

**ANALISA KINERJA *WIRELESS INTRUSION DETECTION SYSTEM*  
SEBAGAI SISTEM KEAMANAN NIRKABEL PADA KANTOR  
KEJAKSAAN NEGERI TUBAN**

**SKRIPSI**



disusun oleh  
**Alvian Adhy Nugraha**  
**15.11.9125**

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



**ANALISA KINERJA *WIRELESS INTRUSION DETECTION SYSTEM*  
SEBAGAI SISTEM KEAMANAN NIRKABEL PADA KANTOR  
KEJAKSAAN NEGERI TUBAN**

**SKRIPSI**

untuk memenuhi sebagian persyaratan  
mencapai gelar Sarjana  
pada Program Studi Informatika



disusun oleh

**Alvian Adhy Nugraha**

**15.11.9125**

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



**PERSETUJUAN**

**SKRIPSI**

**ANALISA KINERJA *WIRELESS INTRUSION DETECTION SYSTEM*  
SEBAGAI SISTEM KEAMANAN NIRKABEL PADA KANTOR  
KEJAKSAAN NEGERI TUBAN**

yang dipersiapkan dan disusun oleh

**Alvian Adhy Nugraha**

**15.11.9125**

telah disetujui oleh dosen pembimbing skripsi  
pada tanggal 4 Maret 2019

**Dosen Pembimbing,**



**Nila Feby Puspitasari, S.Kom, M.Cs**

**NIK. 190302109**

## PENGESAHAN

### SKRIPSI

#### **ANALISA KINERJA *WIRELESS INTRUSION DETECTION SYSTEM* SEBAGAI SISTEM KEAMANAN NIRKABEL PADA KANTOR KEJAKSAAN NEGERI TUBAN**

yang dipersiapkan dan disusun oleh

**Alvian Adhy Nugraha**

**15.11.9125**

telah dipertahankan di depan Dewan Penguji  
pada tanggal 21 Maret 2019

#### **Susunan Dewan Penguji**

##### **Nama Penguji**

**Andika Agus Slameto, M.Kom**

**NIK. 190302161**

**Rizqi Sukma Kharisma, M.Kom**

**NIK. 190302215**

**Nila Feby Puspitasari, S.Kom, M.Cs**

**NIK. 190302109**

##### **Tanda Tangan**



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 11 Maret 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, 2 Januari 2019



Alvian Adhy Nugraha

NIM. 15.11.9125

## PERSEMBAHAN

Dengan rasa hormat, cinta dan sayangku  
Ku dedikasikan karya sederhana ini untuk  
Bapak dan Ibu tercinta :

Bapak Mataji

&

Ibu Siti Maghfiroh

Terima kasih atas cinta, kasih sayang dan doa-nya

“Ya Tuhan kami, beri ampunlah aku dan kedua ibu bapakku dan sekalian orang-orang mukmin pada hari terjadinya hisab (hari kiamat)".  
[QS Ibrahim 14:41]

Dan rendahkanlah dirimu terhadap mereka berdua dengan penuh kesayangan dan ucapkanlah: "Wahai Tuhanku, kasihilah mereka keduanya, sebagaimana mereka berdua telah mendidik aku waktu kecil".  
[QS Al-Isra 16:24]

## KATA PENGANTAR

Assalamu'alaikumn Warahmatullahi Wabarakatuh

*Alhamdulillah* rabbilalamiin, segala puji bagi Allah SWT, atas segala karunia dan anugrah nikmatnya yang tidak terbatas, dengan rahmatnya pula akhirnya peneliti dapat menyelesaikan penyusunan skripsi ini dengan baik. Shalawat dan salam semoga terlimpahcurahkan kepada manusia sempurna yaitu Nabi Besar Muhammad SAW, keluarga, kerabat, dan para sahabatnya dan tentunya kita sebagai umatnya semoga kelak mendapatkan *syafaat* di hari akhir.

Peneliti menyadari bahwa isi maupun materi dari skripsi ini masih banyak kekurangannya, walaupun sudah dupayakan semaksimal mungkin, dikarenakan pengalaman dan ilmu pengetahuan yang masih terbatas. Oleh karena itu kritik dan saran yang bersifat membangun guna kesempatan dalam laporan skripsi ini sangat diperlukan.

Adapun judul skripsi ini yaitu “Analisa Kinerja *Wireless Intrusion Detection System* Sebagai Sistem Keamanan Nirkabel Pada Kantor Kejaksaan Negeri Tuban”. Oleh karena itu dalam kesempatan yang baik ini peneliti ingin menyampaikan rasa terimakasih yang sebesar-besarnya kepada pihak yang secara langsung atau tidak langsung telah turut membantu dalam penulisan skripsi ini, khususnya kepada :

1. Kedua orang tua tercinta yang telah memberi kasih sayang, ilmu, do'a dan dukungan moril maupun materil.
2. Adik tersayang Syilvia Putri Agustina, terimakasih atas support dan do'anya.

3. Keluarga besar Cus Plus Ndiyah Family dan Warsit Family yang telah memberi support serta do'a-do'anya.
4. Bapak Prof., Dr. M. Suyanto, M.M. selaku Rektor Universitas Amikom Yogyakarta.
5. Krisnawati, S.Si, M.T. selaku Dekan Fakultas Ilmu Komputer
6. Ibu Nila Feby Puspitasari, S.Kom, M.Cs selaku Dosen Pembimbing skripsi yang telah memberikan pengarahannya dan bimbingan selama pelaksanaan skripsi dan penulisan laporan ini.
7. Ibu Mardhiya Hayaty, S.T., M.Kom. selaku dosen wali yang selalu memberikan arahan, motivasi, serta dukungan kepada peneliti.
8. Bapak Mustofa, SH. selaku kepala Kejaksaan Negeri Tuban yang telah memberikan izin kepada peneliti untuk melakukan penelitian.
9. Gobek Family yang telah menjadi keluarga selama di Jogja.
10. TKJ 15 juga yang telah menjadi keluarga dari saat SMK sampai saat ini.
11. Heda Vebriani yang telah memberi semangat.
12. Teman-teman seperjuangan Informatika 09 2015, terimakasih.
13. Para partner PUBG sampai pagi dan partner Badminton oaoe, terimakasih.
14. Dan semua pihak yang tidak dapat saya sebutkan satu-persatu.

Semoga kedepannya kami dapat menggunakan ilmu yang telah kami terima dengan sebaik baiknya dan mempunyai manfaat bagi diri saya dan orang lain.

Alvian Adhy Nugraha



## DAFTAR ISI

JUDUL.....	i
PERSETUJUAN.....	iii
PENGESAHAN.....	iv
PERNYATAAN.....	v
MOTTO.....	vi
PERSEMBAHAN.....	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR.....	xiv
INTISARI.....	xvi
<i>ABSTRACT</i> .....	xvii
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
1.4.1 Maksud Penelitian.....	4
1.4.2 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	5
1.5.1 Bagi Peneliti.....	5
1.5.2 Bagi Kejaksaan Negeri Tuban.....	5
1.5.3 Bagi Institusi Perguruan Tinggi.....	6
1.6 Metode Penelitian.....	6
1.6.1 Metode Pengumpulan Data.....	6
1.6.2 Metodologi Pengembangan.....	7
1.7 Sistematika Penulisan.....	8
BAB II LANDASAN TEORI.....	9
2.1 Tinjauan Pustaka.....	9

2.2	Parameter Kinerja Jaringan.....	10
2.3	Jaringan Wireless.....	11
2.3.1	Definisi Jaringan Wireless.....	11
2.3.2	Sejarah WLAN.....	12
2.3.3	Komponen WLAN.....	13
2.3.4	Kelebihan dan Kelemahan menggunakan Jaringan WLAN.....	16
2.3.5	Standart Wireless.....	17
2.4	Model referensi TCP/IP.....	17
2.5	User Datagram Protocol (UDP).....	18
2.6	Kemanan Jaringan.....	18
2.7	Jenis Serangan.....	19
2.7.1	Port Scanning.....	19
2.7.2	Spoofing.....	20
2.7.3	DOS(Denial Of Service).....	22
2.7.4	Teardrop.....	23
2.7.5	UDP Flood.....	24
2.7.6	Packet Interception.....	24
2.7.7	ICMP Flood.....	25
2.8	Tujuan Keamanan Komputer.....	25
2.9	Definisi Firewall.....	26
2.9.1	Karakteristik Firewall.....	26
2.9.2	Teknik Pengamanan Firewall.....	27
2.9.3	Jenis-Jenis Firewall.....	27
2.9.4	Konfigurasi Firewall.....	28
2.10	IDS ( <i>Intrusion Detection System</i> ).....	29
2.10.1	Definisi dan Konsep IDS ( <i>Intrusion Detection System</i> ).....	29
2.10.2	Jenis IDS ( <i>Intrusion Detection System</i> ).....	30
2.10.3	Keuntungan dan Kerugian IDS ( <i>Intrusion Detection System</i> ).....	31
2.10.4	Peran IDS ( <i>Intrusion Detection System</i> ).....	32
2.11	Perangkat Lunak dan Perangkat Keras.....	32
2.11.1	Snort.....	32
2.11.2	BASE ( <i>Basic Analysis And Security Engine</i> ).....	38
2.11.3	Nmap.....	39
2.11.4	Digital Blaster.....	39
2.11.5	IPTables.....	39
2.11.6	Hub.....	40
2.11.7	Ping Attack.....	40
2.12	Program Pendeteksi Intrusion Detection System (IDS).....	41
2.13	Pengertian Metodologi Penelitian.....	42
2.13.1	Pengertian Pengumpulan Data.....	42
2.13.2	Metode Pengembangan System.....	43



BAB III ANALISIS DAN PERANCANGAN .....	46
3.1 Tempat Penelitian .....	46
3.1.1 Mapping Ruangan Kantor Kejaksaan Negeri Tuban .....	47
3.1.2 Denah Kantor Kejaksaan Negeri Tuban .....	49
3.2 Alat Dan Bahan .....	50
3.2.1 <i>Software</i> (Perangkat Lunak) .....	50
3.2.2 <i>Hardware</i> (Perangkat Keras) .....	51
3.3 Prosedur dan Pengumpulan Data .....	52
3.3.1 Prosedur .....	52
3.3.2 Pengumpulan Data .....	52
3.4 Analisis dan Perancangan Sistem .....	54
3.4.1 Analisis Permasalahan Sistem .....	54
3.4.2 Analisis Kebutuhan Sistem .....	54
3.4.3 Rancangan Arsitektur Sistem .....	56
3.4.4 Perancangan Network Intrusion Detection System .....	58
BAB IV IMPLEMENTASI DAN PEMBAHASAN .....	62
4.1 Konfigurasi Komponen IDS .....	62
4.1.1 Instalasi Snort .....	62
4.1.2 Konfigurasi <i>Snort</i> Untuk Dijalankan Sebagai NIDS .....	63
4.1.3 Mengedit File <i>Snort.conf</i> .....	64
4.1.4 Menulis Aturan Sederhana untuk Menguji Deteksi Snort .....	65
4.1.5 Instalasi Barnyard2 .....	67
4.1.6 Installing PulledPork .....	70
4.1.7 Membuat SystemD startup script di Ubuntu 16 .....	72
4.1.8 Installing BASE on Ubuntu .....	74
4.2 Enforcement .....	78
4.2.1 Pengujian Komponen IDS .....	78
4.2.2 Pengujian Fungsionalitas Interkoneksi IDS .....	79
4.2.3 Pengujian Snort Dan BASE Dalam Mendeteksi Serangan .....	82
4.3 Hasil Analisa Kinerja Wireless Intrusion Detection System .....	84
4.4 Solusi Mengatasi Serangan .....	85
4.5 Keuntungan dan Hasil Menggunakan IDS .....	87
4.6 Enhancement .....	88
BAB V PENUTUP .....	89
5.1 Kesimpulan .....	89
5.2 Saran .....	91
DAFTAR PUSTAKA .....	92

## DAFTAR TABEL

Tabel 2.1 Kelemahan dan Kelebihan menggunakan Jaringan WLAN .....	16
Tabel 2.2 Protokol WLAN.....	17
Tabel 3.1 Tabel gambar mapping ruangan kantor Kejaksaan Negeri Tuban .....	47
Tabel 3.2 Software (Perangkat Lunak) .....	50
Tabel 3.3 Hardware (Perangkat Keras).....	51
Tabel 3.4 Rincian Topologi Fisik .....	60
Tabel 3.5 Rincian Topologi Fisik .....	61
Tabel 4.1 Konfigurasi Instalasi Snort .....	62
Tabel 4.2 Konfigurasi <i>Snort</i> Sebagai NIDS.....	63
Tabel 4.3 konfigurasi untuk mengedit file snort.conf.....	65
Tabel 4.4 Konfigurasi File Rules.....	66
Tabel 4.5 Konfigurasi Instalasi Barnyard2.....	68
Tabel 4.6 Konfigurasi MySQL untuk Barnyard2 .....	69
Tabel 4.7 Konfigurasi Instalasi PuledPork .....	70
Tabel 4.8 Konfigurasi Untuk Mengedit PuledPork.conf.....	71
Tabel 4.9 Menambahkan PuledPork ke Contab root .....	72
Tabel 4.10 Konfigurasi System Startup.....	72
Tabel 4.11 Konfigurasi Penginstalan BASE.....	74
Tabel 4.12 Hasil Analisa Kinerja WIDS ( <i>Wireless Intrusion Detection System</i> )..	85



## DAFTAR GAMBAR

Gambar 1.1 Security Policy Development Life Cycle (SPDLC) .....	7
Gambar 2.1 Jangkauan Area Antenna Omnidirectional .....	13
Gambar 2.2 Access Point.....	14
Gambar 2.3 Jaringan Menggunakan Extension Point.....	15
Gambar 2.4 WLAN Card.....	15
Gambar 2.5 NIDS ( <i>Network Intrusion Detection System</i> ).....	30
Gambar 2.6 HIDS ( <i>Host Intrusion Detection System</i> ).....	31
Gambar 2.7 Security Policy Development Life Cycle (SPDLC) .....	44
Gambar 3.1 Kantor kejaksaan Negeri Tuban.....	46
Gambar 3.2 Ruang SIMKARI .....	49
Gambar 3.3 Denah Kantor Kejaksaan Negeri Tuban Lantai 1 .....	49
Gambar 3.4 Denah Kantor Kejaksaan Negeri Tuban Lantai 2 .....	50
Gambar 3.5 Arsitektur Snort.....	57
Gambar 3.6 Flowchart Network Intrusion Detection System.....	57
Gambar 3.7 Topologi jaringan sebelum diterapkan sensor IDS .....	58
Gambar 3.8 Topologi jaringan setelah diterapkan sensor IDS .....	59
Gambar 4.1 Output setelah snort berhasil terinstall.....	63
Gambar 4.2 Output Setelah Snort berhasil dijalankan sebagai NIDS .....	65
Gambar 4.3 Output berhasil membuat aturan untuk snort agar mengingatkan .....	67
Gambar 4.4 <i>Output</i> Barnyard2 berhasil terinstall.....	69
Gambar 4.5 Database MySQL.....	70
Gambar 4.6 Output Pulledpork berhasil terinstall .....	70
Gambar 4.7 Output ICMP event yang ditulis di database .....	72

Gambar 4.8 Snort berhasil berjalan pada saat booting .....	73
Gambar 4.9 Barnyard berhasil berjalan pada saat booting .....	74
Gambar 4.10 Konfigurasi BASE .....	76
Gambar 4.11 Konfigurasi BASE .....	76
Gambar 4.12 Konfigurasi BASE .....	76
Gambar 4.13 Konfigurasi BASE .....	77
Gambar 4.14 Konfigurasi BASE .....	77
Gambar 4.15 Konfigurasi BASE .....	77
Gambar 4.16 Home page BASE setelah dilakukan konfigurasi .....	77
Gambar 4.17 Pengujian Fungsi Snort .....	79
Gambar 4.18 Pengujian Fungsi BASE .....	79
Gambar 4.19 Pengujian Serangan Ping Attack (ICMP Traffic) .....	81
Gambar 4.20 Pengujian Serangan Nmap Port Scanning Attack .....	82
Gambar 4.21 Pengujian Serangan DDos TCP menggunakan Digital Blaster .....	82
Gambar 4.22 Pendeteksi serangan di BASE .....	83
Gambar 4.23 Tampilan Daftar Alert ICMP pada Traffic Profile By Protokol .....	84
Gambar 4.24 Tampilan Daftar Alert TCP pada Traffic Profile By Protokol .....	84
Gambar 4.25 ketika memblok penyerang dalam melakukan <i>Ping Attack</i> .....	86
Gambar 4.26 ketika nmap (Zenmap GUI) ketika dilakukan pemblokiran .....	87

## INTISARI

Kemanan jaringan saat ini menjadi kebutuhan yang sangat penting dalam menjaga validitas dan integritas data bagi *penggunanya*. Sistem harus dilindungi dari berbagai macam serangan dan usaha penyusupan oleh pihak yang tidak berhak, serangan yang dapat mengganggu dan bahkan merusak sistem koneksi antar perangkat yang terhubung akan sangat berbahaya. IDS (*Intrusion Detection System*) adalah sebuah aplikasi perangkat lunak yang dapat mendeteksi aktifitas yang mencurigakan dalam sebuah sistem jaringan, melakukan analisis dan mencari bukti dari percobaan *intruder* (penyusup).

WIDS (*Wireless Intrusion Detection System*) mampu mendeteksi serangan DOS (*Denial of Service*), *Ping Of Death*, Menerapkan pada sistem operasi Linux menggunakan Snort, ACID, BASE, *Barnyard*, pada mesin sensor IDS dan *Iptables* sebagai penanganan dari serangan yang mengancam. Penelitian ini ialah instalasi aplikasi IDS beserta dengan sensor IDS, uji aktifitas normal, pengujian performa memori, dan pengujian respon deteksi.

Metode yang saya gunakan adalah SPDLC (*Security Policy Development Life Cycle*). Hasil penelitian ini menyimpulkan bahwa IDS yang di terapkan dapat mendeteksi intruder atau penyusup pada mesin sensor IDS yang ditampilkan pada BASE (*Basic Analysis and Security Engine*). Aplikasi sistem keamanan jaringan IDS (*Intrusion Detection System*) berbasis *open source*.

**Kata Kunci:** *Wireless*, IDS (*Intrusion Detection System*), BASE (*Basic Analysis and Security Engine*), Keamanan Jaringan, Linux, Snort, *Iptables*, *open source*.



## ***ABSTRACT***

*Network security is now a very important requirement in maintaining data validity and integrity for its users. The system must be protected from various attacks and infiltration efforts by unauthorized parties, attacks that can interfere and even damage the connection system between connected devices will be very dangerous. IDS (Intrusion Detection System) is a software application that can detect suspicious activities in a network system, conduct analysis and look for evidence from intruder experiments (intruders).*

*WIDS (Wireless Intrusion Detection System) is able to detect DOS (Denial of Service) attacks, Ping of Death, Implement Linux operating systems using Snort, ACID, BASE, Barnyard, on IDS sensor machines and Iptables as a defense from threatening attacks. This research is the installation of IDS applications along with IDS sensors, normal activity tests, memory performance testing, and detection response testing.*

*The method I use is SPDL (Security Policy Development Life Cycle). The results of this study conclude that the applied IDS can detect intruders or intruders on the IDS sensor machine displayed on BASE (Basic Analysis and Security Engine). The application of the IDS (Intrusion Detection System) network security system is based on open source.*

**Keyword:** *Wireless, Intrusion Detection System (IDS), Basic Analysis and Security Engine (BASE), Network Security, Linux, Snort, Iptables, open source.*