

**ANALISIS KEAMANAN JARINGAN NIRKABEL MENGGUNAKAN  
WIRELESS INTRUSION DETECTION SYSTEM  
(Studi Kasus: Kantor Kejaksaan Belitung Timur)**

**SKRIPSI**



disusun oleh

**Ferda suganda**

**14.11.7894**

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

2018

**ANALISIS KEAMANAN JARINGAN NIRKABEL MENGGUNAKAN  
WIRELESS INTRUSION DETECTION SYSTEM  
(Studi Kasus: Kantor Kejaksaan Belitung Timur)**

**SKRIPSI**

untuk memenuhi sebagian persyaratan  
mencapai gelar Sarjana  
pada Program Studi Informatika



disusun oleh

**Ferda suganda**

**14.11.7894**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2018**

**PERSETUJUAN**

**SKRIPSI**

**ANALISIS KEAMANAN JARINGAN NIRKABEL MENGGUNAKAN  
WIRELESS INTRUSION DETECTION SYSTEM  
(Studi Kasus: Kantor Kejaksaan Belitung Timur)**

yang dipersiapkan dan disusun oleh

**Ferda Suganda**

**14.11.7894**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 10 Juli 2017

Dosen Pembimbing,



**Joko Dwi Santoso, M.Kom.**

**NIK. 190302181**

**PENGESAHAN**

**SKRIPSI**

**ANALISIS KEAMANAN JARINGAN NIRKABEL MENGGUNAKAN  
WIRELESS INTRUSION DETECTION SYSTEM  
(Studi Kasus: Kantor Kejaksaan Belitung Timur)**

yang dipersiapkan dan disusun oleh

**Ferda Suganda**

**14.11.7894**

telah dipertahankan di depan Dewan Penguji  
pada tanggal 15 Maret 2018

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

**Joko Dwi Santoso, M.Kom.**  
NIK. 190302181



**Sri Ngudi Wahyuni, S.T., M.Kom.**  
NIK. 190302060



**Bayu Setiaji, M.Kom**  
NIK. 190302216

Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
tanggal 16 April 2018

**DEKAN FAKULTAS ILMU KOMPUTER**



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

## PERNYATAAN

Saya yang bertandatangan dibawah 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 adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 15 Maret 2018



Ferda Suganda  
NIM. 14.11.7894

## **Motto**

*"Kegagalan hanya terjadi bila kita menyerah"*

*"Harta yang paling indah didunia ini  
adalah orangtua"*

*"Ada 3 kunci keberhasilan yaitu keyakinan,  
kesungguhan dan kesabaran"*

*"Kesempurnaan hanya milik Alloh SWT"*



## PERSEMBAHAN

Alhamdulillah penulis panjatkan puji syukur atas kepada Allah SWT atas segala rahmat dan hidayahnya, sehingga berkesempatan untuk menyelesaikan skripsi ini dengan segala kekurangan penulis. Segala syukur penulis ucapkan kepadaMu karena telah menghadirkan mereka yang memberikan semangat dan do" a disaat menjalani proses pembuatan skripsi ini. Dengan segala kerendahan hati, saya persembahkan Skripsi ini kepada :

1. Ayah dan ibu tercinta, terimakasih atas segenap ketulusan cinta dan kasih sayangnya selama ini. Untuk segala do" a, nasehat, perjuangan dan pengorbanan untukku.
2. Dosen Pembimbing saya Joko Dwi Santoso, M.Kom yang selama ini sudah sabar membimbing Skripsi saya hingga terselesaikan sebaikbaiknya.
3. Keluarga Kejaksaan Belitung Timur yaitu Bapak Widagdo, S.H, Ibu Sumati, Bapak Andrie P. S.H, Bapak Amardi P.B., SH.MH, Bapak Samsi Thalib, SH.MH, Bapak Adi Candra, S.H., M.H, Bapak Fiskan W. A.Md dan staff kariawan kantor yang tidak bias saya sebutkan namanya satu per satu, yang membantu dan mendukung dalam memberikan informasi sehingga skripsi ini terselesaikan.
4. Teman-teman seangkatan 14 S1 TI 05 yang tidak mungkin untuk disebutkan satu persatu. Terimakasih atas semuanya yang melengkapi keseharian dalam menimba ilmu.
5. Teman seperjuangan skripsi Yanti, Zegy.

Saya ucapkan terimakasih yang sebesar-besarnya, mohon maaf jika ada salah kata baik sengaja atau tidak selama ini. Sukses buat kalian semua dil ancarkan segala urusannya, semoga Allah SWT memberikan rahmat dan hidayahnya kepada kita semua, Amin.....

## KATA PENGANTAR

*Assalamu'alaikum Wr. Wb*

Alhamdulillah penulis panjatkan puji syukur kehadirat Allah SWT atas berkat, rahmat dan hidayah-Nya, penyusun skripsi yang berjudul “Analisi Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System (studi kasus: Kantor Kejaksaan Belitung Timur)” dapat diselesaikan dengan baik.

Penulis menyadari bahwa dalam proses penulisan skripsi ini banyak mengalami kendala, namun berkat bantuan, bimbingan, kerjasama dari berbagai pihak dan berkah dari Allah SWT sehingga kendala-kendala yang dihadapi tersebut dapat dibatasi. Untuk itu penulis menyampaikan ucapan terimakasih dan penghargaan kepada Bapak Joko Dwi Santoso, M.Kom selaku pembimbing yang telah dengan sabar, tekun, tulus dan ikhlas meluangkan waktu, tenaga dan pikiran memberikan bimbingan, motivasi, arahan dan saran-saran yang sangat berharga kepada penulis selama menyusun skripsi.

Selanjutnya ucapan terimakasih penulis sampaikan pula kepada :

1. Bapak Prof, Dr. M.Suyanto,M.M selaku Rektor Universitas Amikom Yogyakarta.
2. Bapak Joko Dwi Santoso, M.Kom selaku Dosen Pembimbing yang telah memberikan banyak masukan yang membantu dalam menyelesaikan skripsi.
3. Ibu Krisnawati, S.Si,M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. Dosen penguji, segenap dosen dan karyawan Universitas Amikom Yogyakarta yang telah memberikan masukan terhadap penelitian ini.
5. Ayah dan Ibu yang telah mendukung dan menyemangati selama menyelesaikan skripsi.
6. Dony Ariyus, M.Kom. Yang telah memberikan masukan terhadap penelitian ini.



7. Bapak Widagdo, S.H, Ibu Sumati, Bapak Andrie P. S.H, Bapak Amardi P.B., SH.MH, Bapak Samsi Thalib, SH.MH, Bapak Adi Candra, S.H., M.H, Bapak Fiskan W. A.Md dan staff kariawan selaku dari pihak Kantor Kejaksaan Belitung Timur.
8. Teman-teman seangkatan 14 S1 TI 05 yang tidak mungkin untuk disebutkan satu persatu yang telah bersama-sama menempuh perkuliahan dalam satu kelas.

Akhirnya, dengan segala kerendahan hati penulis menyadari masih banyak terdapat kekurangan-kekurangan, sehingga penulis mengharapkan adanya saransaran dan kritik yang bersifat membangun demi kesempurnaan skripsi ini.

*Wassalamu'alaikum Wr. Wb.*

Yogyakarta, 15 Maret 2018



Ferda Suganda  
NIM. 14.11.7894

## DAFTAR ISI

PERSETUJUAN .....	iii
PERNYATAAN.....	iv
Motto.....	v
PERSEMBAHAN.....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR .....	xiv
DAFTAR TABEL.....	xvii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	4
1.6 Metode Penelitian.....	4
1.6.1 Metode Pengumpulan Data.....	4
1.6.2 Metode Pengembangan.....	5
1.7 Sistematika Penulisan.....	6
BAB II LANDASAN TEORI.....	7
2.1 Tinjauan pustaka.....	7
2.2 Pengertian Analisa.....	8
2.3 Jaringan Wireless .....	9
2.3.1 Definisi Dan Konsep Jaringan Wireless .....	9
2.3.2 Sejarah Dan Standar WLAN.....	10
2.3.3 Media Transmisi WLAN.....	11

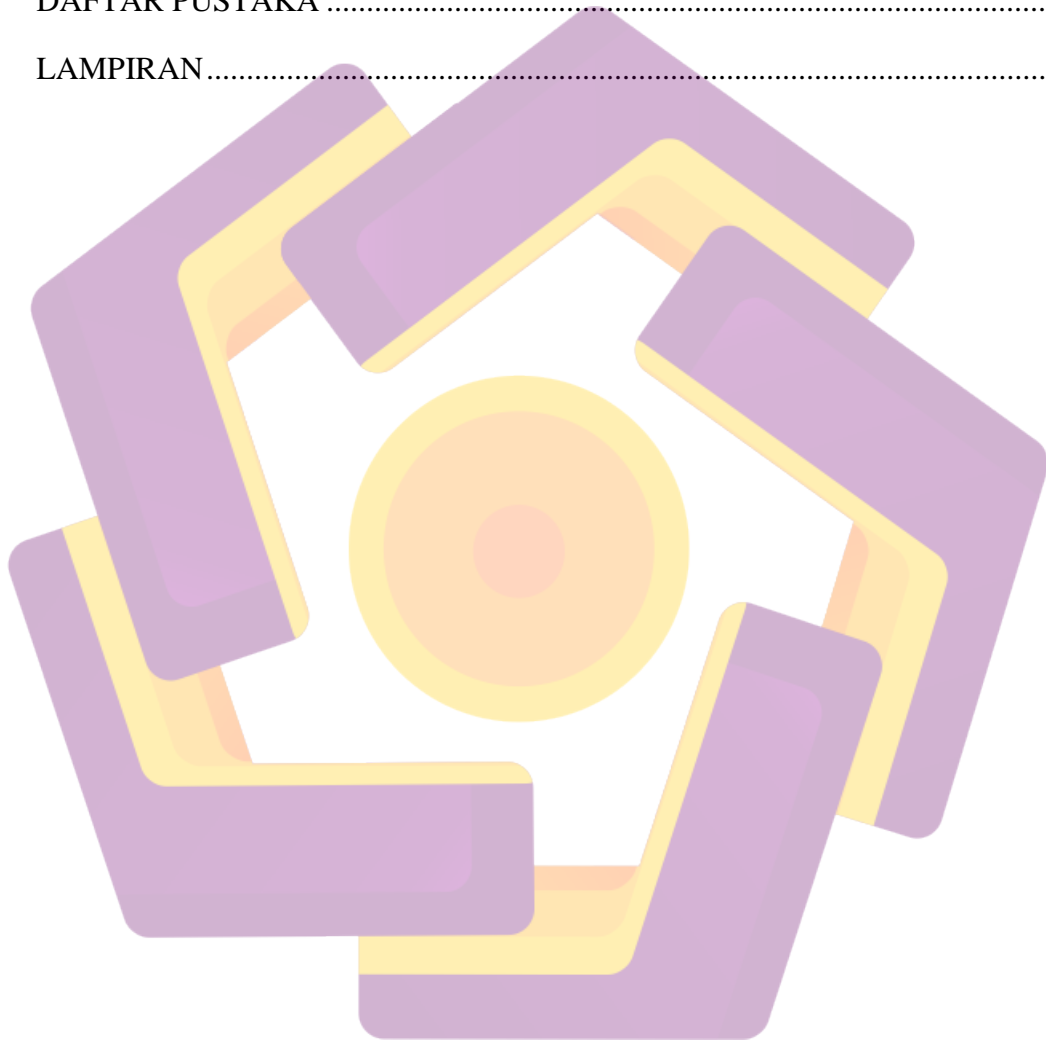
2.3.3.1	Frekuensi Radio (RF).....	11
2.3.3.2	Infrared(IR) .....	11
2.3.4	Komponen WLAN .....	12
2.3.4.1	Antena .....	12
2.3.4.2	Access Point (AP) .....	13
2.3.4.3	Extension Point .....	13
2.4	Model referensi TCP/IP.....	14
2.5	User Datagram Protocol (UDP) .....	14
2.6	Jenis Serangan .....	15
2.6.1	<i>Port Scanning</i> .....	15
2.6.2	<i>Teardrop</i> .....	16
2.6.3	<i>Spoofing</i> .....	16
2.6.4	<i>Land Attack</i> .....	18
2.6.6	<i>UDP Flood</i> .....	19
2.6.7	<i>Packet Interception</i> .....	19
2.6.8	<i>CMP Flood</i> .....	19
2.6.9	<i>Traceroute</i> .....	20
2.7	Keamanan Jaringan .....	21
2.8	Tujuan Keamanan Komputer .....	21
2.9	Definisi Firewall.....	22
2.9.1	Karakteristik <i>Firewall</i> .....	22
2.9.2	Teknik Pengaman <i>Firewall</i> .....	22
2.9.3	Jenis-Jenis <i>Firewall</i> .....	23
2.9.4	Konfigurasi Firewall .....	23
2.10	IDS ( <i>Intrusion Detection System</i> ).....	24

2.10.1	Definisi Dan Konsep IDS .....	24
2.10.2	Jenis <i>Intrusion Detection System</i> ( IDS) .....	25
2.10.2.1	NIDS (Network Intrusion Detection System) .....	25
2.10.2.2	HIDS ( <i>Host Intrusion Detection System</i> ).....	25
2.10.3	Keuntungan dan kerugian IDS .....	26
2.10.4	Peran IDS ( <i>Intrusion Detection System</i> ) .....	27
2.11	Snort .....	27
2.11.1	Komponen Snort .....	28
2.11.3	Fitur-Fitur Snort .....	28
2.11.3	BASE ( <i>Basic Analysis And Security Engine</i> ).....	29
2.11.4	IP Tables.....	29
2.11.5	<i>DOS (Denial Of Service)</i> .....	30
2.4.1.1	Nmap.....	31
2.12	Pengertian Metodologi Penelitian .....	31
2.12.1	Pengertian Pengumpulan Data .....	31
2.12.2.	Metode pengembangan system .....	32
2.12.2.1.	<i>Analysis</i> .....	33
2.12.2.2.	<i>Design</i> .....	33
2.12.2.3.	<i>Implementation</i> .....	33
2.12.2.4.	<i>Enforcement</i> .....	33
2.12.2.5.	<i>Enhancement</i> .....	33
BAB III ANALISIS DAN PERANCANGAN .....		34
3.1	Gambaran Umum .....	34
3.1.1	Profile.....	34
3.1.2	Visi Kejaksaaan .....	35

3.1.3	Misi Kejaksaan.....	35
3.1.4	Fasilitas Kantor Kejaksaan Belitung Timur.....	36
3.1.4.1	Mapping Ruangan .....	37
3.1.4.2	Ruangan Pengiriman Data.....	38
3.1.5	Struktur Organisasi Kantor Kejaksaan Belitung Timur .....	39
3.1.6	Denah Kantor .....	40
3.1.7	Sistem Jaringan Kantor Kejaksaan Belitung Timur.....	40
3.2	Identifikasi Masalah .....	41
3.2.1	Analisis Sistem.....	41
3.2.2	Analisis <i>WIFI</i> .....	41
3.2.3	Standarisasi Jaringan Wireless.....	42
3.2.4	Jenis Keamanan <i>Wifi</i> .....	43
3.2.4.1	Hide SSID .....	43
3.2.4.2	WEP .....	44
3.2.4.3	WPA-PSK atau WPA2-PSK.....	44
3.2.4.4	Kelemahan dan Kekurangan <i>Wifi</i> .....	45
3.2.3	Analisis IDS( <i>Intrusion Detection System</i> ) dengan Snort.....	45
3.3	Analisis Masalah .....	46
3.3.1	Solusi untuk mengetahui aktifitas jaringan dari penyadapan ataupun penyerangan.....	49
3.4	Analisis pengembangan system.....	49
3.4.1	<i>Analysis</i> (Analisis) .....	49
3.4.1.1	Spesifikasi Sistem Yang Akan Dibangun .....	50
3.4.1.2	Spesifikasi Perangkat Lunak.....	50
3.4.1.3	Spesifikasi perangkat keras .....	51

3.4.2	<i>Design</i> (Perancangan) .....	51
3.4.3	<i>Implementation</i> (implementasi) .....	53
BAB IV HASIL DAN PEMBAHASAN .....		54
4.1.	Konfigurasi Mesin Snort .....	54
4.1.1	Instalasi Snort.....	54
4.1.2	Konfigurasikan Snort Untuk Jalankan Sebagai NIDS .....	55
4.1.2.1	Basic konfigurasi.....	55
4.1.2.2	Mengedit File Konfigurasi Snort .....	57
4.1.3	Writing And Testing Single Rule Dengan Snort .....	58
4.1.4	Instaling Barnyard2.....	60
4.1.5	Installing PulledPork.....	63
4.1.6	Creating a systemd startup script in Ubuntu 16 .....	66
4.1.7	Installing BASE On Ubuntu .....	68
4.2	<i>Enforcement</i> .....	71
4.2.1	Pengujian Komponen IDS .....	71
4.2.1.1	Pengujian Snort .....	71
4.2.1.2	Pengujian BASE .....	72
4.2.3	Pengujian Fungsionalitas Interkoneksi IDS .....	72
4.2.3.1	Kasus 1: Ping Attack (ICMP Traffic) .....	73
4.2.3.2	Kasus 2: Nmap Port Scanning Attack .....	73
4.2.3.3	Kasus 3: DDOS .....	74
4.2.3	Pengujian Snort Dan Base Dalam Pendeteksian Serangan .....	75
4.3	Solusi Mengatasi Serangan.....	77
4.4	Keuntungan dan Hasil Menggunakan IDS ( <i>Intrusion Detection System</i> ) .....	79

4.5	<i>Enhacemen</i> .....	79
BAB V KESIMPULAN.....		80
5.1	Kesimpulan.....	80
5.2	Saran.....	81
DAFTAR PUSTAKA .....		82
LAMPIRAN.....		83

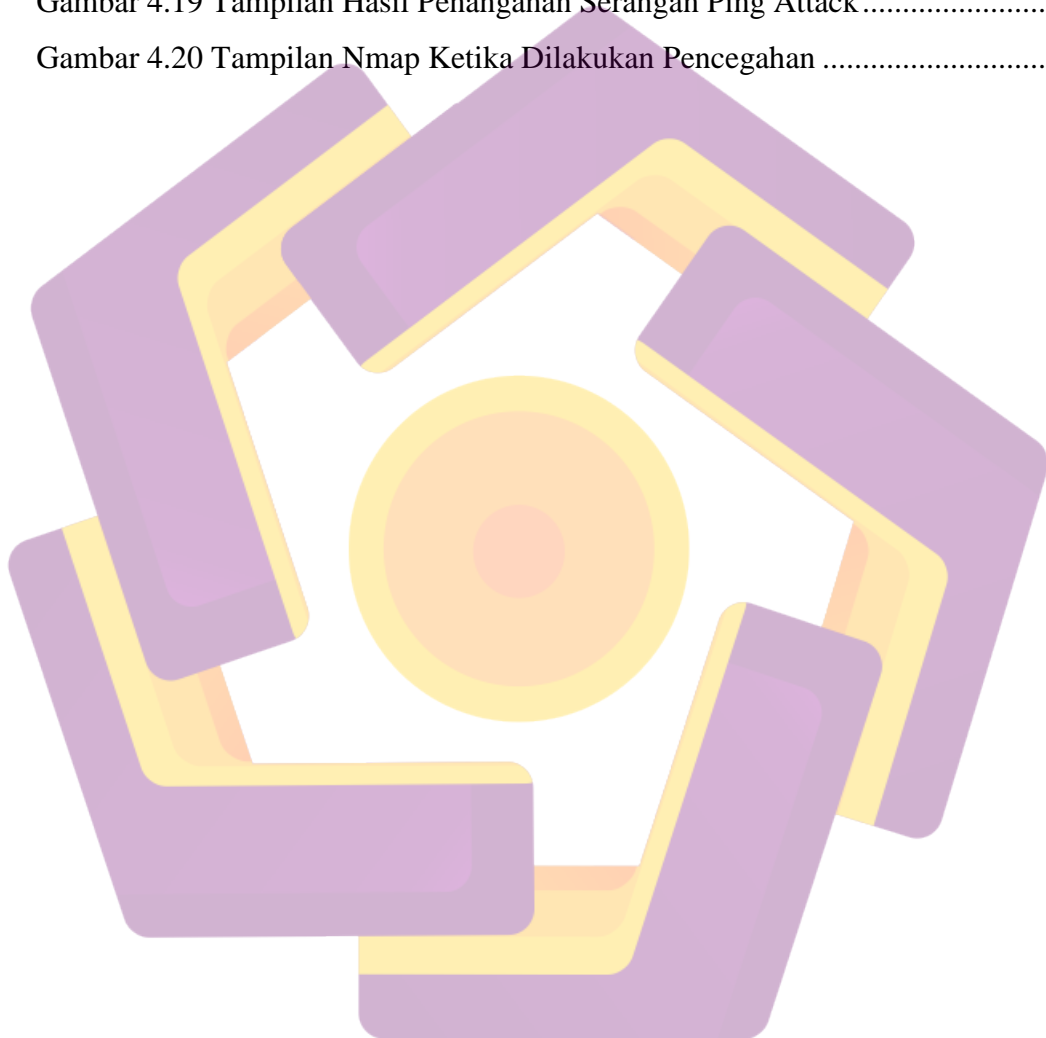


## DAFTAR GAMBAR

Gambar 1.1 SPDLC (Security Policy Development Life Cycle).....	5
Gambar 2.1 Jangkauan Area Antenna Omnidirectional .....	13
Gambar 2.2 Access Point .....	13
Gambar 2.3 Jaringan Menggunakan Extention Point .....	14
Gambar 2.4 Network-Base IDS .....	25
Gambar 2.5 Host-Base IDS.....	26
Gambar 2.6 Security Policy Development Life Cycle (SPDLC).....	33
Gambar 3.1 Kantor Kejaksaan Belitung Timur .....	35
Gambar 3.2 Ruang Pengiriman Data.....	39
Gambar 3.3 Denah Kantor Kejaksaan Belitung Timur.....	40
Gambar 3.4 Proses koneksi di jaringan wifi .....	46
Gambar 3.5 Aliran Paket Data Normal di Jaringan Wifi.....	47
Gambar 3.6 Proses Penyesuaian Koneksi di Jaringan Wifi.....	47
Gambar 3.7 Paket Data Tidak Normal Akan Melalui Penyadap.....	48
Gambar 3.8 Topologi Jaringan.....	52
Gambar 3.9 Rancangan Alur Penelitian.....	52
Gambar 4.1 Proses Instalasi Snort .....	55
Gambar 4.2 Output Berhasil Mengkonfigurasi Snort Untuk Dijalankan Sebagai NIDS .....	58
Gambar 4.3 Output Berhasil Membuat Aturan Untuk Snort Untuk Mengingat .....	60
Gambar 4.4 Database MySQL .....	62
Gambar 4.5 Barnyard2 Berhasil Terinstall .....	62
Gambar 4.6 Sukses Konfigurasi Barnyard2.....	63
Gambar 4.7 Instalasi PulledPork.....	65
Gambar 4.8 SystemD telah berhasil.....	67
Gambar 4.9 Tampilan Basic Analysis and Security Engine (BASE) .....	70
Gambar 4.10 Pengujian Fungsi Snort .....	71
Gambar 4.11 pengujian Fungsi Base .....	72
Gambar 4.12 Pengujian Serangan Ping Attack.....	72



Gambar 4.13 Pengujian Serangan Nmap .....	73
Gambar 4.15 Pendeteksian Serangan di BASE.....	74
Gambar 4.16 Tampilan Daftar Alert ICMP pada Traffic Profile By Protokol .....	75
Gambar 4.17 Tampilan Daftar Alert TCP pada Traffic Profile By Protokol.....	75
Gambar 4.18 DROP IP Dengan Iptables .....	76
Gambar 4.19 Tampilan Hasil Penanganan Serangan Ping Attack.....	77
Gambar 4.20 Tampilan Nmap Ketika Dilakukan Pencegahan .....	77



## DAFTAR TABEL

Tabel 2.1 Point Dan Jenis Serangan.....	20
Tabel 3.1 Unit kerja standarisasi LAN dan WAN .....	43
Tabel 3.2 Spesifikasi Sistem Yang Akan Dibangun .....	50
Tabel 3.3 Spesifikasi Software.....	50
Tabel 3.4 Spesifikasi Hardware .....	51
Tabel 4.1 Inastallasi Snort.....	55
Table 4.2 Basic Konfigurasi Snort Untuk Jalankan Sebagai NIDS .....	56
Tabel 4.3 Edit File Konfigurasi Snort.....	58
Table 4.4 Rule .....	59
Table 4.5 Install Dan Konfigurasi Barnyard2 .....	61
Table 4.6 Database MySQL dan Pengujian Barnyard2 .....	62
Tabel 4.7 Installing PulledPork.....	64
Table 4.8 Creating a systemd startup script in Ubuntu 16 .....	67
Tabel 4.9 Installing BASE On Ubuntu .....	69
Tabel 4.10 Editing File Config.....	70

## INTISARI

Sistem keamanan jaringan menjadi sangat penting dalam menjaga jaringan, serangan yang dapat mengganggu dan bahkan merusak sistem koneksi antar perangkat yang terhubung akan sangat berbahaya. Untuk mendapatkan keamanan di jaringan kadang-kadang kita harus merasakan ketidaknyamanan dalam penggunaannya, ini sering menjadi pertimbangan dalam penerapan sistem keamanan jaringan di Kantor Jaksa Belitung Timur.

WIDS (*Wireless Intrusion Detection System*) mampu mendeteksi serangan DOS (*Denial of Service*), *Ping Of Deat*. Menerapkan pada sistem operasi Linux menggunakan Snort, ACID BASE, Barnyard, pada mesin sensor IDS dan *Iptables* sebagai penanganan serangan dapat menjadi solusi keamanan jaringan nirkabel dari serangan yang mengancam.

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

**Kata kunci:** Wireless, IDS (*Intrusion Detection System*), *Denial of Service*, *Ping Of Deat*, *Iptables*, Keamanan Jaringan, Linux, Snort, ACID BASE, *Security Policy Development Life Cycle*.

## ABSTRACT

*Abstract - Network security system becomes very important in maintaining a network, attacks that can interfere and even damage the connection system between devices connected will be very harmful. To gain security in a network sometimes we have to feel the discomfort in its use, this is often a consideration in the application of a network security system in the East Belitung Prosecutor's Office.*

*WIDS (Wireless Intrusion Detection System) is capable of detecting DOS attacks (Denial of Service), Ping Of Deat. Implementing on a Linux operating system using Snort, ACID BASE, Barnyard, on IDS sensor engines and Iptables as an attack handling can be a wireless network security solution of threatening attacks.*

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

**Keywords:** *Wireless, IDS (Intrusion Detection System), Denial of Service, Ping Of Deat, Iptables, Network Security, Linux, Snort, ACID BASE, Barnyard, Security Policy Development Life Cycle.*