

LAPORAN AKHIR
IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS)
DI JARINGAN POLITEKNIK NEGERI SRIWIJAYA



**Laporan Akhir disusun sebagai salah satu syarat menyelesaikan Pendidikan
Diploma III Jurusan Teknik Komputer**

Disusun Oleh :

DWI PUTRI SALSABILAH

061730701190

POLITEKNIK NEGERI SRIWIJAYA

PALEMBANG

2020

LEMBAR PERSETUJUAN LAPORAN AKHIR
IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS)
DI JARINGAN POLITEKNIK NEGERI SRIWIJAYA



OLEH :

DWI PUTRI SALSABILAH

061730701190

Palembang, September 2020

Menyetujui,

Pembimbing II

Pembimbing I

Ir. Ahmad Bahri Joni Malyan, M.Kom

NIP. 196007101991031001

Adi Sutrisman, S.Kom., M.Kom

NIP. 197503052001121005

Mengetahui,

Ketua Jurusan Teknik Komputer

Azwardi, S.T., M. T

NIP. 197005232005011004

Implementasi Intrusion Detection System (IDS) Di Jaringan Politeknik Negeri Sriwijaya



**Telah diuji dan dipertahankan di depan Dewan Penguji pada sidang Laporan Akhir pada Senin,
24 Agustus 2020**

Ketua Dewan Penguji

Isnainy Azro, S.Kom., M.Kom.
NIP. 197310012002122007

Anggota Dewan Penguji

Slamet Widodo, S.Kom., M.Kom.
NIP. 197305162002121001

Ema Laila, S.Kom., M.Kom.
NIP. 197703292001122002

Adi Sutrisman, S.Kom., M.Kom.
NIP. 197503052001121005

Mustaziri, S.T., M.Kom.
NIP. 196909282005011002

Tanda Tangan

Mengetahui,

Ketua Jurusan Teknik Komputer

Azwardi, S.T., M.T.

NIP. 197005232005011004



KEMENTERIAN RISET, TEKNOLOGI, DAN PENDIDIKAN TINGGI
POLITEKNIK NEGERI SRIWIJAYA

Jalan Srijaya Negara, Palembang 30139

Telp. 0711-353414 Fax. 0711-355918

Website : www.polisriwijaya.ac.id E-mail : info@polsri.ac.id



SURAT PERNYATAAN BEBAS PLAGIARISME

Yang bertanda tangan di bawah ini :

Nama : Dwi Putri Salsabilah
NIM : 0617 3070 1190
Jurusan/Program Studi : Teknik Komputer
Judul Laporan Akhir : Implementasi Intrusion Detection System di Jaringan Politeknik Negeri Sriwijaya

Dengan ini menyatakan :

1. Laporan akhir yang saya buat dengan judul sebagaimana tersebut di atas beserta isinya merupakan hasil penelitian saya sendiri.
2. Laporan akhir tersebut bukan plagiat atau menyalin laporan akhir milik orang lain.
3. Apabila laporan akhir ini dikemudian hari dinyatakan plagiat atau menyalin laporan akhir milik orang lain, maka saya bersedia menanggung konsekuensinya.

Demikian surat pernyataan ini saya buat dengan sebenarnya untuk diketahui oleh pihak-pihak yang berkepentingan.

Palembang, September 2020

Yang membuat pernyataan,

Dwi Putri Salsabilah

NIM 061730701190

MOTTO DAN PERSEMBAHAN

**“Sesungguhnya Allah beserta orang-orang yang sabar”
(QS. Al-Baqarah Ayat 153)**

**“Whatever you are be a good one”
-Abraham Lincoln-**

**“Where there’s a will there’s a way”
-Penulis-**

Kupersembahkan Untuk :

- 1. Allah SWT yang selalu memberi rahmat dan hidayah-Nya.**
- 2. Orang tuaku tercinta, Bapak Syaepudin dan Ibu Rohayani yang telah membesarkan, mendidik dan mendoakan setiap saat. Doa dan kasih sayang kalian menjadi sumber kekuatanku,serta ridho dari Allah SWT yang selalu menyertai setiap langkahku. Semoga ilmu yang ku dapatkan menjadi berkah. Pengorbanan kalian tidak bisa aku balas sampai akhir hayat.**
- 3. Tetehku Ayu Dini Lestari dan Kedua Adikku Muhammad Luthfi Hakim dan Ainun Nabila Syakira yang sangat saya sayangi.**
- 4. Teman-teman yang selalu memotivasi.**
- 5. Teman Seperjuanganku CE 2017.**
- 6. Almamaterku.**

ABSTRAK

Implementasi Intrusion Detection System (IDS) Di Jaringan Politeknik Negeri Sriwijaya

Dwi Putri Salsabilah, 2020 (x + 40 halaman)

Email: dwiputrisalsabilah99@gmail.com

Jurusan Teknik Komputer Politeknik Negeri Sriwijaya

Seorang pengelola server jaringan dan internet (system administrator) memiliki tanggung jawab terhadap keamanan sistem dari waktu ke waktu, memastikan bahwa sistem dan jaringan yang dikelola terjaga dari berbagai peluang ancaman. Perguruan Tinggi merupakan salah satu tempat dimana penggunaan jaringan internet terbuka terhadap pemakai-pemakainya. Penggunaan tersebut bisa dipergunakan dengan benar dan tidak pula disalahgunakan pemakaiannya. Oleh karena itu, dibutuhkan suatu sistem dalam menangani penyalahgunaan jaringan atau ancaman yang akan terjadi. Sistem yang hanya mendeteksi ini akan diimplementasikan dengan menggunakan aplikasi Intrusion Detection System (IDS) yaitu Snort dan PfSense (Router OS) sebagai penindak lanjutnya terhadap alert snort yang dihasilkan. Berdasarkan percobaan serangan dengan komputer yang terpasang snort dapat mengetahui apa yang sedang terjadi yang di hasilkan pada alert seperti serangan Ping Of Death dan Port Scan.

Kata Kunci : Alert, IDS, Snort

ABSTRACT

Implementation of Intrusion Detection System (IDS) in Sriwijaya State Polytechnic Network

Dwi Putri Salsabilah, 2020 (x + 40 pages)

Email: dwiputrisalsabilah99@gmail.com

Computer Engineering Department State Polytechnic of Sriwijaya

A network and internet server manager (system administrator) has the responsibility for system security from time to time, ensuring that the managed system and network is protected from various threats. Higher education is one of the places where the use of the internet network is open to its users. These uses can be used properly and not abused. Therefore, we need a system in dealing with network abuse or threats that will occur. The system that only detects this will be implemented using the Intrusion Detection System (IDS) application, namely Snort and PfSense (Router OS) as a follow-up to the generated snort alerts. Based on attack experiments with computers that have snort installed, you can find out what is going on which results in alerts such as Ping Of Death and Port Scan attacks.

Keywords: Alert, IDS, Snort

KATA PENGANTAR

Dengan memanjatkan puji dan syukur kehadiran Allah subhanahu wa ta'ala, karena atas rahmat dan karunia-Nya penulis dapat menyelesaikan Laporan Akhir ini dengan judul, “**Implementasi Intrusion Detection System (IDS) Di Jaringan Politeknik Negeri Sriwijaya**”

Tujuan dari penulisan laporan ini adalah untuk memenuhi persyaratan menyelesaikan Diploma III Politeknik Negeri Sriwijaya. Selanjutnya penulis mengucapkan terima kasih kepada seluruh pihak yang telah membantu dalam penulisan laporan ini, antara lain:

1. Allah SWT dan Nabi Muhammad Saw atas berkah dan karunia-Nya lah penulis bias menyelesaikan laporan ini.
2. Kedua Orangtua dan saudara tercinta, yang telah memberikan doa dan restu serta dukungan yang sangat besar selama ini.
3. Bapak Dr. Ing. Ahmad Taqwa, M.T. selaku Direktur Politeknik Negeri Sriwijaya.
4. Bapak Azwardi, S.T., M.T. selaku Ketua Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.
5. Bapak Ir. A. Bahri Joni Malyan, M. Kom. selaku Dosen Pembimbing I Jurusan Teknik Politeknik Negeri Sriwijaya yang telah berkenan meluangkan waktunya untuk membimbing serta memberikan masukan kepada penulis sehingga laporan akhir ini dapat diselesaikan sesuai dengan kriteria yang diharapkan.
6. Bapak Adi Sutrisman, S.Kom.,M.Kom. selaku Dosen Pembimbing II Jurusan Teknik Politeknik Negeri Sriwijaya yang telah berkenan meluangkan waktunya untuk membimbing serta memberikan masukan kepada penulis sehingga laporan akhir ini dapat diselesaikan sesuai dengan kriteria yang diharapkan.
7. Seluruh Bapak/Ibu Dosen Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.

8. Staff administrasi Jurusan Teknik Komputer yang telah membantu segala kepentingan perihal administrasi dan akademik selama proses penyusunan laporan akhir ini hingga selesai.
9. Segenap teman-teman dan para sahabatku yang telah memberikan motivasi dan dukungan dalam penyusunan laporan kerja akhir ini.
10. Teman-teman kelas 6 CE tidak bisa disebutkan satu-persatu atas bantuannya.

Semoga laporan ini dapat bermanfaat khususnya bagi penulis umumnya bagi para pembaca. Mengingat pengetahuan dan pengalaman penulis yang masih sedikit. Oleh karena itu penulis memohon kritik dan saran yang membangun demi perbaikan di masa depan. Terima kasih.

Palembang, September 2020

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PENGUJIAN	iii
SURAT PERNYAATAAN BEBAS PLAGIARISME	iv
MOTTO DAN PERSEMBAHAN	v
ABSTRAK	vi
KATA PENGANTAR	viii
DAFTAR ISI	x
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan	2
1.5 Manfaat	2
BAB II TINJAUAN PUSTAKA	
2.1 Penelitian Terdahulu	3
2.2 Jaringan Komputer	4
2.3 <i>Intrusion Detection System</i>	5
2.4 Snort	6
2.5 <i>WinPcap</i>	8
2.6 PfSense	8
2.7 VirtualBox	8
2.8 Jenis Serangan	9

2.9 <i>Manajemen Jaringan Usulan</i>	11
2.10 Firewall	12
2.10.1	Fungsi
Firewall.....	12
2.11 Flowchart.....	13
BAB III RANCANG BANGUN	16
3.1 Tujuan Perancangan.....	16
3.2 Perancangan Sistem.....	16
3.3 Diagram Alir.....	17
3.4 Rancang Bangun Jaringan.....	18
3.5 Rancangan Aplikasi.....	18
3.6 Instalasi Snort.....	19
3.7 Instalasi Snort dari DAQ.....	21
3.8 Bagian Kedua dari Instalasi (Snort).....	25
BAB IV HASIL DAN PEMBAHASAN	31
4.1 Hasil dari serangan yang terdapat di IDS	34
BAB V KESIMPULAN DAN SARAN	35
5.1 Kesimpulan	35
5.2 Saran	35

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

Gambar 2. 1 Simbol Flowchart.....	13
Gambar 3. 1 Blok Diagram.....	15
Gambar 3.2 Diagram Alir/Flowchart.....	16
Gambar 3.3 Topologi Jaringan Usulan.....	17
Gambar 3. 4 Update Snort	19
Gambar 3. 5 Upgrade Snort	20
Gambar 3. 6 Instal Nama Paket	20
Gambar 3.7 Upgrade Snort.....	20
Gambar 3.8 Instalasi Snort (DAQ)	21
Gambar 3.9 Instalasi Bison Flex.....	21
Gambar 3. 10 Situs Web Resmi Snort	22
Gambar 3. 11 Download DAQ Untuk Snort	22
Gambar 3.12 Konfigurasi Pembuatan DAQ.....	22
Gambar 3. 13 Situs Resmi Tcdump.....	23
Gambar 3. 14 Pengelolaan Wibcamp	23
Gambar 3. 15 Instal Libpcap	24
Gambar 3. 16 Membangun Program Libpcap untuk Distribusi Linux	25
Gambar 3. 17 Instalasi Semua Perangkat Lunak	25
Gambar 3. 18 Situs Resmi pcre	26
Gambar 3. 19 File tar pcre	26
Gambar 3. 20 Konfigurasi pcre	27
Gambar 3. 21 Download Luajit	27
Gambar 3. 22 Instalasi Snort Selesai	29
Gambar 4. 1 Serangan Telnet	30
Gambar 4. 2 <i>Telnet Log</i>	30
Gambar 4. 3 Serangan Ping Of Death	31
Gambar 4. 4 Log Ping Of Death.....	31
Gambar 4. 5 Log	32

DAFTAR TABEL

Gambar 4.6 Hasil Pengujian.....	34
---	----