

**IMPLEMENTASI *INTRUSION DETECTION SYSTEM* MENGGUNAKAN  
SNORT UNTUK KEAMANAN JARINGAN  
(Studi Kasus: Universitas Maritim Raja Ali Haji)**



**Skripsi**

Untuk memenuhi syarat memperoleh Derajat  
Sarjana Teknik (S.T.)

**Oleh:**

Raja Dini Kurnianingsi

180155201035

**JURUSAN INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS MARITIM RAJA ALI HAJI  
TANJUNGPINANG  
2022**

**IMPLEMENTASI *INTRUSION DETECTION SYSTEM* MENGGUNAKAN  
SNORT UNTUK KEAMANAN JARINGAN  
(Studi Kasus: Universitas Maritim Raja Ali Haji)**



**Skripsi**

Untuk memenuhi syarat memperoleh derajat  
Sarjana Teknik (S.T.)

**Oleh:**

Raja Dini Kurnianingsi  
180155201035

Telah mengetahui dan disetujui oleh :

**Pembimbing I,**

Muhammad Radzi Rathomi, S.Kom., M.Cs  
NIDN. 0025038904

**Pembimbing II,**

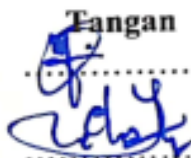





Nurul Hayaty, S.T., M.Cs  
NIDN. 0027039101

## HALAMAN PENGESAHAN

Judul : Implementasi *Intrusion Detection System* menggunakan Snort untuk keamanan jaringan (Studi Kasus: Universitas Maritim Raja Ali Haji)  
Nama : Raja Dini Kurnianingsi  
NIM : 180155201035  
Jurusan : Informatika

telah dipertahankan di depan Dewan Penguji dan dinyatakan lulus pada tanggal 11 Juli 2022

### *Susunan Tim Pembimbing dan Penguji*

Jabatan	Nama	Tanda Tangan	Tanggal
Pembimbing I	: Muhamad Radzi Rathomi, S.Kom., M.Cs		26/7-2022
Pembimbing II	: Nurul Hayaty, S.T., M.Cs		.....
Ketua Penguji	: Muhamad Radzi Rathomi, S.Kom., M.Cs		26/7-2022
Anggota	: 1. Martaleli Bettiza, S.Si., M.Sc.		26/7-22
	: 2. Ferdi Chahyadi, S.Kom., M.Cs		25/7-22
	: 3. Alena Uperiati, S.T., M.Cs		22/7-22

Tanjungpinang, 26 Juli 2022  
Universitas Maritim Raja Ali Haji  
Fakultas Teknik  
Ketua Jurusan Informatika,



Muhamad Radzi Rathomi, S.Kom., M.Cs  
NIP. 198903252019031014

## PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa skripsi saya yang berjudul *Implementasi Intrusion Detection System Menggunakan Snort untuk keamanan jaringan (Studi Kasus: Universitas Maritim Raja Ali Haji)* adalah benar karya saya dengan arahan dari komisi pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir skripsi ini.

Jika kemudian hari ternyata terbukti pernyataan saya ini tidak benar dan melanggar peraturan yang sah dalam karya tulis dan hak intelektual maka saya bersedia ijazah yang telah saya terima untuk ditarik kembali oleh Universitas Maritim Raja Ali Haji.

Tanjungpinang, Agustus 2022

Yang menyatakan

A handwritten signature in black ink is written over a yellow postage stamp. The stamp features the Garuda Pancasila emblem and the text '1000', 'METERAI TEMPEL', and the alphanumeric code 'BBFCBAJX855317917'.

(Raja Dini Kurnianingsi)

## HALAMAN PERSEMBAHAN

### *Bismillahirrahmannirrahim*

Alhamdulillah rabbi 'alamin, pertama-tama saya ucapkan segala puji bagi Allah SWT yang telah melimpahkan rahmat dan karunia-Nya, sehingga saya bisa menyelesaikan tugas akhir ini dengan baik. Saya selalu bersyukur kepada-Mu karena telah membantu, memberikan saya kekuatan setiap langkah, dan juga telah mengabdikan do'a saya dalam proses pengerjaan skripsi ini hingga selesai.

Skripsi ini saya persembahkan untuk:

Kedua orang tua yang sangat saya sayangi, ayah saya Raja Muhammad Khairullah dan Ibu saya Asnah yang selalu membimbing saya dari kecil dengan kasih sayang, selalu berusaha memberi yang terbaik untuk saya, selalu berusaha menjadi contoh yang baik untuk anak-anak nya. Makasi untuk semua jasa kalian, berkat semua doa yang kalian ucapkan lah bisa membuat kakak berada di titik ini, maaf kalau kakak belum bisa membahagika kan, tapi insyaallah dengan segala nilai-nilai baik yang udah kalian tanamkan didiri kakak; kakak bakal berusaha selalu jadi orang yang lebih baik kedepan dan tentu nya menjadi anak yang bisa kalian banggakan.

Untuk adik saya Raja Rosiana Putri dan Raja Muhammad Ar-Rasyid, makasi semua doa nya, semua dukungan nya, selalu jadi penyemangat kakak. Selalu doain kakak agar kakak bisa mencapai cita-cita untuk bisa menyekolahkan kalian berdua setinggi apa pun yang kalian mau.

Untuk sahabat saya Fauzia Alfi Wahyuni, Gina, Alisa Nabila, Sekar kinanti, Rani Afriani, Ais inas, Putri anisa, Nur suci ramadhani terimakasih semua dukungan, support, dan terimakasih selalu ada baik dalam keadaan baik atau pun tidak, makasi untuk semua cerita kita, semoga ilmu yang kita tuntut bersama akan selalu berkah di kemudian hari.

Terakhir saya juga berterimakasih untuk semua orang yang telah berada dihidup saya, berkat kalian saya bisa belajar banyak hal, saya belajar akan hal-hal baru

tentang kehidupan, banyak faktor yang membuat saya termotivasi untuk segera menyelesaikan skripsi ini agar saya bisa segera melangkah ke tahap kehidupan selanjutnya.

## HALAMAN MOTO

*“Sesungguhnya bersama kesulitan itu ada kemudahan”*

*(QS. Al-Insyirah:5-6)*

*“Setiap bunga memiliki waktu mekarnya masing-masing. Setiap orang memiliki waktu sukses yang berbeda”*

## KATA PENGANTAR

Alhamdulillah rabbil ‘alamin Puji dan syukur kepada Allah SWT yang telah memberikan rahmat dan karunia-Nya kepada penulis sehingga bisa menyelesaikan skripsi dengan judul “Implementai *Intrusion Detection System* Menggunakan Snort” dengan waktu yang tepat walaupun banyak rintangan yang penulis hadapi selama proses penyelesaian skripsi ini.

Penulis banyak memperoleh bantuan dari berbagai pihak, berupa doa, bantuan, bimbingan, masukan dan saran dalam penyelesaian skripsi. Penulis ingin mengucapkan terima kasih banyak kepada:

1. Allah SWT yang telah menguatkan agar penulis slalu semangat dalam proses penyelesaian skripsi, serta memberikan jalan dalam setiap cobaan dan ujian yang telah dihadapi oleh penulis.
2. Kedua orang tua tercinta, Ayah Raja Muhammad Khairullah dan Ibu Asnah yang telah merawat penulis dan membesarkan penulis dengan penuh kasih sayang dan juga senantiasa slalu mendoakan serta segalanya bagi penulis yang tak akan penulis lupakan. Terima kasih telah menjadikan penulis menjadi anak yang kuat, dan tidak mudah menyerah sehingga dapat melalui berbagai rintangan hidup hingga saat ini. dan menyayangi hingga tak pernah lelah menyayangi penulis. Terimakasih untuk adik tersayang Raja Rosiana Putri dan Raja Muhammad Ar-Rasyid, Terima kasih telah memberikan semangat, dan selalu mendoakan penulis.
3. Seluruh keluarga besar dari pihak ayah dan ibu penulis yang tak dapat disebutkan satu persatu, terima kasih telah memberikan doa, semangat, dukungan serta motivasi kepada penulis.
4. Bapak Sapta Nugraha, S.T., M.Eng selaku Dekan Fakultas Teknik Universitas Maritim Ali Haji.
5. Bapak Muhamad Radzi Rathomi, S.Kom., M.Cs, selaku Ketua Jurusan Teknik Informatika Universitas Maritim Raja Ali Haji sekaligus Dosen Pembimbing I yang telah meluangkan waktu utnuak memberikan saran,



solusi, dan membimbing penulis dalam melakukan penelitian dan pengerjaan skripsi ini.

6. Ibu Nurul Hayaty, S.T., M.Cs, selaku Dosen Pembimbing II yang telah meluangkan waktu untuk mendampingi penulis selama proses perkuliahan serta membimbing dan memberikan masukan dalam pengerjaan skripsi ini.
7. Bapak Ferdi Chahyadi, S.Kom., M.Cs, selaku Dosen Pembimbing Akademik yang selalu membimbing dan memberi saran bagi penulis selama proses perkuliahan berlangsung.
8. Dosen penguji yang sudah memberikan kritik dan saran sehingga proses pengerjaan skripsi ini menjadi lebih baik.
9. Seluruh Dosen Teknik Informatika Universitas Maritim Raja Ali Haji yang telah memberikan banyak ilmu pengetahuan, nasihat, dan motivasi kepada penulis selama proses perkuliahan.
10. Sahabat yang sudah menjadi keluarga; Fauzia Alfi Wahyuni, Alisa Nabila, Gina, Sekar Kinanti Ramadini N., Rani Afriani, Ais inas TH., Putri Anisa, Nur Suci RM. yang telah memberikan semangat, motivasi, dan selalu ada saat suka maupun duka yang tak bisa diuraikan satu persatu.

Penulis menyadari bahwa penelitian ini masih banyak kekurangan, oleh karena itu penulis meminta kritik dan saran yang membangun demi menghasilkan skripsi dengan sebaik-baiknya. Semoga skripsi ini bermanfaat bagi pembaca, terkhusus untuk pembaca yang ingin menjadikan skripsi ini sebagai referensi penelitian atau membuat skripsi dengan kasus serupa.

Tanjungpinang, 25 Juni 2021

Raja Dini Kurnianingsi

## DAFTAR ISI

HALAMAN JUDUL .....	i
HALAMAN PERSETUJUAN .....	ii
HALAMAN PENGESAHAN .....	iii
PERNYATAAN ORISINALITAS .....	iv
HALAMAN PERSEMBAHAN .....	v
HALAMAN MOTO .....	vii
KATA PENGANTAR .....	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xv
DAFTAR GAMBAR.....	xvi
GLOSARIUM.....	xviii
ABSTRAK.....	xix
ABSTRACT.....	xx
BAB I PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian .....	3
1.5 Manfaat Penelitian .....	3
1.6 Sistematika Penulisan.....	3
BAB II KAJIAN LITERATUR .....	5
2.1 Tinjauan Pustaka .....	5
2.2 Landasan Teori.....	6
2.2.1 Keamanan jaringan.....	6
2.2.2 Server Ubuntu.....	7
2.2.3 IDS ( <i>Intrusion Detection System</i> ).....	7
2.2.4 Snort .....	7
2.2.5 Wireshark.....	8
2.2.6 Sniffing .....	10
2.2.7 TCP.....	10

2.2.8	UDP .....	11
2.2.9	DOS ( <i>Denial of service</i> ) .....	11
2.2.10	<i>Ping of death</i> .....	11
2.2.11	<i>Smurf attack</i> .....	12
2.2.12	<i>Syn Flooding</i> .....	12
2.2.13	<i>UDP flood</i> .....	12
BAB III METODE PENELITIAN.....		13
3.1	Jenis Penelitian.....	13
3.2	Variabel Penelitian .....	13
3.3	Pengumpulan Data .....	13
3.4	Instrumen Penelitian.....	13
3.5	Prosedur Penelitian.....	14
3.6	Jadwal Penelitian.....	17
3.7	Skenario Pengujian.....	18
3.8	Understand .....	19
3.9	Analyze .....	20
3.10	Implementasi .....	20
3.10.1	Identifikasi ip jaringan.....	20
3.10.2	Implementasi IDS ( <i>Intrusion Detection System</i> ).....	21
3.10.3	Implementasi Snort.....	21
3.10.4	Implementasi Wireshark.....	24
BAB IV HASIL DAN PEMBAHASAN .....		25
4.1	Analisis pengujian sistem IDS ( <i>Intrusion Detection System</i> ) .....	25
4.1.1	Pengujian Snort dan Wireshark tanpa ada serangan.....	25
4.1.2	Pengujian Snort dan wireshark di UPT.PTIK UMRAH.....	27
4.1.2.1	Serangan smurf attack.....	28
4.1.2.2	Serangan SYN flooding .....	30
4.1.2.3	Serangan <i>UDP flood</i> .....	33
4.1.2.4	Laporan Analisis data .....	35
4.1.3	Pengujian Snort, wireshark menggunakan serangan manual di fakultas teknik Umrah.....	38

4.1.3.1 Snort mendeteksi ping of death.....	38
4.1.3.2 Snort mendeteksi <i>SYN flooding</i> .....	40
4.1.3.3 Snort mendeteksi <i>UDP flood</i> .....	42
BAB V PENUTUP.....	45
5.1 Kesimpulan .....	45
5.2 Saran.....	45
DAFTAR PUSTAKA .....	47
LAMPIRAN .....	49
Lampiran 1. Tampilan konfigurasi snort berlangsung.....	50
Lampiran 2. Tampilan Snort setelah di jalankan.....	50
Lampiran 3. Tampilan Snort dan Wireshark tanpa serangan (a).....	51
Lampiran 4. Tampilan Snort dan Wireshark tanpa serangan (b).....	51
Lampiran 5. Tampilan Snort dan Wireshark tanpa serangan (c).....	52
Lampiran 6. Tampilan kinerja CPU saat masuk nya serangan <i>smurf attack</i> di UPT.PTIK (a).....	52
Lampiran 7. Tampilan kinerja CPU saat masuk nya serangan <i>smurf attack</i> di UPT.PTIK (b).....	53
Lampiran 8. Tampilan Snort saat mendeteksi <i>SYN flooding</i> di UPT.PTIK (a) .....	53
Lampiran 9. Tampilan Snort saat mendeteksi <i>SYN flooding</i> di UPT.PTIK (b) .....	54
Lampiran 10. Tampilan Snort saat mendeteksi <i>SYN flooding</i> di UPT.PTIK (c) .....	54
Lampiran 11. Tampilan Snort dan CPU saat mendeteksi <i>SYN flooding</i> di UPT.PTIK (a).....	55
Lampiran 12. Tampilan Snort dan CPU saat mendeteksi <i>SYN flooding</i> di UPT.PTIK (b).....	55
Lampiran 13. Tampilan Snort dan CPU saat mendeteksi <i>SYN flooding</i> di UPT.PTIK (c).....	55
Lampiran 14. Tampilan Wireshark saat mendeteksi <i>SYN flooding</i> di UPT.PTIK .....	56

Lampiran 15. Tampilan Wireshark dan kinerja CPU saat mendeteksi <i>SYN flooding</i> di UPT.PTIK .....	57
Lampiran 16. Tampilan snort dan kinerja CPU mendeteksi <i>UDP flood</i> dan <i>SYN flooding</i> di UPT.PTIK .....	56
Lampiran 17. Tampilan Snort saat mendeteksi <i>SYN flooding</i> dan <i>UDP flood</i> di UPT.PTIK .....	58
Lampiran 18. Tampilan Snort saat mendeteksi serangan <i>UDP flood</i> di UPT.PTIK .....	58
Lampiran 19. Tampilan Wireshark saat mendeteksi serangan <i>UDP flood</i> di UPT.PTIK .....	59
Lampiran 20. Tampilan Snort saat mendeteksi serangan <i>ping of death</i> di Fakultas Teknik (a) .....	59
Lampiran 21. Tampilan Snort saat mendeteksi serangan <i>ping of death</i> di Fakultas Teknik (b) .....	60
Lampiran 22. Tampilan Snort dan kinerja CPU saat mendeteksi serangan <i>ping of death</i> di Fakultas Teknik (a).....	60
Lampiran 23. Tampilan Snort dan kinerja CPU saat mendeteksi serangan <i>ping of death</i> di Fakultas Teknik (b).....	61
Lampiran 24. Tampilan Wireshark dan kinerja CPU saat mendeteksi serangan <i>ping of death</i> di Fakultas Teknik (a) .....	61
Lampiran 25. Tampilan Wireshark dan kinerja CPU saat mendeteksi serangan <i>ping of death</i> di Fakultas Teknik (b).....	61
Lampiran 26. Tampilan Snort mendeteksi <i>SYN flooding</i> di Fakultas Teknik (a) .....	62
Lampiran 27. Tampilan Snort mendeteksi <i>SYN flooding</i> di Fakultas Teknik (b) .....	63
Lampiran 28. Tampilan Snort dan kinerja CPU mendeteksi <i>SYN flooding</i> di Fakultas Teknik.....	63
Lampiran 29. Tampilan wireshark dan kinerja CPU saat mendeteksi serangan <i>SYN flooding</i> di Fakultas Teknik (a) .....	64

Lampiran 30. Tampilan wireshark dan kinerja CPU saat mendeteksi serangan <i>SYN flooding</i> di Fakultas Teknik (b).....	64
Lampiran 31. Tampilan wireshark saat mendeteksi serangan <i>SYN flooding</i> di Fakultas Teknik (a) .....	65
Lampiran 32. Tampilan wireshark saat mendeteksi serangan <i>SYN flooding</i> di Fakultas Teknik (b) .....	65
Lampiran 33. Tampilan wireshark saat mendeteksi serangan <i>SYN flooding</i> di Fakultas Teknik (c) .....	66
Lampiran 34. Tampilan wireshark saat mendeteksi serangan <i>SYN flooding</i> di Fakultas Teknik (d) .....	66
Lampiran 35. Tampilan saat uji coba serangan .....	67
Lampiran 36. Tampilan saat uji coba serangan <i>ping of death</i> .....	67

## DAFTAR TABEL

Tabel 3.1 Instrumen Penelitian .....	14
Tabel 3.2 Jadwal Penelitian.....	17
Tabel 3.3 Instalasi ifconfig.....	19
Tabel 3.4 Instalasi Snort.....	21
Tabel 3.5 Instalasi Wireshark.....	23
<u>Tabel 4.1 Analisis Data</u> .....	35

## DAFTAR GAMBAR

Gambar 2.1 <i>Coloring Rules Wireshark</i> .....	9
Gambar 2.2 Penjelasan dari aturan warna Wireshark .....	10
Gambar 3.1 Metode Penelitian.....	15
Gambar 3.2 <i>Flowchart Analisis Intrusion Detection System</i> menggunakan snort	16
Gambar 3.3 Topologi mekanisme serangan.....	17
Gambar 3.4 Skema Teknis Pengujian .....	18
Gambar 3.5 Skema pengujian menggunakan serangan manual.....	19
Gambar 3.6 Tampilan ifconfig.....	21
Gambar 3.7 Konfigurasi snort (a) .....	23
Gambar 3.8 Konfigurasi snort (b) .....	23
Gambar 3.9 Konfigurasi snort (c) .....	23
Gambar 3.10 Tampilan wireshark setelah di jalankan .....	24
Gambar 4.1 Tampilan Snort tanpa serangan .....	25
Gambar 4.2 Tampilan Wireshark tanpa adanya serangan.....	25
Gambar 4.3 Tampilan kinerja CPU tanpa ada nya serangan .....	26
Gambar 4.4 Tampilan Snort saat mendeteksi serangan <i>smurf attack</i> .....	27
Gambar 4.5 Tampilan detail <i>alert</i> yang menunjukkan aktifitas serangan <i>smurf attack</i> .....	27
Gambar 4.6 Tampilan wireshark dalam mendeteksi serangan smurf attack.....	28
Gambar 4.7 Tampilan detail Wireshark yang menunjukkan aktifitas serangan <i>smurf attack</i> .....	28
Gambar 4.8 Tampilan kinerja komputer saat serangan terjadi .....	29
Gambar 4.9 Tampilan snort pada serangan <i>SYN flooding</i> .....	30
Gambar 4.10 Detail tampilan alert snort yang mendeteksi serangan <i>SYN flooding</i> .....	30
Gambar 4.11 wireshark mendeteksi serangan <i>SYN flooding</i> .....	31
Gambar 4.12 Detail tampilan wireshark mendeteksi serangan <i>SYN flooding</i> .....	31
Gambar 4.13 Tampilan kinerja CPU pada serangan <i>SYN flooding</i> .....	31
Gambar 4.14 Tampilan Snort pada serangan <i>UDP flood</i> .....	32



Gambar 4.15 Detail tampilan <i>alert</i> Snort yang menunjukkan serangan <i>UDP flood</i> .....	32
Gambar 4.16 Tampilan Wireshark pada serangan <i>UDP flood</i> .....	33
Gambar 4.17 Detail Wireshark pada serangan <i>UDP flood</i> .....	33
Gambar 4.18 Tampilan CPU pada serangan <i>UDP flood</i> .....	34
Gambar 4.19 Tampilan Snort dan kinerja CPU saat mendeteksi serangan <i>ping of death</i> .....	38
Gambar 4.20 Tampilan Wireshark dan kinerja komputer saat mendeteksi serangan <i>ping of death</i> .....	38
Gambar 4.21 Tampilan Snort saat mendeteksi serangan <i>SYN flooding</i> .....	39
Gambar 4.22 Tampilan Wireshark dan kinerja komputer saat mendeteksi serangan <i>SYN flooding</i> .....	40
Gambar 4.23 Tampilan Snort dan kinerja komputer saat mendeteksi serangan <i>UDP flood</i> .....	41
Gambar 4.24 Tampilan Wireshark saat mendeteksi serangan <i>UDP flood</i> .....	44
Gambar 4.25 Tampilan Wireshark saat mendeteksi serangan <i>UDP flood</i> .....	45
Gambar 4.26 Tampilan Wireshark saat mendeteksi serangan <i>UDP flood</i> .....	45
Gambar 4.27 Tampilan Wireshark saat mendeteksi serangan <i>UDP flood</i> .....	45