

**ANALISIS SERANGAN WEB SERVER MENGGUNAKAN
WAZUH DAN OPNSENSE**

TUGAS AKHIR



Ibnu Riko Ramdani

NIM. 180155201038

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG
2026**

ANALISIS SERANGAN WEB SERVER MENGGUNAKAN WAZUH DAN OPNSENSE

Tugas Akhir

Skema Skripsi

Tugas Akhir diajukan sebagai salah satu persyaratan memperoleh gelar Sarjana

Teknik pada Program Studi Teknik Informatika



Ibnu Riko Ramdani

NIM. 180155201038

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG
2026**

PERNYATAAN MENGENAI TUGAS AKHIR DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa tugas akhir berjudul “Analisis Serangan Web Server menggunakan Wazuh dan Opnsense” 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.

Apabila di kemudian hari terbukti pernyataan saya tidak benar dan melanggar peraturan yang berlaku dalam karya tulis dan hak intelektual, maka saya bersedia ijazah yang telah saya terima untuk ditarik kembali oleh Universitas Maritim Raja Ali Haji dan menerima sanksi lainnya sesuai dengan peraturan yang berlaku. Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Universitas Maritim Raja Ali Haji.

Tanjungpinang, 10 Desember 2025



Ibnu Riko Ramdani
NIM 1801552901038



© Hak Cipta Milik Universitas Maritim Raja Ali Haji, Tahun 2021

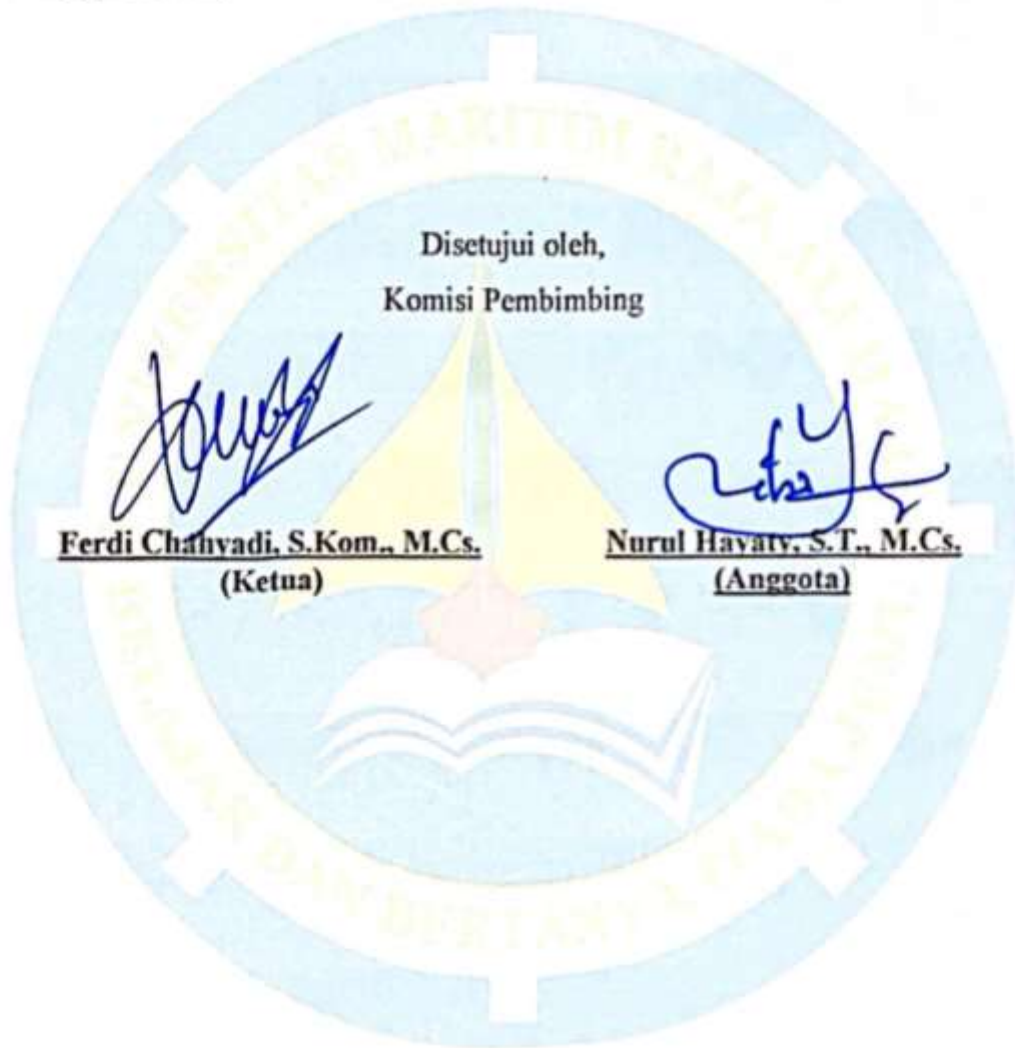
Hak Cipta Dilindungi Undang- Undang

Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan atau menyebutkan sumbernya. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik, atau tinjauan suatu masalah; dan pengutipan tersebut tidak merugikan kepentingan Universitas Maritim Raja Ali Haji.

Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Universitas Maritim Raja Ali Haji.

HALAMAN PERSETUJUAN

Judul : Analisis Serangan Web Server Menggunakan Wazuh dan Opnsense
Nama : Ibnu Riko Ramdani
NIM : 180155201038
Program Studi : Teknik Elektro dan Informatika
Tanggal Persetujuan :



HALAMAN PENGESAHAN

Judul : Analisis Serangan Web Server Menggunakan Wazuh dan Opnsense
Nama : Ibnu Riko Ramdani
NIM : 180155201038

Telah berhasil dipertahankan di hadapan Komisi Penguji sebagai bagian persyaratan yang diperlukan dalam memperoleh gelar Sarjana Teknik pada Program Studi Teknik Informatika, Jurusan Teknik Elektro dan Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji.

KOMISI PENGUJI

Ketua : Muhammad Radzi Rathomi, S.Kom., M.Cs. (.....)
Anggota I : Nolan Efranda, M.Kom (.....)
Anggota II : Rifaldi Herikson, M.Kom (.....)
Anggota III : Ferdi Cahyadi, S.Kom., M.Cs. (.....)
Anggota IV : Nurul Hayaty, S.T., M.Cs. (.....)

Mengetahui,

Ketua Jurusan Teknik Elektro dan Informatika

Hollanda Arief Latsuma, S.IK., M.Si

NIP. 198904012019031016

Tanggal Ujian: 18 Desember 2025. Tanggal Lulus:

PRAKATA

Puji dan syukur dipanjatkan kepada Allah *subhanahu wa ta'ala* atas segala karunia-Nya, sehingga penulis dapat menyelesaikan skripsi dengan judul “*Analisis Serangan Web Server Menggunakan Wazuh dan OPNsense*” dengan baik dan tepat waktu.

Skripsi ini disusun sebagai salah satu syarat untuk meraih gelar Sarjana Teknik pada Program Studi Teknik Informatika, Jurusan Teknik Elektro dan Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji. Penulis berharap hasil penelitian ini dapat memberikan sumbangsih yang berarti bagi pengembangan ilmu pengetahuan, terutama dalam bidang *Cyber Security*.

Penulis menyadari dalam menyusun Skripsi ini mendapat banyak dukungan, bimbingan bantuan dan kemudahan dari berbagai pihak sehingga Skripsi ini dapat diselesaikan. Dengan ketulusan hati, penulis menyampaikan ucapan terima kasih kepada : ☆

1. Orang tua tercinta, Bapak Norzan dan Ibu Maryani, yang senantiasa memberikan dukungan dan doa selama proses penulisan skripsi ini.
2. Prof. Dr. Agung Dharma Syakti, S.Pi, DEA selaku Rektor yang telah memimpin Universitas Maritim Raja Ali Haji menuju arah yang lebih baik.
3. Ibu Martaleli Bettiza, S.Si., M.Sc. Selaku Dekan Fakultas Teknik dan Teknologi Kemaritiman yang telah memberikan motivasi serta dorongan untuk memajukan Program Studi Teknik Informatika
4. Bapak Hollanda Arief Kusuma, S.IK., M.Si. selaku Ketua Jurusan Teknik Elektro dan Informatika yang telah memajukan Program Studi Teknik Informatika
5. Bapak Ferdi Chahyadi, S.Kom., M.Cs. dan Ibu Nurul Hayaty, S.T., M.Cs atas bimbingan, arahan, dan dukungan yang sangat berarti selama proses penulisan skripsi ini.

6. Dosen penguji yang telah memberikan masukan dan saran yang konstruktif bagi penelitian ini.
7. Mentor Bang Wingky dan rekan Lucky, Fikri, Agis, Andika, iqbal, Ridwan, Rezky, Risky, Fajri, Elfelita Fani serta Teknik Informatika Angkatan 2018, yang telah memberikan bantuan dan motivasi selama penyelesaian skripsi ini.
8. Dan semua pihak yang telah membantu saya selama proses penulisan skripsi ini. Semoga kelancaran menyertai teman-teman yang sedang atau akan mengerjakan skripsi di masa mendatang.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan. Oleh karena itu, kritik dan saran yang membangun dari berbagai pihak. Penulis berharap skripsi ini dapat memberikan manfaat bagi siapa saja yang membutuhkan serta menjadi referensi yang berguna untuk penelitian selanjutnya.

Tanjungpinang, 24 Desember 2025



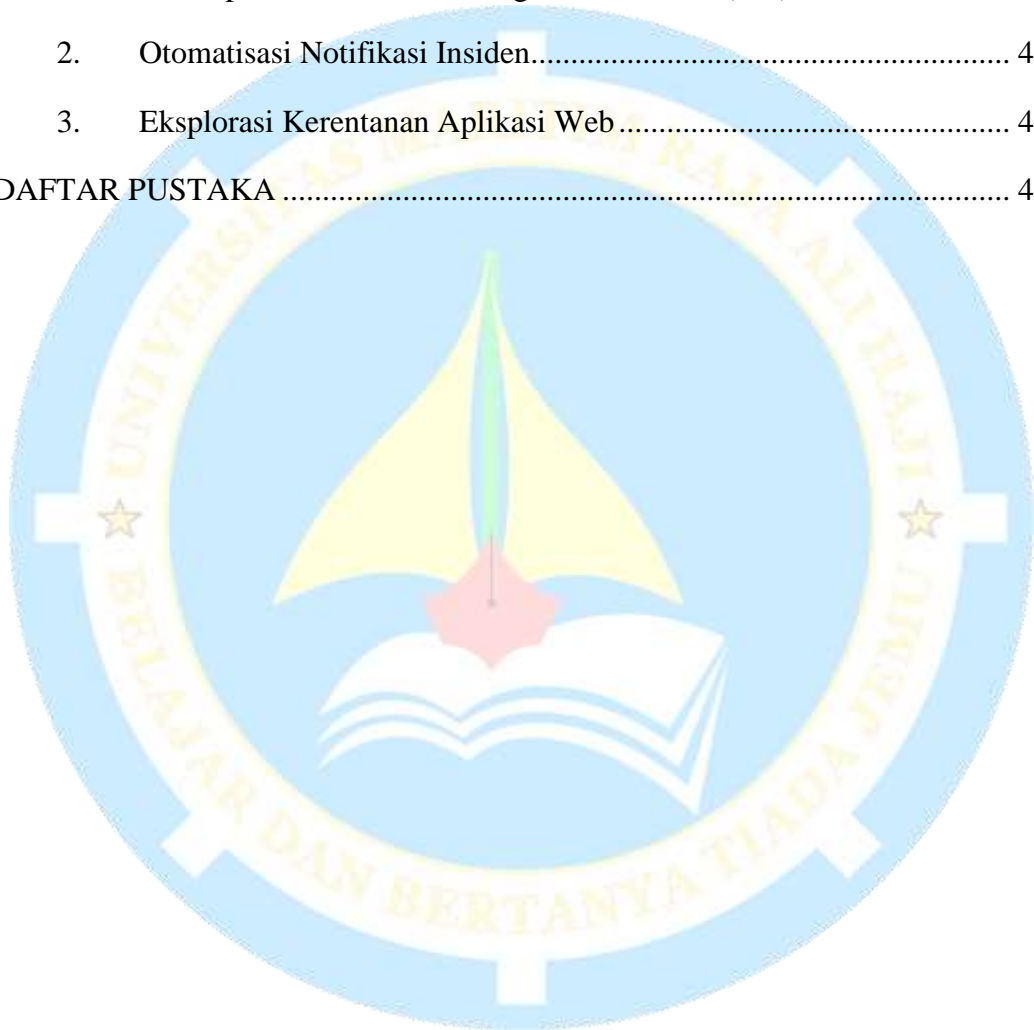
Ibnu Wiko Ramdani

DAFTAR ISI

COVER	i
HALAMAN PERSETUJUAN.....	iv
HALAMAN PENGESAHAN.....	v
ABSTRAK	vi
ABSTRACT.....	vii
PRAKATA.....	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
BAB I PENDAHULUAN	1
A. Latar Belakang	1
B. Perumusan Masalah	2
C. Batasan Penelitian	2
D. Tujuan Penelitian	3
E. Manfaat Penelitian	3
BAB II KAJIAN LITERATUR	4
A. Tinjauan Pustaka	4
B. Landasan Teori.....	8
1. Web Server	8
2. Ubuntu	9
3. Firewall	9
4. Kali Linux	9
5. Wazuh	9
6. OPNsense.....	9

7.	NAT (<i>Network Address Translation</i>)	10
8.	VLAN (<i>Virtual Local Area Network</i>).....	10
9.	DOS (<i>Denials of Service</i>)	10
10.	Brute Force Attack.....	12
BAB III METODE PENELITIAN.....		13
A.	Jenis Penelitian.....	13
B.	Variabel Penelitian.....	13
D.	Instrumen Penelitian.....	14
E.	Prosedur Penelitian.....	14
F.	Skenario Pengujian.....	15
1.	Simulasi Serangan:	15
2.	Pemantauan dan Pencatatan Aktivitas:.....	16
3.	Analisis Hasil Pengujian.....	16
G.	Implementasi dan Konfigurasi Sistem	17
1.	Konfigurasi OPNsense.....	17
2.	Konfigurasi wazuh.....	19
3.	Konfigurasi Lingkungan Pengujian.....	21
BAB IV HASIL DAN PEMBAHASAN		23
A.	Simulasi Serangan Dos Attack.....	23
1.	Langkah-Langkah Serangan DoS Attack	23
2.	Hasil Pemantauan di OPNsense.....	24
B.	Simulasi Serangan Brute Force SSH	25
1.	Langkah-langkah Serangan Brute-Force SSH.....	25
2.	Hasil Pemantauan di Wazuh Dashboard.....	29
C.	Pembahasan.....	32
1.	Analisis Efektivitas Mitigasi Serangan Dos	32

2.	Analisis Efektivitas Deteksi Brute Force.....	37
3.	Analisis Kinerja Pertahanan Berlapis	42
BAB V SIMPULAN DAN SARAN		43
A.	Simpulan	43
B.	Saran.....	43
1.	Penerapan Mekanisme Pencegahan Otomatis (IPS).....	43
2.	Otomatisasi Notifikasi Insiden.....	43
3.	Eksplorasi Kerentanan Aplikasi Web.....	44
DAFTAR PUSTAKA		45



DAFTAR TABEL

Tabel 1. Instrumen penelitian.....	14
Tabel 2. <i>Rule level</i> wazuh	37



DAFTAR GAMBAR

Gambar 1. Topologi Jaringan.....	13
Gambar 2. Metode Penelitian.....	15
Gambar 3. Skema Teknik Pengujian.....	15
Gambar 4. Server OPNsense.....	17
Gambar 5. Tampilan login OPNsense.....	17
Gambar 6. Dashboard OPNsense.....	18
Gambar 7. Tampilan rules.....	18
Gambar 8. Tampilan wazuh server.....	19
Gambar 9. Tampilan Server Ubuntu.....	19
Gambar 10. IP Wazuh Server.....	20
Gambar 11. IP Ubuntu Server.....	20
Gambar 12. Halaman Login Wazuh Dashboard.....	20
Gambar 13. Dashboard Wazuh.....	21
Gambar 14. Halaman Login Kali Linux.....	21
Gambar 15. Tampilan Kali Linux.....	22
Gambar 16. Tes Ping IP Target.....	22
Gambar 17. Perintah serangan hping3.....	23
Gambar 18. Tampilan serangan hping3.....	24
Gambar 19. Dashboard awal.....	24
Gambar 20. Tampilan setelah diserang.....	24
Gambar 21. Tampilan Live view.....	25
Gambar 22. Perintah untuk buat <i>username</i>	26
Gambar 23. Perintah kata sandi admin.....	26
Gambar 24. Perintah Kata sandi admin2.....	26
Gambar 25. Text editor “admin”.....	26
Gambar 26. Text editor “admin2”.....	27
Gambar 27. Perintah serangan <i>hydra</i> users “admin”.....	27
Gambar 28. Perintah serangan <i>hydra</i> users “admin2”.....	27
Gambar 29. Tampilan Serangan <i>Hydra</i> “admin”.....	28
Gambar 30. Tampilan Serangan <i>Hydra</i> “admin2”.....	29
Gambar 31. Dashboard serangan pertama.....	29

Gambar 32. Halaman Endpoints	30
Gambar 33. Tampilan Endpoints ubuntu server	30
Gambar 34. Threat Hunting serangan pertama	30
Gambar 35. Dashboard serangan kedua.....	31
Gambar 36. <i>Threat hunting</i> serangan kedua	31
Gambar 37. Dashboard <i>threat hunting</i>	32
Gambar 38. Trafik sebelum serangan	33
Gambar 39. Trafik selama serangan.....	33
Gambar 40. Trafik masuk	34
Gambar 41. Tampilan statistic serangan	34
Gambar 42. <i>Live view</i> serangan	35
Gambar 43. Rincian <i>log</i> yang diblokir.....	36
Gambar 44. <i>Rule level</i>	37
Gambar 45. Rule serangan pertama	39
Gambar 46. <i>Rule</i> serangan kedua.....	39
Gambar 47. Bagan alur eskalasi aturan wazuh	40
Gambar 48. Grafik <i>dashboard</i>	41

