



UNIVERSITAS
MERCU BUANA

ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN KOMPUTER
MENGUNAKAN INTRUSION PREVENTION SYSTEM di PT XYZ



UNIVERSITAS
SHARIF HIDAYAT
41513110003
MERCU BUANA

PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2017



UNIVERSITAS
MERCU BUANA

ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN KOMPUTER
MENGUNAKAN INTRUSION PREVENTION SYSTEM di PT XYZ

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

UNIVERSITAS
MERCU BUANA

SHARIF HIDAYAT

41513110003

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2017

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41513110003

Nama : Sharif Hidayat

Judul Tugas Akhir : Analisis Dan Implementasi Keamanan Jaringan Komputer
Menggunakan Intrusion Prevention System di Pt Xyz

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

Jakarta, September 2017



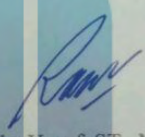
Sharif Hidayat

UNIVERSITAS
MERCU BUANA

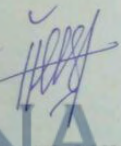
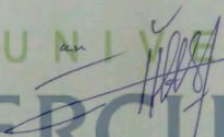
LEMBAR PENGESAHAN

Nama : Sharif Hidayat
NIM : 41513110003
Program Studi : Informatika
Fakultas : Ilmu Komputer
Judul : Analisis Dan Implementasi Keamanan Jaringan Komputer
Menggunakan Intrusion Prevention System di Pt Xyz

Jakarta, September 2017
Disetujui dan diterima oleh,



Raka Yusuf, ST., MTI
Dosen Pembimbing



UNIVERSITAS
MERCU BUANA
Desi Ramayanti, S.KOM., MT Andi Nugroho, ST., M.KOM
Kapodi Teknik Informatika Koordinator Tugas Akhir

KATA PENGANTAR

Puji Syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena atas karunia yang telah diberikan kepada penulis sehingga penulis dapat menyelesaikan Laporan Tugas Akhir ini, dimana Laporan Tugas Akhir tersebut merupakan salah satu persyaratan untuk dapat menyelesaikan Program Studi Strata Satu (S1) pada Jurusan Teknik Informatika Universitas Mercu Buana.

Penulis menyadari bahwa Laporan Tugas Akhir ini masih belum dapat dikatakan sempurna. Karena itu, kritik dan saran akan diterima dengan senang hati. Penulis juga menyadari bahwa Laporan Tugas Akhir ini takkan dapat selesai tepat pada waktunya tanpa bantuan, bimbingan, dan motivasi dari berbagai pihak. Maka dari itu, dengan segala kerendahan hati, Penulis ingin menyampaikan ucapan terima kasih kepada :

1. Kepada kedua orang tua yang selalu memberikan dukungan dan semangat.
2. Kepada keluarga besar yang telah banyak memberikan dukungan dan semangat untuk dapat menyelesaikan Tugas Akhir ini.
3. Kepada teman seperjuangan Agung Fadhilah yang telah menemani dan memberi masukan untuk penulisan.
4. Kepada Bapak Raka Yusuf, ST., MTI. Selaku dosen pembimbing Tugas Akhir Program Studi Informatika Universitas Mercu Buana.
5. Kepada Ibu Desi Ramayanti, S.Kom, MT. Selaku Ketua Program Studi Informatika Universitas Mercu Buana.
6. Kepada Bapak Andi Nugroho, ST., M.Kom. Selaku Koordinator Tugas Akhir Program Studi Informatika Universitas Mercu Buana.
7. Kepada Bapak Handy Noviyarto, S.Si., MT. Selaku dosen Matakuliah Keamanan Jaringan Program Studi Informatika Universitas Mercu Buana.

Semoga Tuhan Yang Maha Esa membalas kebaikan yang telah diberikan kepada penulis dan penulis berharap semoga laporan tugas akhir ini bermanfaat bagi kita semua. Amin

Jakarta, November 2017

Sharif Hidayat

DAFTAR ISI

	Halaman
LEMBAR PERNYATAAN	iii
LEMBAR PERSETUJUAN	iv
LEMBAR PENGESAHAN	v
ABSTRAK	vi
ABSTRACT	vii
KATA PENGANTAR	viii
DAFTAR ISI	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiii
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan dan Manfaat	3
1.4.1 Tujuan	3
1.4.2 Manfaat	3
1.5 Metode Penelitian	3
1.5.1 Metode Pengumpulan Data	3
1.5.2 Metode Pengembangan Sistem	4
1.6 Sistematika Penulisan	5
BAB II LANDASAN TEORI	
2.1 Keamanan Jaringan	6
2.1.1 Prinsip Keamanan Jaringan	7
2.1.2 Kategori Keamanan Jaringan	8
2.1.3 Jenis Serangan Jaringan Komputer	8
2.2 Intrusion Detection System	14
2.2.1 Host Intrusion Detection System	14
2.2.2 Network Intrusion Detection System	15
2.3 Intrusion Prevention System	16
2.3.1 Host Based Intrusion Prevention System	16
2.3.2 Network Based Intrusion Prevention System	17
2.4 Ubuntu	20

2.5 Snort	21
2.6 IP Tables	22
2.7 Network Development Life Cycle	24
BAB III ANALISIS SISTEM	
3.1 Profil Umum PT. XYZ	26
3.2 Analisis Jaringan Saat ini	26
3.3 Identifikasi Permasalahan	27
3.4 Analisis Sistem yang Diusulkan	28
3.5 Analisis Kebutuhan Sistem	29
3.5.1 Kebutuhan Fungsional	29
3.5.2 Kebutuhan Non Fungsional	29
BAB IV PERANCANGAN SISTEM	
4.1 Perancangan Perangkat Jaringan	31
4.2 Perancangan Topology yang Diusulkan	32
4.3 Identifikasi Lalu Lintas Jaringan	33
4.4 Inisialisasi Lalu Lintas Jaringan	34
4.5 Penolakan Terhadap Paket Data Berbahaya	35
4.6 Perancangan Pengujian Sistem	37
BAB V IMPLEMENTASI DAN PENGUJIAN	
5.1 Implementasi	38
5.2 Tahapan Implementasi Sistem IPS	38
5.2.1 Instalasi Snort	38
5.2.2 Konfigurasi Snort	39
5.2.3 Konfigurasi Barnyard2	39
5.2.4 Konfigurasi PulledPork	43
5.2.5 Konfigurasi Startup SystemD	44
5.2.6 Konfigurasi BASE	45
5.2.7 Konfigurasi Snort Inline Mode	46
5.3 Scenario Pengujian	48
5.3.3 Pengujian Port Scanning	48
5.3.4 Pengujian Ping of Death	49
5.4 Analisis Pengujian Sistem IPS	52

BAB IV KESIMPULAN DAN SARAN

6.1 Kesimpulan.....	53
6.2 Saran	52

DAFTAR PUSTAKA



UNIVERSITAS
MERCU BUANA

DAFTAR GAMBAR

Halaman	
Gambar 2.1 Normal TCP/IP handshake.....	9
Gambar 2.2 Synchronize Flooding Exchange	10
Gambar 2.3 Ilustrasi Port Scanning.....	11
Gambar 2.4 Penyadapan Paket.....	12
Gambar 2.5 ICMP Flood.....	12
Gambar 2.6 Diagram Smurf Attack	13
Gambar 2.7 Host-Based Intrusion Detection System	15
Gambar 2.8 Network-Based Intrusion Detection System	15
Gambar 2.9 Host-Based Intrusion Prevention System.....	17
Gambar 2.10 Network-Based Intrusion Prevention System	18
Gambar 2.11 IPTables Process Flow	23
Gambar 2.12 Network Development Life Cycle	24
Gambar 3.1 Topologi Saat Ini.....	27
Gambar 4.1 Topologi Usulan Sistem Intrusion Prevention System.....	32
Gambar 4.2 Proses Identifikasi Lalu Lintas Jaringan	33
Gambar 4.3 Proses Inisialisasi Lalu Lintas Jaringan	34
Gambar 4.4 Penolakan Paket Penyusupan.....	36
Gambar 4.5 Perancangan Pengujian Sistem	37
Gambar 5.1 Verifikasi Snort di Ubuntu.....	39
Gambar 5.2 Database MySql Barnyard2	43
Gambar 5.3 Verifikasi Konfigurasi PulledPork.....	44
Gambar 5.4 Konfigurasi BASE Sukses	46
Gambar 5.5 Drop Paket Scanning Port	49
Gambar 5.6 Drop Paket ICMP.....	50
Gambar 5.7 Pengamatan Alert di BASE.....	51
Gambar 5.8 Alert ICMP di BASE	51

DAFTAR TABEL

Tabel 5.1 Scenario Pengujian Port Scanning	48
Tabel 5.2 Scenario Pengujian Paket ICMP	50

