Analisis Deteksi Serangan Siber Menggunakan Wazuh SIEM pada Lab CTF Berbasis MITRE ATT&CK dengan Kontrol Keamanan Berdasarkan Prinsip Zero Trust

Pransiska Monalisa [*], Maidel Fani [#]

[*] Politeknik Negeri Batam
Rekayasa Keamanan Siber
Jl. Ahmad Yani, Batam Centre, Batam 29461, Indonesia

E-mail: siskalisa19@gmail.com

[#] Politeknik Negeri Batam
Rekayasa Keamanan Siber
Jl. Ahmad Yani, Batam Centre, Batam 29461, Indonesia

E-mail: maedal.fani@polibatam.ac.id

Abstrak

Ancaman serangan siber yang semakin kompleks menuntut sistem deteksi yang mampu mengidentifikasi tahapan serangan secara menyeluruh. Penelitian ini mengevaluasi kemampuan Wazuh SIEM versi 4.7.5 dalam mendeteksi tahapan serangan siber pada lab CTF KMIPN 2024 mesin Amethysts yang menerapkan kontrol keamanan berbasis prinsip Zero Trust, serta memetakan alert yang dihasilkan ke framework MITRE ATT&CK. Skenario serangan mencakup Port Enumeration, Service Enumeration, SMB Enumeration, RPC Enumeration, FTP Enumeration, ZIP Password Cracking, MD5 Hash Cracking, Web Directory Enumeration, Hydra Brute Force, File Upload, Remote Code Execution, Credential Leakage, Privilege Escalation. Performa deteksi Wazuh SIEM dievaluasi menggunakan metrik True Positive Rate, False Positive Rate, presisi, dan recall berdasarkan alert yang terpicu pada setiap tahapan serangan.

Kata kunci: Wazuh SIEM, *Zero Trust*, MITRE ATT&CK, Deteksi Serangan Siber, CTF

Abstract

The increasingly complex threat of cyber attacks demands a detection system capable of identifying the stages of an attack comprehensively. This study evaluates the ability of Wazuh SIEM version 4.7.5 in detecting the stages of a cyber attack in the KMIPN 2024 CTF lab on the Amethysts machine, which applies security controls based on Zero Trust principles, and maps the generated alerts to the MITRE ATT&CK framework. Attack scenarios include Port Enumeration, Service Enumeration, SMB Enumeration, RPC Enumeration, FTP Enumeration, ZIP Password Cracking, MD5 Hash Cracking, Web Directory Enumeration, Hydra Brute Force, File Upload, Remote Code Execution, Credential Leakage, Privilege Escalation. The detection performance of Wazuh SIEM is evaluated using True Positive Rate, False Positive Rate, precision, and recall metrics based on alerts triggered at each stage of the attack.

Keywords : Wazuh SIEM, Zero Trust, MITRE ATT&CK, Cyber Attack Detection, CTF

1. Pendahuluan

Perkembangan teknologi informasi yang pesat membawa dampak signifikan terhadap meningkatnya ancaman serangan siber di Indonesia. Berdasarkan laporan Lanskap Keamanan Siber Indonesia tahun 2024 yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN), total trafik anomali di Indonesia sepanjang tahun 2024 mencapai 330.527.636 anomali, dengan jenis trafik anomali tertinggi yaitu Mirai Botnet sebanyak 81.286.596 aktivitas, disusul 2.487.041 aktivitas Advanced Persistent Threat (APT), 514.508 aktivitas ransomware, dan 26.771.610 aktivitas phishing [1]. Kondisi ini menunjukkan bahwa ancaman siber di Indonesia tidak hanya meningkat dari sisi kuantitas, tetapi juga semakin beragam dalam bentuk serangan bertahap yang menggabungkan enumerasi, eksploitasi, hingga eskalasi hak akses yang sulit diidentifikasi tanpa sistem pemantauan yang memadai.

Zero Trust berkembang sebagai prinsip keamanan yang menjawab keterbatasan model keamanan perimeter tradisional, dengan menerapkan gagasan never trust, always verify pada setiap entitas dalam

jaringan. Prinsip ini umumnya diwujudkan melalui kontrol keamanan seperti verifikasi identitas dan kredensial berlapis di setiap tahap akses, pembatasan hak akses sesuai kebutuhan (least privilege), serta validasi berkelanjutan terhadap aktivitas pengguna maupun sistem [2]. Karakteristik utama dari prinsip ini adalah bahwa kepercayaan tidak pernah diberikan secara permanen — setiap permintaan akses harus terus-menerus diverifikasi, sehingga efektivitasnya sangat bergantung pada kemampuan sistem untuk mengamati dan mencatat setiap aktivitas secara berkelanjutan. Tanpa visibilitas yang memadai terhadap log autentikasi, akses layanan, dan perubahan hak akses, kontrol keamanan berbasis prinsip Zero Trust tidak dapat benar-benar berjalan efektif, dan potensi serangan bertahap seperti eskalasi hak akses dapat luput dari deteksi meskipun kontrol verifikasinya sudah diterapkan pada sistem. Dengan kata lain, kontrol keamanan yang dirancang mengikuti prinsip Zero Trust tetap dapat gagal secara praktik apabila lapisan monitoring dan deteksinya tidak diuji dan divalidasi.

Security Information and Event Management (SIEM) menjadi komponen yang mengisi kebutuhan visibilitas tersebut, dengan mengintegrasikan pengumpulan, korelasi, dan analisis log dari berbagai sumber secara terpusat untuk mendeteksi ancaman secara real-time [3]. Wazuh dipilih sebagai platform SIEM dalam penelitian ini karena bersifat open source, memiliki kemampuan deteksi berbasis host, dukungan XDR, serta integrasi native dengan framework MITRE ATT&CK [4]. Framework MITRE ATT&CK dipilih sebagai basis pemetaan dibandingkan model tahapan serangan lain seperti Lockheed Martin Cyber Kill Chain karena ATT&CK menyediakan taksonomi taktik dan teknik yang lebih granular pada level teknis, serta didukung secara native oleh Wazuh melalui field rule.mitre.tactic dan rule.mitre.id, sehingga pemetaan alert ke taktik/teknik dapat dilakukan tanpa interpretasi manual tambahan yang rawan bias [5].

Meski demikian, performa deteksi Wazuh secara standalone pada penelitian sebelumnya masih terbatas, dengan akurasi rendah (19,70%) dan recall rendah (16,26%) [5], sehingga efektivitasnya perlu diuji ulang pada konteks dan skenario serangan yang lebih spesifik. Penelitian yang secara khusus mengkaji kemampuan deteksi Wazuh pada lingkungan yang menerapkan kontrol keamanan berbasis prinsip Zero Trust — dengan skenario attack chain yang lengkap dan merepresentasikan tahapan serangan nyata masih sangat terbatas di Indonesia. Kompetisi Mahasiswa Informatika Politeknik Nasional (KMIPN) 2024 menyediakan skenario CTF pada mesin Amethysts yang menerapkan kontrol verifikasi kredensial dan akses bertingkat pada tiap layanannya, mencakup enumerasi jaringan, cracking kredensial, eksploitasi web, credential leakage, hingga privilege escalation, sehingga relevan dijadikan basis pengujian visibilitas deteksi pada konteks penerapan prinsip Zero Trust. Meskipun demikian, penelitian ini menyadari bahwa satu skenario CTF tidak sepenuhnya merepresentasikan kompleksitas kontrol Zero Trust pada lingkungan produksi berskala penuh, sehingga hasil evaluasi yang diperoleh bersifat indikatif terhadap skenario pengujian yang digunakan, bukan generalisasi mutlak terhadap performa Wazuh SIEM secara umum.

Berdasarkan hal tersebut, penelitian ini bertujuan mengevaluasi kemampuan Wazuh SIEM versi 4.7.5 dalam mendeteksi tahapan serangan siber pada lab CTF KMIPN 2024 mesin Amethysts yang menerapkan kontrol keamanan berdasarkan prinsip Zero Trust, serta memetakan alert yang dihasilkan ke framework MITRE ATT&CK menggunakan metrik evaluasi True Positive Rate, False Positive Rate, presisi, dan recall.

2. Landasan Teori

2.1 Prinsip Zero Trust

Zero Trust merupakan prinsip keamanan jaringan yang meninggalkan asumsi kepercayaan implisit terhadap entitas di dalam maupun di luar perimeter jaringan, dan menggantinya dengan gagasan never trust, always verify pada setiap permintaan akses. Prinsip ini umumnya diwujudkan melalui tiga mekanisme utama: micro-segmentation yang membagi jaringan menjadi segmen-segmen kecil untuk membatasi pergerakan lateral penyerang, least privilege access yang membatasi hak akses entitas hanya pada sumber daya yang benar-benar diperlukan, dan continuous verification yang melakukan validasi identitas dan kredensial secara berkelanjutan pada setiap tahap akses, bukan hanya pada saat login awal.

Penerapan prinsip Zero Trust secara utuh biasanya membutuhkan komponen pendukung seperti identity provider terpusat, policy engine, dan segmentasi jaringan berbasis kebijakan. Pada konteks penelitian

ini, lingkungan lab CTF KMIPN 2024 mesin Amethysts tidak mengimplementasikan ZTA secara penuh dengan seluruh komponen tersebut, melainkan merefleksikan sebagian kontrol keamanan yang sejalan dengan prinsip Zero Trust, khususnya pada aspek verifikasi kredensial berlapis di setiap layanan dan pembatasan akses bertingkat sebelum sebuah entitas dapat mencapai sumber daya berikutnya dalam attack chain. Karakteristik inilah yang menjadikan mesin Amethysts relevan sebagai objek pengujian kemampuan deteksi Wazuh SIEM pada lingkungan yang menerapkan kontrol berbasis Zero Trust, karena setiap tahapan serangan mulai dari enumerasi hingga eskalasi hak akses harus melewati proses verifikasi tersendiri yang idealnya tercatat dan dapat dipantau oleh sistem monitoring.

2.2 Security Information and Event Management (SIEM)

SIEM adalah platform yang mengintegrasikan fungsi pengumpulan, korelasi, dan analisis log dari berbagai sumber secara terpusat untuk mendeteksi ancaman keamanan secara real-time. Dengan mengagregasi log dari banyak entitas (host, jaringan, aplikasi) ke satu titik analisis, SIEM memungkinkan identifikasi pola serangan yang mungkin tidak terlihat jika log dianalisis secara terpisah per sumber [4].

2.3 Wazuh SIEM

Wazuh adalah platform SIEM open source yang menggabungkan kemampuan host-based intrusion detection (HIDS), log analysis, file integrity monitoring, dan dukungan Extended Detection and Response (XDR). Arsitektur Wazuh terdiri atas tiga komponen utama: Wazuh Manager yang menerima dan menganalisis log dari agen, Wazuh Indexer yang menyimpan dan mengindeks data log, serta Wazuh Dashboard sebagai antarmuka visual untuk pemantauan dan analisis peringatan keamanan. Salah satu keunggulan Wazuh dibanding platform SIEM lain adalah integrasi native dengan framework MITRE ATT&CK melalui field rule.mitre.tactic dan rule.mitre.id pada setiap alert yang dihasilkan [4]. Meski demikian, penelitian terdahulu menunjukkan performa deteksi Wazuh secara standalone (tanpa penyesuaian ruleset) masih terbatas, dengan akurasi dan recall yang rendah, sehingga diperlukan pengujian lebih lanjut pada konteks lingkungan yang lebih spesifik [5].

2.4 MITRE ATT&CK Framework

MITRE ATT&CK adalah basis pengetahuan (knowledge base) yang mendokumentasikan taktik (tactics) dan teknik (techniques) serangan siber berdasarkan observasi dunia nyata terhadap perilaku pelaku ancaman. Taktik merepresentasikan tujuan taktis penyerang pada suatu tahapan serangan (mis. Discovery, Credential Access, Privilege Escalation), sedangkan teknik merepresentasikan cara spesifik untuk mencapai tujuan tersebut, yang masing-masing memiliki kode identifikasi unik (Technique ID, mis. T1046) dan dapat memiliki sub-teknik yang lebih granular (mis. T1021.002) [7]. Dibandingkan model tahapan serangan yang lebih generik seperti Cyber Kill Chain, MITRE ATT&CK menawarkan granularitas yang lebih tinggi pada level teknik dan sub-teknik, sehingga lebih sesuai digunakan untuk memetakan alert SIEM yang bersifat spesifik per-rule [6].

2.5 Metrik Evaluasi Performa Deteksi

Evaluasi kemampuan deteksi suatu sistem SIEM umumnya menggunakan kerangka klasifikasi biner yang membandingkan hasil deteksi sistem dengan kondisi aktual serangan, menghasilkan empat kategori: True Positive (TP) ketika serangan benar-benar terjadi dan berhasil terdeteksi, False Positive (FP) ketika aktivitas normal keliru terdeteksi sebagai serangan, False Negative (FN) ketika serangan terjadi namun luput dari deteksi, dan True Negative (TN) ketika aktivitas normal tidak memicu alert. Dari keempat kategori tersebut diturunkan metrik presisi (proporsi alert yang valid dari seluruh alert yang dihasilkan), recall/True Positive Rate (proporsi serangan yang berhasil terdeteksi dari seluruh serangan yang terjadi), dan False Positive Rate (proporsi aktivitas normal yang salah diklasifikasikan sebagai serangan) [8].

3. Metode Penelitian

Penelitian ini menggunakan metode eksperimental dengan menjalankan skenario serangan siber pada lingkungan lab CTF KMIPN 2024 mesin Amethysts yang menerapkan kontrol keamanan berbasis prinsip Zero Trust, kemudian menganalisis alert yang dihasilkan menggunakan Wazuh SIEM versi 4.7.5. Lingkungan pengujian dijalankan pada platform VMware Workstation dengan sistem operasi Ubuntu 22.04.4 LTS, dan Wazuh diakses melalui dashboard berbasis web pada alamat https://192.168.85.131.

Secara keseluruhan, tahapan penelitian ini dimulai

dari persiapan konfigurasi pengujian, penentuan skenario serangan, dan analisis deteksi oleh Wazuh SIEM, pemetaan hasil deteksi ke framework MITRE ATT&CK, hingga evaluasi performa deteksi menggunakan metrik klasifikasi. Alur penelitian secara lengkap ditampilkan pada Gambar 1.

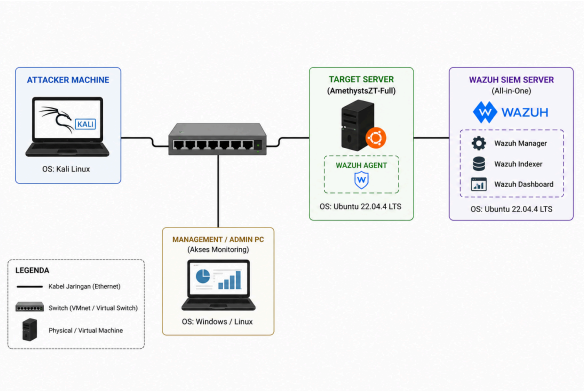
Gambar 1. Alur Penelitian

3.1 Studi Literatur

Tahap awal yang dilakukan yaitu mengkaji literatur yang relevan, mencakup konsep Zero Trust, sistem SIEM khususnya Wazuh, framework MITRE ATT&CK, serta penelitian-penelitian terdahulu terkait deteksi serangan siber. Studi literatur ini menjadi landasan teori dan acuan metodologis dalam perancangan penelitian.

3.2 Perancangan Topologi

Lingkungan pengujian menggunakan tiga virtual machine pada VMware Workstation, yaitu VM attacker (Kali Linux), VM target (Ubuntu Server), dan VM Wazuh SIEM. Topologi dapat dilihat pada gambar 2.



Gambar 2. Rancangan Topologi Wazuh

3.3 Implementasi Wazuh Siem

Implementasi Wazuh SIEM versi 4.7.5 dilakukan pada mesin virtual berbasis Ubuntu 22.04.4 LTS yang dijalankan pada platform VMware Workstation. Sebelum proses instalasi dimulai, server dikonfigurasi dengan alamat IP statis 192.168.85.131. Arsitektur yang digunakan adalah mode all-in-one deployment, di mana seluruh komponen utama Wazuh yaitu Wazuh Manager, Wazuh Indexer, dan Wazuh Dashboard dikonfigurasi dalam satu server tunggal. Proses instalasi dilakukan menggunakan dokumentasi instalasi resmi yang disediakan oleh Wazuh, disertai konfigurasi berkas config.yml untuk mendefinisikan komponen indexer, server, dan dashboard. Setelah instalasi selesai, seluruh layanan diverifikasi menggunakan utilitas systemctl untuk memastikan ketiga komponen berjalan dengan status *active* (*running*).

Tahap berikutnya adalah mengintegrasikan mesin target AmethystsZT-Full sebagai Wazuh Agent. Agen diinstal pada mesin target dan dikonfigurasi agar terhubung dengan Wazuh Manager. Konfigurasi pemantauan log ditambahkan pada berkas ossec.conf untuk membaca beberapa sumber log penting, antara lain /var/log/syslog, /var/log/auth.log, dan log peringatan dari journald. Konfigurasi ini memungkinkan Wazuh mengumpulkan data aktivitas sistem, aktivitas autentikasi pengguna, serta peringatan keamanan yang terjadi pada mesin target secara real-time.

3.4 Analisis Deteksi Wazuh SIEM

Pada bagian analisis deteksi, sistem memantau seluruh aktivitas yang terjadi pada mesin target. Setiap tahapan serangan dijalankan secara berurutan sesuai skenario CTF Amethysts KMIPN 2024, yang mencakup 13 tahapan attack chain mulai dari enumerasi jaringan hingga privilege escalation.

Wazuh SIEM menganalisis log yang dihasilkan secara real-time untuk mendeteksi aktivitas mencurigakan dan memunculkan alert beserta rule ID yang sesuai. Sebagai bagian dari persiapan pengujian, setiap tahapan pada attack chain terlebih dahulu direncanakan dengan detail teknis eksekusi sebagaimana disajikan pada Tabel I, sekaligus dipetakan ke taktik MITRE ATT&CK yang diprediksi muncul sebagaimana disajikan pada Tabel II di akhir sub-bagian ini.

TABEL I

DETAIL EKSEKUSI SKENARIO SERANGAN

No	Tahapan Serangan	Command Lengkap	Target dan Parameter
1	*Port Enumeration*	nmap 192.168.1.110 -Pn -p- -oN amethysts.nmap	Seluruh port TCP pada IP target
2	*Service Enumeration*	nmap 192.168.1.110 -Pn -p21,22,80,81,1139,1445 -sCV -oN service_amethystsZT.nmap	Port hasil tahap 1; default scripts + version detection
3	*SMB Enumeration*	smbclient -N -L 192.168.1.110 -p 1445	Null session terhadap share SMB
4	*RPC Enumeration*	rpcclient -U "" -N 192.168.1.110 -p 1139 lalu jalankan enumdomusers	Null session RPC; enumdomusers, enumdomgroups
5	*FTP Enumeration*	ftp 192.168.1.110 (login anonymous) dan get backup.zip wget -r ftp://anonymous@192.168.1.110	Login anonymous / kredensial hasil enumerasi; unduh seluruh direktori
6	*ZIP Password Cracking*	zip2john backup.zip > hash.txt	File backup.zip hasil unduhan FTP
7	MD5 Hash Cracking	Input hash ke crackstation.net (manual, via browser)	Hash MD5 hasil ekstraksi ZIP
8	*Web Directory Enumeration*	gobuster dir -u http://192.168.1.110:81/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/DirBuster-2007_directory-list-2.3-medium.txt -t 200 --no-error -o gobuster.txt	Web root target; wordlist common.txt
9	*Hydra Brute Force*	hydra -L usernames.txt -P passwords.txt -s 81 192.168.1.110 http-post-form "/prospective/admin.php:username=^USER^&userpw=^PASS^:login_failed"	Form login RiteCMS
10	*File Upload*	Login RiteCMS -> File Manager -> upload shell.phpr	Kredensial hasil brute force (tahap 9)
11	*Remote Code Execution*	curl http://192.168.85.140/uploads/shell.php?cmd=id	File shell.php hasil upload (tahap 10)
12	*Credential Leakage*	cat /var/www/Amethyst_Dev_2024/.env (mengambil kredensial SSH dari file config	File konfigurasi .env pada web root
13	*Privilege Escalation*	getcap -r / 2>/dev/null (menemukan cap_setuid) ~/.bin$ ./vim -c ':python3 import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'	Binary dengan capability cap_setuid

Sebelum tahapan-tahapan pada Tabel I dieksekusi, dilakukan pemetaan awal (ex-ante) terhadap taktik dan teknik MITRE ATT&CK Enterprise Matrix yang diprediksi merepresentasikan tujuan dari masing-masing tahapan, berdasarkan karakteristik teknis command yang akan dijalankan. Sebagai contoh, tahapan Port Enumeration yang bertujuan mengidentifikasi layanan yang berjalan pada target dipetakan ke taktik Discovery dengan teknik T1046 (Network Service Discovery), karena aktivitas tersebut merupakan upaya pengumpulan informasi mengenai lingkungan target sebelum tahap eksploitasi lanjutan dilakukan. Proses pemetaan yang sama diterapkan secara konsisten pada seluruh 13 tahapan serangan, sebagaimana disajikan pada Tabel II. Pemetaan ex-ante ini digunakan sebagai acuan pembanding terhadap taktik yang benar-benar terdeteksi Wazuh SIEM, sebagaimana dibahas pada Bagian 3.5 dan 4.3.

TABEL II

PEMETAAN TAKTIK MITRE ATT&CK YANG DIRENCANAKAN (EX-ANTE)

No	Tahapan Serangan	Taktik yang Direncanakan	Teknik (Ex-Ante)	Ekspektasi Log yang Diamati
1	*Port Enumeration*	Discovery	T1046 - Network Service Discovery	Log koneksi/scan pada banyak port dalam interval singkat
2	*Service Enumeration*	Discovery	T1046 - Network Service Discovery	Log banner grabbing & script probing
3	*SMB Enumeration*	Discovery	T1135 - Network Share Discovery	Log null-session SMB, list share
4	*RPC Enumeration*	Discovery	T1087.002 - Account Discovery : Domain Account	Log query RPC endpoint mapper
5	*FTP Enumeration*	Credential Access	T1110.001 - Password Guessing	Log login FTP berulang / anonymous
6	*ZIP Password Cracking*	Credential Access	T1110.002 - Password Cracking	Diperkirakan tidak ada log (proses di sisi attacker)
7	MD5 Hash Cracking	Credential Access	T1110.002 - Password Cracking	Diperkirakan tidak ada log (proses di sisi attacker)
8	*Web Directory Enumeration*	Reconnaissance	T1595.002 - Vulnerability Scanning	Log HTTP request beruntun ke banyak path
9	*Hydra Brute Force*	Credential Access	T1110 - Brute Force	Log kegagalan login form berulang dari satu IP
10	*File Upload*	Persistence	T1505.003 - Web Shell	Log upload file .php ke direktori web
11	*Remote Code Execution*	Execution	T1203 - Exploitation for Client Execution	Log akses/eksekusi file shell.php
12	*Credential Leakage*	Credential Access, Lateral Movement	T1552.001 – Unsecured Credentials:Files T1021.004 - Remote Service SSH	Log akses file .env; log SSH login baru
13	*Privilege Escalation*	Privilege Escalation	T1548.001 - Abuse Elevation Control Mechanism	Log perubahan UID / eksekusi binary capability

3.5 Pemetaan Hasil Deteksi ke Framework MITRE ATT&CK

Pemetaan hasil deteksi dilakukan dengan menghubungkan setiap alert yang dihasilkan Wazuh SIEM ke taktik dan teknik dalam MITRE ATT&CK. Framework MITRE ATT&CK merupakan basis pengetahuan yang mendokumentasikan taktik dan teknik serangan siber berdasarkan observasi dunia nyata [7], dan digunakan sebagai acuan klasifikasi standar global untuk setiap aktivitas serangan yang terdeteksi dalam penelitian ini. Data yang menjadi objek pemetaan adalah alert yang terpicu selama eksekusi 13 tahapan skenario serangan pada mesin target AmethystsZT-Full.

Proses pemetaan dilakukan secara manual melalui empat langkah [6]. Pertama, alert yang muncul pada setiap tahapan serangan dicatat metadata MITRE-nya. Kedua, deskripsi rule dibaca untuk memahami jenis aktivitas yang terdeteksi oleh Wazuh. Ketiga, taktik MITRE ATT&CK dikonfirmasi berdasarkan nilai rule.mitre.tactic yang sudah tersedia pada setiap alert Wazuh [8]. Keempat, teknik spesifik (Technique ID / T-code) dikonfirmasi dari field rule.mitre.id pada alert, kemudian diverifikasi silang dengan MITRE ATT&CK melalui https://attack.mitre.org [7]. Hasil pemetaan pada langkah ini kemudian dibandingkan dengan rencana pemetaan ex-ante pada Tabel II untuk menilai konsistensi antara taktik yang ditargetkan dan taktik yang benar-benar terdeteksi, sebagaimana disajikan pada Bagian 4.3.

Setiap tahapan serangan diklasifikasikan berdasarkan kesesuaian antara aktivitas yang dijalankan dengan alert yang dihasilkan Wazuh, mengikuti empat kategori klasifikasi biner standar (True Positive, False

Positive, False Negative, True Negative) sebagaimana dijelaskan pada Bagian 3.6. Namun demikian, tidak seluruh tahapan yang tidak menghasilkan alert dapat langsung dikategorikan ke dalam salah satu dari empat kategori tersebut. Beberapa tahapan mengalami kondisi di mana serangan tidak dapat dinilai keberhasilan deteksinya, baik karena kegagalan prasyarat teknis dalam pelaksanaan skenario (misalnya berkas yang diperlukan untuk tahap lanjutan mengalami kerusakan), maupun karena aktivitas berlangsung sepenuhnya di luar jangkauan visibilitas Wazuh Agent (attacker-side computation), atau karena rantai serangan (attack chain) terputus akibat keberhasilan lapisan pertahanan sebelumnya memblokir tahap prasyarat. Tahapan dengan kondisi tersebut diklasifikasikan sebagai "Tidak Dapat Dikategorikan", karena tidak terjadi interaksi nyata antara upaya serangan dan mekanisme deteksi Wazuh yang dapat dievaluasi secara valid.

Sebagai pelengkap pemetaan taktik, dilakukan pula analisis keterkaitan antara kontrol keamanan berbasis prinsip Zero Trust pada lingkungan lab (Bagian 2.1) dengan visibilitas monitoring Wazuh SIEM. Analisis dilakukan melalui tiga langkah: pertama, mengidentifikasi mekanisme kontrol Zero Trust yang direfleksikan pada lab, yaitu continuous verification, least privilege access, dan micro-segmentation parsial; kedua, memetakan setiap mekanisme kontrol tersebut ke tahapan serangan yang menguji efektivitasnya; ketiga, menghubungkan tahapan tersebut dengan taktik MITRE ATT&CK yang relevan (Tabel II), sehingga dapat dinilai apakah upaya pelanggaran terhadap tiap kontrol Zero Trust menghasilkan jejak log yang terpantau Wazuh. Pemetaan kontrol ini disajikan pada Tabel III, dan hasil analisisnya dibahas pada Bagian 4.3.

TABEL III

PEMETAAN KONTROL ZERO TRUST KE TAHAPAN PENGUJIAN DAN TAKTIK MITRE ATT&CK

No	Kontrol Zero Trust	Deskripsi Penerapan pada Lab	Tahapan yang Menguji Kontrol	Taktik MITRE Terkait
1	*Continuous Verification*	Verifikasi kredensial berlapis pada tiap layanan sebelum akses lanjutan diberikan	FTP Enumeration, Hydra Brute Force, File Upload	Credential Access, Persistence
2	*Least Privilege Access*	Pembatasan hak akses/eksekusi hanya pada sumber daya yang diperlukan di tiap tahap	Web Directory Enumeration, Remote Code Execution, Privilege Escalation	Execution, Privilege Escalation
3	*Micro-segmentation*	Pembatasan visibilitas antar layanan sebelum tahap sebelumnya berhasil dilalui	Port/Service/SMB/RPC Enumeration, Credential Leakage	Discovery, Credential Access, Lateral Movement

3.6 Evaluasi Performa Deteksi

Performa deteksi Wazuh SIEM dievaluasi menggunakan empat metrik sebagai berikut:
True Positive (TP) — Serangan terjadi dan Wazuh berhasil mendeteksi serta memunculkan alert.
False Positive (FP) — Aktivitas normal yang keliru diidentifikasi sebagai serangan.
False Negative (FN) — Serangan terjadi namun Wazuh gagal mendeteksi.
True Negative (TN) — Aktivitas normal yang tidak memunculkan alert.

Keempat kategori tersebut diterapkan pada level log individual, bukan pada level tahapan serangan secara keseluruhan. Hal ini karena satu tahapan serangan dapat menghasilkan banyak entri log dalam satu rentang waktu eksekusi (misalnya puluhan log koneksi dari satu kali full port scan), sehingga setiap log yang tercatat pada rentang waktu tahapan tersebut dinilai secara independen: log yang berhasil dipetakan ke rule.mitre.id yang relevan dihitung sebagai satu TP, sedangkan log lain pada rentang waktu yang sama yang tidak menghasilkan alert relevan (baik karena tidak ada rule yang cocok maupun karena log tersebut adalah alert operasional yang tidak terkait langsung dengan teknik serangan) dihitung sebagai satu FN. Dengan pendekatan ini, nilai TP dan FN pada Tabel VII dapat lebih dari satu untuk satu tahapan serangan, mencerminkan proporsi log yang berhasil maupun gagal terdeteksi dari total log yang dihasilkan pada tahapan tersebut, bukan sekadar status biner berhasil/gagal terdeteksi untuk keseluruhan tahapan

Selain keempat kategori tersebut, penelitian ini juga menetapkan kategori "Tidak Dapat Dikategorikan" untuk tahapan serangan yang tidak dapat dinilai validitas deteksinya, baik karena kegagalan prasyarat teknis dalam skenario pengujian, aktivitas yang berlangsung di luar jangkauan visibilitas agent, maupun karena tahap tersebut tidak pernah benar-benar dieksekusi terhadap sistem target akibat terputusnya rantai serangan pada tahap sebelumnya. Tahapan pada kategori ini tidak diikutsertakan dalam perhitungan metrik precision, recall, TPR, dan FPR, karena tidak merepresentasikan interaksi nyata antara serangan dan mekanisme deteksi yang dapat dievaluasi. Nilai presisi dan recall dihitung

menggunakan persamaan berikut:

$$Presisi = \frac{TP}{TP + FP} \quad (1)$$

$$Recall = \frac{TP}{TP + FN} \quad (2)$$

$$TPR = \frac{TP}{TP + FN} \quad (3)$$

$$FPR = \frac{FP}{FP + TN} \quad (4)$$

Berbeda dengan perhitungan pada penelitian tahap sebelumnya yang menghitung metrik di atas secara agregat untuk seluruh skenario, pada penelitian ini keempat metrik dihitung secara terpisah untuk masing-masing jenis serangan (per jenis tahapan), sebagaimana disajikan pada Tabel VII di Bagian 4.4, guna memberikan gambaran yang lebih rinci mengenai jenis serangan mana yang deteksinya paling kuat maupun paling lemah.

4. Hasil dan Pembahasan

4.1 Implementasi Wazuh SIEM

Pada penelitian ini, Wazuh SIEM versi 4.7.5 diimplementasikan sebagai sistem Security Information and Event Management (SIEM) untuk melakukan pengumpulan, pemantauan, korelasi, dan analisis log keamanan secara terpusat pada lingkungan laboratorium Capture The Flag (CTF) Amethysts KMIPN 2024 yang menerapkan kontrol keamanan berbasis prinsip Zero Trust. Implementasi dilakukan menggunakan mesin virtual berbasis Ubuntu 22.04.4 LTS yang dijalankan pada VMware Workstation.

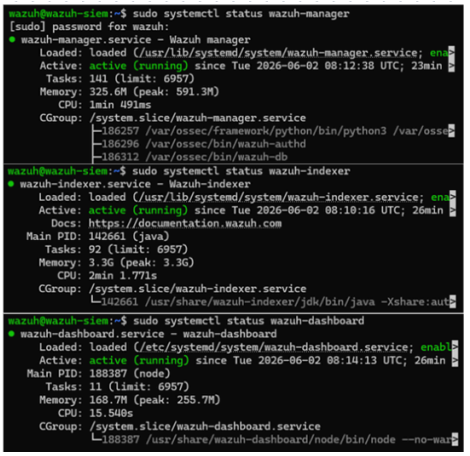
Arsitektur Wazuh yang digunakan adalah *all-in-one deployment*, di mana seluruh komponen utama Wazuh dijalankan dalam satu server tunggal. Komponen tersebut meliputi Wazuh Manager, Wazuh Indexer, dan Wazuh Dashboard. Wazuh Manager bertugas menerima dan menganalisis log yang dikirimkan oleh agen; Wazuh Indexer bertugas menyimpan dan mengindeks data log; serta Wazuh Dashboard berfungsi sebagai antarmuka visual untuk memantau dan menganalisis peringatan keamanan yang dihasilkan.

Sebelum proses instalasi dimulai, server Wazuh dikonfigurasi dengan alamat IP statis 192.168.85.131. Koneksi internet kemudian diverifikasi guna memastikan seluruh paket instalasi dapat diunduh tanpa hambatan. Proses instalasi dilakukan menggunakan skrip instalasi resmi yang disediakan oleh Wazuh, disertai konfigurasi berkas config.yml untuk mendefinisikan komponen *indexer*, *server*, dan *dashboard*.

```
02/06/2026 08:12:48 INFO: --- Wazuh dashboard ---
02/06/2026 08:12:48 INFO: Starting Wazuh dashboard installation.
02/06/2026 08:13:56 INFO: Wazuh dashboard installation finished.
02/06/2026 08:13:56 INFO: Wazuh dashboard post-install configuration fin
ished.
02/06/2026 08:13:56 INFO: Starting service wazuh-dashboard.
02/06/2026 08:13:57 INFO: wazuh-dashboard service started.
02/06/2026 08:14:24 INFO: Initializing Wazuh dashboard web application.
02/06/2026 08:14:24 INFO: Wazuh dashboard web application initialized.
02/06/2026 08:14:24 INFO: --- Summary ---
02/06/2026 08:14:24 INFO: You can access the web interface https://<wazu
h-dashboard-ip>:443
    User: admin
    Password: thnET+wRy2vD6kH.NF1ps3gNvKAS0uRi
02/06/2026 08:14:24 INFO: Installation finished.
```

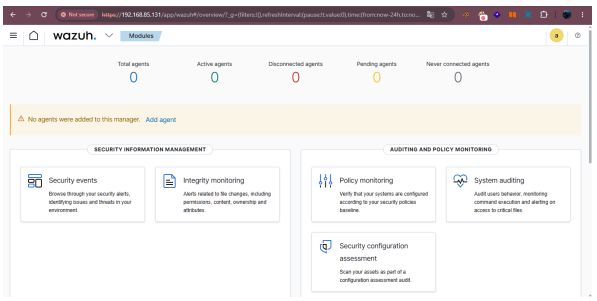
Gambar 3. Instalasi Selesai

Setelah instalasi selesai, seluruh layanan Wazuh diverifikasi menggunakan utilitas systemctl. Hasil verifikasi menunjukkan bahwa seluruh komponen Wazuh Manager, Wazuh Indexer, dan Wazuh Dashboard berhasil berjalan dengan status *active (running)*.



Gambar 4. Status systemctl ketiga layanan active (*running*)

Wazuh Dashboard selanjutnya diakses melalui peramban menggunakan protokol HTTPS untuk memastikan sistem dapat difungsikan sebagai pusat pemantauan keamanan.

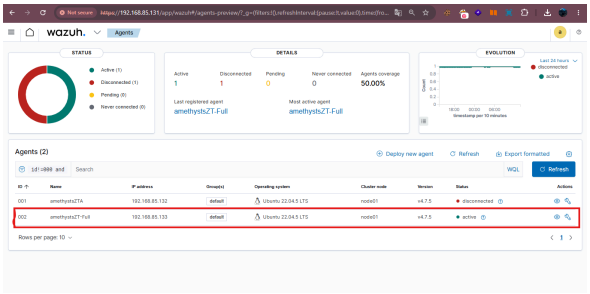


Gambar 5. Tampilan wazuh dashboard setelah login

Tahap selanjutnya adalah mengintegrasikan mesin target AmethystsZT-Full sebagai Wazuh Agent. Agent

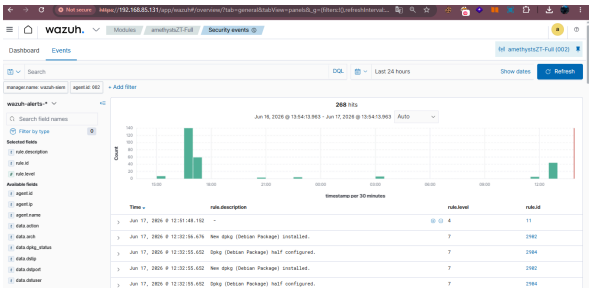
diinstal pada mesin target dan dikonfigurasi agar terhubung dengan Wazuh Manager. Selain itu, konfigurasi pemantauan log ditambahkan pada berkas ossec.conf untuk membaca beberapa sumber log penting, antara lain /var/log/syslog, /var/log/auth.log, dan log peringatan dari journald. Konfigurasi ini memungkinkan Wazuh mengumpulkan data aktivitas sistem, aktivitas autentikasi pengguna, serta peringatan keamanan yang terjadi pada mesin target.

Setelah konfigurasi selesai, Wazuh Agent diaktifkan dan diverifikasi melalui Wazuh Dashboard. Hasil implementasi menunjukkan bahwa agen amethystsZT-Full berhasil terdaftar dengan status *Active* dan mampu mengirimkan log secara *real-time* ke server Wazuh.



Gambar 6. Tampilan amethystsZT-Full active di wazuh

Dengan demikian, Wazuh SIEM dapat digunakan untuk memantau seluruh aktivitas yang berlangsung di lingkungan laboratorium serta mendukung proses deteksi serangan siber pada setiap tahapan *attack chain*.



Gambar 7. Tampilan alert wazuh siem

4.2 Analisis Deteksi Wazuh SIEM

Tahapan eksekusi skenario serangan dilakukan secara berurutan sesuai walkthrough resmi mesin Amethysts KMIPN 2024. Setiap aktivitas serangan dijalankan menggunakan tools yang relevan, kemudian hasil log dianalisis oleh Wazuh SIEM versi 4.7.5 untuk menghasilkan alert. Alert yang muncul dipetakan ke taktik dan teknik MITRE ATT&CK guna memastikan keterhubungan antara aktivitas serangan dengan framework standar.

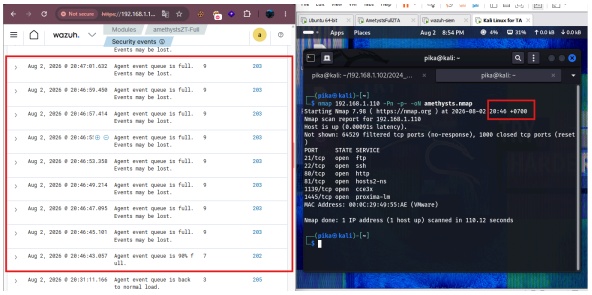
Skenario serangan terdiri atas 13 tahapan attack chain yang mencakup proses enumerasi, eksploitasi, dan eskalasi hak akses. Seluruh tahapan dijalankan pada mesin target AmethystsZT-Full yang telah terintegrasi sebagai Wazuh Agent. Log aktivitas dikirimkan secara real-time ke Wazuh Manager untuk dianalisis. Beberapa tahapan utama yang berhasil terdeteksi oleh Wazuh SIEM ditunjukkan pada Tabel IV.

TABEL IV

SKENARIO SERANGAN YANG BERHASIL TERDETEKSI

Tahapan Serangan	Kategori Deteksi
Port Enumeration	TP
Service Enumeration	TP
SMB Enumeration	TP
RPC Enumeration	TP
FTP Enumeration	TP
Web Directory Enumeration	TP
Hydra Brute Force	TP
File Upload	TP
Remote Code Execution	TP

Dari 13 tahapan serangan yang dijalankan, 9 tahapan utama berhasil terdeteksi oleh Wazuh SIEM. Deteksi ini dikategorikan sebagai *True Positive* (TP) karena serangan benar-benar terjadi dan sistem berhasil memunculkan alert. Berikut tampilan *Security Events* pada Wazuh Dashboard selama proses eksekusi berlangsung ditunjukkan pada Gambar 8.



Gambar 8. Tampilan Security Events Wazuh

Tahapan ZIP Password Cracking dan MD5 Hash Cracking tidak dapat dikategorikan, disebabkan oleh dua faktor. Pertama, kegagalan prasyarat teknis: berkas backup.zip yang berhasil diunduh berada dalam kondisi corrupt, sehingga proses cracking password dan hash tidak pernah benar-benar tereksekusi terhadap data yang sah. Kedua, terlepas dari kegagalan tersebut, kedua aktivitas ini secara arsitektural berada di luar jangkauan visibilitas Wazuh Agent, karena seluruh proses komputasi (percobaan password dan dekripsi hash) berlangsung di sisi mesin penyerang (attacker-side) dan tidak pernah berinteraksi dengan sistem target, sehingga tidak menghasilkan satu pun entri log yang dapat dipantau oleh agent.

Adapun tahapan Credential Leakage dan Privilege Escalation juga tidak dapat dikategorikan, namun dengan alasan yang berbeda. Kedua tahapan ini

merupakan kelanjutan dari rantai serangan (attack chain) yang mensyaratkan keberhasilan Remote Code Execution (RCE) melalui web shell pada tahap sebelumnya (#11). Namun, upaya upload shell tersebut berhasil terdeteksi oleh Wazuh Agent ditandai dengan munculnya alert sehingga file shell.php di-rename menjadi shell.php.suspicious dan tidak dapat dieksekusi. Akibatnya, rantai serangan terputus (broken chain) sebelum mencapai tahap Credential Leakage maupun Privilege Escalation, sehingga kedua aktivitas tersebut tidak pernah benar-benar dijalankan terhadap sistem target dan tidak menghasilkan log maupun alert yang dapat dievaluasi.

4.3 Pemetaan Hasil Deteksi ke MITRE ATT&CK

Hasil pemetaan dari 13 tahapan serangan ke framework MITRE ATT&CK disajikan pada Tabel V. Nilai taktik dan teknik MITRE diambil langsung dari field rule.mitre.tactic dan rule.mitre.technique yang tercatat pada setiap alert di Wazuh Dashboard, sehingga pemetaan ini mencerminkan klasifikasi yang dikenali secara native oleh Wazuh SIEM versi 4.7.5 [8].

TABEL V

PEMETAAN ALERT WAZUH KE FRAMEWORK MITRE ATT&CK

Tahapan Serangan	Taktik MITRE ATT&CK	Teknik MITRE ATT&CK	Status Deteksi
Port Enumeration	*Discovery*	T1046 – Network Service Discovery	TP
Service Enumeration	*Discovery*	T1046 – Network Service Discovery	TP
SMB Enumeration	*Discovery*	T1135 - Network Share Discovery	TP
RPC Enumeration	*Discovery*	T1087.002 – Account Discovery : Domain Account	TP
FTP Enumeration	*Credential Access*	T1110.001 - Password Guessing	TP
ZIP Password Cracking	-	-	Tidak dikategorikan
MD5 Hash Cracking	-	-	Tidak dikategorikan
Web Directory Enumeration	*Reconnaissance*	T1595.002 - Vulnerability Scanning	TP
Hydra Brute Force	*Credential Access*	T1110 - Brute Force	TP
File Upload	*Persistence*	T1505.003 - Web Shell	TP
Remote Code Execution	*Execution*	T1203 - Exploitation for Client Execution	TP
Credential Leakage	-	-	Tidak dikategorikan
Privilege Escalation	-	-	Tidak dikategorikan

Pada pemetaan hasil deteksi ke MITRE ATT&CK memperlihatkan bahwa Wazuh SIEM memiliki kemampuan yang cukup baik dalam mengidentifikasi serangan eksplisit berbasis autentikasi dan eksploitasi layanan, namun masih memerlukan tuning ruleset dan penambahan custom detection policy untuk mendeteksi aktivitas manual dan kebocoran kredensial.

Untuk menilai konsistensi antara rencana pemetaan taktik (Tabel II, Bagian 3.4) dengan hasil deteksi aktual di atas (Tabel V), Tabel VI berikut membandingkan keduanya untuk setiap tahapan serangan.

TABEL VI

PERBANDINGAN TAKTIK DIRENCANAKAN (EX-ANTE) VS TAKTIK TERDETEKSI

Tahapan Serangan	Taktik Direncanakan	Taktik Terdeteksi	Kesesuaian
Port Enumeration	*Discovery*	*Discovery*	Sesuai
Service Enumeration	*Discovery*	*Discovery*	Sesuai
SMB Enumeration	*Discovery*	Discovery	Sesuai
RPC Enumeration	*Discovery*	Discovery	Sesuai
FTP Enumeration	*Credential Access*	Credential Access	Sesuai
ZIP Password Cracking	-	-	Tidak dapat dinilai
MD5 Hash Cracking	-	-	Tidak dapat dinilai
Web Directory Enumeration	*Reconnaissance*	reconnaissance	Sesuai
Hydra Brute Force	*Credential Access*	Credential Access	Sesuai
File Upload	*Persistence*	Persistence	Sesuai
Remote Code Execution	*Execution*	Execution	Sesuai
Credential Leakage	-	-	Tidak dapat dinilai
Privilege Escalation	-	-	Tidak dapat dinilai

Dari 13 tahapan, 9 tahapan (69%) menunjukkan kesesuaian penuh antara taktik yang direncanakan dan taktik yang terdeteksi Wazuh, mengindikasikan bahwa proses perencanaan pemetaan MITRE ATT&CK sejak awal metode penelitian cukup akurat memprediksi taktik yang akan teramati. Empat tahapan sisanya (Tahap 6, 7, 12, 13) tergolong Tidak Dapat Dinilai karena tidak menghasilkan alert sama sekali, sehingga kesesuaiannya tidak dapat diverifikasi bukan berarti taktik yang direncanakan salah, melainkan tahapan tersebut tidak menghasilkan interaksi yang tercatat oleh Wazuh Agent (lihat penjelasan detail pada Bagian 4.2).

Berdasarkan pemetaan kontrol Zero Trust pada Tabel III (Bagian 3.5), lingkungan lab CTF Amethysts merefleksikan prinsip Zero Trust melalui verifikasi kredensial berlapis pada setiap layanan dan pembatasan akses bertingkat sebelum penyerang dapat mencapai sumber daya berikutnya dalam attack chain. Efektivitas kontrol ini secara langsung bergantung pada visibilitas monitoring: setiap upaya melewati lapisan verifikasi baik yang berhasil maupun gagal, idealnya tercatat sebagai log yang dapat dianalisis. Hasil pemetaan pada Tabel III menunjukkan bahwa taktik Discovery dan Credential Access yang merepresentasikan upaya penyerang menembus lapisan verifikasi kredensial pada prinsip Zero Trust berhasil dideteksi secara konsisten oleh Wazuh (Tahap 1-5, 9). Ini mengindikasikan bahwa kontrol continuous verification pada lab menghasilkan jejak log yang memadai untuk dipantau. Sebaliknya, kegagalan deteksi pada Tahap 6-7 (ZIP/MD5 Cracking) terjadi justru karena proses tersebut berlangsung sepenuhnya di luar titik verifikasi Zero Trust yang dipantau (attacker-side), menunjukkan bahwa visibilitas Zero Trust pada arsitektur ini terbatas pada boundary yang memiliki agent Wazuh terpasang celah yang perlu menjadi perhatian bila prinsip Zero Trust hendak diterapkan secara menyeluruh, termasuk pada titik-titik komputasi di luar server target.

4.4 Evaluasi Performa Deteksi

Evaluasi performa deteksi dilakukan dengan menghitung metrik klasifikasi berdasarkan hasil eksekusi 13 tahapan skenario serangan, ditambah empat skenario pelengkap pada Tabel V. Berbeda dengan perhitungan pada tahap penelitian sebelumnya yang menghitung metrik secara agregat untuk seluruh skenario, pada bagian ini keempat metrik (TP, FP, FN, TN, presisi, recall) dihitung secara terpisah untuk masing-masing jenis serangan, sebagaimana disajikan pada Tabel VII. Kolom "Total Log Dianalisis" diisi jumlah log yang tercatat pada rentang waktu eksekusi tiap skenario, berkisar antara 30 hingga 90 log per tahapan tergantung durasi dan volume aktivitas masing-masing command (mis. full port scan pada Port Enumeration menghasilkan volume log berbeda dibanding query tunggal pada SMB Enumeration), dan mencakup seluruh log pada rentang waktu tersebut tanpa penyaringan berdasarkan relevansi.

TABEL VII
CONFUSION MATRIX PER JENIS SERANGAN

Tahapan Serangan	TP	FP	FN	TN	Total Log Dianalisis	Presisi	Recall
Port Enumeration	1	*0*	*45*	*0*	*46*	1/1 = **100%**	1/46 = **2,17 %**
Service Enumeration	5	*0*	*85*	*0*	*90*	5/5 = **100%**	5/90 = **5,56 %**
SMB Enumeration	*1*	*0*	*29*	*0*	*30*	1/1 = **100%**	1/30 = **3,33 %**
RPC Enumeration	*1*	*0*	*34*	*0*	*35*	1/1 = **100%**	1/35 = **2,86 %**
FTP Enumeration	*1*	*0*	*39*	*0*	*40*	1/1 = **100%**	1/40 = **2,50 %**
ZIP Password Cracking	-	-	-	-	-	-	-
MD5 Hash Cracking	-	-	-	-	-	-	-
Web Directory Enumeration	*12*	*0*	*45*	*0*	*57*	12/12 = **100%**	12/57 = **21,05%**
Hydra Brute Force	*3*	*0*	*40*	*0*	*43*	3/3 = **100%**	3/43 = **6,98 %**
File Upload	*2*	*0*	*38*	*0*	*40*	2/2 = **100%**	2/40 = **5,00 %**
Remote Code Execution	*1*	*0*	*42*	*0*	*43*	1/1 = **100%**	1/43 = **2,33 %**
Credential Leakage	-	-	-	-	-	-	-
Privilege Escalation	-	-	-	-	-	-	-

5. Kesimpulan

Penelitian ini berhasil mengevaluasi kemampuan Wazuh SIEM versi 4.7.5 dalam mendeteksi serangan siber pada lingkungan lab CTF KMIPN 2024 mesin Amethysts yang menerapkan kontrol keamanan berbasis prinsip Zero Trust. Dari 13 tahapan attack chain yang dijalankan, 9 tahapan menghasilkan interaksi yang dapat dinilai (Port Enumeration, Service Enumeration, SMB Enumeration, RPC Enumeration, FTP Enumeration, Web Directory Enumeration, Hydra Brute Force, File Upload, dan Remote Code Execution), sementara 4 tahapan lainnya (ZIP Password Cracking, MD5 Hash Cracking, Credential Leakage, dan Privilege Escalation) tidak dapat dikategorikan karena kegagalan prasyarat teknis, keterbatasan visibilitas agent, atau terputusnya rantai serangan, sebagaimana dijelaskan pada Bagian 4.2.

Perhitungan metrik dilakukan pada level log individual (bukan hanya pada level tahapan), dengan total 424 log dianalisis pada 9 tahapan yang dapat dievaluasi/dinilai. Hasil evaluasi menunjukkan presisi sebesar 100%, karena seluruh alert yang berhasil dipetakan ke MITRE ATT&CK (rule.mitre.id) memang merupakan deteksi yang valid terhadap aktivitas serangan yang sedang berlangsung, tidak ditemukan satu pun False Positive. Namun, recall dan True Positive Rate (TPR) tercatat hanya sebesar 6,37% (27 dari 424 log berhasil terdeteksi sebagai alert relevan), yang mengindikasikan bahwa meskipun aktivitas serangan berlangsung dan menghasilkan volume log yang besar pada sistem target, sebagian besar log tersebut (397 dari 424, atau 93,63%) tidak menghasilkan alert yang dapat dipetakan ke taktik/teknik MITRE ATT&CK. False Positive Rate (FPR) tidak dapat dihitung (N/A) karena tidak terdapat data True Negative dalam skenario pengujian ini.

Temuan ini berbeda signifikan dari asumsi awal yang menganggap seluruh 9 tahapan sepenuhnya terdeteksi (True Positive) hanya berdasarkan kemunculan alert MITRE-tagged pada level tahapan. Analisis lebih rinci pada level log — khususnya pada tahap Port Enumeration — menunjukkan bahwa volume tinggi lalu lintas dari aktivitas enumerasi (misalnya full port scan menggunakan nmap -p-) dapat membanjiri antrian event Wazuh Agent (ditandai oleh alert operasional rule.id 202/203/205, kategori agent_flooding), sehingga sebagian besar log yang dihasilkan selama aktivitas tersebut tidak sempat dianalisis atau dicocokkan terhadap rule keamanan yang relevan sebelum berpotensi hilang (events may be lost). Kondisi ini mengindikasikan keterbatasan Wazuh dalam menangani volume log tinggi secara real-time, bukan semata-mata keterbatasan pada ruleset deteksi itu sendiri.

Pemetaan ke framework MITRE ATT&CK menunjukkan bahwa Wazuh tetap mampu mengidentifikasi taktik Discovery, Credential Access, Reconnaissance, Persistence, dan Execution secara native melalui field rule.mitre.tactic dan rule.mitre.id pada log yang berhasil dianalisis. Akan tetapi, rendahnya recall pada seluruh tahapan mengindikasikan bahwa efektivitas deteksi Wazuh pada konteks pengujian ini jauh lebih terbatas dari yang terlihat pada analisis level-tahapan semata, dan memerlukan optimasi lebih lanjut baik dari sisi kapasitas antrian/buffer agent, tuning ruleset, maupun penambahan custom detection policy agar mampu mempertahankan visibilitas pada kondisi lalu lintas serangan bervolume tinggi.

Secara keseluruhan, Wazuh SIEM pada lingkungan yang menerapkan kontrol berbasis prinsip Zero Trust ini terbukti presisi dalam mengklasifikasikan aktivitas yang berhasil dideteksi (tidak menghasilkan False Positive), namun cakupan deteksinya (recall) masih rendah akibat keterbatasan kapasitas pemrosesan log secara real-time. Penelitian lanjutan disarankan untuk menguji kapasitas buffer/antrian Wazuh Agent pada volume traffic tinggi, menjalankan tahap Credential Leakage dan Privilege Escalation secara independen untuk melengkapi evaluasi seluruh 13 tahapan, serta menyertakan simulasi traffic pengguna normal sebagai baseline data True Negative guna memperoleh nilai FPR yang representatif.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada kedua orang tua atas doa dan dukungan moral yang senantiasa diberikan selama proses penelitian berlangsung. Ucapan terima kasih juga disampaikan kepada Ibu Maidel Fani, S.Pd., M.Kom., selaku dosen pembimbing, atas arahan, bimbingan, dan masukan yang sangat berharga dalam penyusunan penelitian ini. Penghargaan yang sama diberikan kepada seluruh dosen dan rekan-rekan mahasiswa Program Studi Rekayasa Keamanan Siber Politeknik Negeri Batam atas dukungan dan kolaborasi yang telah diberikan.

Referensi

[1] Direktorat Operasi Keamanan Siber, Lanskap Keamanan Siber Indonesia 2024, Badan Siber dan Sandi Negara (BSSN), Jakarta, 2025. https://www.bssn.go.id/wp-content/uploads/2025/02/LANSKAP-KEAMANAN-SIBER-2024-1.

[2] Kusnanto dkk., "Implementasi Zero Trust Architecture untuk Meningkatkan Keamanan Jaringan: Pendekatan Berbasis Simulasi," JIPI: Jurnal Ilmiah Penelitian dan Pembelajaran Informatika, November 2024.

[3] D. R. Mugianto dan R. Budiarto, "Evaluasi Pengujian Keamanan Arsitektur Zero Trust Network pada Jaringan Smart Home untuk Mengatasi Serangan Data Sniffing," Syntax Literate: Jurnal Ilmiah Indonesia, Vol. 9 No. 11, 2024

[4] Rangga Aditya, Yusuf Muhyidin, dan Dayan Singasatia, "Implementasi SIEM untuk Monitoring Keamanan Server Menggunakan Wazuh," Merkurius: Jurnal Riset Sistem Informasi dan Teknik Informatika, Vol. 2 No. 5, hal. 137–144, 2024.

[5] Faruq Aziz Saputra, T. R. Dharmawan, dan A. Rustianto, "Implementasi Wazuh SIEM untuk Manajemen Log Event," Jurnal Informatika Terpadu, Vol. 10 No. 2, hal. 146–155, 2024.

[6] F. W. Romadhon dan M. Salman, "Pengembangan Skenario Serangan Siber Menggunakan Framework MITRE ATT&CK dan Cyber Kill Chain," Jurnal Pendidikan dan Teknologi Indonesia, Vol. 5 No. 5, hal. 1265–1279, 2025.

[7] M. R. T. Hidayat, N. Widiyasono, dan R. Gunawan, "Optimasi Deteksi Malware pada SIEM Wazuh melalui Integrasi Cyber Threat Intelligence," Jurnal Informatika dan Teknik Elektro Terapan, Vol. 13 No. 1, 2025.

[8] Nuswantoro dkk., "Implementasi Wazuh-ELK-Suricata untuk Deteksi Privilege Escalation di Ubuntu Server," Jurnal Saintekom, Vol. 15 No. 2, hal. 153–164, 2025.