

**IMPLEMENTASI *INTRUSION DETECTION SYSTEM*
(IDS) MENGGUNAKAN METODE *SIGNATURE*
RULES PADA *DATA CENTER* UPA TIK UNDIKSHA**



**OLEH:
GEDE BENY INDRAWAN
NIM 1915101002**

**PROGRAM STUDI ILMU KOMPUTER
JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KEJURUAN
UNIVERSITAS PENDIDIKAN GANESHA
SINGARAJA**

2024



**IMPLEMENTASI *INTRUSION DETECTION SYSTEM*
(IDS) MENGGUNAKAN METODE *SIGNATURE*
RULES PADA *DATA CENTER* UPA TIK UNDIKSHA**

SKRIPSI

**Diajukan kepada
Universitas Pendidikan Ganesha
Untuk Memenuhi Salah Satu Persyaratan dalam Menyelesaikan
Program Sarjana Ilmu Komputer**



**Oleh
Gede Beny Indrawan
NIM 1915101002**

**PROGRAM STUDI ILMU KOMPUTER
JURUSAN TEKNIK INFORMATIKA
FAKUTLAS TEKNIK DAN KEJURUAN
UNIVERSITAS PENDIDIKAN GANESHA
SINGARAJA**

2024

SKRIPSI

**DIAJUKAN UNTUK MELENGKAPI TUGAS DAN
MEMENUHI SYARAT-SYARAT UNTUK MENCAPAI
GELAR SARJANA KOMPUTER**



Pembimbing I,

Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D.
NIP. 197803242005011001

Pembimbing II,

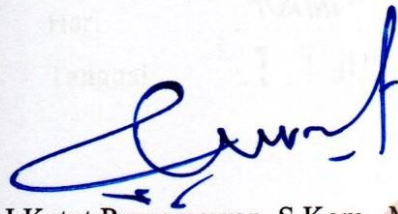
Ketut Resika Arthana, S.T., M.Kom.
NIP. 198412012012121002

Skripsi oleh Gede Beny Indrawan ini

Telah dipertahankan di depan dewan penguji

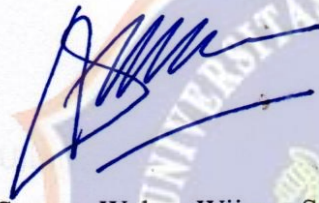
Pada tanggal 15 Mei 2024

Dewan Penguji,



I Ketut Purnamawan, S.Kom., M.Kom.
NIP. 197905112006041004

(Ketua)



I Nyoman Saputra Wahyu Wijaya, S.Kom., M.Cs.
NIP. 198910262019031004

(Anggota)



Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D.
NIP. 197803242005011001

(Anggota)



I Ketut Resika Arthana, S.T., M.Kom.
NIP. 198412012012121002

(Anggota)

Diterima oleh Panitia Ujian Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha
guna memenuhi syarat-syarat untuk mencapai gelar sarjana .

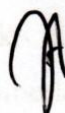
Pada:

Hari

Kamis

Tanggal

1 1 JUL 2024



Mengetahui,

Ketua Ujian,



Sekretaris Ujian,



Made Windu Antara Kesiman, S.T., M.Sc., Ph.D.
NIP. 198211112008121001

I Nyoman Saputra Wahyu Wijaya, S.Kom., M.Cs.
NIP. 198910262019031004

Mengesahkan,

Dekan Fakultas Teknik dan Kejuruan



Dr. Kadek Rihendra Dantes, S.T., M.T.
NIP. 197912012006041001

PERNYATAAN

Dengan ini saya menyatakan bahwa karya tulis yang berjudul “**Implementasi Intrusion Detection System (IDS) Menggunakan Metode Signature Rules Pada Data Center UPA TIK**” dan seluruh isi di dalamnya adalah hasil pemikiran dan usaha sendiri tanpa melakukan penjiplakan atau pengutipan yang melanggar etika penulisan pada pedoman skripsi. Jika terbukti adanya pelanggaran, saya bersedia menerima konsekuensi atau sanksi yang diberlakukan sesuai dengan ketentuan yang berlaku.

Singaraja , 14 Mei 2024

Yang membuat pernyataan,



Gede Beny Indrawan
NIM. 1915101002



MOTTO

“Aiming for Success with Precision and Determination”

PRAKATA

Dengan penuh rasa syukur dan kebahagiaan, saya membuat prakata ini sebagai wujud rasa terima kasih kepada semua pihak yang telah memberikan dukungan serta bimbingan selama perjuangan saya dalam menyelesaikan skripsi. Pembuatan skripsi ini menjadi puncak perjalanan pendidikan saya dan memberikan saya pengalaman tentang bagaimana rasa mencapai sebuah keberhasilan pada titik akhir untuk menyelesaikan tanggung jawab sebagai mahasiswa. Dengan judul skripsi “Implementasi *Intrusion Detection System (IDS)* Menggunakan Metode *Signature Rules* Pada *Data Center UPA TIK*”, saya ingin menyampaikan rasa tulus dan terima kasih kepada Ida Sang Hyang Widhi Wasa atas rahmat dan petunjuk-Nya, saya dapat mencapai kesuksesan dalam menyelesaikan skripsi ini. Semua perjuangan saya sampai menyelesaikan skripsi ini, tentu tidak lepas dari pertolongan dan dukungan yang diberikan kepada semua pihak. Saya juga ingin mengucapkan rasa terima kasih kepada :

1. Bapak Prof. Dr. I Wayan Lasmawan, M.Pd., selaku Rektor Universitas Pendidikan Ganesha beserta semua stafnya yang telah memberikan fasilitas dan dukungan penelitian sehingga dapat menyelesaikan studi dan melaksanakan penelitian skripsi sesuai dengan yang direncanakan.
2. Bapak Prof. Dr. I Gede Rasben Dantes, S.T., M.T.I., selaku Wakil Rektor 1 Bidang Akademik dan Kerjasama atas motivasi yang telah diberikan serta memberikan fasilitas untuk peneliti, sehingga bisa menyelesaikan studi dan melaksanakan penelitian skripsi sesuai dengan yang direncanakan.
3. Bapak Dr. Kadek Rihendra Dantes, S.T., M.T., selaku Dekan Fakultas Teknik dan Kejuruan beserta semua stafnya yang telah memberikan fasilitas dan dukungan penelitian sehingga dapat menyelesaikan studi dan melaksanakan penelitian skripsi sesuai dengan yang direncanakan.
4. Bapak Gede Arna Jude Saskara, S.T., M.T, selaku ketua Divisi Infrastruktur, Jaringan, dan Keamanan UPA TIK yang telah memberikan fasilitas, bimbingan, dan arahan kepada peneliti dalam menyelesaikan skripsi ini sehingga peneliti dapat menyelesaikan skripsi sesuai dengan yang direncanakan.

5. Bapak I Nyoman Saputra Wahyu Wijaya, S.Kom., M.Cs. selaku Kaprodi Ilmu Komputer atas motivasi dan fasilitas yang diberikan sehingga peneliti dapat menyelesaikan studi ini sesuai dengan yang direncanakan.
6. Bapak Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D. selaku pembimbing I yang telah memberikan arahan, bimbingan, dan motivasi kepada peneliti dalam menyelesaikan skripsi ini sehingga peneliti dapat menyelesaikan skripsi dengan yang direncanakan.
7. Bapak I Ketut Resika Arthana, S.T., M.Kom. selaku pembimbing II yang telah memberikan banyak motivasi, bimbingan, arahan, petunjuk skripsi, kepada peneliti dalam menyelesaikan skripsi ini sehingga peneliti dapat menyelesaikan skripsi dengan yang direncanakan.
8. Seluruh staf dosen di lingkungan Jurusan Teknik Informatika/Program Studi Ilmu Komputer yang telah memberikan ilmu, pengalaman, motivasi, serta semangat selama menjalani studi di Universitas Pendidikan Ganesha.
9. Tak lupa, terima kasih kepada Sahabat saya yakni Gede Subiksa, Agung Bajra, Eugene, Wawan Arimbawa, dan Nyoman Gotama dan teman teman lainnya yang saya tidak bisa sebutkan satu per satu yang selalu memberikan semangat dan dukungan dalam menghadapi setiap tantangan. Mereka adalah sumber kekuatan dan keceriaan selama perjalanan ini.
10. Dan juga saya ucapkan terima kasih atas dukungan dan doanya kepada seluruh mahasiswa ilmu komputer angkatan 2019 yang telah memberikan motivasi dan pengalaman yang berharga dalam proses penyelesaian Skripsi ini.
11. Seluruh pihak yang tidak bisa disebutkan satu persatu yang telah membantu peneliti dalam penyusunan skripsi sehingga dapat selesai tepat waktu.

Semoga Dengan Rahmat dan Karunia Tuhan Yang Maha Esa memberikan anugerah atas kebaikan yang telah diberikan oleh semua pihak yang turut membantu dalam menyelesaikan skripsi ini. Harapannya, skripsi ini dapat memberikan manfaat yang luas dan berkontribusi pada perkembangan dunia pendidikan, khususnya dalam bidang Pendidikan Teknik Informatika di masa depan.

Singaraja, 14 Mei 2024

Peneliti



DAFTAR ISI

ABSTRAK	xi
DAFTAR ISI.....	xiii
DAFTAR TABEL.....	xv
DAFTAR GAMBAR	xvi
DAFTAR LAMPIRAN.....	xviii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	2
1.3 Tujuan Penelitian.....	3
1.4 Manfaat Penelitian.....	3
1.4.1 Manfaat Teoritis.....	4
1.4.2 Manfaat Praktis	4
1.5 Batasan Masalah.....	5
BAB II KAJIAN TEORI.....	6
2.1 Penelitian Terkait.....	6
2.2 <i>Intrusion Detection System (IDS)</i>	8
2.3 Suricata	10
2.4 <i>Security Information and Event Management (SIEM)</i>	10
2.5 Kali Linux.....	11
2.6 <i>Path Traversal</i>	11
2.7 Burpsuite.....	12
2.8 XSS (<i>Cross Site Scripting</i>).....	13
2.9 <i>Port Mirroring</i> Mikrotik.....	14
2.10 <i>Wireshark</i>	14
2.11 Htop	15
2.12 <i>Zed Attack Proxy (ZAP)</i>	15
2.13 Performa Evaluasi Metrik IDS	16
BAB III METODE PENELITIAN.....	17

3.1 Kerangka Penelitian.....	17
3.2 Studi Literatur.....	18
3.3 Observasi	18
3.4 Wawancara	18
3.5 Pemilihan <i>Hardware</i> dan <i>Software</i>	19
3.6 Rancangan Topologi Jaringan	20
3.7 Proses Instalasi dan Konfigurasi	21
3.8 Konfigurasi IDS Secara Default.....	22
3.9 Simulasi Serangan	22
3.10 Analisis Paket Serangan	22
3.11 Konfigurasi <i>Signature-Based</i> IDS.....	23
3.12 Uji Kinerja <i>Rules</i> IDS.....	23
3.13 Hasil Pengujian.....	24
BAB IV HASIL DAN PEMBAHASAN	25
4.1 Hasil Penelitian.....	25
4.1.1 Hasil Proses Instalasi dan Konfigurasi.....	25
4.1.2 Simulasi Serangan.....	36
4.1.3 Analisis Paket Serangan.....	46
4.1.4 Konfigurasi <i>Signature-Based</i> IDS	47
4.1.5 Hasil Kinerja IDS.....	50
4.2 Pembahasan	59
4.2.1 Alur Mekanisme Pembuatan <i>Rules</i> dan Deteksi Serangan	59
4.2.2 Hasil Implementasi dan Pengujian.....	66
BAB V PENUTUP.....	95
5.1 Kesimpulan.....	95
5.2 Saran	95
DAFTAR PUSTAKA	97
LAMPIRAN	100
RIWAYAT HIDUP.....	104

DAFTAR TABEL

Tabel 3.1 Daftar <i>Hardware</i> dan <i>Software</i>	19
Tabel 3.2 Keterangan Alamat IP Perangkat Keras.....	21
Tabel 4.1 Proses Instalasi Suricata.....	27
Tabel 4.2 Konfigurasi Suricata	28
Tabel 4.3 Instalasi Certbot	28
Tabel 4.4 Konfigurasi Pembuatan SSL Untuk Domain.....	28
Tabel 4.5 Instalasi Elasticsearch	29
Tabel 4.6 Konfigurasi Elasticsearch	30
Tabel 4.7 Konfigurasi Kibana.....	32
Tabel 4.8 Proses Penambahan Server Fleet	34
Tabel 4.9 Hasil Performa Serangan DOS	56
Tabel 4.10 Hasil Performa Serangan ZAP <i>Scanning</i>	57
Tabel 4.11 Hasil Performa Serangan XSS <i>Stored</i>	58
Tabel 4.12 Tabel Konfigurasi Tambahan <i>Rules</i> Suricata	59
Tabel 4.13 Rangkuman Evaluasi IDS Percobaan Pertama	91
Tabel 4.14 Hasil DOS Pada Pengaturan Batasan Nilai.....	92
Tabel 4.15. Tabel Rangkuman Evaluasi Percobaan Kedua	94

DAFTAR GAMBAR

Gambar 3.1 Kerangka Penelitian	17
Gambar 3.2 Topologi Jaringan.....	21
Gambar 4.1 Konfigurasi Mikrotik.....	25
Gambar 4.2 Konfigurasi <i>Port Mirroring</i>	26
Gambar 4.3 Mendaftarkan SSL Pada Domain.....	29
Gambar 4.4 Menambahkan Sub Domain Elastic	31
Gambar 4.5 Menambahkan Sub Domain Kibana	33
Gambar 4.6 Konfigurasi Fleet Server	33
Gambar 4.7 Konfigurasi Output Fleet Server	34
Gambar 4.8 Hasil Penambahan Fleet Server.....	35
Gambar 4.9 Penambahan Integrasi Suricata	35
Gambar 4.10 <i>Log</i> Suricata.....	35
Gambar 4.11 Alur Mekanisme Serangan	36
Gambar 4.12 Percobaan Serangan DOS	37
Gambar 4.13 Hasil <i>Capture</i> Serangan DOS	37
Gambar 4.14 <i>Log</i> Elasticsearch Suricata Serangan DOS.....	38
Gambar 4.15 Aplikasi <i>ZAP Scanning</i>	39
Gambar 4.16 Website Sipepeng.....	39
Gambar 4.17 Input Data Pada Website Sipepeng	40
Gambar 4.18 Hasil <i>Capture</i> ZAP.....	40
Gambar 4.19 Percobaan Serangan <i>ZAP Scanning</i>	41
Gambar 4.20 Hasil Serangan <i>ZAP Scanning</i>	42
Gambar 4.21 Hasil <i>Log</i> Suricata Serangan <i>ZAP Scanning</i>	43
Gambar 4.22 <i>Payloads</i> Burpsuite	45
Gambar 4.23 Hasil Serangan Burpsuite	45
Gambar 4.24 <i>Log</i> Suricata Serangan <i>XSS Stored</i>	46
Gambar 4.25 <i>Log</i> Suricata Dengan <i>Signature-Rule</i> DOS.....	51
Gambar 4.26 <i>Log</i> IDS Suricata Serangan Slowloris.....	52
Gambar 4.27 <i>Log</i> Suricata Dengan <i>Signature-Rule</i> <i>ZAP Scanning</i>	52

Gambar 4.28 Log IDS Suricata Serangan sqlmap.....	53
Gambar 4.29 Log IDS Suricata Serangan Path Traversal	54
Gambar 4.30 Log Suricata Dengan Signature-Rule XSS Stored	54
Gambar 4.31 Log IDS Suricata Serangan XSS Script	55
Gambar 4.32 Pengujian Hasil Deteksi Serangan DOS	56
Gambar 4.33 Pengujian Hasil Deteksi Serangan ZAP Scanning.....	58
Gambar 4.34 Pengujian Hasil Deteksi Serangan XSS Stored.....	59



DAFTAR LAMPIRAN

Lampiran 1. Hasil Wawancara Dengan Ketua Divisi Infrastruktur, Jaringan dan Keamanan UPA TIK UNDIKSHA	101
Lampiran 2. Penempatan Komputer IDS Pada Ruang Server UPA TIK.....	103

