



**ANALISIS KINERJA SIEM WAZUH DENGAN FIM,
YARA, DAN VIRUSTOTAL DALAM MENDETEKSI
MALWARE PADA UBUNTU SERVER**

SKRIPSI

ROBBY AKBAR ABDULLAH

2107421004

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA**

2025



**ANALISIS KINERJA SIEM WAZUH DENGAN FIM,
YARA, DAN VIRUSTOTAL DALAM MENDETEKSI
MALWARE PADA UBUNTU SERVER**

SKRIPSI

**Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan
untuk Memperoleh Diploma Empat Politeknik**

ROBBY AKBAR ABDULLAH

2107421004

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA**

2025



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Robby Akbar Abdullah
NIM : 2107421004
Jurusan / Program Studi : Teknik Informatika dan Komputer /
Teknik Multimedia dan Jaringan
Judul Skripsi : Analisis Kinerja SIEM Wazuh dengan FIM,
YARA, dan VirusTotal dalam Mendeteksi
Malware pada Ubuntu Server

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 11 Juli 2025

Yang membuat pernyataan,



(Robby Akbar Abdullah)

NIM. 2107421004



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama : Robby Akbar Abdullah
NIM : 2107421004
Program Studi : Teknik Multimedia dan Jaringan
Judul Skripsi : Analisis Kinerja SIEM Wazuh dengan FIM, YARA,
dan VirusTotal dalam Mendeteksi Malware pada
Ubuntu Server

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Senin,
tanggal 23, bulan Jun, tahun 2025 dan
dinyatakan **LULUS**.

Disahkan oleh

Pembimbing I : Iik Muhamad Malik Matin, S.Kom., M.T. ()
Penguji I : Asep Kurniawan, S.Pd., M.Kom. ()
Penguji II : Fachroni Arbi Murad, S.Kom., M.Kom. ()
Penguji III : Ariawan Andi Suhandana, S.Kom., M.Ti. ()

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua



(Dr. Anita Hidayati, S.Kom., M.Kom.)

NIP. 197908032003122003



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Allah *subhanahu wa ta'ala* atas pertolonganNya dan karuniaNya sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisis Kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam Mendeteksi Malware pada Ubuntu Server”. Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk memperoleh gelar Diploma Empat Politeknik. Penulis menyadari bahwa tanpa bantuan dan dukungan dari berbagai pihak, penulis kesulitan dalam menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Bapak Iik Muhammad Malik Matin, S.Kom., M.T. selaku dosen pembimbing yang telah banyak membantu, mendukung, dan memberikan masukan serta saran kepada penulis selama pengerjaan skripsi ini hingga selesai.
2. Bunda, ayah, dan kakak yang telah memberikan bantuan dan dukungan material maupun moral yang nilainya tak terhingga.
3. Sahabat dan teman-teman seperjuangan yang telah memberikan bantuan dan dukungan dalam pengerjaan skripsi ini.
4. Seseorang bernama “Zae” yang selalu mendoakan, memberikan semangat, dan menjadi motivasi dalam menyelesaikan skripsi ini.

Penulis meminta maaf sebesar-besarnya apabila ada kesalahan atau kekurangan dalam proses pengerjaan skripsi ini. Penulis juga mengucapkan terima kasih sebanyak-banyaknya kepada seluruh pihak dan semoga Allah membalas kebaikan kalian semua. Penulis berharap skripsi ini bermanfaat bagi pembaca dan menjadi rujukan untuk melakukan penelitian selanjutnya.

Jakarta, 4 Juni 2025

Penulis



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan di bawah ini:

Nama : Robby Akbar Abdullah
NIM : 2107421004
Jurusan / Program Studi : Teknik Informatika dan Komputer /
Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

**Analisis Kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal
dalam Mendeteksi Malware pada Ubuntu Server**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 11 Juli 2025

Yang menyatakan,



(Robby Akbar Abdullah)

NIM. 2107421004



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

ANALISIS KINERJA SIEM WAZUH DENGAN FIM, YARA, DAN VIRUSTOTAL DALAM MENDETEKSI MALWARE PADA UBUNTU SERVER

ABSTRAK

Seiring dengan pesatnya perkembangan teknologi, maka serangan siber juga semakin kompleks dan beragam. Serangan siber tersebut terjadi dalam berbagai sektor sehingga menyebabkan banyak permasalahan keamanan siber. Oleh karena itu, dibutuhkan suatu sistem yang dapat mendeteksi, mencegah, dan merespon serangan siber melalui Security Information and Event Management (SIEM). Solusi SIEM yang tepat adalah Wazuh karena bersifat zero-cost dan open-source. Namun, perlu dilakukan analisis kinerja SIEM Wazuh tersebut dalam mendeteksi serangan siber. Berdasarkan penelitian terdahulu, analisis kinerja SIEM hanya sebatas parameter tertentu dan menguji serangan web dan network attack saja sehingga perlu dianalisis dari sisi malware agar kinerjanya lebih baik. Analisis kinerja SIEM Wazuh menggunakan FIM, YARA, dan VirusTotal untuk mengetahui mana yang paling baik kinerjanya dalam mendeteksi malware dengan menggunakan parameter-parameter tertentu. Hasil dari penelitian ini adalah FIM tidak berhasil mendeteksi semua malware, YARA berhasil mendeteksi semua malware, dan VirusTotal hanya mendeteksi dua dari tiga malware karena bergantung kepada database threat intelligence VirusTotal.

Kata Kunci: FIM, Malware, VirusTotal, Wazuh, YARA



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR ISI

SURAT PERNYATAAN BEBAS PLAGIARISME.....	i
LEMBAR PENGESAHAN	ii
KATA PENGANTAR	iii
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	iv
ABSTRAK.....	v
DAFTAR ISI.....	vi
DAFTAR GAMBAR.....	ix
DAFTAR TABEL.....	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah	1
1.2 Perumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan dan Manfaat	4
1.5 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA	6
2.1 Tinjauan Pustaka.....	6
2.1.1 <i>Security Information and Event Management (SIEM)</i>	6
2.1.2 Wazuh	6
2.1.3 <i>Server</i>	6
2.1.4 <i>File Integrity Monitoring (FIM)</i>	7
2.1.5 YARA	7
2.1.6 VirusTotal	7
2.1.7 <i>Malware</i>	7



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

2.2 Penelitian Terkait	8
BAB III METODE PENELITIAN	11
3.1 Rancangan Penelitian	11
3.1.1 Model atau <i>framework</i> yang digunakan	11
3.1.2 Teknik Pengumpulan dan Analisis Data	11
3.2 Tahapan Penelitian	12
3.3 Objek Penelitian	13
BAB IV HASIL DAN PEMBAHASAN	14
4.1 Analisis Kebutuhan	14
4.1.1 Spesifikasi Sistem	14
4.1.2 Konfigurasi Jaringan	14
4.2 Perancangan Sistem	15
4.2.1 Arsitektur sistem	15
4.2.2 <i>Flowchart</i> sistem	16
4.3 Implementasi Sistem	17
4.3.1 Instalasi Wazuh	17
4.3.2 Instalasi Wazuh <i>Agent</i>	22
4.3.3 Instalasi Suricata pada Wazuh <i>Agent</i>	23
4.3.4 Instalasi <i>Web Server</i> pada Wazuh <i>Agent</i>	29
4.3.5 Konfigurasi <i>Firewall</i> pada Wazuh <i>Agent</i>	31
4.3.6 Penerapan FIM pada Wazuh <i>Agent</i>	33
4.3.7 Penerapan YARA pada Wazuh <i>Agent</i>	34
4.3.8 Penerapan VirusTotal pada Wazuh <i>Agent</i>	40
4.4 Pengujian	42
4.4.1 Deskripsi Pengujian	42
4.4.2 Prosedur Pengujian	42



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.4.2.1	Pengujian Serangan <i>Port Scanning</i>	42
4.4.2.2	Pengujian Serangan <i>Denial of Service</i> (DoS)	43
4.4.2.3	Pengujian Serangan SSH <i>Brute-force</i>	43
4.4.2.4	Pengujian Serangan <i>Malware</i>	45
4.4.3	Data Hasil Pengujian.....	48
4.4.3.1	Hasil Pengujian Serangan <i>Port Scanning</i>	48
4.4.3.2	Hasil Pengujian Serangan <i>Denial of Service</i> (DoS).....	50
4.4.3.3	Hasil Pengujian Serangan SSH <i>brute-force</i>	52
4.4.3.4	Hasil Pengujian Serangan <i>Malware</i>	57
4.4.4	Analisis Data / Evaluasi Pengujian	63
4.4.4.1	Analisis Data Hasil Pengujian Serangan <i>Port Scanning</i>	63
4.4.4.2	Analisis Data Hasil Pengujian Serangan <i>Denial of Service</i> (DoS)	63
4.4.4.3	Analisis Data Hasil Pengujian Serangan SSH <i>Brute-force</i>	64
4.4.4.4	Analisis Data Hasil Pengujian Serangan <i>Malware</i>	64
BAB V PENUTUP.....		70
5.1	Kesimpulan	70
5.2	Saran.....	70
DAFTAR PUSTAKA		72
DAFTAR RIWAYAT HIDUP		73



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR GAMBAR

Gambar 1.1 Grafik Rekapitulasi Serangan <i>Malware</i>	1
Gambar 4.1 Arsitektur Sistem	15
Gambar 4.2 <i>Flowchart</i> Sistem	16
Gambar 4.3 Instalasi <i>Script</i> dan Konfigurasi Awal Wazuh	17
Gambar 4.4 Pengeditan <i>File</i> Konfigurasi Wazuh	17
Gambar 4.5 Isi <i>File</i> Konfigurasi Wazuh yang Telah Diedit	18
Gambar 4.6 Instalasi Wazuh	18
Gambar 4.7 Pengekstrakan <i>Password</i> Wazuh.....	19
Gambar 4.8 Instalasi Wazuh <i>Indexer</i>	19
Gambar 4.9 Inisiasi <i>Cluster</i> Wazuh	19
Gambar 4.10 Pengujian Keberhasilan Instalasi Wazuh	20
Gambar 4.11 Instalasi Wazuh <i>Server</i>	20
Gambar 4.12 Instalasi Wazuh <i>Dashboard</i>	21
Gambar 4.13 Tampilan Halaman <i>Login</i> Wazuh <i>Dashboard</i>	21
Gambar 4.14 Tampilan Halaman <i>Overview</i> Wazuh <i>Dashboard</i>	22
Gambar 4.15 Instalasi Wazuh <i>Agent</i>	22
Gambar 4.16 Pengaktifan Wazuh <i>Agent</i>	23
Gambar 4.17 Hasil Wazuh <i>Agent</i> yang Telah Berhasil Diinstalasi.....	23
Gambar 4.18 Penambahan Repositori Suricata.....	24
Gambar 4.19 Pembaruan Daftar Paket.....	24
Gambar 4.20 Instalasi Suricata.....	25
Gambar 4.21 Pengunduhan <i>Rules</i> Suricata	25
Gambar 4.22 Pengekstrakan <i>Rules</i> Suricata.....	26
Gambar 4.23 Pengubahan <i>Permission File Rules</i> Suricata	26
Gambar 4.24 Pengeditan <i>File Rules</i> Suricata.....	26
Gambar 4.25 Isi <i>File Rules</i> Suricata yang Telah Diedit.....	27
Gambar 4.26 Pengecekan Konfigurasi Jaringan	27
Gambar 4.27 Pembaruan Konfigurasi Suricata yang Telah Ditambahkan	27
Gambar 4.28 Pengeditan <i>File</i> Konfigurasi OSSEC	28



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.29 Isi <i>File</i> Konfigurasi OSSEC yang Telah Diedit	28
Gambar 4.30 Pembaruan Konfigurasi OSSEC yang Telah Ditambahkan	28
Gambar 4.31 Hasil Suricata yang Telah Berhasil Diinstal pada Wazuh <i>Agent</i>	29
Gambar 4.32 Pembaruan Daftar Paket	29
Gambar 4.33 Instalasi <i>Web Server Apache</i>	30
Gambar 4.34 Pengecekan Keberhasilan Instalasi <i>Web Server Apache</i>	30
Gambar 4.35 Tampilan <i>Web Server Apache</i> pada Wazuh <i>Agent</i>	31
Gambar 4.36 Pengecekan dan Pengaktifan <i>Firewall</i> pada Wazuh <i>Agent</i> ..	31
Gambar 4.37 Pengeditan <i>File</i> Konfigurasi SSH	31
Gambar 4.38 Isi <i>File</i> Konfigurasi SSH yang Telah Ditambahkan	32
Gambar 4.39 Pembaruan Konfigurasi SSH yang Telah Ditambahkan	32
Gambar 4.40 Hasil Konfigurasi <i>Firewall</i> yang Telah Ditambahkan	32
Gambar 4.41 Pengeditan <i>File</i> Konfigurasi OSSEC	33
Gambar 4.42 Penerapan FIM pada <i>File</i> Konfigurasi OSSEC	33
Gambar 4.43 Pembaruan Konfigurasi yang Telah Ditambahkan	33
Gambar 4.44 Pembaruan Daftar Paket	34
Gambar 4.45 Instalasi Dependensi	34
Gambar 4.46 Pengunduhan <i>Source Code YARA</i>	35
Gambar 4.47 Pengekstrakan <i>Source Code YARA</i>	35
Gambar 4.48 Proses <i>Build</i> dari <i>Source Code YARA</i>	36
Gambar 4.49 Pengecekan Keberhasilan Instalasi YARA	36
Gambar 4.50 Pembuatan Direktori untuk <i>YARA Rules</i>	36
Gambar 4.51 Pengunduhan <i>YARA Rules</i>	37
Gambar 4.52 Pembuatan <i>Script</i> untuk <i>Scanning YARA</i>	37
Gambar 4.53 Pengubahan <i>Owner</i> dan <i>Permission</i> pada <i>File Script YARA</i>	37
Gambar 4.54 Pembaruan Konfigurasi OSSEC yang Telah Ditambahkan	38
Gambar 4.55 Pengeditan <i>File</i> Konfigurasi <i>Local Rules</i>	38
Gambar 4.56 Isi <i>File</i> Konfigurasi <i>Local Rules</i> yang Telah Ditambahkan	38
Gambar 4.57 Pengeditan <i>File Local Decoder</i>	39



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.58 Isi <i>File</i> Konfigurasi <i>Local Decoder</i> yang Telah Ditambahkan	39
Gambar 4.59 Pengeditan <i>File</i> Konfigurasi OSSEC	39
Gambar 4.60 Isi <i>File</i> Konfigurasi OSSEC yang Telah Ditambahkan.....	40
Gambar 4.61 Pembaruan Konfigurasi yang Telah Ditambahkan	40
Gambar 4.62 Pengambilan <i>API Key</i> VirusTotal	41
Gambar 4.63 Pengeditan <i>File</i> Konfigurasi OSSEC	41
Gambar 4.64 Penerapan VirusTotal pada <i>File</i> Konfigurasi OSSEC	41
Gambar 4.65 Pembaruan Konfigurasi OSSEC yang Telah Ditambahkan	42
Gambar 4.66 Serangan <i>Port Scanning</i> ke Wazuh <i>Agent</i>	42
Gambar 4.67 Serangan DoS ke Wazuh <i>Agent</i>	43
Gambar 4.68 Pengujian Pertama Serangan SSH <i>Brute-force</i> ke Wazuh <i>Agent</i>	43
Gambar 4.69 Pengujian Kedua Serangan SSH <i>Brute-force</i> ke Wazuh <i>Agent</i>	44
Gambar 4.70 Pengujian Ketiga Serangan SSH <i>Brute-force</i> ke Wazuh <i>Agent</i>	44
Gambar 4.71 Pengujian Keempat Serangan SSH <i>Brute-force</i> ke Wazuh <i>Agent</i>	45
Gambar 4.72 Pembuatan <i>Script Malware</i> Pertama pada Wazuh <i>Agent</i>	45
Gambar 4.73 Serangan <i>Malware</i> Pertama ke Wazuh <i>Agent</i>	46
Gambar 4.74 Pembuatan <i>Script Malware</i> Kedua pada Wazuh <i>Agent</i>	46
Gambar 4.75 Serangan <i>Malware</i> Kedua ke Wazuh <i>Agent</i>	47
Gambar 4.76 Pembuatan <i>Script Malware</i> Ketiga pada Wazuh <i>Agent</i>	48
Gambar 4.77 Serangan <i>Malware</i> Ketiga ke Wazuh <i>Agent</i>	48
Gambar 4.78 Hasil Serangan <i>Port Scanning</i> pada Wazuh <i>Agent</i>	49
Gambar 4.79 Hasil Deteksi Serangan <i>Port Scanning</i> pada Wazuh <i>Agent</i>	49
Gambar 4.80 Hasil <i>Traffic</i> Serangan DoS pada Wazuh <i>Agent</i>	50
Gambar 4.81 Dampak Serangan DoS pada <i>Web Server</i> Wazuh <i>Agent</i> Sebelum Diblokir <i>Firewall</i>	51
Gambar 4.82 Konfigurasi <i>Firewall</i> pada Wazuh <i>Agent</i>	51



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.83 Dampak Serangan DoS pada <i>Web Server Wazuh Agent</i> Setelah Diblokir <i>Firewall</i>	52
Gambar 4.84 Hasil Serangan Pertama SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	52
Gambar 4.85 Hasil Deteksi Serangan Pertama SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	53
Gambar 4.86 Hasil Serangan Kedua SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	53
Gambar 4.87 Hasil Deteksi Serangan Kedua SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	54
Gambar 4.88 Hasil Serangan Ketiga SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	54
Gambar 4.89 Hasil Deteksi Serangan Ketiga SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	55
Gambar 4.90 Hasil Serangan Keempat SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	55
Gambar 4.91 Hasil Deteksi Serangan Keempat SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	56
Gambar 4.92 Pengujian <i>Login</i> SSH ke <i>Wazuh Agent</i>	56
Gambar 4.93 Hasil Deteksi Pengujian <i>Login</i> SSH ke <i>Wazuh Agent</i>	57
Gambar 4.94 Hasil Serangan <i>Malware</i> Pertama pada <i>Wazuh Agent</i>	57
Gambar 4.95 Hasil Serangan <i>Malware</i> Kedua pada <i>Wazuh Agent</i>	58
Gambar 4.96 Hasil Serangan <i>Malware</i> Ketiga pada <i>Wazuh Agent</i>	58
Gambar 4.97 Hasil Serangan <i>Malware</i> Pertama pada <i>Wazuh Agent</i>	59
Gambar 4.98 Hasil Serangan <i>Malware</i> Kedua pada <i>Wazuh Agent</i>	59
Gambar 4.99 Hasil Serangan <i>Malware</i> Ketiga pada <i>Wazuh Agent</i>	60
Gambar 4.100 Hasil Serangan <i>Malware</i> Pertama pada <i>Wazuh Agent</i>	60
Gambar 4.101 Detail <i>Malware</i> Pertama di VirusTotal	61
Gambar 4.102 Hasil Serangan <i>Malware</i> Kedua pada <i>Wazuh Agent</i>	61
Gambar 4.103 Detail <i>Malware</i> Kedua di VirusTotal	62
Gambar 4.104 Hasil Serangan <i>Malware</i> Ketiga pada <i>Wazuh Agent</i>	62
Gambar 4.105 Beban Sistem yang Digunakan.....	63



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait	8
Tabel 4.1 Spesifikasi Sistem	14
Tabel 4.2 Kebutuhan NAT <i>Network</i>	14
Tabel 4.3 Kebutuhan <i>Port Forwarding</i>	15
Tabel 4.4 Analisis Data Hasil Pengujian Serangan <i>Malware</i> Menggunakan FIM.....	64
Tabel 4.5 Analisis Data Hasil Pengujian Serangan <i>Malware</i> Menggunakan YARA.....	65
Tabel 4.6 Analisis Data Hasil Pengujian Serangan <i>Malware</i> Menggunakan VirusTotal.....	67
Tabel 4.7 Analisis Data Hasil Pengujian Serangan <i>Malware</i> pada Wazuh <i>Agent</i>	69

**POLITEKNIK
NEGERI
JAKARTA**

Hak Cipta :

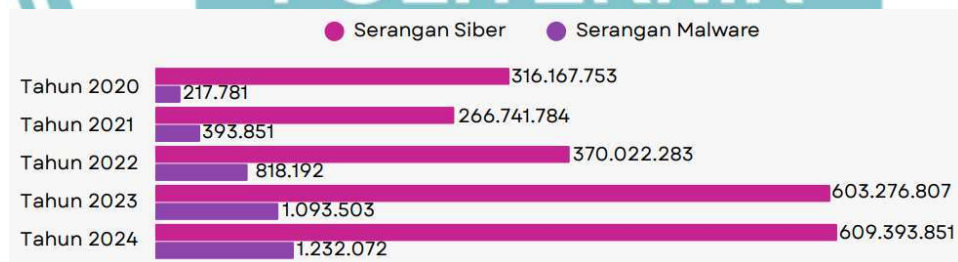
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB I PENDAHULUAN

1.1 Latar Belakang Masalah

Era digital adalah era yang mengalami perkembangan teknologi dengan sangat pesat. Seiring dengan pesatnya perkembangan teknologi tersebut, maka serangan siber juga semakin kompleks dan beragam. Serangan siber tersebut ditujukan kepada infrastruktur teknologi dan informasi dalam berbagai sektor. Hal tersebut menyebabkan banyak sekali terjadinya permasalahan keamanan siber dikarenakan lemahnya sistem keamanan. (Husnul Khotimah, 2022)

Berdasarkan laporan tahunan *honeynet* yang diterbitkan oleh (Badan Siber dan Sandi Negara, 2024) jumlah serangan siber terutama *malware* setiap tahunnya mengalami peningkatan pada sistem *honeynet* secara keseluruhan. Data serangan *malware* yang tercatat pada sistem *honeynet* sebanyak 1.232.072 pada tahun 2024. Berikut adalah rekapitulasi serangan *malware* lima tahun terakhir pada sistem *honeynet* yang tercantum pada Gambar 1.1.



Gambar 1.1 Grafik Rekapitulasi Serangan Malware

Sumber: (Badan Siber dan Sandi Negara, 2024)

Berdasarkan permasalahan-permasalahan keamanan siber tersebut, maka dibutuhkan adanya suatu sistem yang dapat mendeteksi, mencegah, dan meresponnya. Oleh karena itu, dibutuhkan penerapan yang lebih efektif melalui *Security Information and Event Management* (SIEM). Teknologi SIEM ini dapat melakukan pengumpulan informasi keamanan yang berasal dari data *log* berbagai sumber secara *real-time*. (Husnul Khotimah, 2022)



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Solusi SIEM yang tepat adalah menggunakan Wazuh karena bersifat *zero-cost* dan *open-source* sehingga mudah melakukan *custom* tanpa mengeluarkan biaya. Namun, perlu dilakukan analisis mengenai kinerja SIEM Wazuh tersebut dalam mendeteksi serangan siber. Penelitian yang dilakukan oleh (Oky Dwi Prasetyo, 2023) menganalisis kinerja SIEM Wazuh untuk menguji serangan *brute-force* dan *Denial of Service* (DoS) dengan parameter *signature-based detection* dan *anomaly-based detection*. Selain itu, terdapat penelitian yang serupa menganalisis kinerja SIEM IBM QRadar oleh (Adirosa, 2021) untuk menguji serangan *port scanning*, *password checking*, DoS, dan eksploit metasploitable 3 dengan parameter *flow source* dan *log source*. Selanjutnya, terdapat penelitian menganalisis kinerja SIEM Elastic Stack dan Splunk oleh (Alfandi, 2022) untuk menguji serangan *fingerprinting*, *SQL injection*, DoS, dan *port scanning* dengan parameter pengiriman notifikasi dan pengujian selama tiga hari.

Berdasarkan beberapa penelitian tersebut, pengujian hanya dilakukan dari serangan *web* dan *network attack* saja sehingga perlu dianalisis dari sisi *malware* agar kinerjanya lebih baik. *Malware* atau *malicious software* dapat berdampak berbahaya bagi sistem, rusaknya data, tersebarnya infeksi, dan banyak kerugian lainnya. Oleh karena itu, perlu dilakukan analisis kinerja SIEM Wazuh dalam mendeteksi *malware* pada *server* agar kinerjanya lebih baik. SIEM Wazuh secara *default* hanya terdapat *File Integrity Monitoring* (FIM) sehingga harus diinstalasi dengan YARA dan VirusTotal agar kinerjanya lebih baik. Selanjutnya, dapat dianalisis kinerja tersebut berdasarkan parameter-parameter yang telah ditentukan, yaitu jumlah *malware* yang terdeteksi, kecepatan deteksi *malware*, tingkat kesalahan, jenis *malware* yang terdeteksi, dan beban sistem yang digunakan sehingga dapat lebih cepat dan tanggap dalam menangani serangan siber terutama *malware*.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1.2 Perumusan Masalah

Berdasarkan hal-hal yang telah disampaikan di atas, maka rumusan permasalahannya:

1. Bagaimana rancang bangun SIEM Wazuh untuk mendeteksi serangan *port scanning*, *DoS*, *brute-force*, dan *malware*?
2. Bagaimana penerapan FIM, YARA, dan VirusTotal ke dalam SIEM Wazuh untuk mendeteksi *malware*?
3. Bagaimana hasil analisis kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam mendeteksi *malware*?

1.3 Batasan Masalah

Penelitian ini berfokus pada:

1. SIEM yang digunakan terbatas pada Wazuh.
2. Penerapan *tools* dalam mendeteksi *malware* pada SIEM Wazuh terbatas pada FIM, YARA, dan VirusTotal.
3. *Server* yang dimonitoring terbatas pada sistem operasi Ubuntu *Server*.
4. Eksperimen yang dilakukan terbatas menggunakan *virtual machine* dalam ruang lingkup lokal dan berada pada jaringan yang sama.
5. Pengujian yang dilakukan terbatas pada serangan *port scanning*, *Denial of Service* (DoS), *brute-force*, dan *malware*.
6. Parameter-parameter yang diuji dalam mendeteksi *malware* terbatas pada jumlah *malware* yang terdeteksi, kecepatan deteksi *malware*, tingkat kesalahan, jenis *malware* yang dideteksi, dan beban sistem yang digunakan.
7. Analisis kinerja yang dilakukan pada SIEM Wazuh terbatas pada hasil pengujian serangan *port scanning*, *Denial of Service* (DoS), *brute-force*, dan *malware*.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1.4 Tujuan dan Manfaat

Penelitian ini memiliki tujuan yang akan dicapai, antara lain:

1. Merancang bangun SIEM Wazuh untuk mendeteksi serangan *port scanning*, *DoS*, *brute-force*, dan *malware*.
2. Menerapkan FIM, YARA, dan VirusTotal ke dalam SIEM Wazuh untuk mendeteksi *malware*.
3. Mengukur kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam mendeteksi *malware*.

Penelitian ini diharapkan dapat memberikan manfaat bagi berbagai pihak, antara lain:

1. Mahasiswa
Penelitian ini dapat menjadi referensi dalam memahami dan mengembangkan penelitian di bidang keamanan siber.
2. Dosen
Penelitian ini dapat menjadi bahan kajian tambahan dalam pengajaran topik-topik terkait keamanan siber.
3. Institusi
Penelitian ini dapat menjadi bukti bahwa mahasiswa telah lulus kompetensi sesuai bidangnya.
4. Industri
Penelitian ini dapat menjadi informasi teknis atau acuan dalam memilih metode deteksi yang sesuai untuk kebutuhan industri.
5. Masyarakat
Penelitian ini dapat meningkatkan kesadaran akan bahayanya serangan siber dan pemahaman tentang pentingnya deteksi dini terhadap serangan siber.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1.5 Sistematika Penulisan

Adapun sistematika penulisan skripsi ini:

A. BAB I PENDAHULUAN

Bab I berisi penjelasan mengenai jawaban apa dan mengapa penelitian ini perlu dilakukan. Bagian ini meliputi latar belakang masalah, perumusan masalah, batasan masalah, serta tujuan dan manfaat analisis kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam mendeteksi *malware* pada Ubuntu Server.

B. BAB II TINJAUAN PUSTAKA

Bab II berisi penjelasan mengenai landasan teori atau studi literatur yang berhubungan antara karya peneliti sebelumnya dengan riset penelitian yang dilakukan saat ini.

C. BAB III METODOLOGI PENELITIAN

Bab III berisi penjelasan mengenai rancangan penelitian, tahapan penelitian, dan objek penelitian.

D. BAB IV HASIL DAN PEMBAHASAN

Bab IV berisi hasil dan pembahasan mengenai penelitian yang dilakukan meliputi analisis kebutuhan, perancangan, pengujian, dan hasil analisis pengujian.

E. BAB V PENUTUP

Bab V berisi penjelasan mengenai hasil akhir dari penelitian berupa kesimpulan dan saran secara singkat terhadap pembahasan yang telah diuraikan pada bagian isi.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat diambil kesimpulan sebagai berikut:

- a. Rancang bangun SIEM Wazuh untuk mendeteksi serangan (*port scanning*, *DoS*, *brute-force*, dan *malware*) berjalan dengan baik, mulai dari instalasi Wazuh *server*, Wazuh *indexer*, Wazuh *dashboard*, Wazuh *agent*, Suricata, *web server* Apache, dan konfigurasi *firewall*.
- b. Penerapan FIM, YARA, dan VirusTotal ke SIEM Wazuh berjalan dengan baik. Penerapan FIM dengan cara menambahkan direktori yang ingin dimonitor pada *file* konfigurasi OSSEC. Penerapan YARA dengan cara melakukan instalasi dan konfigurasi YARA, serta menambahkan *rules* dari YARA. Penerapan VirusTotal dengan cara menambahkan *API key* dari VirusTotal pada *file* konfigurasi OSSEC.
- c. Hasil analisisnya adalah FIM tidak berhasil mendeteksi semua *malware* karena hanya mendeteksi berdasarkan integritas *file* saja, YARA berhasil mendeteksi semua *malware* karena mendeteksi berdasarkan *rules*, dan VirusTotal hanya berhasil mendeteksi dua dari tiga *malware* saja karena bergantung pada *database*. Oleh karena itu, *tools* yang paling baik dalam mendeteksi *malware* adalah YARA.

5.2 Saran

Saran yang dapat diterapkan untuk melakukan penelitian lebih lanjut sebagai berikut:

- a. Melakukan analisis kinerja SIEM lain dalam mendeteksi serangan, seperti IBM QRadar, Elastic, Splunk, dan lain-lain untuk mengukur kinerja SIEM yang paling baik.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- b. Menerapkan *tools* lain dalam mendeteksi *malware*, seperti MISP, Kaspersky, Hybrid Analysis, dan lain-lain. Selain itu, menerapkan *tools Endpoint Detection and Response* (EDR) untuk pemblokiran *malware*, seperti CrowdStrike, Microsoft Defender, SentinelOne, dan lain-lain.
- c. Melakukan monitoring *server* dengan sistem operasi yang berbeda, seperti CentOS, Debian, Red Hat Enterprise Linux (RHEL), dan lain-lain.
- d. Melakukan eksperimen menggunakan perangkat nyata dalam ruang lingkup global dan berada pada jaringan yang berbeda.
- e. Menambahkan pengujian serangan-serangan lain, seperti berpacu pada MITRE ATT&CK dan OWASP Top 10.
- f. Menambahkan pemblokiran *malware* dengan parameter seberapa cepat dan tepat *malware* tersebut diblokir.
- g. Menambahkan analisis kinerja hasil pengujian serangan-serangan lain, seperti berpacu pada MITRE ATT&CK dan OWASP Top 10.

**POLITEKNIK
NEGERI
JAKARTA**



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR PUSTAKA

- Adirosa, G., 2021. ANALISIS KINERJA SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) IBM QRADAR COMMUNITY EDITION DALAM MENDETEKSI ANCAMAN DAN SERANGAN SIBER PADA SERVER.
- Alfandi, M., 2022. Analisa Security Information and Event Management (SIEM) Menggunakan Elastic Stack SIEM dan Splunk.
- Azzah Shafiyah, G. F. N. R. A. P., 2024. IMPLEMENTASI WAZUH MENGGUNAKAN METODE PPDIIOO DI SISTEM KEAMANAN JARINGAN PSDKU UNIVERSITAS LAMPUNG WAYKANAN SEBAGAI DETEKSI DAN RESPON SERANGAN SIBER. *JITET (Jurnal Informatika dan Teknik Elektro Terapan)*, 12(2), pp. 1-13.
- Badan Siber dan Sandi Negara, 2024. *Laporan Tahunan Layanan Honeynet BSSN*, s.l.: s.n.
- Husnul Khotimah, F. B. R. S. K. I. B. K. W., 2022. Implementasi Security Information And Event Management (SIEM) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat. *JBegaTI*, September, 3(2), p. 7.
- Lintang, D., 2020. MONITORING AKTIVITAS USER PADA SYSTEM DENGAN MENGGUNAKAN EFK (ELASTICSEARCH, FLUENTD, KIBANA) STACK.
- Muhammad Rijal Kamal, M. A. S., 2021. Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII. *Automata*, 2(2), pp. 1-6.
- Nur Rohman Rosyid, B. B. M. B. P. A. F. R. L. S., 2023. Deteksi Malware pada Jaringan Lokal Berbasis Honeypot dan Yara. *JURNAL SISTEMASI*, 12(1), pp. 186-193.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Nurul Qomariah, E. I. A. M. A. A., 2023. Analisis Malware Hummingbad Dan Copycat Pada Android Menggunakan Metode Hybrid. *Jurnal Cyber Security dan Forensic Digital*, 6(2), pp. 39-47.

Okky Dwi Prasetyo, P. H. T. A. B., 2023. Uji Kinerja Host-Based Intrusion Detection System WAZUH terhadap Serangan Brute Force dan Dos. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, Juni, 7(6), pp. 2686-2692.

Prakoso, R. D., 2017. IMPLEMENTASI DAN PERBANDINGAN PERFORMA PROXMOX DALAM VIRTUALISASI DENGAN TIGA VIRTUAL SERVER. *JURNAL MANAJEMEN INFORMATIKA*, 8(1), pp. 1-8.

Stefan Stanković, S. G. R. P., 2022. A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis.

Thorarensen, C., 2021. A Performance Analysis of Intrusion Detection with Snort and Security Information Management. *DiVA*.

Yuriansyah Ilhamdi, Y. N. K., 2017. ANALISIS MALWARE PADA SISTEM OPERASI WINDOWS. *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia)*, 2(1), pp. 1-12.

DAFTAR RIWAYAT HIDUP



Robby Akbar Abdullah

Lahir di salah satu kota Indonesia pada tahun 2003. Penulis merupakan anak kedua dari dua bersaudara. Saat ini penulis berdomisili di daerah Jakarta Selatan. Penulis menyelesaikan pendidikan Sekolah Dasar (SD) pada tahun 2015 dan pendidikan Sekolah Menengah Pertama (SMP) pada tahun 2018.

Kemudian, penulis menyelesaikan pendidikan Sekolah Menengah Kejuruan (SMK) dengan jurusan Teknik Komputer dan Jaringan (TKJ) pada tahun 2021. Lalu, penulis menyelesaikan pendidikan Diploma Empat (D4) di Politeknik Negeri Jakarta dengan program studi Teknik Multimedia dan Jaringan (TMJ) pada tahun 2025.

**POLITEKNIK
NEGERI
JAKARTA**

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

