# ANALISIS DETEKSI PENYUSUPAN PADA JARINGAN KOMPUTER MENGGUNAKAN SNORT

## (Studi Kasus Pada Dinas Pariwisata Propinsi Daerah Istimewa Yogyakarta)

Skripsi

untuk memenuhi sebagian persyaratan mencapai derajat Sarjana S-1


**Disusun Oleh:**

**TRIAWAN ADI CAHYANTO**

**NIM. 06650051**



**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS SAINS DAN TEKNOLOGI**

**UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA**

**YOGYAKARTA**

**2011**

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

**PENGESAHAN SKRIPSI/TUGAS AKHIR**

Nomor : UIN.02/D.ST/PP.01.1/1195/2011

Skripsi/Tugas Akhir dengan judul : Analisis Deteksi Penyusupan Pada Jaringan Komputer Menggunakan Snort (Studi Kasus Pada Dinas Pariwisata Propinsi Daerah Istimewa Yogyakarta)

Yang dipersiapkan dan disusun oleh :

Nama : Triawan Adi Cahyanto

NIM : 06650051

Telah dimunaqasyahkan pada : 27 Juni 2011

Nilai Munaqasyah : A -

Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

**TIM MUNAQASYAH :**

Ketua Sidang

Imam Riadi, M.Kom
NIY. 60020397

Penguji I

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

Penguji II

M. Didik R. Wahyudi, S.T, M.T
NIP. 19760812 200901 1 015

Yogyakarta, 1 Juli 2011
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

Prof. Drs. H. Akh. Minhaji, M.A, Ph.D
NIP. 19580919 198603 1 002

# 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 | : Triawan Adi Cahyanto |
| NIM | : 06650051 |
| Judul Skripsi | : Analisis Deteksi Penyusupan Pada Jaringan Komputer Menggunakan Snort (Studi Kasus Pada Dinas Pariwisata Propinsi Daerah Istimewa Yogyakarta) |

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 dimunaqosyahkan. Atas perhatiannya kami ucapkan terima kasih.

Yogyakarta, 14 Juni 2011
Pembimbing I

Imam Riadi, M.Kom
NIY. 60020397

# 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 : Triawan Adi Cahyanto
NIM : 06650051
Judul Skripsi : Analisis Deteksi Penyusupan Pada Jaringan Komputer *(Studi Kasus Pada Dinas Pariwisata Propinsi Daerah Istimewa Yogyakarta)*

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.

Yogyakarta, 8 Juni 2011
Pembimbing II

Sumarsono, M.Kom
NIP. 19710209-200501-1-003

## SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini :

Nama : Triawan Adi Cahyanto

NIM : 06650051

Program Studi : Teknik Informatika

Fakultas : Sains dan Teknologi

Menyatakan dengan sesungguhnya bahwa skripsi ini merupakan hasil pekerjaan penulis sendiri dan sepanjang pengetahuan penulis tidak berisi materi yang dipublikasikan atau ditulis orang lain, dan atau telah digunakan sebagai persyaratan penyelesaian Tugas Akhir di Perguruan Tinggi lain, kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 10 Juni 2011
Yang menyatakan

METERAI TEMPEL 9B58BAAF402062636 ENAM RIBU RUPIAH 6000 DJP

Triawan Adi Cahyanto
NIM : 06650051

# MOTTO

**Usaha dan doa merupakan rumus mujarab dalam hidup, janganlah pernah merasa puas terhadap hasil yang sudah dicapai, akan tetapi janganlah selalu mencari kesempurnaan terhadap suatu hal karena kesempurnaan hanya milik ALLAH SWT semata**

**~Triawan Adi Cahyanto~**

**Dalam kehidupan, manusia terkadang mudah mengeluh dan menyerah pada keadaan. Tapi dengan dorongan orang-orang yang kita cintai disekitar kita, semangat kita akan bangkit kembali dan meraih kemenangan.**

**~katamutiara.net~**



**"You may never know what results come of your action, but if you do nothing there will be no result."**

**~Mahatma Gandhi~**

# PERSEMBAHAN

*Skripsi ini aku persembahkan :*

*Untuk almamaterku tercinta Program Studi Teknik Informatika*

*Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.*

## KATA PENGANTAR

Segala puji bagi Allah SWT yang telah memberikan pertolongan dan ilmu-Nya kepada penulis sehingga dapat terselesaikan penelitian ini. Penelitian yang berjudul "Analisis Deteksi Penyusupan Pada Jaringan Komputer Menggunakan Snort" ini mengambil contoh studi kasus di Dinas Pariwisata Propinsi Daerah Istimewa Yogyakarta. Selanjutnya penulis mengucapkan terima kasih kepada :

1. Bapak Prof. Drs. H. Akh. Minhaji, M.A.Ph.D, selaku Dekan Fakultas Sains & Teknologi UIN Sunan Kalijaga.
2. Bapak Agus Mulyanto, M.Kom, sebagai Kepala Program Studi Teknik Informatika UIN Sunan Kalijaga.
3. Bapak Imam Riadi, M.Kom, sebagai Dosen Pembimbing I yang dengan kesabarannya telah membimbing baik di kampus maupun di rumah selama penyusunan skripsi ini.
4. Bapak Sumarsono, M.Kom, sebagai Dosen Pembimbing II yang membantu penulis dalam penelitian dan memberikan koreksi, saran, dan kritikan kepada penulis selama penyusunan skripsi.
5. Bapak Adi, S.E sebagai *administrator* beserta staff pada Dinas Pariwisata Propinsi Daerah Istimewa Yogyakarta yang telah membantu penulis memberikan kemudahan sehingga penelitian pada lokasi berjalan dengan baik.

6. Seluruh Dosen Program Studi Teknik Informatika yang telah memberi bekal ilmu pengetahuan kepada penulis, semoga ilmunya menjadi amal sholeh yang berkesinambungan di dunia hingga akhirat.
7. Kedua orang tuaku Bapak Sugiyono dan Ibu Restumini serta kakak-kakakku tercinta Dedi Hernawan dan Nurnaeni Fatimah beserta keluarga besar yang selalu memberikan motivasi doa dan nasehat untuk senantiasa bersyukur atas semua nikmat yang diberikan Allah SWT.
8. All member xcode, jasakom, echo, kaskus, Mas pandu, terima kasih banyak atas bantuan dan bimbingannya dalam penyelesaian dan persiapan skripsi ini.
9. Wahid "wagem", Rifqi, Ali, Iksan, Doyok, Agung, Didik, Uki, beserta teman-teman program Studi Teknik Informatika yang tidak bisa ditulis satu persatu khususnya angkatan 2006 yang telah banyak memberi dukungan, hiburan, beserta memberi pencerahan dalam penyusunan skripsi ini.
10. Sopanudin, Rita, Zaenul, Adib, Alvi, Zandi, Fajri, Rukmini, Iksan Fatah, Andri, Ibu Wieny, Pak Wawan, Ibu Yuntari, terima kasih atas dukungannya.
11. Semua pihak yang telah memberikan bantuan selama penyusunan skripsi ini.

Semoga Allah SWT memberikan balasan kebaikan yang berlipat ganda kepada semuanya dan Semoga karya kecil ini dapat memberikan manfaat bagi penulis khususnya dan bagi pembaca pada umumnya.

Yogyakarta, Juni 2011

Penulis

**DAFTAR ISI**

## DAFTAR TABEL

## DAFTAR GAMBAR

## DAFTAR LAMPIRAN

# Analisis Deteksi Penyusupan Pada Jaringan Komputer Menggunakan Snort

**(Studi Kasus Pada Dinas Pariwisata Propinsi Daerah Istimewa Yogyakarta)**

Oleh :

Triawan Adi Cahyanto
NIM.06650051

## ABSTRAKSI

Pada saat ini jaringan komputer merupakan hal yang sangat penting. Jaringan komputer dibutuhkan untuk melakukan pertukaran data atau pemakaian perangkat keras secara bersama-sama sehingga pekerjaan dapat diselesaikan dengan mudah. Ancaman keamanan data juga menyertai keberadaan jaringan komputer yang semakin canggih ini. Sistem ini akan diujicoba dan diimplementasikan untuk mengurangi ancaman tersebut.

Sistem ini dibuat berbasis sistem operasi *Linux* dan menggunakan *Snort* untuk menangkap dan menganalisa paket data. Penelitian dilakukan dengan menggunakan metode studi literatur dan observasi data pada lokasi penelitian. Metode penelitian dengan studi literatur yaitu mengumpulkan referensi dan informasi terkait dengan objek penelitian, sedangkan metode observasi dilakukan untuk mengetahui kebutuhan yang diinginkan pada lokasi penelitian sehingga pada saat penelitian tidak mengalami kendala. Tahapan pada observasi itu diantaranya wawancara, konfigurasi awal, pembuatan sistem dan pengujian sistem. Setelah analisa paket data, Snort akan melakukan pencatatan ke dalam *MySQL* untuk keperluan *database*. Untuk memudahkan penggunaan, maka akan dibuat sebuah sistem yang digunakan sebagai tampilan web dari database yang digunakan *Snort*.

Hasil pengujian terhadap program, menunjukkan bahwa program ini dapat menangkap paket data yang lewat, menganalisis paket data dan menampilkan sebuah tampilan berbasis web dari *MySQL*. Berdasarkan hasil pengujian itu, dengan mengintegrasikan penggunaan Snort beserta mengamankan *port-port* sesuai kebutuhan maka semua aktivitas paket-paket data yang melewati jaringan komputer akan selalu terawasi.

Kata kunci : Snort, IDS, Jaringan Komputer, Linux, *MySQL*

# Infiltration Detection Analysis On Computer Network Using Snort

## (A Case Study of Tourism Department of Yogyakarta Special Province)

Triawan Adi Cahyanto
NIM.06650051

## ABSTRACT

Computer network represent very important matter now. Computer network required to transfer file or hardware usage together so that work can be finished easily. Security data threat also accompany existence of computer network which sophisticated progressively. This system will be tried and implementation to lessen the amount of the threat.

This system made base on Linux operating system and use Snort to catch and analyze data package. Research conducted by using literature study method and data observation at research location. Research method with literature study that is collect information and reference related to research object, while observation method conducted to know wanted by requirement at research location so that at the time of research not experience of constraint. Step at observation among others interview, configuration early, making system, and system examination. After data package analysis, Snort will record in MySQL for database. To facilitate use, will be made a system used as web appearance from used Snort database.

Result of examination program, indicating that program can catch late data package, analyzing data package and present a appearance base on web from MySQL. Result of that examination, by integrating use of Snort along with protecting port according to requirement hence all data package activity passing computer network will always observed.



Keywords: Snort, IDS, Network Computing, Linux, MySQL

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang Masalah

Keamanan jaringan komputer merupakan hal yang sangat penting, namun sering dipandang sebelah mata bahkan sebagian orang tidak memperdulikan soal keamanan jaringan. Hingga saat ini jaringan komputer terus mengalami perkembangan yang cukup pesat baik dari sisi pengguna, komputer, maupun teknologi yang digunakan. Namun dampak dari semakin berkembangnya hal ini, membuat hal-hal yang bersifat mengganggu keamanan jaringan komputer juga semakin marak. Salah satu contoh sederhana adalah melakukan pengiriman paket-paket pada suatu sistem atau jaringan dengan maksud melumpuhkan aktivitas pada saat itu. Tentu saja ini sangat merugikan salah satu pihak.

Berdasarkan hal tersebut, manajemen jaringan terhadap keamanan (*security management*) sangat dibutuhkan sebagai langkah pencegahan (*preventif*) dan sekaligus proteksi terhadap sumber-sumber (*resource*) di dalam suatu sistem atau jaringan. Untuk itu diperlukan suatu cara atau langkah pencegahan sedini mungkin dengan melakukan sistem keamanan pada jaringan komputer yang mampu melakukan deteksi adanya serangan atau penyusupan. Salah satu fungsi manajemen keamanan ini adalah mampu mendeteksi adanya penyusup (*intruder*) yang berusaha masuk pada jaringan, sehingga nantinya diharapkan dapat mencegah adanya kerugian yang

disebabkan oleh serangan tersebut. Sistem ini dikenal dengan sebutan IDS (*Intrusion Detection System*).

Melalui tugas akhir ini diharapkan bisa menghasilkan suatu perangkat keamanan sederhana bagi pengelola jaringan (*administrator*) dengan mengadopsi kinerja IDS dari Snort, yang dilengkapi dengan kemampuan analisis adanya penyusupan berbasis web. Adapun yang menjadi fokus dari IDS yang akan dibangun adalah kemampuan dalam mendeteksi berbagai serangan serta mampu mengintegrasikan dalam suatu sistem pelaporan adanya penyusupan berbasis web. Penelitian ini akan dilaksanakan dan diujicoba pada Dinas Pariwisata Propinsi Daerah Istimewa Yogyakarta.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, diperoleh suatu rumusan permasalahan sebagai berikut :

a. Bagaimana cara mendeteksi penyusup pada jaringan komputer?
b. Bagaimana membuat *report* data serangan sehingga dapat mengetahui mana serangan berbahaya, serangan sedang, dan serangan tidak berbahaya.

## 1.3 Batasan Masalah

Berdasarkan rumusan masalah yang ada, maka penelitian ini akan saya batasi permasalahannya sebagai berikut :

a. Data serangan yang dipakai hanya yang berasal dari database *log* snort dengan pemilihan data-data yang dibutuhkan sebagai data serangan yaitu data, protokol, *d_port*, *size*, dan *tcp_flags*.
b. Yang dilakukan dalam sistem hanya mendeteksi dan tidak melakukan aksi.
c. *Report* yang dihasilkan hanya menampilkan statistik serangan berdasarkan waktu, tingkat bahaya serangan dan jumlah serangan.

## 1.4 Tujuan Penelitian

Dengan mengacu pada perumusan masalah maka tujuan yang hendak dicapai dari penelitian ini adalah sebagai berikut :

a. Mengembangkan aplikasi deteksi adanya penyusupan (IDS) menggunakan Snort yang berfungsi untuk *capture paket* pada lalu lintas jaringan (*network traffic*), melakukan pengecekan header paket dan melaporkannya.
b. Mengimplementasikan sistem pelaporan adanya penyusupan berbasis web menggunakan bahasa pemrograman PHP dan *database* MySQL yang bekerja berdasarkan IDS yang dibangun.

## 1.5 Manfaat Penelitian

Dengan adanya penelitian ini diharapkan dapat memberikan manfaat diantaranya:

a. Membantu para pengguna / khalayak untuk mengetahui lebih dalam mengenai pengembangan-pengembangan yang dapat dilakukan terhadap kinerja IDS.
b. Meningkatkan keamanan sistem yang terdapat pada jaringan-jaringan vital baik internet maupun intranet.

## 1.6 Keaslian Penelitian

Penelitian yang berhubungan dengan masalah analisis deteksi penyusupan pada jaringan komputer menggunakan Snort belum pernah dilakukan pada Universitas Islam Negeri Sunan Kalijaga Yogyakarta akan tetapi pernah dibuat oleh mahasiswa di kampus lain dengan tema yang berbeda.

# BAB V

# KESIMPULAN DAN SARAN

## 5.1 Kesimpulan

Berdasarkan penelitian yang telah dikerjakan maka dapat ditarik kesimpulan sebagai berikut:

1. Pendeteksian penyusup pada jaringan komputer dengan mengintegrasikan penggunaan Snort dan mengamankan *port-port* sesuai kebutuhan, maka semua aktivitas paket-paket data yang melewati jaringan komputer akan selalu terawasi.
2. Analisis sistem informasi pelaporan adanya penyusupan akan mempermudah penggunaan Snort (dalam linux) sehingga dapat digunakan melalui web, beserta mampu melihat aktivitas paket-paket data yang melalui jaringan komputer.
3. Berdasarkan hasil pengujian, dapat disimpulkan bahwa aplikasi sistem deteksi penyusupan pada jaringan komputer berbasis web berjalan dengan baik.

## 5.2 Saran

Pada penelitian ini terdapat beberapa kelebihan namun tidak terlepas dari kekurangan yang membutuhkan saran-saran untuk mendukung kesempurnaan, saran tersebut diantaranya adalah sebagai berikut.

1. Sistem ini bersifat sistem deteksi dan tidak ada aksi, hanya berupa pesan *alert*, maka jauh lebih bagus jika diintegrasikan juga dengan sistem lain yang bisa memberikan aksi langsung terhadap *host* yang melakukan serangan berbahaya misalnya *iptables.*
2. Pembuatan analisis sistem deteksi adanya penyusupan berbasis web alangkah lebih baik jika dikembangkan menggunakan metode algoritma klasifikasi yang modern supaya rasio kesalahan dalam menganalisis paket mampu dikurangi. Selain itu juga bisa dilakukan *update rules* otomatis ketika terdapat serangan baru dan belum ada pada *rules* Snort yang ada.

## DAFTAR PUSTAKA


Aharoni.2006.*Offensive Security*.http://offensive-security.com.

*Anonymous*.2009.http://digilib.unsri.ac.id/download/2tierVS3tier14082009.pdf.

Andri.2009.*Perancangan Aplikasi Intrusion Detection System Menggunakan Bacon-MVV*.Jakarta:Universitas Tarumanegara.

Ariyus, Doni.2007.*Intrusion Detection System*.Yogyakarta: Penerbit Andi.

Ashari, Ahmad dkk. 2009.*Linux System Administrator*.Bandung:Penerbit Informatika.

Beale, Jay dkk.2004.*Snort 2.1 Intrusion Detection Second Edition*.

Christoper.2004.*Managing Security with Snort and IDS Tools.*

Cole, Eric.2001.*Hackers Beware:Defending Your Network From The Wiley Hacker*.

Collings, Terry dkk.2002.*Redhat linux networking and system administrator.*

Di pietro, Roberto dkk.2008.*Advance In Information Security Intrusion Detection System.*

Eri.*http://eri.staff.gunadarma.ac.id/Downloads/files/8862/introduction.ppt*.

Fauziah, Lilis.2006.*Pendeteksian Serangan Pada Jaringan Komputer Berbasis IDS Snort Dengan Algoritma Clustering K-Means.*Surabaya: ITS.

Gregory, Tom.*Tutorial Membangun Snort Sebagai Intrusion Detection System*.http://ilmukomputer.org.

Indrato.2009.*Modul Pemrograman Web Dengan Php Dan Mysql*.Yogyakarta:Imagine.

Jovan.2007.*Panduan Membuat Web dengan PHP untuk Pemula*.Jakarta : Mediakita.

Kurniawan.2010.*Sistem Deteksi Dan Penanganan Intrusi Menggunakan Snort Dan Base* http://ie.akprind.ac.id/content/sistem-deteksi-dan-penanganan-intrusi-menggunakan-snort-dan-base .Yogyakarta:IST Akprind.

Maulidani, Destana Dwi. 2007.*Rancang Bangun Intrusion Detection System Pada Jaringan Berbasis Protokol SNMP Memanfaatkan Java Management Extensions*.Surabaya:Stikom.

Muhammad, Alva Hendi.2007.*Rahasia dan Trik Mengamankan Server Linux*. Yogyakarta: Penerbit Gavamedia.

Nugroho, Arianto.2005.*Kerangka Tulisan Keamanan Jaringan Komputer Dan Komunikasi* diakses 6 januari 2011 jam 03.42 http://bebas.vlsm.org/v06/Kuliah/MTI-Keamanan-Sistem-Informasi/2005/123/123P-03-draft-Network_Security.pdf

Pressman, Roger S.2001.Software Engineering – A practitioner's Approach 5th.New York:McGraw-Hill.

Proffitt, Brian.2011.*Introducing Fedora : Dekstop Linux.*

Provos, Niels.2008.*Virtual Honeypots: From Botnet Tracking to Intrusion Detection*.

Rafiudin, Rahmat.2006.*IP Routing dan Firewall dalam Linux*.Yogyakarta:Penerbit Andi.

Rafiudin, Rahmat.2006.*OpenBSD*.Yogyakarta:Penerbit Andi.

Rafiudin, Rahmat.2010.*Mengganyang Hacker dengan Snort*.Yogyakarta:Penerbit Andi.

Susanto, Budi.*Keamanan Jaringan* http://lecturer.ukdw.ac.id/budsus/jarkom/Week12.pdf

Sutedjo, Budi dkk.2006.*Konsep dan Aplikasi Pemrograman Client Server dan Sistem Terdistribusi*. Yogyakarta: Penerbit Andi.

Syafii.2006.*Membangun Aplikasi Berbasis PHP dan MySQL*. Yogyakarta: Penerbit Andi.

Tim Inixindo.2004.*Linux System Administration*.