

**IMPLEMENTASI KEAMANAN JARINGAN MENDETEKSI
ADANYA PEYUSUPAN PADA SERVER MENGGUNAKAN
IDS DENGAN SNORT DI WARNET CYBER TOBOALI
KABUPATEN BANGKA SELATAN**

SKRIPSI



ARIE PRATAMA

1511500036

**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
ATMA LUHUR
PANGKALPINANG**

2019

**IMPLEMENTASI KEAMANAN JARINGAN MENDETEKSI
ADANYA PEYUSUPAN PADA SERVER MENGGUNAKAN
IDS DENGAN SNORT DI WARNET CYBER TOBOALI
KABUPATEN BANGKA SELATAN**

SKRIPSI

**Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer**



Oleh :

ARIE PRATAMA

1511500036

**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
ATMA LUHUR
PANGKALPINANG**

2019

LEMBAR PENGESAHAN SKRIPSI

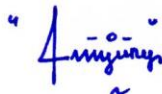
**IMPLEMENTASI KEAMANAN JARINGAN MENDETEKSI ADANYA
PEYUSUPAN PADA SERVER MENGGUNAKAN IDS
DENGAN SNORT DI WARNET CYBER TOBOALI
KABUPATEN BANGKA SELATAN**

Yang dipersiapkan dan disusun oleh

ARIE PRATAMA
1511500036

Telah dipertahankan di depan Dewan Penguji
Pada Tanggal 05 Juli 2019

Dosen Penguji II



Dwi Yuny Sylfania, M.Kom.
NIDN.0207069301

Dosen Pembimbing



Benny Wijaya, S.T, M.Kom
NIDN. 0202097902

Kaprodi Teknik Informatika



R. Burham Isnanto F, S.Si, M.Kom
NIDN. 0224048003

Dosen Penguji I



Dian Novianto, S.Kom., M.Kom
NIDN.0209119001

Skripsi ini telah diterima dan sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 12 Juli 2019

KETUA STMIK ATMA LUHUR PANGKALPINANG



Dr. Husni Feja Sukmana, ST. M.Sc.

LEMBAR PERNYATAAN

Nama : Arie Pratama
NIM : 1511500036
Judul Skripsi : **IMPLEMENTASI KEAMANAN JARINGAN
MENDETEKSI ADANYA PEYUSUPAN PADA
SERVER MENGGUNAKAN IDS DENGAN SNORT
DI WARNET CYBER TOBOALI KABUPATEN
BANGKA SELATAN**

Menyatakan bahwa laporan tugas akhir saya adalah hasil karya sendiri, tidak membeli, tidak membayar pihak lain untuk membuatkan, dan bukan plagiat. Apabila ternyata ditemukan didalam laporan tugas akhir saya terdapat unsur di atas maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Pangkalpinang, 01 Juli 2019



Arie Pratama

NIM.1511500036

KATA PENGANTAR

BISMILLAHIRROHMANNIRROHIM

Sebagai umat yang beriman, marilah penulis panjatkan puji syukur kehadiran Tuhan yang Maha Esa, yang telah memberikan rahmat, hidayah serta nikmat-Nya kepada penulis sehingga dapat menyelesaikan skripsi ini tepat pada waktunya, Penelitian ini yang berjudul “Implementasi Keamanan Jaringan Mendeteksi Adanya Penyusupan pada *Server* Menggunakan IDS Dengan Snort di Warnet Cyber Toboali Kabupaten Bangka Selatan.”

Pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih dan penghargaan kepada yang terhormat :

1. Allah SWT yang telah menciptakan dan memberikan kehidupan di dunia
2. Keluarga, Bapak dan Ibu serta Adik saya yang telah mendoakan dan memberikan dukungan kepada saya baik secara moril maupun material.
3. Bapak Dr. Husni Teja Sukmana, ST. M.Sc selaku Ketua STMIK Atma Luhur Pangkalpinang dimana penulis menuntut ilmu.
4. Bapak R. Burham Isnanto Farid, S.Si, M.Kom selaku Kaprodi Teknik Informatika.
5. Bapak Benny Wijaya, S.T, M.Kom selaku dosen pembimbing skripsi.
6. Sahabat terbaik saya yang menemani hingga saat ini, Rangga, Fadhel Muhammad.
7. Kekasih saya Hellen Saparindah yang memberikan motivasi saya dan memberi semangat untuk mengerjakan skripsi saya sampai selesai.
8. Teman-teman seperjuangan yang telah membantu saya secara langsung maupun tidak langsung dalam mengerjakan laporan ini

Saya mengharapkan sekali masukan yang sifatnya membangun, supaya penulis dapat lebih baik lagi dimasa mendatang. Demikianlah laporan skripsi ini saya buat, semoga bermanfaat bagi kita semua.

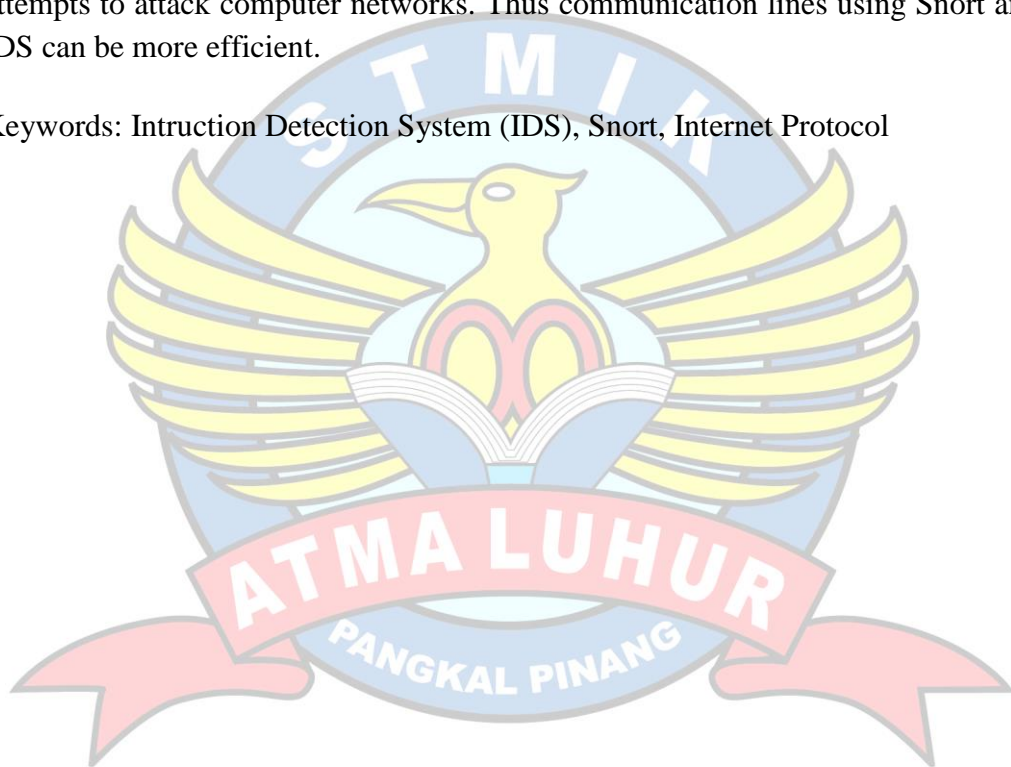
Pangkalpinang 01 Juli 2019

Penulis,

ABSTRACT

The problems that exist in cyber internet are located in the level of internet cafe security that is currently running is still missing, therefore within a few months the cyber warnet server has experienced problems due to attacks carried out by other parties such as flood ping, smurf attack and others. There are several alternative solutions to overcome the problems of internet cafe security that are less than optimal, one of which is the application of the IDS (Intrusion Detection System) method. This system works by making a warning that an intrusion from outside can read the parameters in the attacker's IP (Internet Protocol) address. With the implementation of this application, the system is able to close access to attempts to attack computer networks. Thus communication lines using Snort and IDS can be more efficient.

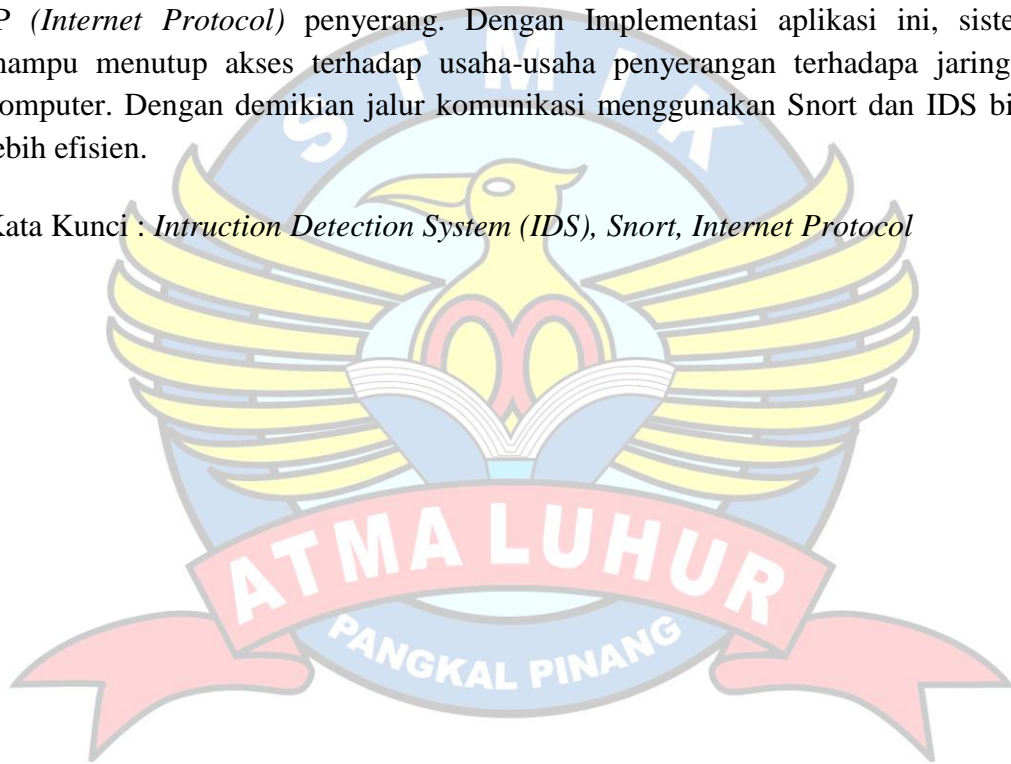
Keywords: Intrusion Detection System (IDS), Snort, Internet Protocol



ABSTRAK

Permasalahan yang ada diwarnet *cyber* terletak pada tingkat keamanan *server* warnet yang saat ini berjalan masih belum ada, oleh karena itu dalam beberapa bulan kebelakangan *server* warnet *cyber* mengalami permasalahan karena adanya penyerangan yang dilakukan oleh pihak lain seperti ping flood, smurf attack dan lain - lain. Ada beberapa alternatif solusi untuk mengatasi permasalahan keamanan warnet yang kurang maksimal salah satunya adalah penerapan metode IDS (*Intrusion Detection System*). Sistem ini bekerja dengan membuat peringatan bahwa adanya penyusupan dari luar yang bisa membaca parameter berupa alamat IP (*Internet Protocol*) penyerang. Dengan Implementasi aplikasi ini, sistem mampu menutup akses terhadap usaha-usaha penyerangan terhadap jaringan komputer. Dengan demikian jalur komunikasi menggunakan Snort dan IDS bisa lebih efisien.

Kata Kunci : *Intrusion Detection System (IDS), Snort, Internet Protocol*



DAFTAR ISI

	Halaman
LEMBAR PENGESAHAN SKRIPSI	i
LEMBAR PERNYATAAN	ii
KATA PENGANTAR.....	iii
ABSTRACT	iv
ABSTRAK	v
DAFTAR ISI.....	vi
DAFTAR GAMBAR.....	ix
DAFTAR TABEL	xi
DAFTAR SIMBOL	xii
 BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian	3
1.5 Sistematika Penulisan	3
 BAB II LANDASAN TEORI	
2.1. Intrusion Detection System (IDS).....	5
2.2. Metode Deteksi	6
2.3. Model Open System Interconnection (OSI)	8
2.3.1 Snort 2.9.13	10
2.3.2 Mode Snort.....	11
2.3.3 Komponen Snort	12
2.3.4 Rule	14
2.3.5 Alerts	15
2.3.6 Mode Pengoperasian	16

BAB III METODOLOGI PENELITIAN

3.1. Model Pengembangan Sistem.....	25
3.2. Metode Pengembangan	27
3.3. Pengembangan Sistem	28

BAB IV PEMBAHASAN

4.1. Sejarah Singkat Warnet Cyber Toboali	29
4.2. Struktur Organisasi	29
4.3. Analisis	30
4.3.1 Analisis Sistem Berjalan.....	30
4.3.2 Pemecahan Masalah.....	30
4.4. Analisis Kebutuhan.....	30
4.5. Rancangan Sistem.....	31
4.5.1 Activity Diagram	31
4.5.2 Deplomymment Diagram.....	32
4.5.3 Rancangan Aplikasi	33
4.5.4 Manajemen Jaringan Usulan.....	33
4.5.5 Topologi Jaringan Usulan.....	34
4.6. Konfigurasi Snort	34
4.6.1 Pengenalan Snort	34
4.6.2 Instalasi Snort.....	36
4.7. Pengujian Jaringan	42
4.7.1 Konfigurasi IP	42
4.7.2 Konfigurasi Rules	43
4.7.3 Menjelankan Snort	43
4.7.4 Pengujian Jaringan Akhir.....	44
4.8. Tahapan Pengujian	45
4.9. Analisis	47

BAB V PENUTUP

5.1. Kesimpulan 49

5.2. Saran 49

DAFTAR PUSTAKA 50

LAMPIRAN



DAFTAR GAMBAR

	Halaman
Gambar 2.1 Penerapan NIDS	5
Gambar 2.2 Penerapan HIDS	6
Gambar 2.3 Arsitektur IDS	8
Gambar 2.4 Komponen Snort	13
Gambar 2.5 PPDIOO	19
Gambar 3.1 Pengembangan Sistem	25
Gambar 4.1 Struktur Organisasi Warnet Cyber	29
Gambar 4.2 Activity Diagram.....	32
Gambar 4.3 Deployment Diagram	33
Gambar 4.4 Topologi Jaringan Usulan	34
Gambar 4.5 Konfigurasi Snort	35
Gambar 4.6 Tampilan Update-Upgrade.....	36
Gambar 4.7 Tampilan Pendukung Install Snort.....	36
Gambar 4.8 Tampilan Untuk Isntall Snort.....	37
Gambar 4.9 Tampilan Untuk Downlonds Snort	37
Gambar 4.10 Tampilan Extrak Kode Snort.....	37
Gambar 4.11 Tampilan Install DAQ.....	38
Gambar 4.12 Tampilan Install Snort.....	38
Gambar 4.13 Tampilan Install Source Snort.....	38
Gambar 4.14 Tampilan Extrack Snort	39
Gambar 4.15 Tampilan Direkctory Snort.....	39
Gambar 4.16 Tampilan Sudo Idconfig.....	40
Gambar 4.17 Tampilan Konfigurasi Direkctory	41
Gambar 4.18 Buat File Rules	41
Gambar 4.19 Buat Konfigurasi	41
Gambar 4.20 Komputer yang Belum Terpasang Snort.....	42
Gambar 4.21 Tampilan IP Adress Server	42
Gambar 4.22 Tampilan Rules	43

Gambar 4.23 Tampilan Snort Berjalan	44
Gambar 4.24 Tampilan untuk Serangan Ping Windows.....	44
Gambar 2.25 Tampilan Serangan Ping	45
Gambar 2.26 Tampilan Aplikasi PUTY SSH	45
Gambar 2.27 Tampilan Serangan SSH	46
Gambar 2.28 Tampilan Aplikasi PUTY Telanet.....	46
Gambar 2.29 Tampilan Serangan Telanet.....	46
Gambar 2.30 Tampilan Log	47



DAFTAR TABEL

	Halaman
Tabel 2.1 OSI Layer	9
Tabel 4.1 Kebutuhan Perangkat Keras	31
Tabel 4.2 Kebutuhan Perangkat Lunak	31



DAFTAR SIMBOL

1. Activity Diagram



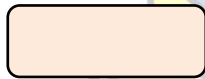
Start Point

Menggambarkan awal dari suatu aktivitas yang berjalan pada sistem.



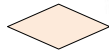
End Point

Menggambarkan akhir dari suatu aktivitas yang berjalan pada sistem.



Activity State

Menggambarkan suatu proses / kegiatan bisnis.



Decision Points

Menggambarkan pilihan untuk pengambilan keputusan, true atau false.

