# IMPLEMENTASI *SNORT* SEBAGAI TOOL *INTRUSION DETECTION SYSTEM* PADA SERVER *FREEBSD* DI PT. POWER TELECOM

**SKRIPSI**

Disusun sebagai salah satu syarat menyelesaikan Program Studi
Strata I pada Jurusan Teknik Informatika Fakultas Komunikasi dan Informatika
Universitas Muhammadiyah Surakarta

Oleh:

*Atiq Zahrial Firdaus*
NIM : L200070054

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS MUHAMMADIYAH SURAKARTA
2012

**HALAMAN PERSETUJUAN**

Skripsi dengan judul

# IMPLEMENTASI *SNORT* SEBAGAI TOOL *INTRUSION DETECTION SYSTEM* PADA SERVER *FREEBSD* DI PT. POWER TELECOM

ini telah diperiksa dan disetujui pada :

Hari : Kamis.

Tanggal : 1 Februari 2012.

| Pembimbing I | Pembimbing II |
|---|---|
| Husni Tamrin, S.T, M.T, Ph.D. | Dedi Ary Prasetya, S. T. |
| NIK: 706 | NIK: 982 |

**HALAMAN PENGESAHAN**

# IMPLEMENTASI *SNORT* SEBAGAI TOOL *INTRUSION DETECTION SYSTEM* PADA SERVER *FREEBSD* DI PT. POWER TELECOM

dipersiapkan dan disusun oleh

**Atiq Zahrial Firdaus**

NIM : L200070054

telah dipertahankan di depan Dewan Penguji

pada tanggal 21 Februari 2012

**Susunan Dewan Penguji**

| Pembimbing I | Anggota Dewan Penguji Lain |
|---|---|
| Husni Tamrin, S.T., M.T., Ph.D. | Fajar Suryawan, S.T., M.Eng.Sc., Ph.D. |
| Pembimbing II | |
| Dedi Ary Prasetya, S.T. | Jan Wantoro, S.T. |

Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar sarjana

Tanggal … Maret 2012

| Dekan<br>Fakultas Komunikasi dan Informatika | Ketua Program Studi<br>Teknik Informatika |
|---|---|
| Husni Thamrin, S.T., M.T., Ph.D.<br>NIK : 706 | Aris Rakhmadi, S.T., M.Eng.<br>NIK : 983 |

## MOTTO DAN PERSEMBAHAN

**MOTTO:**

- *Kapan seseorang akan benar-benar mati? Saat seseorang tertembus peluru di jantungnya? Tidak. Saat seseorang mengidap penyakit paling mematikan? Tidak. Saat seseorang meminum sup jamur paling beracun? Tidak. Seseorang hanya akan benar-benar mati saat orang itu benar-benar telah dilupakan.*

  (Dr. Hiluluk)

- *Semua jiwa manusia adalah abadi, namun jiwa manusia yang berbudi, abadi dan dalam lindungan Yang Maha Kuasa.*

  (Socrates)

**PERSEMBAHAN :**

Penulis persembahkan tulisan sederhana ini kepada:

1. Bapak dan Ibu tercinta, beserta seluruh keluarga besar yang selalu mendukung penulis dalam banyak hal.
2. Teman-teman Teknik Informatika angkatan 2007 yang banyak menghabiskan waktu bersama penulis.
3. Kawan-kawan komunitas Beta House yang selalu berbagi ilmu dan pengetahuan bersama.

# DAFTAR KONTRIBUSI

Dengan ini saya menyatakan bahwa dalam skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Berikut ini saya sampaikan daftar kontribusi dalam penyusunan laporan skripsi ini:

1. Pengaturan skema jaringan beserta alokasi IP Address yang digunakan dalam penelitian mengikuti aturan jaringan intranet PT. Powertel dan dilakukan oleh Mas Rofiq dan Mas Anwar, teknisi jaringan dari PT. Power Telecom cabang Solo.
2. Tahap installasi dan konfigurasi Snort IDS dilakukan sendiri oleh penulis dengan mengikuti referensi yang disebutkan dalam daftar pustaka laporan skripsi.
3. Persiapan peralatan penelitian dan langkah pengujian Snort IDS dilakukan penulis dengan dibantu oleh Dadik Wuryanto dan Murniati, partner penelitian penulis di PT. Power Telecom.

Demikian pernyataan dan daftar kontribusi ini saya buat dengan sejujurnya. Saya bertanggungjawab atas isi dan kebenaran daftar di atas.

Surakarta, 24 Januari 2012

Atiq Zahrial Firdaus

Mengetahui:

| Pembimbing I | Pembimbing II |
| --- | --- |
| Husni Thamrin, S.T., M.T., Ph.D. | Dedi Ary Prasetya, S.T. |
| NIK : 706 | NIK : 982 |

# KATA PENGANTAR

Dengan mengucapkan syukur Alhamdulillah kepada Allah SWT yang telah memberikan rahmat, hidayah serta nikmat yang tiada terkira kepada hamba-Nya, sehingga penulis dapat menyelesaikan skripsi dengan judul "Implementasi *Snort* Sebagai Tool *Intrusion Detection System* pada Server *FreeBSD* di PT. Power Telecom" ini.

Laporan Skripsi ini disusun untuk memenuhi syarat kurikulum dalam menyelesaikan Program Sarjana pada Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta.

Penulis telah berusaha untuk menyelesaikan laporan skripsi ini sebaik mungkin, namun demikian penulis menyadari bahwa laporan ini masih jauh dari kesempurnaan. Oleh karena itu, penulis mengharapkan saran serta kritik yang bersifat membangun demi perbaikan. Tidak lupa, penulis ingin mengucapkan terima kasih dan penghargaan setinggi-tingginya, kepada:

1. Allah SWT atas Iman dan Islam yang telah dianugerahkan-Nya.
2. Rasulullah Muhammad SAW dan keluarga beserta para sahabatnya.
3. Bapak Aris Rakhmadi, S.T., M.Eng. selaku Ketua Jurusan teknik Informatika, Fakultas Komunikasi dan Informatika, Universitas Muhammadiyah Surakarta.
4. Bapak Husni Thamrin, S.T., M.T., Ph.D. selaku pembimbing I yang telah memberikan bimbingan secara sabar dalam penulisan laporan skripsi ini kepada penulis.

5. Bapak Dedi Ary Prasetya, S.T. selaku pembimbing II sehingga penulis dapat menyelesaikan penulisan laporan skripsi ini.
6. Seluruh jajaran Direksi PT. Power Telecom cabang Solo yang telah memberikan ijinnya sehingga penulis dapat menyelesaikan penelitian ini.
7. Kedua orang tua tercinta, beserta seluruh keluarga besar atas dukungannya terhadap penulis selama ini.
8. Mas Rofiq dan Mas Anwar dari PT. Power Telecom yang sudah memberikan banyak masukan selama penelitian.
9. Partner selama penelitian yang sangat membantu, Murniati dan Dadik Wuryanto. Terima Kasih atas kerjasamanya selama ini.
10. Seluruh kru Beta House yang selalu memberikan kritikan, masukan dan kebersamaannya selama ini dengan penulis. Teman seangkatan Informatika 2007 dan seluruh pihak yang membantu sehingga terselesaikannya penulisan laporan skripsi ini.

Akhirnya penulis berharap semoga skripsi ini berguna bagi semua pihak dan bermanfaat dalam menambah pengetahuan dan wawasan ilmu. Amiin.

Surakarta, 24 Januari 2012

Penulis

## DAFTAR ISI


Halaman Judul ..... i

Halaman Persetujuan ..... ii

Halaman Pengesahan ..... iii

Motto dan Persembahan ..... iv

Daftar Kontribusi ..... v

Kata Pengantar ..... vii

Daftar Isi ..... ix

Daftar Tabel ..... xi

Daftar Gambar ..... xii

Abstraksi ..... xiv

**BAB I PENDAHULUAN** ..... 1

A. Latar Belakang Masalah ..... 1

B. Rumusan Masalah ..... 3

C. Batasan Masalah ..... 3

D. Tujuan Penelitian ..... 4

E. Manfaat Penelitian ..... 4

F. Sistematika Penulisan ..... 4

**BAB II TINJAUAN PUSTAKA** ..... 6

A. Telaah Penelitian ..... 6

B. Landasan Teori ..... 7

1. *FreeBSD* ..... 7

2. *Intrusion Detection System* ..... 9

3. *Snort* ..... 11

4. *Basic Analysis and Security Engine* ..... 21

5. *Damn Vurnerable Web Application* ..... 22

**BAB III METODE PENELITIAN** ..... 24

A. Waktu dan Tempat ..... 24

B. Perangkat Penelitian ..... 25

C. Alur Penelitian ..... 26

1. Installasi dan Konfigurasi *FreeBSD* ..... 30

2. Installasi software pendukung ..... 32

3. Installasi dan Konfigurasi *Snort* ..... 33

4. Persiapan database ..... 34

5. Installasi BASE ..... 35

6. Konfigurasi rule *Snort* ..... 37

7. Pengujian sistem IDS *Snort* ..... 38

**BAB IV HASIL DAN PEMBAHASAN** ..... 43

A. Hasil Penelitian ..... 43

B. Pembahasan ..... 61

**BAB V KESIMPULAN DAN SARAN** ..... 65

A. Kesimpulan ..... 65

B. Saran ..... 66

**DAFTAR PUSTAKA** ..... 68

Lampiran ..... 69

# DAFTAR TABEL

Tabel 3.1. Alokasi waktu penelitian ..... 24

Tabel 3.2. Spesifikasi perangkat yang digunakan ..... 25

Tabel 4.1. Perbandingan hasil pengujian *Snort* IDS ..... 62

# DAFTAR GAMBAR


Gambar 2.1. Skema jaringan *Snort NIDS* ..... 13

Gambar 2.2. Skema jaringan *Snort HIDS* ..... 15

Gambar 2.3. Skema jaringan *Snort DIDS* ..... 16

Gambar 2.4. Komponen IDS *Snort* ..... 18

Gambar 2.5. Contoh penulisan rule *Snort* ..... 19

Gambar 2.6. Contoh tampilan BASE ..... 22

Gambar 2.7. Contoh tampilan web DVWA v1.0.7 ..... 23

Gambar 3.1. Skema jaringan penelitian ..... 27

Gambar 3.2. Diagram Alir Penelitian ..... 28

Gambar 3.3. Diagram Alir Perancangan dan Pengujian ..... 29

Gambar 3.4. Konfigurasi kartu jaringan server ..... 30

Gambar 3.5. Opsi tambahan pada konfigurasi kernel ..... 31

Gambar 3.6. Informasi kernel server ..... 31

Gambar 3.7. Pengaturan network *Snort* ..... 33

Gambar 3.8. *ERD Diagram* database *Snort* ..... 34

Gambar 3.9. Grant akses database pengguna *Snort* ..... 35

Gambar 3.10. Daftar tabel tambahan database *Snort* ..... 37

Gambar 3.11. File *local.rules Snort* untuk pengujian ..... 38

Gambar 4.1. Pengujian port scan dengan *Zenmap* ..... 43

Gambar 4.2. Rule Snort untuk deteksi *nmap port scan* ..... 45

Gambar 4.3. Peringatan *Snort* untuk pengujian *port scan* ..... 46

Gambar 4.4. Pengujian EICAR virus test ..... 47

Gambar 4.5. Rule *Snort* untuk deteksi EICAR virus test ..... 48

Gambar 4.6. Deteksi *Snort* terhadap EICAR virus test ..... 49

Gambar 4.7. Pengujian *buffer overflow* ..... 50

Gambar 4.8. Rule *Snort* untuk deteksi *buffer overflow* ..... 51

Gambar 4.9. Deteksi *Snort* terhadap uji *buffer overflow* ..... 52

Gambar 4.10 . Injeksi untuk informasi user ..... 53

Gambar 4.11 . Injeksi informasi database ..... 54

Gambar 4.12 . Hasil injeksi skema tabel database ..... 55

Gambar 4.13. Ekstraksi username dan password ..... 56

Gambar 4.14. Rule *Snort* untuk *SQL Injection* ..... 57

Gambar 4.15. Deteksi *Snort SQL Injection attack* ..... 58

Gambar 4.16. Pengujian pengaksesan database ..... 59

Gambar 4.17. Rule *Snort* untuk deteksi pengaksesan database ..... 60

Gambar 4.18. Peringatan *Snort* untuk uji akses database ..... 60

# ABSTRAKSI

Sistem keamanan jaringan pada perusahaan *Internet Service Provider* (ISP) merupakan faktor penting untuk menjamin stabilitas, integritas dan validitas data. Implementasi *Intrusion Detection System* berbasis *Snort* dapat menghemat biaya pengadaan software karena bersifat gratis dan cukup handal dalam mendeteksi serangan keamanan.

Sistem IDS berbasis *Snort* dapat di-implementasikan pada sistem operasi *FreeBSD* yang banyak dipakai sebagai sistem operasi server di PT. Power Telecom cabang Solo. Pengaturan utama *Snort* terutama pada pengaturan jaringan dan rule Snort yang ada. Sebuah serangan dapat terdeteksi atau tidak oleh *Snort IDS*, tergantung dari ada atau tidaknya rule yang sesuai. Pengujian pada sistem IDS dilakukan dengan beberapa pola serangan untuk menguji kehandalan *Snort* dalam mendeteksi sebuah serangan terhadap sistem keamanan.

Berdasarkan hasil pengujian sistem *Snort IDS* dengan *port scan*, tes virus, *buffer overflow*, *SQL Injection*, dan pengaksesan database, *Snort* dapat memberikan peringatan adanya serangan keamanan terhadap sistem jaringan. Hasil peringatan tersebut dapat digunakan sebagai acuan untuk menentukan kebijakan keamanan jaringan perusahaan.

Kata Kunci: *FreeBSD, Intrusion Detection System, Snort*.