan NIDS dalam mengidentifikasi setiap paket data yang keluar dan masuk ke jaringan. Pada penelitian ini, penulis melakukan uji performa NIDS dengan metode *Signature Based* dalam mendeteksi serangan DoS berbasis *UDP Flooding*. Penelitian ini juga melakukan analisis terhadap hasil dan evaluasi performa NIDS untuk mengetahui kinerja diterapkannya NIDS dan keakuratan NIDS dalam mengklasifikasikan serangan.

Kata Kunci : IDS, *Network Intrusion Detection System*, NIDS, *Cloud* Computing, Signature Based

Analysis Performances of Network Intrusion Detection System (NIDS) Using Signature Based Method in Detecting Denial of Service (DoS) Based on *UDP Flooding* Attack

Muhammad Rien Suryatama Idrus

Abstract

Nowadays, *cloud* computing has become a new trend technology used in various areas, especially in startup and big companies. *Cloud* computing offers some advantages such as the easiness to create their own *cloud* services, cost-effective infrastructure and flexible to increase or decrease the capacity of the service in accordance with the requirements. Apart from these advantages, the security aspects of *cloud* computing is becoming one of the factors that must be considered by the company. The use of antivirus and firewall doesn't guarantee the *cloud* system is fully secure. Besides that, the limitation of administrator to monitor traffic and attacks throughout the *cloud* network become a constraint in *cloud* computing management. One solution to improve network security, traffic monitoring and overseeing attacks on *cloud* computing using Network-based Intrusion Detection System (NIDS). NIDS is one type of Intrusion Detection System (IDS) which can monitor the attacks and traffic throughout the network. Signature Based is one method that can be used NIDS to identify each packet of data in or out to the network. In this research, the author conducted performances test NIDS with Signature Based method based on *UDP Flooding*. This research also perform conducted analysis of the result and performance evaluation of NIDS on *cloud* computing. The aim to determine the performance of NIDS and the accuracy of NIDS in classifying attacks.

Kata Kunci : IDS, *Network Intrusion Detection System*, NIDS, *Cloud* Computing, Signature Based

DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS...**Error! Bookmark not defined.**

HALAMAN PENGESAHAN.....**Error! Bookmark not defined.**

UNGKAPAN TERIMA KASIH.....**Error! Bookmark not defined.**

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI..**Error! Bookmark not defined.**

ABSTRAK .....**Error! Bookmark not defined.**

DAFTAR ISI..... ix

DAFTAR GAMBAR .....**Error! Bookmark not defined.**

DAFTAR TABEL.....**Error! Bookmark not defined.**

DAFTAR SINGKATAN .....**Error! Bookmark not defined.**

BAB I .....**Error! Bookmark not defined.**

PENDAHULUAN .....**Error! Bookmark not defined.**

1.1. Latar Belakang Penelitian .....**Error! Bookmark not defined.**

1.2. Rumusan Masalah .....**Error! Bookmark not defined.**

1.3. Tujuan dan Manfaat Penelitian .....**Error! Bookmark not defined.**

1.3.1. Tujuan Penelitian.....**Error! Bookmark not defined.**

1.3.2. Manfaat Penelitian.....**Error! Bookmark not defined.**

1.4. Batasan Masalah .....**Error! Bookmark not defined.**

BAB II.....**Error! Bookmark not defined.**

TINJAUAN PUSTAKA .....**Error! Bookmark not defined.**

2.1. Penelitian Terdahulu .....**Error! Bookmark not defined.**

2.2. *Cloud Computing* .....**Error! Bookmark not defined.**

2.2.1. Layanan *Cloud Computing*.....**Error! Bookmark not defined.**

2.2.2. *Deployment Model Cloud Computing*..... **Error! Bookmark not defined.**

2.3. OpenStack .....**Error! Bookmark not defined.**

2.4. IDS .....**Error! Bookmark not defined.**

2.4.1. Jenis IDS.....**Error! Bookmark not defined.**

2.4.2. Metode IDS .....**Error! Bookmark not defined.**

2.4.3. Perangkat Lunak yang Digunakan**Error! Bookmark not defined.**

2.5. *Denial of Service* (DoS) .....**Error! Bookmark not defined.**

2.6. Top .....**Error! Bookmark not defined.**

2.7. Iptraf.....**Error! Bookmark not defined.**

BAB III .....**Error! Bookmark not defined.**

METODE PENELITIAN.....**Error! Bookmark not defined.**

3.1. Fase Penelitian .....**Error! Bookmark not defined.**

3.2. Perangkat Penelitian.....**Error! Bookmark not defined.**

3.3. Kerangka Kerja Penelitian .....**Error! Bookmark not defined.**

3.3.1. Perancangan dan Desain Simulasi Jaringan**Error! Bookmark not defined.**

3.3.2. Perancangan Modul Sistem IDS...**Error! Bookmark not defined.**

3.3.3. Pengujian Performa .....**Error! Bookmark not defined.**

5.4. Rencana Kegiatan Penelitian.....**Error! Bookmark not defined.**

BAB IV .....**Error! Bookmark not defined.**

Analisis dan Hasil .....**Error! Bookmark not defined.**

4.1. Simulasi Pengujian.....**Error! Bookmark not defined.**

4.1.1. Fungsional .....**Error! Bookmark not defined.**

4.1.1.1. Hasil Uji Fungsional dan Analisis ..... **Error! Bookmark not defined.**

4.1.2. Penggunaan CPU.....**Error! Bookmark not defined.**

4.1.2.1. Hasil Uji Penggunaan CPU dan Analisis **Error! Bookmark not defined.**

4.1.3. Pemakaian Memori.....**Error! Bookmark not defined.**

4.1.3.1. Hasil Uji Pemakaian Memori dan Analisis ..... **Error! Bookmark not defined.**

4.2. Evaluasi Hasil .....**Error! Bookmark not defined.**

4.2.1. Hasil Evaluasi Keakurasian.....**Error! Bookmark not defined.**

4.2.2. Hasil Evaluasi Damage, Recovery, Time to Run.. **Error! Bookmark not defined.**

BAB V.....**Error! Bookmark not defined.**

SIMPULAN DAN SARAN .....**Error! Bookmark not defined.**

5.1. Simpulan .....**Error! Bookmark not defined.**

5.2. Saran.....**Error! Bookmark not defined.**

DAFTAR PUSTAKA .....**Error! Bookmark not defined.**

LAMPIRAN 1 - Konfigurasi Modul-Modul NIDS**Error! Bookmark not defined.**

LAMPIRAN 2 – Data Hasil Pengujian.....**Error! Bookmark not defined.**

DAFTAR TABEL

Tabel 2.1 Komparasi Penelitian 8

Tabel 2.2 Perbandingan *IaaS, PaaS* dan *SaaS* 10

Tabel 2.3 Komparasi *Deployment Model Cloud computing* 11

Tabel 2.4 Arsitektur OpenStack 13

Tabel 2.5 Perbandingan NIDS dan HIDS 18

Tabel 2.6 Perbandingan *Signature based* dan *Anomaly based* 20

Tabel 2.7 Struktur *Snort Rules* 21

Tabel 3.1 Spesifikasi CISCO Switch Managed 28

Tabel 3.2 Spesifikasi PC *Client* 28

Tabel 3.3 Spesifikasi PC *Server* OpenStack 28

Tabel 3.4 *Confusion Matrix* 42

Tabel 3.5 Rencana Kegiatan Penelitian 45

Tabel 4.1 Hasil Klasifikasi Serangan 57

Tabel 4.2 Hasil Keakurasian Pendeteksian NIDS 57

DAFTAR GAMBAR

Gambar 2.1 Komponen Utama OpenStack....13

Gambar 2.2 Penempatan NIDS Pada Suatu Jaringan Komputer 17

Gambar 2.3 Penempatan HIDS Pada Suatu Jaringan Komputer 18

Gambar 2.4 Tampilan *Tools* LOIC 24

Gambar 2.5 Tampilan Awal Iptraf....25

Gambar 3.1 Fase Penelitian 26

Gambar 3.2 Kerangka Kerja Penelitian 30

Gambar 3.3 Desain Jaringan Pengujian 31

Gambar 3.4 Perancangan Modul-Modul Sistem IDS 32

Gambar 3.5 *Flowchart* Cara Kerja IDS Secara Umum 34

Gambar 3.6 Pengujian dengan Kondisi Normal 36

Gambar 3.7 Pengujian dengan Kondisi Menggunakan NIDS 37

Gambar 3.8 Pengujian dengan Kondisi Diserang 38

Gambar 3.9 Pengujian CPU NIDS Sebelum Mendeteksi Serangan 39

Gambar 3.10 Pengujian CPU NIDS Pada Saat Mendeteksi Serangan 40

Gambar 3.11 Pengujian Pemakaian Memori NIDS Sebelum Mendeteksi Serangan 41

Gambar 3.12 Pengujian Pemakaian Memori NIDS Pada Saat Mendeteksi Serangan 41

Gambar 4.1 NIDS Berhasil Memberika *Alert* Pada Host Openstack 47

Gambar 4.2 NIDS Berhasil Memberikan *Alert* Pada Host VM Ubuntu dengan 1 *Threads*.....48

Gambar 4.3 NIDS Berhasil Memberikan Alert Pada Host VM Fedora dengan 1 *Threads*.....48

Gambar 4.4 Hasil Deteksi Serangan DoS Host Openstack Pada Kondisi Di Serang.....49

Gambar 4.5 Hasil Deteksi Serangan DoS Pada VM Ubuntu dengan 1 *Threads* Pada Kondisi Di Serang 49

Gambar 4.6 *Traffic* UDP Host Openstack Tiap Kondisi Pengujian 50

Gambar 4.7 *Traffic* UDP Host VM Ubuntu Tiap Kondisi Pengujian.....51

Gambar 4.8 *Traffic* UDP Host VM Fedora Tiap Kondisi Pengujian.....51

Gambar 4.9 Rata-rata Perbandingan Penggunaan CPU NIDS Tiap Skenario...53

Gambar 4.10 Rata-rata Perbandingan Pemakaian Memori NIDS Tiap Skenario 55

Gambar L1.1 Tes Snort 67

Gambar L1.2 Tes *Sniffer Mode* 69

Gambar L1.3 Tes *Logger Mode* 70

Gambar L1.4 Tes *NIDS Mode* 70

DAFTAR SINGKATAN

CR	CLASSIFICATION RATE
DAQ	DATA-ACQUISTION
DOS	DENIAL OF SERVICE
DR	DETECTION RATE
FRP	FALSE POSITIVE RATE
GPL	GENERAL PUBLIC LICENSE
GRO	GENERIC RECEIVE OFFLOAD
GUI	GRAPHIC USER INTERFACE
HIDS	*HOST* INTRUSION DETECTION SYSTEM
IAAS	INFRASTRUCTURE AS A SERVICE
LRO	LARGE RECEIVE OFFLOAD
LOIC	LOW ORBIT ION CANON
NIDS	NETWORK INTRUSION DETECTION SYSTEM
OS	OPERATING SYSTEM
PAAS	PLATFORM AS A SERVICE
PR	PRECISION
RRDTOOL	ROUND-ROBIN DATABASE TOOL
SAAS	SOFTWARE AS A SERVICE
VM	VIRTUAL MACHINE