

**IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN
WIDS (WIRELESS INTRUSION DETECTION SYSTEM)
BERBASIS NOTIFIKASI LINE PADA SMK NEGERI 2 KOTA
MAGELANG**

SKRIPSI



disusun oleh

Jihan Insan Akmal

15.11.9117

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019**

**IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN
WIDS (WIRELESS INTRUSION DETECTION SYSTEM)
BERBASIS NOTIFIKASI LINE PADA SMK NEGERI 2 KOTA
MAGELANG**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Informatika



disusun oleh

Jihan Insan Akmal

15.11.9117

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019**

PERSETUJUAN

SKRIPSI

**IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN
WIDS (WIRELESS INTRUSION DETECTION SYSTEM) BERBASIS
NOTIFIKASI LINE PADA SMK NEGERI 2 KOTA MAGELANG**

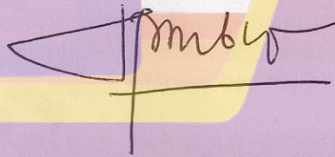
yang dipersiapkan dan disusun oleh

Jihan Insan Akmal

15.11.9117

telah disetujui oleh dosen pembimbing skripsi
pada tanggal 2 November 2019

Dosen Pembimbing,



Agung Pambudi, S.T., M.A.

NIK. 190302012

PENGESAHAN

SKRIPSI

**IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN
WIDS (WIRELESS INTRUSION DETECTION SYSTEM) BERBASIS
NOTIFIKASI LINE PADA SMK NEGERI 2 KOTA MAGELANG**

yang dipersiapkan dan disusun oleh

Jihan Insan Akmal

15.11.9117

telah dipertahankan di depan Dewan Penguji
pada tanggal 18 November 2019

Susunan Dewan Penguji

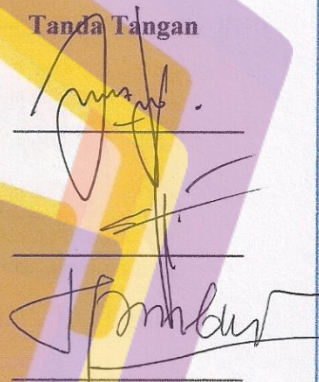
Nama Penguji

Lukman, M.Kom.
NIK. 190302151

Eli Pujastuti, M.Kom.
NIK. 190302227

Agung Pambudi, S.T., M.A.
NIK. 190302012

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 4 Desember 2019

DEKAN FAKULTAS ILMU KOMPUTER



Krisnawati, S.Si., M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertanda tangan di bawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat menjadi tanggungjawab pribadi.

Yogyakarta, 10 Desember 2019



Jihan Insan Akmal

NIM. 15.11.9117

MOTTO

"Rahasia keberhasilan adalah kerja keras dan belajar dari kegagalan"

" Percaya pada diri sendiri, bekerja keras, dan berpikir positif"

"Tiada doa yang lebih indah selain doa agar skripsi ini cepat selesai"

"Saat kita melibatkan Tuhan dalam semua impian, yakinlah bahwa tidak ada yang tidak mungkin"

PERSEMBAHAN

Terimakasih kepada Allah SWT sebagai tanda rasa syukur atas nikmat dan karunia-Nya sehingga skripsi ini dapat terselesaikan. Skripsi ini penulis persembahkan kepada:

1. Kepada Allah SWT
2. Kepada kedua orang tua, bapak Nuroh Hadi dan ibu Tri Widiastuti yang selalu berdoa dan selalu bersabar mencurahkan kasih sayang kepada saya.
3. Bapak Agung Pambudi, S.T., M.A. sebagai dosen pembimbing skripsi, saya mengucapkan terima kasih banyak atas saran, himbauan, dan masukan sehingga dapat terselesaikannya skripsi ini dengan baik dan lancar.
4. Kepada Kepala Sekolah SMK N 2 Magelang, yang sudah memberikan ijin dan bekerjasama dalam penyelesaian skripsi.
5. Kepada teman-teman saya Alvian , Dany, Jihan, Japale, Anang, teman-teman kos dan teman-teman kontrakan yang sudah membantu dalam menyelesaikan skripsi ini.

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas segala rahmat, hidayah, dan kekuatan yang telah diberikan, sehingga penulis dapat menyelesaikan skripsi dengan judul “Implementas Sistem Keamanan Jaringan Menggunakan WIDS (WIRELESS INSTRUSION DETECTION SYSTEM) Berbasis Notifikas Line pada SMK Negeri 2 Kota Magelang”. Skripsi ini disusun sebagai salah satu syarat guna menyelesaikan studi pada jenjang Strata Satu (S1) pada program studi Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta.

Dalam kesempatan ini dengan segala kerendahan hati penulis sampaikan rasa terima kasih yang sebesar-besarnya kepada pihak yang telah mendukung, membantu dan membimbing, sehingga skripsi ini dapat diselesaikan seperti yang diharapkan, khususnya kepada :

1. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas Amikom Yogyakarta.
2. Ibu Krisnawati, S.Si., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
3. Bapak Agung Pambudi, S.T., M.A. selaku dosen pembimbing yang telah banyak memberikan pengarahan bagi penulis dalm pembuatan skripsi.
4. Seluruh para Dosen, Asisten Dosen, Karyawan dan Teknisi Universitas Amikom Yogyakarta yang telah memberikan fasilitas, dukungan dan ilmu selama di perkuliahan.

5. Kedua orang tua tercinta beserta segenap keluarga yang senantiasa memberikan doa, dukungan, dan motivasi.
6. Teman-teman saya yang telah membantu dan mendukung dalam penulisan skripsi ini.
7. Dan semua pihak yang tidak dapat penulis sebutkan satu persatu, yang telah banyak membantu dalam melancarkan penyusunan skripsi ini sampai selesai.

Dalam penulisan skripsi ini, penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan, oleh karena itu dengan segala kerendahan hati penulis bersedia menerima kritik dan saran, serta masukan yang bersifat membangun agar selanjutnya skripsi ini menjadi lebih baik lagi. Harapan penulis semoga skripsi ini berguna bagi semua pihak yang membutuhkan.

Yogyakarta, 10 Desember 2019

Jihan Insan Akmal

15.11.9117

DAFTAR ISI

JUDUL	ii
PERSETUJUAN	ii
PENGESAHAN	iii
PERNYATAAN	iv
MOTTO	v
PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR TABEL	xiv
DAFTAR GAMBAR	xv
INTISARI	xviii
ABSTRACT	xix
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Maksud dan Tujuan Penelitian.....	4
1.5 Manfaat Penelitian	4
1.6 Metode penelitian.....	5
1.6.1 Metode Pengumpulan Data.....	5
1.6.2 Metode Pengembangan	6

1.7	Sistematika Penulisan	6
BAB II LANDASAN TEORI		8
2.1	Tinjauan Pustaka.....	8
2.2	Intrusion Detection System.....	9
2.2.1	Definisi Intrusion Detection System	9
2.2.2	Fungsi Intrusion Detection System (IDS)	10
2.2.3	Tipe IDS (Intrusion Detection System).....	11
2.2.4	Keuntungan dan Kekurangan (IDS) Intrusion Detection System.....	12
2.2.5	Peran IDS (Intrusion Detection System).....	12
2.3	Jaringan Wireless	13
2.3.1	Sejarah WLAN.....	13
2.3.2	Definisi Jaringan Wireless	14
2.3.3	Komponen WLAN.....	14
2.3.4	Kelebihan dan Kekurangan Jaringan WLAN	17
2.3.5	Standart Wireless	18
2.4	Model Refrensi TCP/IP.....	19
2.5	User Datagram Protocol (UDP).....	19
2.6	Keamanan Jaringan.....	20
2.7	Macam-Macam Jenis Serangan	20
2.7.1	Port Scanning	21
2.7.2	Spoofing	21
2.7.3	DOS (Denial Of Service)	24
2.7.4	Teardrop	25

2.7.5 UDP Flood	26
2.7.6 ICMP Flood.....	26
2.8 Perangkat Lunak	26
2.8.1 Snort	26
2.8.2 Nmap.....	27
2.8.3 BASE (Basic Analysis And Security Engine)	27
2.8.4 Digital Blaster	28
2.8.5 IPTables.....	28
2.8.6 Hub.....	29
2.8.7 Ping Attack.....	29
2.9 Notifikasi Alert System.....	30
2.10 Instant Messaging Line	30
2.11 Web Service Heroku	31
2.12 Pengertian Metodologi Penelitian.....	31
2.12.1 Pengertian Pengumpulan Data	32
2.12.2 Metode Pengembangan System.....	33
BAB III ANALISIS DAN PERANCANGAN.....	35
3.1 Tempat penelitian.....	35
3.1.1 Mapping Ruangn SMK Negeri 2 Magelang.....	35
3.1.2 Denah SMK Negeri 2 Magelang.....	38
3.2 Alat Dan Bahan.....	39
3.2.1 Software (Perangkat Lunak)	39
3.2.2 Hardware (Perangkat Keras).....	40

3.3	Prosedur dan Pengumpulan Data	41
3.3.1	Prosedur	41
3.3.2	Pengumpulan Data	42
3.3.2.1	Studi Pustaka	42
3.3.2.2	Wawancara	42
3.4	Analisis dan Perancangan Sistem	43
3.4.1	Analisis Permasalahan Sistem	43
3.4.2	Analisis Kebutuhan Sistem	43
3.4.3	Rancangan Arsitektur Sistem	45
3.4.4	Perancangan Network Intrusion Detection System.....	47
BAB IV IMPLEMENTASI DAN PEMBAHASAN		51
4.1	Konfigurasi Komponen IDS	51
4.1.1	Instalasi Snort.....	51
4.1.2	Konfigurasi Snort Untuk Dijalankan Sebagai NIDS	53
4.1.3	Mengedit File Snort.conf	55
4.1.4	Menulis Aturan Sederhana untuk Menguji Deteksi Snort	56
4.1.5	Membuat Rules Serangan	59
4.1.6	Instalasi Barnyard2.....	61
4.1.7	Membuat System startup script di Ubuntu 16.....	68
4.1.8	Installing BASE on Ubuntu	71
4.2	Pembuatan Akun Line Bot.....	76
4.2.1	Pendaftaran Akun Line Devloper.....	76
4.2.2	Pembuatan Line Channel	78

4.2.3 Konfigurasi Line Channel	79
4.2.4 Deploy Aplikasi ke Heroku.....	80
4.2.5 Integrasi Line Channel	81
4.2.6 Push Message	82
4.2.7 Penerapan Trigger Send Message API Bot Line.....	83
4.3 Enforcement.....	84
4.3.1 Pengujian Komponen IDS	85
4.3.2 Pengujian Fungsionalitas Interkoneksi IDS	86
4.3.3 Pengujian Snort Dan BASE Dalam Mendeteksi Serangan	92
4.4 Hasil Analisa Kinerja Wireless Intrusion Detection System	93
4.5 Hasil Analisa Perbandingan Sistem Lama dan Sistem Baru	94
4.6 Solusi Mengatasi Serangan.....	95
4.7 Keuntungan dan Hasil Menggunakan IDS	97
4.8 Enhancement.....	98
BAB V PENUTUP.....	99
5.1 Kesimpulan	99
5.2 Saran	99
DAFTAR PUSTAKA	100
LAMPIRAN.....	103

DAFTAR TABEL

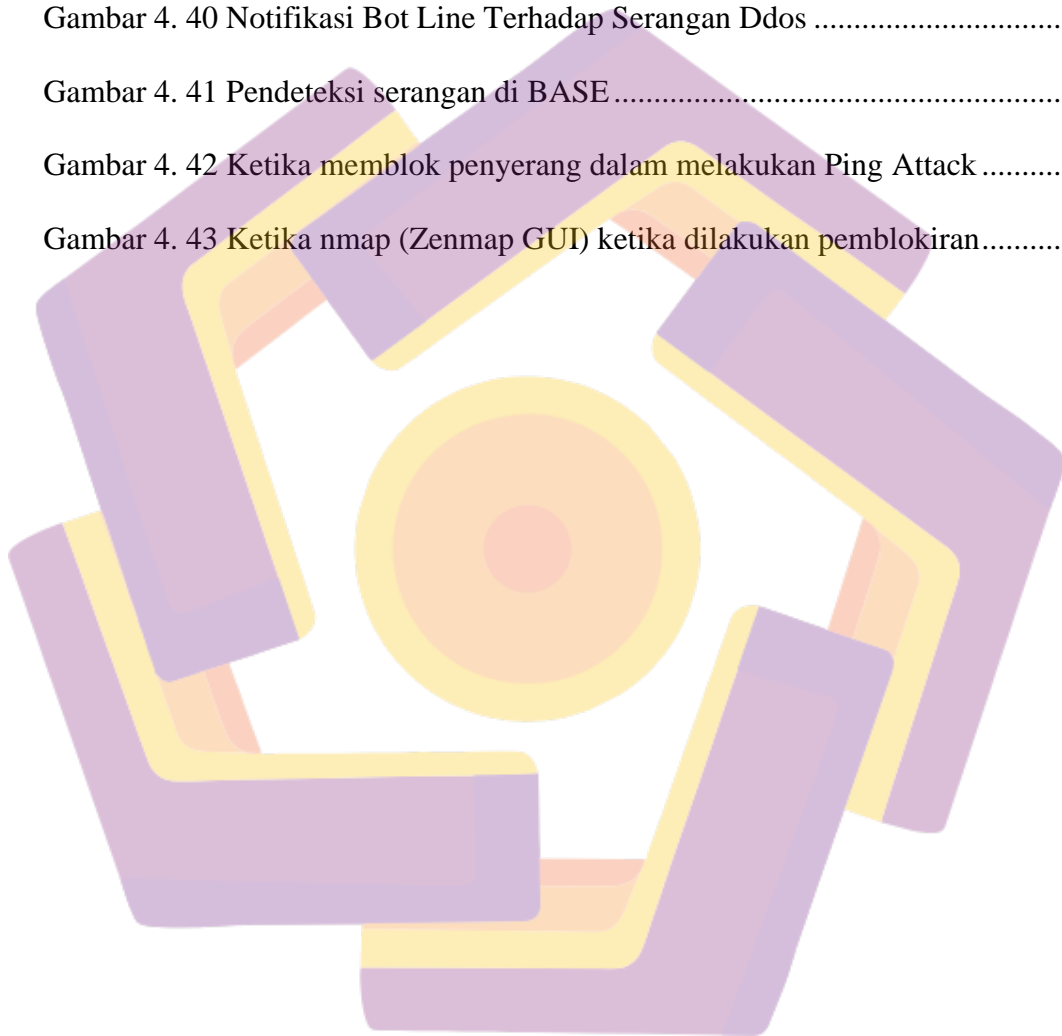
Tabel 2. 1 Kelemahan dan Kelebihan menggunakan Jaringan WLAN	17
Tabel 2. 2 Protokol WLAN.....	18
Tabel 3. 1 Mapping Gambar Ruangan SMK Negeri 2 Magelang.....	36
Tabel 3. 2 Gambar Ruang Server SMK Negeri 2 Magelang	38
Tabel 3. 3 Software (Perangkat Lunak)	39
Tabel 3. 4 Hardware (Perangkat Keras).....	40
Tabel 3. 5 Rincian Topologi Fisik	50
Tabel 3. 6 Rincian IP Address	50
Tabel 4. 1 Konfigurasi Instalasi Snort	51
Tabel 4. 2 Konfigurasi Snort Sebagai NIDS	53
Tabel 4. 3 Konfigurasi mengedit file snort.conf	55
Tabel 4. 4 Konfigurasi File Rules	57
Tabel 4. 5 Konfigurasi Instalasi Barnyard2	61
Tabel 4. 6 Konfigurasi MySQL untuk Barnyard2	63
Tabel 4. 7 Konfigurasi Instalasi PulledPork	65
Tabel 4. 8 Konfigurasi Untuk Mengedit PulledPork.conf	66
Tabel 4. 9 Menambahkan PulledPork ke Crontab	67
Tabel 4. 10 Konfigurasi System Startup	68
Tabel 4. 11 Konfigurasi Penginstalan BASE.....	71
Tabel 4. 12 Hasil Analisa Kinerja WIDS	93
Tabel 4. 13 Hasil Analisa Perbandingan Sistem	94

DAFTAR GAMBAR

Gambar 1. 1 Security Policy Development Life Cycle.....	6
Gambar 2. 1 Jangkauan Area Antenna.....	15
Gambar 2. 2 Access Point.....	15
Gambar 2. 3 Jaringan Menggunakan Extension Point.....	16
Gambar 2. 4 WLAN Card.....	17
Gambar 3. 1 Denah Sekolah SMK Negeri 2 Magelang.....	38
Gambar 3. 2 Arsitektur Snort.....	46
Gambar 3. 3 Flowchart Network Intrusion Detection System.....	47
Gambar 3. 4 Topologi jaringan sebelum diterapkan sensor IDS.....	48
Gambar 3. 5 Topologi jaringan setelah diterapkan sensor IDS.....	48
Gambar 4. 1 Output setelah snort berhasil terinstall.....	52
Gambar 4. 2 Output Setelah Snort berhasil dijalankan sebagai NIDS.....	56
Gambar 4. 3 Output berhasil membuat aturan Snort serangan.....	59
Gambar 4. 4 Output Barnyard2 berhasil terinstall.....	63
Gambar 4. 5 Database MySQL.....	65
Gambar 4. 6 Output Pulledpork berhasil terinstall.....	66
Gambar 4. 7 Output ICMP event yang ditulis di database.....	67
Gambar 4. 8 Snort berhasil berjalan pada saat booting.....	70
Gambar 4. 9 Barnyard berhasil berjalan pada saat booting.....	70
Gambar 4. 10 Konfigurasi BASE.....	73
Gambar 4. 11 Konfigurasi BASE.....	74
Gambar 4. 12 Konfigurasi BASE.....	74

Gambar 4. 13 Konfigurasi BASE.....	75
Gambar 4. 14 Konfigurasi BASE.....	75
Gambar 4. 15 Konfigurasi BASE.....	75
Gambar 4. 16 Home page BASE setelah dilakukan konfigurasi	76
Gambar 4. 17 Halaman Login Line Developer.....	76
Gambar 4. 18 Halaman Pendaftaran Akun Line Developer	77
Gambar 4. 19 Penamaan Provider.....	77
Gambar 4. 20 Pemilihan Provider	78
Gambar 4. 21 Informasi Bot yang akan dibuat	78
Gambar 4. 22 Pemilihan developer.....	79
Gambar 4. 23 Persetujuan pembuatan line channel	79
Gambar 4. 24 Tampilan Webhook	80
Gambar 4. 25 Pembuatan dan pemberian nama project.....	80
Gambar 4. 26 Tampilan Dashboard Project.....	81
Gambar 4. 27 Tampilan project Heroku berhasil dibuat.....	81
Gambar 4. 28 Channel Secret dan Channel Access Token.....	81
Gambar 4. 29 Mengganti Channel Secret dan Channel Access Token.....	82
Gambar 4. 30 Penggantian Webhook.....	82
Gambar 4. 31 QR Code Bot Line atau UserID Bot Line	83
Gambar 4. 32 Coding Send Api pada Main Base	84
Gambar 4. 33 Pengujian Fungsi Snort	85
Gambar 4. 34 Pengujian Fungsi BASE.....	86
Gambar 4. 35 Pengujian Serangan Ping Attack (ICMP Traffic)	87

Gambar 4. 36 Notifikasi Bot Line Terhadap Serangan Ping Attack.....	88
Gambar 4. 37 Pengujian Serangan Nmap Port Scanning Attack.....	89
Gambar 4. 38 Notifikasi Bot Line Terhadap Serangan Port Scanning Attack.....	90
Gambar 4. 39 Pengujian Serangan DDos menggunakan UDP Unicorn	91
Gambar 4. 40 Notifikasi Bot Line Terhadap Serangan Ddos	92
Gambar 4. 41 Pendeteksi serangan di BASE	93
Gambar 4. 42 Ketika memblok penyerang dalam melakukan Ping Attack.....	96
Gambar 4. 43 Ketika nmap (Zenmap GUI) ketika dilakukan pemblokiran.....	97



INTISARI

Seiring dengan perkembangan teknologi yang semakin pesat, seperti pada jaringan komputer. Jaringan komputer yang pada awalnya menggunakan kabel, kini berubah menjadi nirkabel atau wireless. Jaringan wireless merupakan jaringan yang menggunakan gelombang radio dan jaringan wireless.

Wireless lebih modern untuk menggantikan jaringan yang menggunakan kabel, dimana pengguna dapat bebas menggunakan dimana saja selama masih terhubung di area yang mencakup sinyal wireless tersebut. Semakin mudah dan bebasnya pengguna untuk dapat menyambung wireless, maka hal tersebut dapat berdampak buruk bagi sistem. Sistem akan semakin mudah untuk mendapatkan segala macam serangan, dan diretas oleh penyusup dari pihak yang tidak bertanggung jawab.

Keamanan jaringan sangat dibutuhkan untuk menjaga data bagi para pengguna. Sistem harus di lindungi untuk mencegah terjadi berbagai serangan dan usaha penyusupan oleh pihak yang tidak bertanggung jawab yang mengakibatkan rusaknya sebuah sistem koneksi antar perangkat yang terhubung. IDS adalah aplikasi yang dapat mendeteksi aktifitas yang mencurigakan dalam sistem jaringan.

Kata kunci: Keamanan Jaringan , IDS (*Intrusion Detection System*), *Linux*, *Snort*, *Wireless*.

ABSTRACT

Along with the development of increasingly rapid technology, such as in computer networks. Computer networks that originally used cable, now turned into wireless or wireless.

Wireless networks are networks that use radio waves and wireless networks. Wireless is more modern to replace networks that use cables, where users can freely use anywhere while still connected in an area that includes the wireless signal. The more easy and free the user is to be able to connect wirelessly, then this can have a bad impact on the system. The system will be easier to get all kinds of attacks, and hacked by intruders from irresponsible parties. Network security is needed to protect data for users.

The system must be protected to prevent various attacks and intrusion attempts by irresponsible parties that cause damage to a system of connections between devices that are connected. Children are applications that can detect suspicious activity in network systems.

Keywords : *Network Security, IDS (Intrusion Detection System), Linux, Snort.*

Wireless.

