

**PENINGKATAN KEAMANAN JARINGAN BERBASIS
INTRUSION DETECTION SYSTEM
(STUDI KASUS UNIVERSITAS SAHID SURAKARTA)**

TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat
Mencapai Gelar Sarjana Komputer
Program Studi Teknik Informatika
Universitas Sahid Surakarta



Disusun Oleh:

DARNO
NIM. 2012061009

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS SAHID SURAKARTA
2016**

**SURAT PERNYATAAN
ORISINALITAS KARYA ILMIAH**

Saya mahasiswa Program Studi Teknik Informatika Fakultas Teknik Universitas Sahid Surakarta yang bertanda tangan dibawah ini,

Nama : Darno

NIM : 2012061009

Menyatakan dengan sesungguhnya bahwa Tugas Akhir / Skripsi

JUDUL : Peningkatan Keamanan Jaringan Berbasis *Intrusion Detection System* (Studi Kasus Universitas Sahid Surakarta)

adalah benar-benar karya yang saya susun sendiri. Apabila kemudian terbukti bahwa saya ternyata melakukan tindakan menyalin atau meniru tulisan/ karya orang lain seolah-olah hasil pemikiran saya sendiri, saya bersedia menerima sanksi sesuai peraturan yang berlaku di Universitas termasuk pencabutan gelar yang telah saya peroleh.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya dan apabila dikemudian hari terbukti melakukan kebohongan maka saya sanggup menanggung segala konsekuensinya.

Surakarta, 30 Maret 2016

Yang Menyatakan



(DARN0)

NIM : 2012061009

**PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS**

Sebagai Sivitas Akademik Universitas Sahid Surakarta, Saya yang bertanda tangan di bawah ini :

NAMA : Darno

NIM : 2012061009

Program Studi : Teknik Informatika

Fakultas : Fakultas Teknik

Jenis Karya : Tugas Akhir/Skripsi/Laporan Penelitian*

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Sahid Surakarta Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty Free Right*) atas Tugas Akhir/Skripsi/Laporan Penelitian* saya yang berjudul : Peningkatan Keamanan Jaringan Berbasis *Intrusion Detection System* (Studi Kasus Universitas Sahid Surakarta).

Beserta instrument/desain/perangkat (jika ada). Berhak menyimpan, mengalihkan bentuk, mengalihmediakan, mengelola dalam bentuk pangkalan data (*database*), merawat serta mempublikasikan karya ilmiah saya selama tetap mencantumkan nama saya sebagai penulis (*autor*) dan Pembimbing sebagai *co autor* atau pencipta dan juga sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sesungguhnya secara sadar tanpa paksaan dari pihak manapun.

Dibuat di : Surakarta

Pada Tanggal : 30 Maret 2016

Yang membuat pernyataan,



DARNO

NIM :2012061009

*) coret yang tidak perlu

LEMBAR PERSETUJUAN
PENINGKATAN KEAMANAN JARINGAN BERBASIS
INTRUSION DETECTION SYSTEM
(STUDI KASUS UNIVERSITAS SAHID SURAKARTA)

Disusun Oleh:

DARNO
NIM.2012061009

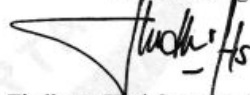
Tugas Akhir ini telah disetujui untuk dipertahankan
di hadapan dewan penguji
pada tanggal 17 Maret 2016

Pembimbing I



Ir. Dahlan Susilo, M.Kom
NIDN : 0614016701

Pembimbing II



Firdhaus Hari Saputro A H, ST
NIDN : 0614068201



Mengetahui,
Ketua Program Studi

Firdhaus Hari Saputro A H, ST
NIDN : 0614068201

LEMBAR PENGESAHAN




PENINGKATAN KEAMANAN JARINGAN BERBASIS *INTRUSION DETECTION SYSTEM* (STUDI KASUS UNIVERSITAS SAHID SURAKARTA)

Disusun Oleh:

DARNO
NIM.2012061009

Tugas Akhir ini telah diterima dan disahkan
oleh dewan penguji Tugas Akhir
Program Studi Teknik Informatika
Universitas Sahid Surakarta
pada hari Rabu tanggal 30 Maret 2016

Dewan Penguji

- | | | |
|----------------|--|---|
| 1. Penguji I | Ir. Dahlan Susilo, M.Kom NIDN : 0614016701 |  |
| 2. Penguji II | Firdhaus Hari Saputro A H, ST NIDN : 0614068201 |  |
| 3. Penguji III | Sri Huning A., S.T., M.Kom NIDN : 0017067901 |  |

Mengetahui,

Ketua Program Studi
Teknik Informatika



Firdhaus Hari Saputro A H, ST
NIDN : 0614068201

Dekan
Fakultas Teknik



Ir. Dahlan Susilo, M.Kom
NIDN : 0614016701

KATA PENGANTAR

Bismillaahirrahmaanirrahiim

Puji dan syukur selalu penulis panjatkan kepada Allah SWT atas segala karunia, rahmat, kekuatan, kesabaran dan hidayat-Nya serta petunjuk dan kemudahan sehingga penulis dapat menyelesaikan Tugas Akhir ini untuk memenuhi salah satu persyaratan guna memperoleh Gelar Sarjana Program Studi Teknik Informatika Universitas Sahid Surakarta dengan judul “Peningkatan Keamanan Jaringan Berbasis Intrusion Detection System (Studi Kasus Universitas Sahid Surakarta)” dengan baik. Shalawat serta salam selalu kita haturkan kepada junjungan kita Nabi besar Muhammad SAW. beserta keluarganya, para sahabatnya dan para pengikutnya.

Penulis mengucapkan terima kasih kepada pihak-pihak yang telah membantu dalam penyelesaian Tugas Akhir ini yang diantaranya:

1. Bapak Prof. Dr. Trisno Martono, MM. selaku Rektor Universitas Sahid Surakarta.
2. Bapak Ir. Dahlan Susilo, M.Kom selaku Ketua Dekan Fakultas Teknik Universitas Sahid Surakarta sekaligus sebagai Pembimbing I.
3. Bapak Firdhaus Hari Saputro A H, ST. selaku Ketua Program Studi Teknik Informatika Universitas Sahid Surakarta sekaligus sebagai Pembimbing II.
4. Bapak, Ibu, dan Adikku yang tercinta dan tersayang terima kasih atas do'a dan dukungannya.

Semoga Laporan Tugas Akhir ini dapat bermanfaat bagi pembaca dan Universitas Sahid Surakarta sehingga dapat dikembangkan menjadi lebih baik lagi. Kritik serta sarannya sangat penulis harapkan untuk kesempurnaan dalam Tugas Akhir ini.

Surakarta, 30 Maret 2016

Penulis

MOTTO

Jangan lupakan Tuhan walau selagi bahagia.

Jauhkan diri dari sifat malas karena malas akan menunda kesuksesan.

Tataplah kedepan untuk meju gerbang meraih kesuksesan

Niat adalah sumber kekuatan.

Orang Tua adalah semangat untuk maju.

Bersabarlah dan yakin.

DAFTAR ISI

| | |
|---|----|
| 2.1.2.2. Metode Analisis <i>Event</i> IDS | 9 |
| 2.1.2.2.1. <i>Signature Based</i> | 9 |
| 2.1.2.2.2. <i>Anomaly Based</i> | 9 |
| 2.1.2.3. Cara Kerja IDS | 9 |
| 2.1.3. <i>Snort</i> | 9 |
| 2.1.3.1. Komponen <i>Snort</i> | 10 |
| 2.1.3.2. <i>Sniffer Mode</i> | 13 |
| 2.1.3.3. <i>Packet Logger Mode</i> | 14 |
| 2.1.3.4. <i>Intrusion Detection Mode</i> | 14 |
| 2.1.4. <i>Firewall</i> | 16 |
| 2.1.5. Jenis-jenis Serangan | 19 |
| 2.2. Kerangka Berfikir | 20 |
| | |
| BAB III ANALISIS DAN PERANCANGAN SISTEM | 22 |
| 3.1. Analisis Sistem | 22 |
| 3.1.1. Analisis Sistem yang Berjalan Saat Ini | 23 |
| 3.1.1.1. Analisis <i>Hardware</i> dan Struktur Jaringan Komputer . | 23 |
| 3.1.1.2. Analisis <i>Software</i> | 24 |
| 3.1.1.3. Analisis Jaringan Internet dan Keamanannya | 25 |
| 3.1.1.4. Sistem Kerja Jaringan Komputer Yang Sedang Berjalan | 27 |
| 3.1.2. Analisis Sistem Yang baru | 28 |
| 3.1.2.1. Analisis <i>Hardware</i> dan Struktur Jaringan Yang Baru . | 29 |
| 3.1.2.2. Analisis <i>Software</i> Pada Sistem Yang Baru | 31 |
| 3.1.2.2.1. Snort dan IDScenter | 31 |
| 3.1.2.2.2. WinPcap | 32 |
| 3.1.2.2.3. Winbox | 32 |
| 3.2. Perancangan Sistem | 32 |
| 3.2.1. Perancangan Sistem Yang Akan Diterapkan | 32 |
| 3.2.2. Cara Kerja Pengamanan Jaringan | 33 |
| | |
| BAB IV IMPLEMENTASI DAN ANALISIS HASIL | 36 |

| | |
|---|----|
| 4.1. Implementasi Sistem Keamanan Jaringan | 36 |
| 4.1.1. Inisialisasi dan Konfigurasi Snort | 36 |
| 4.1.2. Simulasi Pada Oracle VM VirtualBox | 38 |
| 4.1.2.1. Simulasi Penyerangan (<i>intrusion</i>) Melalui <i>Attacker</i> .. | 39 |
| 4.1.2.2. Hasil Simulasi Oleh <i>Router</i> atau <i>Server</i> Dengan Snort | 40 |
| 4.1.2.3. Hasil Simulasi Oleh <i>Router</i> atau <i>Server</i> Dengan Winbox | 40 |
| 4.1.2.4. Simulasi Penanganan Serangan Melalui Winbox | 43 |
| 4.2. Implementasi <i>Intrusion Detection System</i> (IDS) di Universitas Sahid Surakarta | 45 |
| 4.2.1. Penerapan Snort | 46 |
| 4.2.2. Pemberian <i>Intrusion</i> atau Serangan | 46 |
| 4.2.3. Hasil Laporan Dari Snort | 47 |
| 4.2.3.1. Penyimpanan Hasil Analisis Dari Snort | 47 |
| 4.2.3.2. Membaca IP <i>Attacker</i> | 48 |
| 4.2.4. Penanganan Serangan | 49 |
| 4.2.4.1. Penanganan Melalui Winbox | 49 |
| 4.2.4.2. Konfigurasi Pada IDSCenter | 50 |
| 4.2.4.2.1. Konfigurasi Menu <i>General (Configuration)</i> .. | 50 |
| 4.2.4.2.2. Konfigurasi Menu <i>General (Snort Option)</i> | 51 |
| 4.2.4.2.3. Konfigurasi Menu <i>General (Activity Log)</i> | 52 |
| 4.2.4.2.4. Konfigurasi Menu <i>Wizard (network</i> <i>variables)</i> | 52 |
| 4.2.4.2.5. Konfigurasi Menu <i>Wizard (output plugins)</i> ... | 53 |
| 4.2.4.2.6. Konfigurasi Menu <i>Wizard (Rule Signatures)</i> . | 55 |
| 4.2.4.2.7. Konfigurasi Menu <i>Log (Option, Active</i> <i>Snort inline)</i> | 57 |
| 4.2.4.2.8. Konfigurasi Menu <i>Log (Log Rotation)</i> | 58 |
| 4.2.4.2.9. Konfigurasi Menu <i>Alerts(Alert detection)</i> | 59 |
| 4.2.5. Penanganan Oleh <i>Router</i> atau <i>Server</i> Dengan IDSCenter | 60 |

| | |
|---|----|
| 4.3. Pengujian Sistem | 61 |
| 4.3.1. Pengujian Sistem <i>Server</i> dan <i>Client</i> | 61 |
| 4.3.1.1. Pengujian <i>Server</i> | 61 |
| 4.3.1.2. Pengujian <i>Client</i> | 62 |
| 4.3.2. Deteksi Alamat IP <i>Attacker</i> Melalui Snort | 62 |
| 4.4. Analisis Hasil Pengujian | 63 |
| BAB V SIMPULAN DAN SARAN | 66 |
| 5.1. Simpulan | 66 |
| 5.2. Saran | 66 |
| DAFTAR PUSTAKA | 68 |
| LAMPIRAN | 69 |

DAFTAR GAMBAR

| | Halaman |
|---|---------|
| Gambar 2.1 Komponen <i>Snort</i> | 10 |
| Gambar 2.2 Desain Fungsi <i>Firewall</i> | 18 |
| Gambar 2.2 Kerangka Pemikiran | 21 |
| Gambar 3.1 Struktur Perangkat Keras dan Jaringan di Usahid | 23 |
| Gambar 3.2 Aplikasi Winbox v2.2.16 | 24 |
| Gambar 3.3 Fasilitas atau Menu Pada Winbox V2.2.16 | 26 |
| Gambar 3.4 Desain Penggunaan IP Address | 26 |
| Gambar 3.5 Desain Penggunaan Pengamanan Jaringan Melalui <i>Username</i> dan <i>Password</i> | 27 |
| Gambar 3.6 Fungsi dan Peran <i>Server</i> | 28 |
| Gambar 3.7 Penambahan <i>Firewall</i> dan <i>Alert</i> | 29 |
| Gambar 3.8 Struktur Perangkat Keras dan Jaringan di Usahid Yang Baru | 30 |
| Gambar 3.9 Sistem Pada <i>Router</i> atau <i>Server</i> | 30 |
| Gambar 3.10 Aplikasi <i>Snort</i> | 31 |
| Gambar 3.11 Menu-menu Pada <i>IDScener</i> | 32 |
| Gambar 3.12 Alur Proses Penyerangan Hingga Penanganannya | 33 |
| Gambar 4.1 Inisialisasi <i>Snort</i> | 36 |
| Gambar 4.2 Pemanggilan <i>Snort.conf</i> Untuk Melakukan Konfigurasi | 37 |
| Gambar 4.3 Konfigurasi <i>Snort.conf</i> | 37 |
| Gambar 4.4 Contoh Konfigurasi Pada <i>Snort.conf</i> | 38 |
| Gambar 4.5 Penyerangan Dengan Aplikasi <i>Loic</i> | 39 |
| Gambar 4.6 Hasil Deteksi Melalui <i>Snort</i> | 40 |
| Gambar 4.7 Paket Data Yang Masuk Sebelum Terjadi Penyerangan | 41 |
| Gambar 4.8 Paket Data Yang Masuk Setelah Terjadi Penyerangan | 41 |
| Gambar 4.9 IP <i>Scan</i> Sebelum Terjadi Serangan | 42 |
| Gambar 4.10 IP <i>Scan</i> Setelah Terjadi Serangan | 43 |
| Gambar 4.11 Pemutusan Hak Akses Melalui IP Firewall | 43 |
| Gambar 4.12 Proses Penyaringan IP | 44 |

| | |
|--|----|
| Gambar 4.13 Pemberian Tindakan (<i>action</i>) Pada IP <i>Attacker</i> | 44 |
| Gambar 4.14 Konfigurasi <i>Snort.conf</i> Untuk IP <i>Home</i> dan IP DNS | 45 |
| Gambar 4.15 Serangan Pengguna Menuju <i>Router</i> | 46 |
| Gambar 4.16 Hasil pelaporan dari <i>Snort</i> | 47 |
| Gambar 4.17 Penyimpanan Aktivitas <i>Snort</i> Dalam <i>Log</i> | 48 |
| Gambar 4.18 Terjadi Penyerangan | 48 |
| Gambar 4.19 Pemutusan Hak Akses Melalui <i>Firewall</i> | 49 |
| Gambar 4.20 Memanggil <i>Snort</i> dan Menyimpan <i>Log</i> | 51 |
| Gambar 4.21 <i>Snort Option</i> atau Konfigurasi <i>Snort</i> melalui <i>IDScenter</i> | 51 |
| Gambar 4.22 <i>Activity Log</i> | 52 |
| Gambar 4.23 <i>Network Variable</i> | 53 |
| Gambar 4.24 Pembuatan <i>Output Plugins</i> Baru | 53 |
| Gambar 4.25 Hasil Pembuatan <i>Output Plugins</i> | 54 |
| Gambar 4.26 Konfigurasi Menu <i>Syslog Alert Plugin</i> | 55 |
| Gambar 4.27 Hasil Konfigurasi <i>Output Plugin</i> | 55 |
| Gambar 4.28 Konfigurasi <i>Rule</i> atau <i>Signatures</i> | 56 |
| Gambar 4.29 Pengisian <i>Rule</i> Dengan <i>Rule Wizard</i> | 56 |
| Gambar 4.30 Hasil Pengisian <i>Rule</i> Dengan <i>Rule Wizard</i> | 57 |
| Gambar 4.31 Pemilihan Mode <i>Snort Inline</i> | 58 |
| Gambar 4.32 Pemilihan Waktu Untuk <i>Reload Snort</i> | 58 |
| Gambar 4.33 <i>Alert Detection</i> | 59 |
| Gambar 4.34 <i>Alert notification</i> | 60 |
| Gambar 4.35 Konfigurasi <i>IDScenter</i> Berjalan | 61 |
| Gambar 4.36 <i>Log</i> Saat Terjadi Serangan Dari <i>Attacker</i> | 62 |
| Gambar 4.37 Grafik Jumlah <i>Dropped</i> dan <i>Received</i> | 64 |
| Gambar 4.38 Grafik Jumlah Paket | 64 |
| Gambar 4.39 Grafik Jumlah <i>Analyzed</i> | 65 |

DAFTAR TABEL

| | Halaman |
|--|---------|
| Tabel 2.1 Perintah <i>Sniffer Mode</i> | 13 |
| Tabel 2.2 <i>Packet Logger Mode</i> | 14 |
| Tabel 2.3 Pencarian Penyusup | 15 |
| Tabel 2.4 Pengiriman <i>Alert</i> ke <i>Syslog</i> | 15 |
| Tabel 4.1 Perubahan Perintah Pada <i>Snort.conf</i> | 39 |
| Tabel 4.2 Pengujian <i>Server</i> | 61 |
| Tabel 4.3 Hasil Deteksi Dari <i>Snort</i> Terhadap <i>Attacker</i> | 63 |

DAFTAR ISTILAH

Administrator = Petugas IT

| | |
|-----------------------|---|
| <i>Attacker</i> | = Serangan atau penyerang |
| <i>Alert</i> | = Peringatan |
| <i>Firewall</i> | = Pembatas untuk pengamanan jaringan dalam dan luar |
| IDS | = <i>Intrusion Detection System</i> (sistem mendeteksi gangguan atau penyerangan) |
| IDScenter | = Aplikasi dari IDS untuk memberi tindakan untuk penyerang |
| <i>Log</i> | = Pencatatan aktifitas |
| Loic | = Aplikasi untuk melakukan penyerangan |
| <i>Router/ server</i> | = Sebuah alat untuk mengatur jalur jaringan |
| <i>Rule</i> | = Pengaturan atau berkas pengaturan |
| Snort | = Aplikasi dari IDS untuk deteksi serangan |
| <i>Threads</i> | = Susupan (penyusupan) |
| VirtualBox | = Aplikasi untuk miniatur / replika sistem yang ada |
| Winbox | = Aplikasi Untuk <i>Setting Router</i> |

DAFTAR LAMPIRAN

Lampiran 1 Hasil Deteksi Snort

Lampiran 2 Surat Penelitian

Lampiran 3 Buku Konsultasi

ABSTARCT

Intrusion Detection System (IDS) is a network security methods to investigate attack from attacker to network server Sahid University Surakarta. IDS to help administrators or network operator to determine the activities of the existing network of Sahid University Surakarta. IDS is using a tool or method-based security Intrusion Detection System (IDS) with the main application is Snort as detection systems and the use of supporting applications that WinPcap to arrest data packets passing through the router, Winbox to cut off access rights attacker manually and IDScener to decide right attacker access automatically. If there was an attack, the administrator can grant permissions disconnection actions of the attacker's IP address (attacker) Winbox or application IDScener will automatically break the attacker's IP address (attacker). The result of the of IDS are dealing with the abuse of network access rights of users and their security intrusion detection system based networks of Sahid University Surakarta will stable with an average speed of Internet access for each user 200 Kbps.

Key Word : *Attacker, IDS, IDScener, Intrusion, Network Scurity, Snort, Threads.*

ABSTRAK

Intrusion Detection System (IDS) adalah sebuah metode pengamanan jaringan untuk mengetahui adanya penyerangan dari *attacker* terhadap *server* jaringan Universitas Sahid Surakarta. Penerapan IDS ini bertujuan untuk membantu *administrator* atau *operator* jaringan untuk mengetahui aktivitas jaringan yang ada di Universitas Sahid Surakarta. Penerapan IDS ini menggunakan *tool* atau metode pengamanan berbasis *Intrusion Detection System (IDS)* dengan aplikasi utama yaitu Snort sebagai sistem deteksi dan menggunakan aplikasi pendukung yaitu WinPcap untuk penangkapan paket data yang melewati *router*, Winbox untuk memutus hak akses *attacker* secara *manual* dan IDScenter untuk memutus hak akses *attacker* secara otomatis. Jika terjadi penyerangan maka *administrator* dapat memberi tindakan pemutusan hak akses dari alamat IP penyerang (*attacker*) melalui Winbox atau aplikasi IDScenter akan memutus secara otomatis alamat IP penyerang (*attacker*). Hasil penerapan IDS ini adalah menangani penyalahgunaan hak akses jaringan atau penyerangan dari pengguna sehingga dapat membantu jaringan Universitas Sahid Surakarta lebih stabil dengan kecepatan rata-rata akses internet setiap pengguna 200 Kbps.

Kata Kunci : *Attacker*, IDS, IDScenter, *Intrusion*, Keamanan jaringan, Snort, *Threads*.