

HALAMAN PENGESAHAN

PENERAPAN SNORT SEBAGAI *HOST INTRUSION DETECTION SYSTEM* DI UBUNTU SERVER 10.04

Dipertahankan di Depan Dewan Penguji Tugas Akhir Sekolah Tinggi
Manajemen Informatika dan Komputer AKAKOM Yogyakarta
dan Dinyatakan Diterima untuk Memenuhi Syarat Guna Memperoleh

Gelar Ahli Madya

Pada Hari :

Tanggal :

Mengetahui,

Ketua Jurusan Teknik Komputer

LN. Harnaningrum, S.Si, M.T

Menyetujui,

Dosen Pembimbing

Totok Budioko, S.T, M.T

Halaman Persembahan

Laporan tugas akhir ini dipersembahkan kepada **Ayah , Ibu dan Keluarga** yang selalu memberikan motivasi dan dorongan serta memberikan doa kepada penulis agar sukses dalam menempuh pendidikannya. **Bapak Totok Budioko, S.T, M.T** yang telah memberikan bimbingan kepada penulis. **Dosen STMIK Akakom** yang telah membina penulis dalam menempuh pendidikan di kampus tercinta ini. **Teman-teman** seperjuangan jurusan Teknik Komputer yang tidak dapat saya sebutkan satu-persatu, tetap semangat.

MOTTO

- ❖ Semua amal tergantung pada niat, maka niatkan setiap amal dengan niat yang baik.
- ❖ Orang-orang yang berhenti belajar akan menjadi pemilik masa lalu, orang-orang yang masih terus belajar akan menjadi pemilik masa depan.
- ❖ Sabar dalam mengatasi kesulitan dan bertindak bijaksana dalam mengatasinya adalah sesuatu yang utama.
- ❖ The quitter you become, the more you able to hear.

KATA PENGANTAR

Puji dan syukur dipanjatkan ke hadirat Allah SWT yang telah melimpahkan rahmat-Nya sehingga penulis dapat menyusun laporan tugas akhir dengan judul “PENERAPAN SNORT SEBAGAI HOST INTUSION DETECTION SYSTEM DI UBUNTU SERVER 10.04” ini dengan lancar.

Tujuan dari penulisan laporan tugas akhir ini adalah untuk memenuhi syarat dalam menyelesaikan program studi Teknik Komputer STMIK Akakom serta untuk menambah wawasan tentang penerapan snort sebagai host intusion detection system bagi penulis khususnya dan pembaca pada umumnya.

Atas segala bimbingan, dorongan dan bantuan yang secara langsung maupun tidak langsung yang telah diberikan, penulis menyampaikan terima kasih yang sebesar-besarnya kepada :

1. Bapak Sigit Anggoro, S.T, M.T. selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer AKAKOM Yogyakarta.
2. Bapak Drs. Berta Bednar, M.T. selaku Pembantu Ketua I Bidang Akademik di Sekolah Tinggi Manajemen Informatika dan Komputer AKAKOM Yogyakarta.
3. Ibu LN. Harnaningrum, S.Si, M.T selaku Ketua Jurusan Teknik Komputer di Sekolah Tinggi Manajemen Informatika dan Komputer AKAKOM Yogyakarta.

4. Bapak Totok Budioko, S.T, M.T. selaku dosen pembimbing tugas akhir.
5. Seluruh staf dan karyawan STMIK AKAKOM Yogyakarta yang banyak membantu lancarnya segala aktivitas penulisan karya tulis.
6. Semua pihak yang telah membantu sampai terselesaikannya penyusunan laporan tugas akhir ini.

Penulis menyadari bahwa penyajian laporan ini masih ada kekurangan. Oleh karena itu, saran dan kritik membangun sangat penulis perlukan demi penyajian laporan yang lebih baik di masa yang akan datang. Semoga laporan ini dapat bermanfaat bagi semua pembaca.

Yogyakarta, Juli 2012

Penulis,

Suyadi

DAFTAR ISI

| | |
|---------------------------|-----|
| Halaman Judul | i |
| Halaman Pengesahan | ii |
| Halaman Persembahan | iii |
| Motto | iv |
| Kata Pengantar..... | v |
| Daftar Isi | vii |
| Daftar Gambar | x |

BAB I PENDAHULUAN

| | |
|----------------------------------|---|
| 1.1 Latar Belakang Masalah | 1 |
| 1.2 Rumusan Masalah | 2 |
| 1.3 Tujuan | 2 |
| 1.4 Batasan Masalah | 2 |

BAB II ANALISIS DAN PERANCANGAN

| | |
|---|----|
| 2.1 Analisis..... | 4 |
| 2.1.1 <i>Intrusion Detection System</i> | 4 |
| 2.1.1.1 Snort | 5 |
| 2.1.1.2 Prinsip Kerja Snort..... | 6 |
| 2.1.1.3. <i>Rule</i> Snort..... | 7 |
| 2.1.2 <i>Flag</i> TCP | 10 |
| 2.1.3 <i>Three Way Handshake</i> | 11 |

| | |
|------------------|----|
| 2.2 Diagram..... | 13 |
|------------------|----|

BAB III IMPLEMENTASI

| | |
|--|----|
| 3.1. Proses Instalasi..... | 14 |
| 3.2. Konfigurasi..... | 14 |
| 3.2.1. Konfigurasi Ubuntu Server..... | 14 |
| 3.2.2. Konfigurasi Snort..... | 16 |
| 3.2.2.1 Konfigurasi Snort Untuk Mendeteksi Intrusi Ke Beberapa Host Tertentu..... | 15 |
| 3.2.3. Konfigurasi Backtrack5 r1..... | 21 |
| 3.3. Menjalankan Snort..... | 21 |
| 3.4. Penetrasi..... | 22 |
| 3.4.1. <i>Port Scanning</i> | 23 |
| 3.4.2. DoS (<i>Denial of Service</i>)..... | 26 |
| 3.5. Melihat Hasil Monitoring..... | 30 |
| 3.5.1. Melihat <i>alert</i> dari serangan <i>port scanning</i> dan DoS. | 31 |
| 3.5.2. Melihat <i>alert port scanning</i> ke host tertentu..... | 32 |
| 3.5.3. Melihat <i>log</i> dari serangan <i>port scanning</i> dan DoS... | 33 |
| 3.5.4. Melihat <i>log port scanning</i> ke beberapa host tertentu | 36 |

BAB IV PENUTUP

| | |
|-----------------------|----|
| 4.1. Kesimpulan | 38 |
|-----------------------|----|

4.2. Saran-saran..... 38

DAFTAR PUSTAKA..... 39

LAMPIRAN

DAFTAR GAMBAR

| | | |
|--------------------|--|----|
| Gambar 2.1 | Prinsip kerja Snort..... | 7 |
| Gambar 2.2 | Contoh struktur <i>rule</i> Snort..... | 10 |
| Gambar 2.3 | Ilustrasi <i>three way handshake</i> | 12 |
| Gambar 2.4 | Rancangan jaringan..... | 13 |
| Gambar 2.5 | Rancangan jaringan kasus mendeteksi serangan ke beberapa host tertentu..... | 13 |
| Gambar 3.1 | Hasil konfigurasi <i>interface</i> jaringan..... | 15 |
| Gambar 3.2 | Konfigurasi <i>interface</i> jaringan Backtrack5 r1..... | 21 |
| Gambar 3.3 | Snort berjalan pada mode IDS..... | 22 |
| Gambar 3.4 | <i>Scan</i> FIN pada port yang terbuka..... | 24 |
| Gambar 3.5 | <i>Scan</i> FIN pada port yang tertutup..... | 24 |
| Gambar 3.6 | <i>Port scanning</i> dengan Nmap..... | 25 |
| Gambar 3.7 | <i>Port scanning</i> oleh <i>host</i> 10.0.2.9..... | 21 |
| Gambar 3.8 | Ilustrasi cara kerja serangan <u>Denial of Service</u> dengan menggunakan metode SYN <i>Flooding Attack</i> | 29 |
| Gambar 3.9 | DoS menggunakan hping3..... | 30 |
| Gambar 3.10 | File <i>output</i> Snort pada /var/log/snort..... | 30 |
| Gambar 3.11 | <i>Alert</i> yang dihasilkan..... | 32 |
| Gambar 3.12 | <i>Alert</i> yang dihasilkan dari <i>port scanning</i> ke <i>host</i> 10.0.2.2 | 33 |

Gambar 3.13 Melihat file *log* yang dihasilkan..... 35

Gambar 3.14 Melihat file *log port scanning* ke beberapa host tertentu... 37