



**UJI IMPLEMENTASI KEAMANAN JARINGAN DENGAN METODE
INTRUSION DETECTION SISTEM
(STUDI KASUS : LAB FASILKOM MERCU BUANA)**

DISUSUN OLEH :

Danang Eko Prayogo

41514010011

**UNIVERSITAS
MERCU BUANA**

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA**

2017



**UJI IMPLEMENTASI KEAMANAN JARINGAN DENGAN METODE INTRUSION
DETECTION SISTEM
(STUDI KASUS : LAB FASILKOM MERCU BUANA)**

Laporan Tugas Akhir

Diajukan untuk Melengkapi Salah Satu Syarat Memperoleh Gelar
Sarjana Strata Satu (1) Komputer

UNIVERSITAS
MERCU BUANA

Disusun Oleh :

Danang Eko Prayogo

41514010011

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA**

2017

i

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini :

NIM : 41514010011

Nama : Danang Eko Prayogo

Judul : Uji Implementasi Keamanan Jaringan Dengan Metode Intrusion Detection Sistem (Studi Kasus: Lab Fasilkom Mercu Buana Jakarta)

Menyatakan bahwa Tugas Akhir dengan judul tersebut adalah hasil karya saya sendiri dan bukan plagiat kecuali kutipan-kutipan dan teori-teori yang digunakan dalam skripsi ini. Apabila ternyata ditemukan di dalam Laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 11 Desember 2017

Hormat saya,



Danang Eko Prayogo

UNIVERSITAS
MERCU BUANA

LEMBAR PERSETUJUAN

Nama : Danang Eko Prayogo
NIM : 41514010011
Jurusan : Informatika
Fakultas : Ilmu Komputer
Judul : Uji Implementasi Keamanan Jaringan Dengan Metode Intrusion Detection
Sistem (Studi Kasus: Lab Fasilkom Mercu Buana Jakarta)

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI

Jakarta, 11 Desember 2017

Disetujui dan diterima oleh,



UNIVERSITAS

Dr. Harwikarya

Dosen Pembimbing

MERCU BUANA

LEMBAR PERSETUJUAN

Nama : Danang Eko Prayogo
NIM : 41514010011
Jurusan : Informatika
Fakultas : Ilmu Komputer
Judul : Uji Implementasi Keamanan Jaringan Dengan Metode Intrusion Detection
Sistem (Studi Kasus: Lab Fasilkom Mercu Buana Jakarta)

Jakarta, 11 Desember 2017

Disetujui dan diterima oleh,



Dr. Harwikarya
Dosen Pembimbing



UNIVERSITAS
MERCU BUANA

Desi Ramayanti S.Kom., MT.

Kaprodi Informatika

Andi Nugroho ST., M.Kom

Koordinator Tugas Akhir

KATA PENGANTAR

Puji syukur kehadiran Allah subhanahu wa ta'ala atas petunjuk, rahmat, dan hidayahNya sehingga penulis dapat menyelesaikan laporan Tugas Akhir dengan judul “Uji Implementasi Keamanan Jaringan Dengan Metode Intrusion Detection Sistem (Studi Kasus: Lab Fasilkom Mercu Buana Jakarta) ” sesuai dengan waktu yang telah ditentukan. Laporan Tugas Akhir ini merupakan salah satu persyaratan untuk dapat menyelesaikan Program Studi Strata 1 (S1) pada Program Studi Informatika Universitas Mercu Buana.

Laporan Tugas Akhir ini masih belum dapat dikatakan sempurna. Karena itu, kritik dan saran akan diterima dengan senang hati. Laporan Tugas Akhir ini dapat selesai tepat pada waktunya atas bantuan, bimbingan, dan motivasi dari berbagai pihak. Maka dari itu, dengan segala kerendahan hati, ucapan terima kasih akan disampaikan kepada:

1. Bapak Dr. Harwikarya, selaku Dosen Pembimbing Tugas Akhir yang telah membimbing dengan nasehat, semangat, dan ilmunya.
2. Bapak Leonard Goeirmanto, ST, M.Sc, selaku Dosen Pembimbing Akademik yang selalu memberikan nasehat kepada mahasiswa/i beliau.
3. Bapak Andi Nugroho ST., M.TI., selaku Koordinator Tugas Akhir Informatika Universitas Mercu Buana.
4. Ibu Desi Ramayanti S.Kom., MT., selaku Kaprodi Informatika Universitas Mercu Buana
5. Kedua orang tua yang selama ini telah membesarkan dan menyemangati penulis.
6. Teman-teman terdekat, Rifki Aditia Ningrum, Tantry Nur Herawati, Luqman Bhakti, Atikah Fatmawati, Group TeamWorkNgops, Group Panik Panik, Group Menuju Hidup Baru yang selalu membantu, mendoakan dan mendukung.
7. Semua pihak yang telah memberikan semangat dan bantuan yang namanya tidak dapat disebutkan satu per satu.

Mohon maaf apabila masih banyak kekurangan dalam penulisan laporan Tugas Akhir ini. Saya sangat mengharapkan kritik dan saran yang dapat membangun. Semoga laporan ini dapat bermanfaat khususnya bagi penulis laporan ini dan pada umumnya bagi para pembaca.



DAFTAR ISI

LEMBAR PERNYATAAN	ii
LEMBAR PERSETUJUAN.....	iii
ABTRAKSI.....	iv
ABSTRACT.....	v
KATA PENGANTAR	vi
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR LAMPIRAN.....	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan dan Manfaat Penelitian	2
1.4 Batasan Penelitian	3
1.5 Metode Penelitian.....	3
1.6 Sistematika Penulisan.....	4
BAB II LANDASAN TEORI.....	5
2.1 Keamanan Jaringan	5
2.1.1 Tujuan Keamanan Jaringan.....	6
2.2 Intrusions Detection System	7
2.2.1 Jenis Intrusions Detection System.....	7
2.3 Jenis Serangan Pada Jaringan.....	8
2.3.1 Port Scanning.....	8
2.3.2 Teardrop.....	9
2.3.3 Spoofing.....	10
2.3.4 Land Attack.....	12
2.3.4 Smurf Attack.....	13
2.3.5 Packet Interuption.....	13

2.4	Snort.....	14
2.5	Komponen Snort	15
2.6	Fitur Snort.....	17
2.7	Firewall.....	19
BAB III Analisa Sistem.....		20
3.1	Analisa Masalah.....	20
3.2	Analisa Sistem.....	21
3.3	Analisa Alur Kerja	21
3.4	Analisa Kebutuhan Sistem	22
3.4.1	Analisa Kebutuhan Perangkat Keras	22
3.4.2	Analisa Kebutuhan Perangkat Lunak	22
BAB IV PERANCANGAN SISTEM IDS.....		23
4.1	Perancangan Sistem	23
4.2	Alur Kerja Intrusion Detection System.....	24
4.3	Instalasi Prerequisites.....	25
4.4	Instalasi Snort.....	27
4.5	Instalasi Barnyard2.....	29
4.6	Instalasi Puledpork.....	31
4.7	Instalasi & Konfigurasi BASE serta ADODB	31
BAB V PENGUJIAN DAN HASIL.....		34
5.1	Metode Pengujian	34
5.2	Functionality Test	34
5.2.1	Port Scan	35
5.2.2	Ping Attack (ICMP Traffic)	35
5.2.3	FTP Attack	36
5.3	Response Time.....	38
5.3.1	Port Scan	38
5.3.2	FTP Attack	39

5.4 Menghitung Nilai QoS Pengiriman Data dari Serangan.....	40
BAB VI PENUTUP	41
6.1 Kesimpulan	41
6.2 Saran.....	41
DAFTAR PUSTAKA	42
LAMPIRAN	43



DAFTAR GAMBAR

Gambar 2.1 (<i>SYN/ACK Scanning Packet Exchange</i>)	9
Gambar 1.2 Teardrop.....	9
Gambar 2.3 Interupsi jawaban dan paket di palsukan.....	11
Gambar 2.4 Pemalsuan Paket	11
Gambar 2.5 Pemalsuan Paket Untuk Pihak Ke Tiga	12
Gambar 2.6 Serangan menggunakan paket palsu secara berulang ulang	12
Gambar 2.7 Diagram Smurf Attack.....	13
Gambar 2.8 Penyadapan Paket	14
Gambar 2.9 Komponen-Komponen Snort.....	16
Gambar 2.10 Linux Sebagai Firewall.....	19
Gambar 3.1 Rancangan Intrusions Detection System	21
Gambar 4.1 Alur Kerja Intrusions Detection System.....	24
Gambar 4.2 Install Libpcap	25
Gambar 4.3 Install Bison Flex.....	25
Gambar 4.4 Install DAQ.....	26
Gambar 4.5 Kompilasi DAQ.....	26
Gambar 4.6 Install Openssl	27
Gambar 4.7 Install libnghttp2.....	27
Gambar 4.8 Instalasi Snort	28
Gambar 4.9 Versi Snort.....	28
Gambar 4.10 Instalasi Barnyard	29
Gambar 4.11 Instalasi Packet Libdumbnet.....	29
Gambar 4.12 Instalasi ke MySQL Library	30
Gambar 4.13 Menyalin berkas barnyard2	30
Gambar 4.14 Membuat Database	30
Gambar 4.15 Instalasi PulledPork	31
Gambar 4.16 Install Image Graph	31

Gambar 4.17 Instalasi Adodb	32
Gambar 4.18 Install Base.....	32
Gambar 4.19 Tampilan Base	33
Gambar 5.1 Ping Attack	36
Gambar 5.2 FTP Attack.....	37
Gambar 5.3 Tampilan serangan di BASE	37
Gambar 5.4 Tampilan Waktu Port Scan.....	38
Gambar 5.5 Tampilan waktu pada BASE	39
Gambar 5.6 Jumlah Paket dan Waktu	40



DAFTAR LAMPIRAN

Lampiran I Surat Riset	46
Lampiran II Kartu Eksistensi	47

