



**IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS)
UNTUK MONITORING
TRAFIK JARINGAN INTERNET**

Laporan Tugas Akhir

**Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Sistem Informasi**

Oleh :

U N I M E R C U B U A N A S
Imam Abdurahman

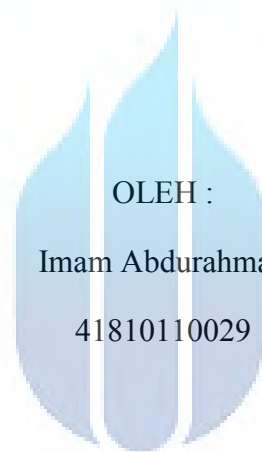
41810110029

M E R C U B U A N A

**PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
TAHUN 2015**



**IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS)
UNTUK MONITORING
TRAFIK JARINGAN INTERNET**



OLEH :

Imam Abdurahman

41810110029

**UNIVERSITAS
MERCU BUANA
PROGRAM STUDI SISTEM INFORMASI**

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

TAHUN 2015

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini:

NIM : 41810110029
Nama : Imam Abdurrahman
Fakultas : Ilmu Komputer
Program Studi : Sistem Informasi
Judul : **Implementasi Intrusion Detection System (IDS) Untuk Monitoring Trafik Jaringan Internet**

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya saya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam Laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapat sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 14 Agustus 2015

UNIVERSI
MERCU BUANA

Imam Abdurrahman


LEMBAR PENGESAHAN

Nomor : 41810110029
Nama : Imam Abdurahman
Jurusan : Ilmu Komputer
Studi : Sistem Informasi
Judul : **Implementasi Intrusion Detection System (IDS) Untuk Monitoring Trafik Jaringan Internet**


SKRIPSI INI TELAH DIPERIKSA DAN DISIDANGKAN

JAKARTA, 13 Agustus 2015

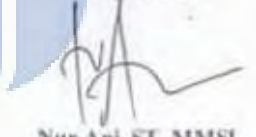
Menyetujui,


Wahyu Hari Hagi, S.Kom, MM
Dosen Pembimbing

Mengetahui,


Rigus Priambodo, ST, M.TI
Koordinator Tugas Akhir

Mengesahkan,


Nur Ani, ST, MMSI
Kaptodi Sistem Informasi

MERCU BUANA

KATA PENGANTAR

Segala puji bagi Allah SWT berkat Rahmat dan Ridho-Nya yang diberikan kepada penulis sehingga dapat menyelesaikan dan menyusun Tugas Akhir ini dengan judul **“Implementasi Intrusion Detection System (IDS) Untuk Monitoring Trafik Jaringan Internet”**.

Penulis menyadari bahwa dalam penyusunan tugas akhir ini masih terdapat beberapa kekurangan, karena keterbatasan kemampuan penulis dalam mendapatkan sumber yang menjadi bahan acuan dalam penyusunan. Oleh karena itu penulis mengharapkan saran dan kritik yang membangun agar dapat dimanfaatkan pada masa yang akan datang.

Untuk itu pada kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu, sehingga terlaksananya penulisan Tugas Akhir ini. Ucapan terima kasih terutama kepada:

1. Bapak Wachyu Hari Haji, S.Kom, MM selaku dosen pembimbing yang telah memberikan bimbingan dan masukan serta dukungan, sehingga dapat menyelesaikan skripsi ini.
2. Ibu Nur Ani, ST., MMSI, selaku Ka. Prodi Sistem Informasi.
3. Bapak Bagus Priambodo, ST, M.TI selaku koordinator TA Program studi Sistem Informasi.
4. Bapak dan Ibu dosen yang memberi bekal ilmu selama penulis kuliah di Universitas Mercu Buana.
5. Pihak keluarga yang tanpa henti memberikan dukungan, semangat, dan doa yang sangat luar biasa kepada penulis baik moril maupun materil.
6. Bapak Rudi Lumanto, Bisyrn Wahyudi, Iwan Sumantri, Muhammad Salahuddin, Mizamil, Muhammad Salman, dan segenap staff IDSIRTII yang telah memberikan banyak kemudahan dalam membantu penulis untuk memenuhi kelengkapanskripsi ini.
7. Mahasiswa/i Jurusan Sistem Informasi angkatan 2010 yang memberikan semangat, dukungan, dan doa yang luar biasa kepada penulis.

Akhir kata, semoga Allah SWT memberikan balasan yang melimpah kepada mereka yang telah membantu penulis dalam penyusunan Tugas Akhir ini. Amin.

Jakarta,.....2015

Imam Abdurahman



DAFTAR ISI

Halaman

LEMBAR PERSETUJUAN SIDANG	i
LEMBAR PERNYATAAN.....	ii
LEMBAR PENGESAHAN	iii
KATA PENGANTAR	iv
ABSTRAK.....	v
ABSTRACT.....	vi
BAB I	1
PENDAHULUAN	2
3.1 1.1 Latar Belakang.....	3
3.2 1.2 Rumusan Masalah.....	4
3.3 1.3 Batasan Masalah	5
3.4 1.4 Tujuan dan manfaat	5
3.5 1.5 Metodologi penelitian.....	6
3.6 1.6 Sistematika Penulisan	7
BAB II.....	8
LANDASAN TEORI.....	9
3.7 2.1 Konsep Sistem Informasi.....	10
2.1.1 Definisi Sistem.....	11
2.1.2 Karakteristik Sistem.....	12
2.1.3 Klasifikasi Sistem	13
3.8 2.2 Konsep Dasar Informasi	14
2.2.1 Pengertian Informasi	15
2.2.2 Jenis-jenis Informasi	16
2.2.3 Nilai dan Kualitas Informasi	17
2.2.4 Komponen dan Jenis Sistem Informasi.....	18
3.9 2.3 Konsep Basis Data	19
2.3.1 Pengertian Basis Data	20
2.3.2 Pengertian DBMS	21
2.3.3 Alur Hidup Basis Data	22
3.10 2.4 Analisa Perancangan Perangkat Lunak	23

2.4.1	Pengertian SDLC	24
3.11	2.5 Model SDLC	25
2.5.1	Model Waterfall	26
3.12	2.6 <i>Unified Modeling Language (UML)</i>	27
2.6.1	Pengenalan UML	28
2.6.2	Sejarah UML.....	29
3.13	2.7 Diagram UML	30
2.7.1	Use Case Diagram.....	31
2.7.2	Activity Diagram	32
2.8.3	Sequence Diagram	33
2.9.4	Class Diagram.....	34
3.14	2.8 Perangkat Lunak Pendukung.....	35
2.8.1	PHP	36
2.8.2	PostgreSQL	37
2.8.3	Snort.....	38
2.8.4	Linux (Ubuntu)	39
2.9	Teori IP Address	40
BAB III.....		41
ANALISA DAN PERANCANGAN SISTEM.....		42
3.15	3.1 Gambaran Umum IDSIRTII	43
3.1.1	Struktur Organisasi	44
3.16	3.2 Analisa Sistem Berjalan.....	45
3.2.1	Use Case berjalan.....	46
3.2.2	Identifikasi Permasalahan	47
3.2.3	Pemecahan Masalah.....	48
3.17	3.4 Usecase Diagram Usulan pada Monitoring.....	49
3.4.1	<i>Activity Diagram</i> Melihat Dashboard	50
3.4.2	<i>Activity Diagram</i> Melihat Monitoring	51
3.4.3	<i>Activity Diagram</i> Melihat Laporan	52
3.4.4	<i>Activity Diagram</i> Manajemen Sensor	53
3.4.5	<i>Activity Diagram</i> Manajemen User.....	54
3.5	Sequence Diagram Usulan.....	55
3.5.1	Sequence Diagram Login Usulan	56
3.5.2	Sequence Diagram Melihat Monitoring.....	57

3.5.3 Sequence Diagram Melihat Laporan.....	58
3.5.4 Sequence Diagram Manajemen Sensor.....	58
3.5.5 Sequence Diagram Manajemen User.....	59
3.6 Class Diagram Usulan Pada Monitoring IDSIRTII.....	60
1. Tabel ci_session.....	61
2. Tabel configuration.....	62
2. Tabel data.....	63
3. Tabel detail.....	64
4. Tabel encoding.....	65
5. Tabel event.....	67
6. Tabel icmphdr.....	68
7. Tabel ip2c.....	69
8. Tabel ip_cache.....	70
9. Tabel iphdr.....	71
10. Tabel login_attempts.....	72
11. Tabel metadata.....	73
12. Tabel opt.....	74
13. Tabel protocols.....	75
14. Tabel reference.....	76
15. Tabel reference_system.....	77
16. Tabel schema.....	78
17. Tabel sensor.....	79
18. Tabel sensor_detail.....	80
19. Tabel sig_class.....	81
20. Tabel sig_reference.....	82
21. Tabel signature.....	83
22. Tabel tcphdr.....	84
23. Tabel udphdr.....	85
24. Tabel user_autologin.....	86
25. Tabel user_profiles.....	87
26. Tabel users.....	88
3.7 Rancangan Layar Usulan.....	89
3.7.1 Struktur Menu Seluruh Pengguna Usulan.....	90
3.7.2 Rancangan Layar Login Usulan.....	91

3.7.3 Rancangan Layar Dashboard	92
3.7.4 Rancangan Layar Monitoring	93
3.7.6 Rancangan Layar Manajemen User	94
3.7.6 Rancangan Layar Manajemen Sensor	94
BAB IV.....	95
4. IMPLEMENTASI DAN PENGUJIAN	95
4.1 Kebutuhan Hardware & Software Pengujian.....	95
4.2 Kebutuhan Hardwre & Software Minimum.....	95
A. Dashboard.....	96
B. Monitoring	96
C. Laporan	96
D. User management	97
4.5 Metode Pengujian.....	97
4.6 Skenario Pengujian.....	98
4.7 Hasil Pengujian.....	98
BAB V.....	99
PENUTUP.....	99
5.1 Kesimpulan.....	99
5.2 Saran	99
DAFTAR PUSTAKA	100



DAFTAR GAMBAR

Gambar 2. 1 Alur Hidup Basis Data(Shalahuddin, 2013)	21
Gambar 2. 2 Tahapan Metode <i>Waterfall</i> (Mulyanto, 2008)	22
Gambar 2. 3 Diagram UML(Shalahuddin, 2013)	26
Gambar 3. 1 Use Case Sistem Berjalan	42
Gambar 3. 2 <i>Usecase</i> Sistem Usulan Pada Monitoring IDSIRTII.....	46
Gambar 3. 3 <i>Activity Diagram</i> Melihat Dashboard.....	50
Gambar 3. 4 <i>Activity Diagram</i> Melihat Monitoring.....	52
Gambar 3. 5 <i>Activity Diagram</i> Melihat Laporan	54
Gambar 3. 6 <i>Activity Diagram</i> Manajemen Sensor	56
Gambar 3. 7 <i>Activity Diagram</i> Manajemen User.....	58
Gambar 3. 8 <i>Sequence Diagram</i> Login Usulan	60
Gambar 3. 9 <i>Sequence Diagram</i> Melihat Monitoring	60
Gambar 3.10 <i>Sequence</i> Melihat Laporan.....	61
Gambar 3. 11 <i>Sequence Diagram</i> Manajemen Sensor	63
Gambar 3. 12 <i>Sequence Diagram</i> Manajemen User.....	64
Gambar 3. 13 <i>Class Diagram</i> usulan pada IDSIRTII.....	67
Gambar 3. 14 Rancangan Layar Menu Staff	88
Gambar 3. 15 Menu Admin	89
Gambar 3. 16 Rancangan Layar Dashboard	90
Gambar 3. 17 Rancangan Layar Monitoring	91
Gambar 3. 18 Rancangan Layar Laporan	92
Gambar 3. 19 Rancangan Layar User	93
<u>Gambar 4. 1</u> Tampilan Localhost PGadmin	95
<u>Gambar 4. 2</u> Tampilan Awal Pembuatan Database	96
<u>Gambar 4. 3</u> Tampilan Database Aplikasi Pemeliharaan	97
<u>Gambar 4. 4</u> Tampilan tabel ci_sessions.....	98
<u>Gambar 4. 5</u> Tampilan tabel configuration	98
<u>Gambar 4. 6</u> Tampilan tabel data	99
<u>Gambar 4. 7</u> Tampilan tabel detail.....	99
<u>Gambar 4. 8</u> Tampilan tabel encoding	100
<u>Gambar 4. 9</u> Tampilan tabel event	100
<u>Gambar 4. 10</u> Tampilan tabel icmphdr	100
<u>Gambar 4. 11</u> Tampilan tabel ip2c.....	101
<u>Gambar 4. 12</u> Tampilan tabel ip_cach	101
<u>Gambar 4. 13</u> Tampilan tabel iphdr	101
<u>Gambar 4. 14</u> Tampilan tabel login_attempt	102
<u>Gambar 4. 15</u> Tampilan tabel metadata	102
<u>Gambar 4. 16</u> Tampilan tabel opt	102

<u>Gambar 4. 17</u> Tampilan tabel protocols.....	103
<u>Gambar 4. 18</u> Tampilan tabel reference.....	103
<u>Gambar 4. 19</u> Tampilan tabel reference_system.....	104
<u>Gambar 4. 20</u> Tampilan tabel schema.....	104
<u>Gambar 4. 21</u> Tampilan tabel sensor	105
<u>Gambar 4. 22</u> Tampilan tabel sensor_detail	105
<u>Gambar 4. 23</u> Tampilan tabel sig_class	105
<u>Gambar 4. 24</u> Tampilan tabel sig_reference	106
<u>Gambar 4. 25</u> Tampilan tabel signature.....	106
<u>Gambar 4. 26</u> Tampilan tabel tcphdr	106
<u>Gambar 4. 27</u> Tampilan tabel udphdr	107
<u>Gambar 4. 28</u> Tampilan tabel user_autologin.....	107
<u>Gambar 4. 29</u> Tampilan tabel user_profiles.....	107
<u>Gambar 4. 30</u> Tampilan tabel users	108
<u>Gambar 4. 31</u> Tampilan Dashboard.....	109
<u>Gambar 4. 32</u> Tampilan Monitoring.....	110
<u>Gambar 4. 33</u> Tampilan Laporan	111
<u>Gambar 4. 34</u> Tampilan User Management.....	111



UNIVERSITAS
MERCU BUANA

DAFTAR TABEL

Tabel 2. 1 Simbol <i>Use case</i> (Wiley, 2010)	27
Tabel 2. 2 Simbol pada diagram aktivitas (Wiley, 2010)	29
Tabel 2. 3 Simbol pada diagram sekuen (Wiley, 2010).....	31
Tabel 2. 4 Simbol diagram kelas (Wiley, 2010)	33
Tabel 2. 5 Tabel 2.5. Tabel Representasi Kelas IPv4 (Rahmat, 2005)	37
Tabel 3. 1 Struktur Organisasi IDSIRTII.....	39
Tabel 3. 2 Deskripsi Use Case Melakukan permintaan log ISP	43
Tabel 3. 3 Deskripsi Use Case Menerima log.....	43
Tabel 3. 4 Use Case Analisa Log.....	44
Tabel 3. 5 Deskripsi Use Case Membuat Laporan	44
Tabel 3. 6 Deskripsi Usecase Login	46
Tabel 3. 7 Deskripsi Melihat Dashboard	47
Tabel 3. 8 Deskripsi Melihat Monitoring	47
Tabel 3. 9 Deskripsi Melihat Laporan	48
Tabel 3. 10 Deskripsi Manajemen Sensor	48
Tabel 3. 11 Deskripsi Manajemen User.....	49
Tabel 3. 12 Deskripsi Activity Melihat Dashboard	51
Tabel 3. 13 Deskripsi Activity Melihat Monitoring	53
Tabel 3. 14 Deskripsi Activity Melihat Laporan	55
Tabel 3. 15 Deskripsi Activity Manajemen Sensor	56
Tabel 3. 16 Deskripsi Activity Manajemen User	59
Tabel 3. 17 Deskripsi <i>Sequence</i> Login	60
Tabel 3. 18 Deskripsi <i>Sequence</i> Melihat Monitoring	61
Tabel 3.19 Deskripsi <i>Sequence</i> Melihat Laporan	62
Tabel 3. 20 Deskripsi <i>Sequence</i> Manajemen Sensor	64
Tabel 3. 21 Deskripsi <i>Sequence</i> Manajemen User.....	66
<u>Tabel 4. 1 Skenario Pengujian</u>	<u>113</u>