ANALISA DAN IMPLEMENTASI *NETWORK INTRUSION DETECTION* DAN *PREVENTION SYSTEM* BERBASIS *OPEN SOURCE* MENGGUNAKAN SNORT DI PT. TIME EXCELINDO

TUGAS AKHIR

disusun oleh

Nur Tantio Pratomo

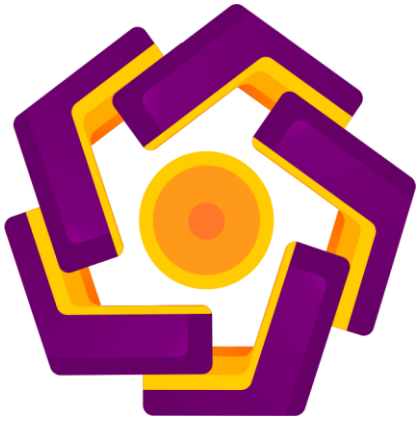
14.01.3355

PROGRAM DIPLOMA
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2017

ANALISA DAN IMPLEMENTASI *NETWORK INTRUSION DETECTION* DAN *PREVENTION SYSTEM* BERBASIS *OPEN SOURCE* MENGGUNAKAN SNORT DI PT. TIME EXCELINDO

TUGAS AKHIR

untuk memenuhi sebagian persyaratan mencapai gelar Ahli Madya
pada jenjang Program Diploma – Program Studi Teknik Informatika



disusun oleh

Nur Tantio Pratomo

14.01.3355

PROGRAM DIPLOMA
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2017

PERSETUJUAN

TUGAS AKHIR

ANALISA DAN IMPLEMENTASI *NETWORK INTRUSION DETECTION* DAN *PREVENTION SYSTEM* BERBASIS *OPEN SOURCE* MENGGUNAKAN SNORT DI PT. TIME EXCELINDO

yang dipersiapkan dan disusun oleh

Nur Tantio Pratomo

14.01.3355

telah disetujui oleh Dosen Pembimbing Tugas Akhir
pada tanggal 19 Februari 2017

Dosen Pembimbing

Melwin Syafrizal, S. Kom., M. Eng.
NIK. 190302105

PENGESAHAN

TUGAS AKHIR

ANALISA DAN IMPLEMENTASI *NETWORK INTRUSION DETECTION* DAN *PREVENTION SYSTEM* BERBASIS *OPEN SOURCE* MENGGUNAKAN SNORT DI PT. TIME EXCELINDO

yang dipersiapkan dan disusun oleh

Nur Tantio Pratomo

14.01.3355

telah dipertahankan di depan Dewan Penguji
pada tanggal 29 Agustus 2017

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Nila Feby Puspitasari, S. Kom., M.Cs. **NIK. 190302161**	
Andika Agus Slameto, M.Kom. **NIK. 190302109**	

Tugas Akhir ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Ahli Madya Komputer
Tanggal 11 September 2017

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si., M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa, Tugas Akhir ini merupakan karya saya sendiri (ASLI), dan isi dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi maupun, 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 tanggung jawab saya pribadi.

Yogyakarta, 05 September 2017

Nur Tantio Pratomo

NIM. 14.01.3355

MOTTO

"Bersikaplah jujur, karena itu akan menjadikan mu mutiara dunia" ~

Nur Tantio Pratomo

"Prinsip yang teguh adalah kompas kehidupan" ~ Nur Tantio Pratomo

"That is the definition of faith - acceptance of that which we imagine to be true, that which we cannot prove." ~ Dan Brown

PERSEMBAHAN

Karya ini penulis persembahkan untuk kedua orang tua yang tersayang, Bapak Slamet dan Ibu Sumi atas segala doa, semangat, waktu serta segala pengorbanan dan didikannya yang diberikan kepada penulis hingga saat ini, semoga Allah SWT selalu melindungi dan mengasihi keduanya.

Juga untuk istriku tercinta Emelia Kusuma Wanti atas kesabaran, pengertian dan semangatnya yang selalu diberikan kepada penulis. Yang selalu mengingatkan ketika lalai terhadap tanggungjawab – tanggungjawab yang dimiliki. Terima kasih atas senyuman dan tawa yang diberikan ketika di rumah. Semoga Allah SWT selalu merahmati dirinya.

Untuk adik penulis satu – satunya Namira Dwi Pangestuti atas segala dukungan yang diberikan. Semoga Allah SWT selalu menjaga dirinya.

Persembahan juga diberikan kepada kedua mertua penulis Bapak Maskar dan Ibu Wantinem serta adik ipar Sela Rusmala atas segala pengertian dan dukungan yang diberikan. Semoga Allah SWT selalu memberikannya kesehatan.

Matur Sembah Nuwun

KATA PENGANTAR

Puji syukur selalu penulis panjatkan kehadirat Allah SWT atas segala limpahan rahmat, taufik dan hidayah-Nya sehingga penulis dapat menyeselaikan penyusunan tugas akhir yang berjudul "Analisa dan Implementasi *Network Intrusion Detection* dan *Prevention System* Berbasis *Open Source* Menggunakan Snort di PT. Time Excelindo".

Penulis sadari bahwa dalam proses penyusunan tugas akhir ini banyak mengalami kendala, namun tidak terlepas dari bantuan berbagai pihak untuk bimbingan, kerjasama dan kuasa dari Allah SWT sehingga segala kendala yang dihadapi tersebut dapat diatasi. Untuk itu penulis sampaikan terimakasih kepada Bapak Melwin Syafrizal, S.Kom., M. Eng. selaku pembimbing yang telah meluangkan waktu, tenaga dan fikiran dalam memberikan bimbingan, masukan, saran dan ide – idenya yang sangat membantu penulis dalam menyusun tugas akhir.

Selanjutnya penulis sampaikan juga rasa terima kasih yang sebesar – besarnya kepada :

1. Bapak Prof. Dr. M. Suyanto, M. M. selaku Ketua Universitas AMIKOM Yogyakarta.
2. Bapak Hanafi, S.Kom., M. Eng. selaku Direktur Utama PT. Time Excelindo.
3. Bapak Sugeng Riyadi, S. Kom. selaku Manager Dept. Teknis di PT. Time Excelindo.
4. Mas Andi Kriswantono, S. Kom. selaku leader NOC di PT. Time Excelindo.
5. Bapak dan Ibu Dosen Universitas AMIKOM Yogyakarta.
6. Rekan – rekan di PT. Time Excelindo yang telah memberikan izin serta membantu selama perkuliahan dan penyusunan tugas akhir ini.
7. Teman – teman mahasiswa/mahasiswi D3 TI 01 yang telah banyak memberikan dukungan dan semangat serta masukan kepada penulis baik selama mengikuti perkuliahan maupun dalam penyusunan tugas akhir ini.

8. Bapak Slamet, Ibu Sumi, Bapak Maskar, Ibu Wantinem, Dwi dan Sela yang telah memberikan banyak bantuan berupa moril, materil, serta doa yang selalu menyertai penulis.
9. Istri tercinta Emelia Kusuma Wanti yang dengan sabar memberikan doa, waktu, perhatian, pengertian, semangat dan dukungan yang besar kepada penulis.
10. Semua pihak yang tidak dapat penulis sebutkan satu per satu yang telah membantu dalam penyelesaian penyusunan tugas akhir ini.

Akhir kata, penulis sampaikan mohon maaf apabila terdapat banyak kekurangan dalam penyusunan tugas akhir ini. Penulis sangat mengharapkan saran dan kritik yang membangun untuk hasil yang lebih baik lagi di karya – karya selanjutnya. Semoga tugas akhir ini dapat bermanfaat bagi semua pihak yang membacanya.

Yogyakarta, 11 Agustus 2017

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR SINGKATAN

DDoS	= *Distributed Denial of Service*
DoS	= *Denial of Service*
VPS	= *Virtual Private Server*
LTS	= *Long Term Support*
DAQ	= *Data Acquisition*
FTP	= *File Transfer Protocol*
NOC	= *Network Operations Center*
IP	= *Internet Protocol*
CLI	= *Command Line Interface*
SQL	= *Structured Query Language*
IDS	= *Intrusion Detection System*
IPS	= *Intrusion Prevention System*
CGI	= *Computer Generated Imagery*
TCP	= *Transmission Control Protocol*
UDP	= *User Datagram Protocol*
ICMP	= *Internet Control Message Protocol*
ASCII	= *American Standard Code for Information Interchange*
PID	= *Process Identification*
IPQ	= *Internet Protocol Quota*
ARP	= *Address Resolution Protocol*
IGRP	= *Interior Gateway Routing Protocol*
GRE	= *Generic Routing Encapsulation*
OSPF	= *Open Shortest Path First*
RIP	= *Routing Information Protocol*
IPX	= *Internetwork Packet Exchange*

INTISARI

Keamanan data pada jaringan internet adalah suatu yang sangat penting. Banyak orang diluar sana yang mencoba mencuri data – data seseorang melalui koneksi internet atau menyerang computer – computer yang terhubung internet baik dengan phising, malware, virus maupun DDoS. Tidak hanya mencuri data – data penting namun ada juga yang hanya bertujuan untuk mengganti merubah tampilan dari suatu web, baik milik suatu organisasi, perusahaan bahkan pemerintahan dan juga ada yang bertujuan untuk mematikan suatu layanan dari organisasi tertentu. PT. Time Excelindo sebagai salah satu penyelenggara jasa layanan internet yang memiliki layanan colocation server dan hosting / VPS perlu memiliki suatu system monitoring atau pencegahan terhadap penyusupan ke server – server maupun computer yang ada di PT. Time Excelindo agar layanan internet yang diberikan ke pelanggan dapat berjalan dengan normal secara kontinu.

Pada tugas akhir ini, penulis akan menganalisa dan mengimplementasikan NIDPS (Network Intrusion Detection and Prevention System) Berbasis Open Source Menggunakan Snort di PT. Time Excelindo. System yang akan memonitor trafik dan memblok trafik mencurigakan yang berjalan pada jaringan PT. Time Excelindo. Metode yang penulis gunakan yaitu analisa, instalasi, konfigurasi dan pengujian serta melakukan evaluasi.

Network Intrusion Detection and Prevention System (NIDPS) akan memonitor trafik yang berjalan pada network tertentu. Bila ada suatu aktifitas yang mencurigakan yang sesuai dengan rule yang ada pada system maka IP Address yang membawa trafik mencurigakan tersebut akan di blok oleh system sehingga tidak dapat mengakses network server pada PT. Time Excelindo.

Kata kunci : keamanan, pencegahan, real-time

ABSTRACT

Data security on the Internet is a very important. Many people out there who try to steal many datas through an internet connection or internet-connected computer to attack well with phishing, malware, viruses and DDoS. Not only steal important data but some are only intended to change the look of the web, both belong to organizations, companies and even government and there is also aiming to turn off a service from a particular organization. PT. Time Excelindo as one of internet services provider that have a server colocation services and hosting / VPS need to have a system of monitoring or prevention of intrusion into the server and computer in the PT. Time Eexcelindo order internet service provided to customers running normally continuously.

In this final project, the author will analyze and implement NIDPS (Network Intrusion Detection and Prevention System) Based Open Source Using Snort PT. Time Excelindo. System that will monitor traffic and block suspicious traffic running on the network of PT. Time Excelindo. The authors use the method of analysis, installation, configuration, and testing and evaluating.

Network Intrusion Detection and Prevention System (NIDPS) will monitor traffic running on particular networks. If there is a suspicious activity in accordance with the existing rules in the system, then the IP Address that brings suspicious traffic will be blocked by the system and so can not access the server network in PT. Time Excelindo.

***Keywords**: security, prevention, real-time*