ANALISIS JARINGAN WEBSITE E-JOURNAL STMIK PALANGKARAYA MENGGUNAKAN WAZUH UNTUK DETEKSI TRAFIK NORMAL DAN ANOMALI

PROPOSAL TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat Penulisan Tugas Akhir
pada Sekolah Tinggi Manajemen Informatika Dan Komputer
(STMIK) Palangkaraya

OLEH

RHEMA SHELVIA PUTRI
C2255201004
PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
2025

ANALISIS JARINGAN WEBSITE STMIK MENGGUNAKAN WAZUH UNTUK DETEKSI TRAFIK NORMAL DAN ANOMALI

PROPOSAL TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat Penulisan Tugas Akhir
pada Sekolah Tinggi Manajemen Informatika Dan Komputer
(STMIK) Palangkaraya

OLEH

RHEMA SHELVIA PUTRI
C2255201004
PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
2025

PERSETUJUAN

ANALISIS JARINGAN WEBSITE STMIK MENGGUNAKAN WAZUH UNTUK DETEKSI TRAFIK NORMAL DAN ANOMALI

Proposal Tugas Akhir Ini Telah Disetujui dan Disahkan

Pembimbing I,	Pembimbing II,
Ir. Abdul Hadi, S.T., M.Kom	Herkules, S.Kom.,M.Cs.
NIK. 198505102021101	NIK. 198510042010106

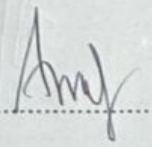
Mengetahui	Mengesahkan
Ketua STMIK Palangkaraya,	Ketua Prodi Teknik Informatika,
Ir. Hj. Siti Maryamah, M.M	Ir. Abdul Hadi, S.T., M.Kom
NIK. 196902021995004	NIK. 198505102021101

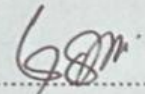
PENGESAHAN

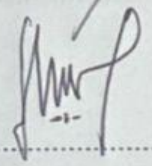
ANALISIS JARINGAN WEBSITE STMIK MENGGUNAKAN WAZUH UNTUK DETEKSI TRAFIK NORMAL DAN ANOMALI

Proposal Tugas Akhir ini telah Diseminarkan, Dinilai, dan Disahkan
Oleh Tim Seminar pada Tanggal 15 Desember 2025

Tim Seminar Proposal :

1. Amaya Andri Damaini, S.Kom., M.T ..... 
   Ketua

2. Ir. Abdul Hadi, S.T., M.Kom ..... 
   Sekretaris

3. Elia Zakharia, M.T. ..... 
   Anggota

DAFTAR ISI

PENGESAHAN ..... Error! Bookmark not defined.
DAFTAR ISI ..... **v**
DAFTAR TABEL ..... **vi**
DAFTAR GAMBAR ..... **vii**
DAFTAR LAMPIRAN ..... **viii**
BAB I PENDAHULUAN **1**
1.1 Latar Belakang Masalah 1
1.2 Perumusan Masalah 4
1.3 Batasan Masalah 5
1.4 Tujuan dan Manfaat 5
1.5 Sistematika Penulisan 8
BAB II TINJAUAN PUSTAKA **9**
2.1 Kajian Teori 9
2.1.1 Analisis 9
2.1.2 Jaringan Komputer 9
2.1.3 Website 10
2.1.4 Security Information and Event Management (SIEM) 11
2.1.5 Wazuh 12
2.1.6 Virtualbox 14
2.1.7 Ubuntu 15
2.1.8 Trafik Jaringan Dan Aktivitas Anomali 16
2.1.9 Metode Eksperimen 17
2.1.10 Deskriptif 17
2.1.11 Kualitatif 17
2.2 Penelitian Yang Relevan 18
BAB III METODOLOGI PENELITIAN **22**
3.1 Tinjauan Umum 22
3.2 Jenis penelitian 23
3.3 Desain Penelitian 24
3.4 Instrumen Penelitian 26
3.5 Analisis Kebutuhan 27
3.6 Desain 35
3.7 Jadwal Penelitian 39
DAFTAR PUSTAKA

DAFTAR TABEL

Tabel 2. 1 Penelitian Relevan..... 19
Tabel 3. 1 Kebutuhan Perangkat Lunak..... 28
Tabel 3. 2 Jadwal Penelitian..... 39

DAFTAR GAMBAR

Gambar 3. 2 Desain Penelitian 25
Gambar 3. 3 Wawancara bersama administrator STMIK Palangkaraya.....27
Gambar 3. 4 gambaran alur analisis proses 34
Gambar 3. 5 Desain Jaringan Eksisting STMIK Palangkaraya 37
Gambar 3. 6 Desain Eksisting Yang Dikaitkan Dengan Penelitian 38

DAFTAR LAMPIRAN

Lampiran 1. Surat tugas pembimbing tugas akhir
Lampiran 2. Lembar konsultasi bimbingan Tugas Akhir
Lampiran 3. Surat izin penelitian
Lampiran 4. Surat keterangan telah melakukan penelitian
Lampiran 5. Lembar wawancara
Lampiran 6. Lembar dokumentasi wawancara
Lampiran 7. Surat tugas penguji seminar
Lampiran 8. Berita acara penilaian seminar proposal TA

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Di era digital saat ini, institusi pendidikan tinggi tidak hanya bergantung pada situs web sebagai sumber informasi, tetapi juga menggunakan platform digital untuk mendukung kegiatan riset dan penerbitan karya ilmiah. Salah satu sistem penting yang diterapkan adalah website E-Journal STMIK Palangkaraya (ojs.stmikplk.ac.id). Platform ini berfungsi sebagai sarana untuk pengelolaan jurnal ilmiah kampus, mencakup seluruh tahapan penerbitan, mulai dari pengiriman naskah *(submission)*, peninjauan oleh reviewer *(peer-riview)*, hingga tahap penerbitan oleh editor. Sebagai media resmi untuk publikasi ilmiah, keberadaan E-Journal yang handal dan aman sangat penting untuk menjaga kelancaran proses akademik, kualitas publikasi, dan kredibilitas institusi.

Namun, peningkatan penggunaan website juga membawa tantangan tersendiri, terutama terkait keamanan dan kinerja jaringan. Beberapa masalah yang sering muncul di website E-Journal STMIK Palangkaraya adalah sering terjadinya aktivitas spam. Salah satu masalah yang sering muncul banyak percobaan upload dokumen secara otomatis, dimana file yang diunggah bukanlah naskah ilmiah melainkan file kosong, dokumen acak, atau bahkan file berbahaya. Kondisi semacam ini sering kali menjadi indikator adanya gangguan atau bahkan upaya perentasan terhadap sistem. Tidak jarang pula ditemukan spam *submission* yang berisi link ilegal, seperti tautan perjudian online, situs penipuan, atau konten

promosi yang tidak berkaitan dengan aktivitas akademik. Aktivitas ini dilakukan oleh bot dengan membuat akun palsu, kemudian mencoba mengisi metadata jurnal atau kolom abstrak dengan tautan berbahaya menggunakan pola yang terdeteksi seperti penyisipan URL secara otomatis.

Dengan demikian fenomena spam ini menimbulkan ancaman serius, karena selain memenuhi database dengan data yang tidak valid, juga dapat mengancam keselamatan pengguna jika link berbahaya yang terbuka secara tidak sengaja. Ini menimbulkan beban ekstra bagi pengelola E-Journal yang harus melakukan verifikasi manual terhadap akun, menghapus pengiriman tidak sah, serta memastikan bahwa sistem tetap terlindungi dari serangan yang lebih besar. Situasi ini menunjukan betapa pentingnya untuk terus memantau aktivitas jaringan secara berkelanjutan untuk mendeteksi pola trafik anomali sedini mungkin.

Selain dari spam, terdapat ancaman eksternal lain seperti upaya login yang sering dari alamat IP yang tidak dikenal, serangan brute force dihalaman login penulis atau editor, akses otomatis yang berlebihan *(trafik flooding)*, serta permintaan file yang tidak wajar mencurigakan dalam sistem. Sementara ancaman internal dapat muncul dari kesalahan konfigurasi, penggunaan akun administrator yang tidak tepat, atau aktivitas pengguna yang melanggar prosedur keamanan. Apabila tidak segera ditangani, ancaman-ancaman tersebut dapat mengganggu proses publikasi, mengancam keamanan data penulis dan reviewer, serta menurunkan kepercayaan pengguna terhadap layanan E-Journal kampus

Salah satu pendekatan yang relevan dalam menjaga keamanan jaringan adalah penggunaan sistem network monitoring dan Security Information and Event

Management (SIEM), yang berfungsi untuk memantau aktivitas jaringan mengelola log, serta mendeteksi ancaman real-time. Salah satu platform *open-source* yang banyak digunakan adalah Wazuh yang memiliki kemampuan dalam memonitor log sistem, mendeteksi aktivitas mencurigakan, serta memvisualisasikan pola trafik normal secara langsung. Dengan Wazuh, administrator dapat membedakan antara aktivitas normal dan aktivitas yang berpotensi membahayakan, sehingga langkah pencegahan dapat dilakukan lebih cepat dan tepat. Selain itu, Wazuh juga memungkinkan pengumpulan data secara terstruktur yang memudahkan analisis serta penyususnan laporan keamanan serta berkala, sebagaimana dibuktikan dalam beberapa penelitian implementasi SIEM dilingkungan pendidikan.

Sejalan dengan hal tersebut, beberapa penelitian di Indonesia telah memanfaatkan Wazuh dalam konteks keamanan jaringan salah satunya adalah Penelitian oleh Saputra, Dahramawan dan Rustianto (2024) di pasantren Teknologi Informasi dan Komunikasi (PeTIK) mengimplementasikan Wazuh sebagai Security Information and Event Management (SIEM) untuk mendeteksi ancaman keamanan jaringan secara real-time. Wazuh dipilih karena memiliki keunggulan dalam manajemen log, kemudahan pengguna, serta mendukung komunitas yang luas. Dan penelitian oleh Rahmatullah ddk. (2024) dalam saber Jurnal Teknik Informatika, Sains dan Ilmu Komunikasi mengkaji implementasi Security Information and Event Management (SIEM) dengan Wazuh dan Teler mampu mendeteksi berbagai serangan web. Sistem ini tidak hanya menampilkan log secara real-time, tetapi juga memberikan fleksibilitas bagi administrator untuk menyesuaikan aturan deteksi sesuai kebutuhan.

Berdasarkan kondisi tersebut, penulis memandang perlu dilakukan analisis terhadap pola trafik jaringan pada website E-Journal STMIK Palangkaraya, untuk memahami perbedaan antara aktivitas normal dan aktivitas anomali. Melalui ini, penulis berupaya mengidentifikasi karakteristik trafik yang dapat menjadi acuan dalam membedakan aktivitas wajar dengan aktivitas mencurigakan yang berpotensi mengancam keamanan jaringan. Hasil dari analisis ini diharapkan dapat memberikan kontribusi dalam upaya peningkatan keamanan website kampus serta mendukung kelancaran layanan informasi informasi bagi seluruh pengguna.

Dengan penelitian ini, diharapkan pihak kampus dapat memiliki pemahaman yang lebih mendalam mengenai kondisi keamanan jaringan website. Selain itu intitusi dapat meningkatkan kemampuan deteksi dini terhadap ancaman, mencegah kerusakan atau gangguan yang lebih besar, serta memastikan layanan E-Journal tetap aman, stabil, dan dapat dipercaya oleh penulis, reviewer, maupun editor. Penelitian ini juga diharapkan menjadi landasan bagi pengembangan sistem keamanan yang lebih baik dimasa depan, sehingga website kampus tidak hanya menjadi pusat informasi, tetapi juga aman dan andal sebagai sarana pendukung aktivitas akademik dan administrasi.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang sudah jelas, maka rumusan masalah dalam penelitian ini adalah bagaimana karakteristik trafik normal dan anomali pada jaringan website E-Journal Stimik Palangkaraya yang dapat dianalisis dan dideteksi menggunakan Wazuh?

1.3 Batasan Masalah

Agar penelitian ini tetap terarah dan sesuai dengan tujuan yang hendak dicapai, batasan suatu masalah digunakan penyimpangan atau pun pelembaran pokok masalah supaya penelitian ini mudah dipahami, maka ditetapkan beberapa batasan permasalahan sebagai berikut:

a. Penelitian ini hanya difokuskan pada website E-Journal STMIK Palangkaraya (ojs.stmikplk.ac.id). Pembatasan ini dilakukan agar penelitian memiliki ruang lingkup yang jelas dan tidak kewebsite lain maupun diluar domain STMIK Palangkaraya.

b. Tools yang dipakai untuk menganalisis hanya Wazuh, jadi tidak membandingkan hasil dengan yang lainnya.

c. Fokus penelitian hanya pada ciri-ciri trafik normal dan anomali, tanpa membahas lebih dalam tentang jenis serangan spesifik seperti DDoS, SQL Injection dan lainnya.

d. Penelitian ini bersifat Analisis dan Deteksi tidak sampai pada tahap Implementasi system keamanan.

e. Hal-hal diluar teknis seperti kebijakan keamanan kampus tidak dibahas.

f. Penelitian ini dibatasi oleh oleh durasi waktu tertentu, sehingga hasil analisis hanya menggambarkan kondisi jaringan pada saat pengambilan data berlangsung dan tidak mewakili kondisi jangka panjang.

1.4 Tujuan dan Manfaat

Tujuan berisikan 1 paragraf dan manfaat dapat dikondisikan menyesuaikan dari pemanfaatannya sendiri.

a. Tujuan

Penelitian ini bertujuan untuk menganalisis dan membedakan karakteristik trafik normal dan anomali pada website E-Journal STMIK Palangkaraya berdasarkan data log yang diolah menggunakan Wazuh sebagai sistem (SIEM). Analisis ini dilakukan untuk memperoleh gambaran yang lebih jelas mengenai pola aktivitas jaringan yang terjadi, mengidentifikasi perbedaan antara aktivitas yang wajar dan aktivitas yang menyimpang, serta menyediakan informasi yang dapat digunakan sebagai bahan evaluasi awal terhadap kondisi trafik jaringan pada website E-Journal STMIK Palangkaraya selama periode pengamatan.

b. Manfaat

Penelitian ini diharapkan memberikan manfaat baik secara akademis, praktis, maupun pengembangan ke depan.

1. Bagi Penulis

   Manfaat bagi penulis, penelitian ini memberikan kesempatan untuk memperdalam pemahaman mengenai analisis trafik jaringan serta penerapan Wazuh dalam mendeteksi aktivitas normal dan anomali, sekaligus menjadi pengalaman praktis dalam penelitian bidang keamanan jaringan.

2. Bagi STMIK Palangkaraya

   Manfaat bagi STMIK Palangkaraya yaitu hasil penelitian dapat menjadi bahan evaluasi sekaligus referensi untuk meningkatkan keamanan website kampus, memperkuat sistem deteksi dini, serta menjaga kepercayaan pengguna terhadap layanan informasi akademik dan administrator.

3. Bagi Administrator Sistem

   Manfaat bagi administrator penelitian ini menyediakan acuan dalam mengenali perbedaan pola trafik normal dan anomali, sehingga dapat membantu pengambilan keputusan yang lebih cepat tepat dalam menjaga kestabilan jaringan.

4. Bagi pengguna Website (mahasiswa, Dosen, Staf)

   Manfaat langsung dirasakan berupa layanan website yang lebih aman, dan minim gangguan, sehingga proses akademik mampu administrasi dapat berjalan dengan baik.

1.5 Sistematika Penulisan

Adapun sistematika penulisan dalam penulisan tugas akhir ini terdiri dari bebrapa bab dan masing-masing bab membahas dan menguraikan pokok permasalahan yang berbeda, sebagai gambaran disini penulis menyertakan garis-garis besarnya yaitu :

BAB I PENDAHULUAN

Bab ini berisikan latar belakang masalah, rumusan masalah, Batasan masalah, tujuan dan manfaat, serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisikan tentang tinjauan pustaka yang diambil dari penelitian yang relevan beserta susunan kajian teori yang disesuaikan dengan tema Tugas Akhir.

BAB III METODOLOGI PENELITIAN

Bab ini berisikan tentang tahapan yang dilakukan peneliti dalam mengumpulkan informasi atau data yang dibutuhkan.

BAB II

TINJAUAN PUSTAKA

2.1 Kajian Teori

Pada tahap ini berisi kajian teori yang menjadi dasar penelitian, meliputi konsep jaringan komputer , website, dan sistem *Security Information and Event Management* (SIEM) platform Wazuh, serta trafik jaringan dan aktivitas anomali. Maka kajian ini digunakan untuk memperkuat landasan pemikiran dan mendukung analisis yang dilakukan dalam penelitian ini.

2.1.1 Analisis

Analisis merupakan proses menguraikan, meneliti, dan mengevaluasi data yang diperoleh dari aktivitas jaringan untuk mengetahui kondisi, perform, dan permasalahan yang terjadi didalam jaringan komputer. Nursi dkk. (2025). Sementara itu, dalam penelitian Analisis jaringan komputer LAN dirumah sakit UNRAM menjelaskan bahwa analisis dilakukan untuk mengetahui proses kerja sistem jaringan komputer serta mengidentifikasi kelebihan dan kekurangannya, guna meningkatkan efektivitas komunikasi data. Irawan dkk. (2022).

Dengan demikian, analisis dapat diartikan sebagai kegiatan sistematis untuk menguraikan dan menilai data jaringan guna memahami pola kerja, performa serta potensi permasalahan dalam sistem komputer.

2.1.2 Jaringan Komputer

Jaringan komputer adalah koneksi yang memungkikan dua atau lebih perangkat seperti komputer, server, atau printer terhubungan satu sama lain, baik

secara fisik maupun login, untuk bertukar data dan informasi. Menurut Antariksa dkk, (2022), jaringan komputer dapat diartikan sebagai kumpulan komputer yang saling terhubung dengan tujuan utama untuk berbagi sumber daya (resources) seperti data, printer, dan koneksi internet dilingkungan tertentu. Sementara itu, Buana dkk (2023) menjelaskan bahwa jaringan komputer adalah dua komputer yang saling terkoneksi dalam sebuah jaringan jika keduannya mempunyai kemampuan untuk berkomunikasi dan bertukar data serta informasi.

Dengan demikian, jaringan komputer berperan penting sebagai sarana komunikasi yang terhubungkan dua atau lebih perangkat melalui media trasmisi kabel maupun nirkabel untuk mendukung pertukaran data, kolaborasi, dan pemanfaatan sumber daya secara efesien disuatu institusi. Dalam konteks ini, jaringan komputer menjadi fondasi utama dalam proses analisis trafik dan deteksi anomali pada Website E-Journal STMIK Palangkaraya menggunakan platform Wazuh sebagai sistem pemantauan keamanan jaringan.

2.1.3 Website

Website merupakan komponen penting dalam komputer yang berperan sebagai saranan untuk informasi, komunikasi, layanan, digital. Khirdany (2024) mencatat bahwa website mendukung organisasi, lembaga, dan institusi pendidikan dalam memperbaiki efektivitas kerja serta mutu layanan kepada masyarakat. Secara teoritis, Dalam Khirdany (2024) menjelaskan bahwa website terdiri dari kumpulan halaman digital yang saling terhubung melalui URL dan dapat menyajikan informasi dalam berbagai format seperti teks, gambar, atau video secara interaktif.

Efektivitas suatu situs web dapat dinilai berdasarkan mutu sistem, tingkat kepuasan pengguna, dan kualitas informasi yang meliputi ketepatan, keamanan, serta pembaruan data (Khindany, 2024). Dan Indriani (2018) berpendapat bahwa proses pembuatan situs web tidak hanya fokus pada desain antarmuka, tetapi juga pada struktur dan fungsi yang memudahkan pengguna. Dari segi, situs web dikembangkan menggunakan bahasa pemrograman seperti HTML, CSS, dan PHP serta dibagi menjadi situs web statis dan dinamis.

Dalam penelitian ini, Website STMIK Palangkaraya adalah situs yang aktif, berperan sebagai sumber informasi akademis serta alat analisis lalu lintas jaringan. Mengingat sifatnya yang terbuka di internet, dibutuhkan sistem keamanan Wazuh (SIEM) untuk mengawasi log dan mengidentifikasi aktivitas yang tidak biasa sehingga layanan akademik dapat terjaga dan tetap dapat di akses.

2.1.4 Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) merupakan teknologi keamanan yang berfungsi untuk mendeteksi, menganalisis, dan merespons ancaman siber secara terpusat dengan mengumpulkan dan memproses log dari berbagai sumber sistem dan jaringan. SIEM mengeintegrasikan dua fungsi utama, yaitu Manajemen Informasi keamanan (SIM) dan Manajemen peristiwa keamanan (SEM), sehingga mampu memberikan perspektif komprehensif tentang keadaan keamanan jaringan dan memberikan sinyal awal terhadap kemungkinan ancaman.

Menurut Widyawanti dkk, (2025) penggunaan SIEM seperti Wazuh terbukti efektif untuk menangkal serangan seperti *XSS, Injection SQL,* dan *Brute-force* melalui proses analisis log otomatis dari server, *firewall*, dan aplikasi.

Kolaborasi dengan sistem notifikasi seperti WhatApp Bot berhasil mempercepat waktu respons menjadi kurang dari satu menit. Di sisi lain, penelitian yang dilakukan oleh Nugraha dkk, (2025) menunjukkan bahwa penerapa SIEM dalam sistem pendidikan dapat meningkatkan ketepatan deteksi hingga 85% dan mengurangi kesalahan deteksi sebesar 20% dengan waktu deteksi ancaman yang kurang dari lima menit.

Secara umum, penggunaan SIEM tidak hanya memperkuat kemampuan untuk memdeteksi dan merespons insiden, tetapi juga membantu, memastikan kepatuhan terhadap standar keamanan seperti ISO 27001, meningkatkan ke efisienan pengawasan, serta menjaga keutuhan, kerahasiaan, dan ketersediaan data dalam organisasi, Dengan kemajuan teknologi seperti chatbot dan machine learning, SIEM kini berkembang menjadi sistem keamanan yang lebih responsif , cerdas, dan mampu beradaptasi dengan ancaman siber terkini.

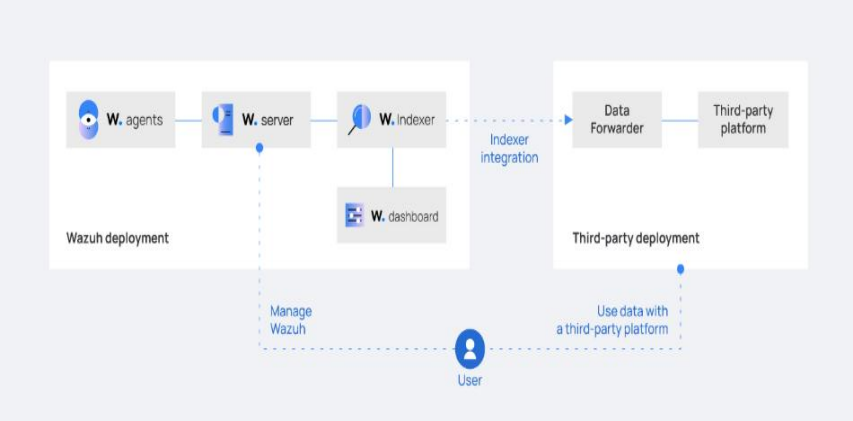
2.1.5 Wazuh

Wazuh Adalah perangkat lunak *open source* yang berfungsi sebagai sistem deteksi berbasis host *(endpoint)* yang menyatukan kemampuan XDR *(External Data Representation)* dan SIEM (*Security Information and Event Management)* diantaranya menganalisis log, deteksi intrusi dan *Malware, monitor file integrity*, penilaian konfigurasi sesuai standar industri, deteksi kerentanan, dan dukungan kepatuhan, kemudian wazuh memberikan fitur visibilitas keamanan yang lebih pada infrastruktur dengan memantau host sistem operasi dan tingkat aplikasi Azzah dkk (2025).

1. Wazuh Agent di pasangkan pada perangkat *(endpoint)* seperti komputer atau server yang ingin dipantau. Agent ini bertugas untuk mengumpulkan log, aktivitas sistem, dan informasi keamanan, lalu agent memiliki beberapa modul seperti *log collection, vulnerability detection, sistem inventory,* dan lainnya, semua data yang dikumpulkan oleh agent kemudian dikirim ke wazuh server.
2. Wazuh server berperan sebagai komponen pusat (central component) yang menerima data dari banyak agent. Server ini menganalisis data, mendeteksi ancaman, melakukan korelasi log, serta membuat alert keamanan. Setelah diproses analisis selesai, hasil dikirim ke Wazuh Indexer.
3. Wazuh Indexer berfungsi sebagai tempat penyimpanan utama log dan hasil analisis yang diterima dari wazuh server. Indexer menggunakan sistem pencarian cepat untuk memudahkan pengambilan data Ketika dibutuhkan, misalnya saat pengguna ingin melihat detail log atau melakukan pencarian berdasarkan waktu kejadian tertentu.
4. Wazuh Dashboard merupakan antar muka berbasis web yang memungkinkan pengguna untuk melihat grafik, laporan, status keamanan, dan hasil deteksi ancaman secara real-time. Dashboard ini juga menjadi tempat bagi admin untuk memantau seluruh agent dan aktivitas sistem secara visual.

Berikut ini disajikan arsitektur Wazuh yang digunakan sebagai acuan dalam penelitian, sebagaimana ditunjukkan pada Gambar 2.1 Arsitektur Wazuh. Arsitektur Wazuh terdiri dari beberapa komponen utama,

yaitu *Wazuh Agent* yang mengumpulkan log dari server, *Wazuh Server* yang menganalisis dan mendeteksi aktivitas mencurigakan, *Wazuh Indexer* yang menyimpan dan mengindeks data, serta *Wazuh Dashboard* yang menampilkan hasil analisis dalam bentuk grafik dan alert. Alur ini memungkinkan pemantauan trafik normal dan anomali secara terpusat dan real-time.



Gambar 2. 1 Arsitektur Wazuh

2.1.6 Virtualbox

Virtualbox merupakan aplikasi virtualisasi yang bersifat open-soure, dirancang untuk menciptakan dan mengoperasikan mesin virtual pada satu perangkat keras. Dengan menggunakan dapat menginstal sistem operasi tambahan seperti Linux atau Ubuntu tanpa mengganggu sistem utama dilaptop. Teknologi ini memberikan kesempatan bagi peneliti untuk menciptakan lingkungan pengujian yang terpisah, aman, dan luwes, untuk tujuan pengembangan maupun simulasi.

Dalam penelitian ini, VirtualBox berfungsi sebagai platform untuk menjalankan server yang dibutuhkan dalam penerapan Wazuh. Dengan menggunakan VirtualBox, peneliti dapat menginstal dan mengatur elemen-elemen

Wazuh seperti Wazuh server, Wazuh Indexer dan Wazuh Dashboard pada mesin virtual berbasis ubuntu. Lingkungan virtual tersebut memfasilitasi pemantauan dan analisis log jaringan berlangsung tanpa merubah atau mengganggu konfigurasi asli dari perangkat fisik maupun jaringan kampus.

Penggunaan VirtualBox juga membawa manfaat dalam simulasi lalu lintas normal dan anomali. Dengan menggunakan mesin virtual, para peneliti dapat melakukan eksperimen seperti mengirim lalu lintas pengujian, mencoba login yang tidak sah, atau melakukan akses berulang untuk mengamati cara Wazuh mendeteksi dan menandai aktivitas tersebut. Fitur snapshot di VirtualBox memudahkan peneliti untuk mengembalikan sistem ke kondisi sebelumnya jika terjadi kesalahan saat melakukan konfigurasi dimasa pengujian.

Dengan demikian, VirtualBox berperan penting dalam ini sebagai lingkungan yang terkontrol untuk menguji, menjalankan, dan menganalisis kinerja Wazuh dalam mengenali lalu lintas normal maupun anomali pada situs.

2.1.7 Ubuntu

Ubuntu adalah distribusi Linux yang terdiri dari banyak perangkat lunak bebas dan terbuka, serta merupakan versi komersial dari Debian. Ubuntu hadir dalam beberapa edisi, termasuk Desktop, Server, dan Core untuk perangkat internet *of Things (loT)* dan roboy, yang dikembangkan melalui kolaborasi komunitas pengembang dan perusahaan *British, Canonical Ltd.* Banyak fitur yang didukung Ubuntu, seperti pembaruan semestral dan dua tahunan dengan dukungan panjang waktu (LTS), yang didasarkan pada model pengembangan meritokratisnya (Encep, dkk, 2024).

Ubuntu adalah salah satu distribusi Linux yang berbasiskan Debian GNU/Linux dan memiliki interface desktop. Ubuntu adalah sepenuhnya sistem operasi *open source* yang dibangun berdasarkan kernel Linux. (Wikipedia, 2008).

Berdasarkan pengertian diatas dapat disimpulkan ubuntu adalah salah satu varian Linux yang terdiri dari berbagai perangkat lunak yang bersifat terbuka, dan menggunakan versi resmi dari Debian. Ubuntu memiliki beberapa jenis, antaranya Desktop, Server, dan Core yang ditujukan untuk perangkat internet dan robot pengembang.

2.1.8 Trafik Jaringan Dan Aktivitas Anomali

Trafik jaringan merujuk pada gerakan data antara perangkat dalam sistem komputer yang menunjukkan interaksi antara pengguna dan server. Menurut Pratama dkk (2022), pola trafik digunakan untuk mengevaluasi apakah jaringan berfungsi dengan baik atau mengalami masalah. Trafik yang normal ditandai dengan kemampuan sistem, sedangkan trafik yang anomali dapat dikenali melalui lonjakan permintaan, koneksi yang mencurigakan, atau serangan siber seperti *DoS dan SQL Injection* yang dapat merusakan performa jaringan. Sistem keamanan seperti Wazuh dapat menganalisis log jaringan secara langsung untuk membedakan antara trafik yang normal dan tidak biasa. Berdasarkan studi oleh Pratama dkk (2022) dan Rachmawati (2024), Wazuh terbukti sangat efektif dalam mengidentifikasi serangan seperti DoS dan HTTP Flood melalui peringatan otomatis yang aktif saat terdapat aktivitas mencurigakan di jaringan.

Dalam studi ini, penelaahan dilakukan terhadap lalu lintas situs web STMIK Palangkaraya dengan memanfaatkan Wazuh untuk mendeteksi pola yang

menyimpang. Tujuan utama penelitian ini adalah menemukan dan mengenali, bukannya mengatasi, untuk memperoleh pemahaman tentang situasi dan kemungkinan ancaman dalam jaringan.

2.1.9 Deskriptif

Metode Deskriptif merupakan pendekatan penelitian yang bertujuan untuk mengdeskripsikan fenomena yang ada baik, fenomena alam atau fenomena buatan manusia yang digunakan untuk menganalisis serta mendeskripsikan hasil subjek, tetapi tidak dimaksudkan untuk memberikan implikasi yang lebih luas, Kusnadi dkk, (2021).

Disimpulkan Metode deskriptif digunakan untuk menggambarkan daan menganalisis fenomena secara sistematis sesuai dengan kondisi nyata taanpa memberikan kesimpulan yang bersifat umum.

2.1.10 Kualitatif

Metode Kualitatif merupakan penelitian yang dipilih karena sesuai dengan tujuan untuk menggali secara mendalam fenomena sosial. Metode kualitatif memberikan fleksibilitas dalam pengumpulan data melalui wawancara mendalam dan observasi langsung, sehingga hasil penelitian yang diperoleh bersifat konteksual dan mampu menggambarkan kondisi nyata dilapangan (Yuliani and Supriatna 2023).

Dapat disimpulkan metode kualitatif digunakan untuk menggali dan memahami fenomena secara mendalam melalui wawancara dan observasi, dengan hasil penelitian yang bersifat deskriptif dan mencerminkan kondisi nyata.

2.1.11 Eksperimen

Eksperimen dalam penelitian ini digunakan sebagai teknik pendukung observasi, bukan sebagai metode penelitian utama. Eksperimen dilakukan dalam bentuk simulasi trafik jaringan untuk mengamati bagamaimana sistem Wazuh merekam dan menampilkan aktivitas normal maupun anomaly pada log keamanan. Hasil simulasi tersebut tidak dianalisis secara ststistik, tetapi diinterpretasikan secara deskriptif dan kualitatif berdasarkan informasi pemantauan yang dihasilkan oleh sistem. Pendekatan ini digunakan untuk memperjelas perbedaan karakteristik antara aktivitas jaringan yang normal dan yang tidak biasa, sehingga tetap selaras dengan jenis penelitian deskriptif kualitatif.

2.2 Penelitian Yang Relevan

Sub bab ini menguraikan tentang penelitian yang relevan, yaitu penelitian sebelumnya oleh penulis lain yang memiliki topik serupa atau mendekati persamaan. Penelitian yang relevan merupakan penelitian yang memiliki keterkaitan dengan topik, variabel, atau permasalahan yang sedang diteliti. Kajian ini digunakan sebagai acuan dan pembandingan untuk memperkuat landasan teori, menunjukkan keaslian penelitian, serta membantu peneliti memahami hasil dan metode yang telah digunakan sebelumnya. Berikut disajikan penelitian -penelitian yang relevan pada tabel 2.2 penelitian yang relevan sebagai acuan dan pembanding dalam penelitian ini.

Tabel 2. 1 Penelitian Relevan

No	Penulis / Tahun	Topik Penelitian	Metode	Pembahasan	Hasil
1	Mardhiyah dkk/2023	Analisis Sistem Security Information and Event Management (SIEM) Aplikasi Wazuh pada Dinas komunikasi Informatika Statistik dan Persandian Sulawesi Selatan	*Metode Eksperimen dengan melakukan pengujian langsung terhadap aplikasi Wazuh menggunakan dua jenis serangan yaitu DDos Slowloris dan Brute force*	Penerapan Wazuh (SIEM) untuk mendeteksi serangan siber secara real-time di Dinas Komunikasi Informatika Statistik, khususnya DDoS Slowloris dan Bruce force	Hasil pembahasan menunjukan Wazuh berhasil mendeteksi kedua jenis serangan tersebut dengan cepat tanpa jeda waktu (real-time) dan dapat mengklarifikasikan Tingkat keparahan serangan dari level rendah hingga tinggi.
2	Bagas Haryanto ddk/2024	Implementasi Wazuh Integritas File untuk Perlindungan Keamanan Berdasarkan Aktivitas Log di BTSI UKSW	*Analisis kebutuhan, Desain, Perancangan Sistem, Implementasi, Pengujian Sistem, Penulisan Laporan*	Mengimplementasi SIEM pada salah satu aplikasi SMS Center Pemerintah Daerah Provinsi NTB untuk memantau dan mengaudit intergritas file.	Dari Hasil menggunkan Wazuh diukur pada Tingkat keakuratan Wazuh dalam memantau dan mengaudit intergritas file. Dalam hal ini Wazuh melakukan Audit dan analisis log file untuk mengindentifikasi kejadian keamanan yang tidak biasa atau mencurigakan.
3	Gede Parama ddk/2024	Impelementasi dan Analisis Wazuh Sebagai Intrusion Detection System (IDS) dan Platform Monitoring	*Metode Pengumpulan data (Wawancaradan Penelitian Kepustakaan), Metode*	Pengembangan IDS sebagai platform Monitoring dilakukan dengan cara membangun sebuah aplikasi berbasis web pada server lokal dan mengeksploitasi celah keamanan pada bagian kode	Hasilnya dalah untuk menguji efektivitas IDS dalam mendeteksi serangan dan mengidentifikasi kelemahan-kelemahan pada sistem. Proses ini juga dilakukan untuk menguji website pada uji coba menggunakan serangan LFI, XXE dan DoS dengan melihatkan efektivitas wazuh sebagai platform monitoring dalam mendeteksi serangan

No	Penulis / Tahun	Topik Penelitian	Metode	Pembahasan	Hasil
			Pengembangan Sistem	program sebuah website oleh IDS yang telah dikembangkan	yang mengirimkan alert atau notifikasi pada Discord, sehingga memudahkan dalam melakukan monitoring terhadap serangan.
4	Faruq dkk/2024	Implementasi Wazuh SIEM Untuk Manajemen Log Event di Pesantren Teknologi Informasi dan Komunikasi Jombang	*Metode analisis dan Pengumpulan Data*	Membahas tentang penerapan sistem keamanan jaringan menggunakan Wazuh, yaitu tools security Information and event management (SIEM) berbasis open-source yang digunakan untuk mendeteksi, memantau dan menganalisis	Hasil Adalah Wazuh berhasil mendeteksi dan memantau serangan Brute force, DoS, dan SQL Injection secara real-time, serta integrasi dengan telegram Bot mampu memberikan notifikasi serangan secara cepat, sementara kinerja CPU dan memori tetap dalam batas normal saat serangan terjadi.
5	Azzah dkk/ 2024	Impementasi Wazuh menggunakan metode PPDIOO di sistem keamanan jaringan PSDKU universitasi lampung waykanan sebagai deteksi dan respon serangan siber	*Metode PPDIOO*	Dalam sistem ini semua aktivitas dari wazuh agenrt akan dikirimkan ke wazuh server untuk dilakukan pemantauan dan deteksi derangan siber.	Hasil sistem keamanan jaringan yang dapat mendeteksi dan merespon serangan siber menggunakan wazuh. Wazuh berhasil mendeteksi serangan Brufe Force yang dilakukam didalam jaringan.
6	Alvin dkk/2024	Implementasi Wazuh FIM(file Integrity Monitoring) untuk perlindungan Keamanan Sistem Informasi pada Unit Kegiatan Mahasiswa di Universitas Trunojoyo Madura	*Metode penelitian Analysis, Design, Implementation, Testing, Maintenance*	Membahas tentang implementasi Wazuh dengan modul File Integrity Monitoring (FIM) untuk melindungi keamanan data dan memantau perubahan file penting secara real-time pada Unit kegiatan Mahasiswa (UKM) Triple-C Universitas Trunojoyo Madura	Hasil pembahasan menunjukan bahwa wazuh dengan modul file Integrity Monitoring (FIM) berhasil mendeteksi perubahan pada file penting seperti penambahan, modifikasi, dan penghapusan secara real-time.

Berdasarkan table 2.1 dari hasil 6 penelitian terdahulu yang relevan dapat disimpulkan bahwa penerapan sistem Wazuh memberikan kontribusi yang signifikan dalam memantau dan menjaga keamanan jaringan website. Wazuh mampu mendeteksi berbagai aktivitas mencurigakan maupun ancaman serangan yang sulit teridentifikasi secara manual. Melalui hasil monitoring yang disajikan dalam bentuk grafik dan laporan analisis, administrator dapat lebih mudah memahami kondisi sistem serta mengambil Langkah penanganan dengan cepat. Penerapan Wazuh juga membuat sistem menjadi lebih aman, responsive, dan terkontrol, sehingga mempermudah proses identifikasi Ketika terjadi gangguan serta meningkatkan keandalan layanan website secara keseluruhan.

BAB III

METODOLOGI PENELITIAN

3.1 Tinjauan Umum

Penelitian ini dilaksanakan pada jaringan serta website E-Journal STMIK Palangkaraya (ojs.stmikplk.ac.id) yang berfungsi sebagai saluran resmi untuk penerbitan ilmiah dikampus. sebagai media untuk menyebarkan pengetahuan dan hasil penelitian dibidang teknologi informasi dan komputer. Sistem ini dibangun menggunakan *Open Journal System* (OJS), sebuah platform manajemen jurnal ilmiah yang secara luas digunakan oleh institusi pendidikan untuk mendukung proses publikasi yang terstruktur dan profesional.

Saat ini, E-Journal STMIK Palangkaraya mengelola dua jurnal akademik, yaitu Jurnal Saintekom merupakan jurnal bidang sains, teknologi, komputer, dan manajemen yang berfungsi sebagai media komunikasi ilmiah antara akademisi dan peneliti. Sedangkan Jurnal SIMTEK merupakan sarana untuk mempublikasi hasil penelitian yang berkaitan dengan sistem informasi, manajemen teknologi informasi serta pemanfaatan teknologi informasi serta pemanfaatan teknologi komputer atau teknologi informatika dalam bidang bisnis dan bidang Pendidikan serta social lainnya, publikasi ini bertujuan untuk menyediakan informasi dan referensi bagi masyarakat luas terkait bidang ilmu komputer, sistem informasi, manajemen dan teknologi informasi serta menerapkan dan manfaatnya secara nyata dalam masyarakat.

Sebagai sebuah sistem layanan publikasi E-Journal memiliki Tingkat interaksi pengguna yang tinggi, mulai dari akses, proses login bagi penulis,

penggunggahan naskah, serta kegiatan yang dilakukan oleh editor dan reviewer. Seluruh aktivitas tersebut menghasilkan trafik dan log server yang dapat dianalisis untuk memahami pola aktivitas normal maupun mendeteksi adanya anomali. Oleh karena itu, penelitian ini berfokus pada analisis trafik jaringan portal E-Journal Stmik Palangkaraya dengan memanfaatkan Wazuh, sebuah sistem pengelolaan informasi dan kejadian keamanan (SIEM) yang mampu mengumpulkan log, menganalisis aktivitas jaringan, serta memberikan peringatan ancaman secara real-time.

Data penelitian diperoleh dari pemantauan log jaringan pada server yang menjalankan E-Journal dan telah dipasang agen Wazuh. Melalui analisis tersebut, penelitian ini bertujuan mengidentifikasi perbedaan karakteristik antara trafik normal dan trafik anomali yang mungkin mengindikasikan aktivitas mencurigakan seperti percobaan login berulang dari IP yang tidak dikenal, spam, atau akses otomatis dari bot. Hasil penelitian diharapkan dapat memberikan wawasan penting bagi pengelola sistem dalam meningkatkan keamanan jaringan, mengurangi gangguan akses, serta memastikan portal E-Journal tetap andal sebagai sarana publikasi ilmiah STMIK Palangkaraya

3.2 Jenis penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian deskriptif kualitatif.

Penelitian deskriptif kualitatif digunakan untuk menggambarkan dan menjelaskan kondisi nyata trafik jaringan pada website E-Journal STMIK Palangkaraya berdasarkan data log yang dihasilkan oleh sistem Wazuh. Penelitian

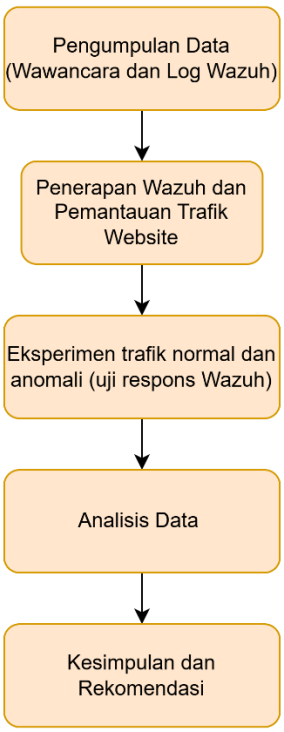
ini tidak bertujuan untuk menguji hipotesis atau membandingkan perlakuan tertentu, melainkan untuk mendeskripsikan karakteristik trafik normal dan trafik anomali yang terjadi selama proses pemantauan.

Pendekatan kualitatif dilakukan melalui wawancara dengan pengelola jaringan website STMIK Palangkaraya untuk mengumpulkan informasi tambahan mengenai kondisi nyata website serta observasi terhadap aktivitas jaringan dan log keamanan yang ditampilkan pada Wazuh Dashboard. Selain itu, dilakukan simulasi aktivitas jaringan secara terbatas sebagai bagian dari proses pengamatan, yang bertujuan untuk membantu memperjelas bagaimana respon sistem Wazuh dalam mendeteksi aktivitas normal dan anomali. Simulasi ini tidak dimaksudkan sebagai metode penguji, melainkan seluruh hasil pengamatan tersebut dianalisis dan dijelaskan secara deskriptif sesuai dengan pendekatan kualitatif.

3.3 Desain Penelitian

Desain penelitian ini dilakukan untuk menjelaskan alur dan tahapan yang dilakukan peneliti dalam melaksanakan penelitian agar tujuan yang telah ditetapkan dapat tercapai secara sistematis.

Penelitian ini dirancang menggunakan pendekatan studi kasus deskriptif kualitatif yang berfokus pada analisis jaringan website E-Journal STMIK Palangkaraya (ojs.stmikplk.ac.id) dengan memanfaatkan sistem Wazuh sebagai alat bantu pemantauan log dan deteksi aktivitas anomali. Untuk mencapai hasil yang diharapkan, penelitian ini dilakukan melalui beberapa tahapan:



Gambar 3. 1 Desain Penelitian

Tahap penerapan Wazuh dilakukan dengan menginstal dan mengonfigurasi sistem pada server website E-Journal STMIK Palangkaraya (ojs.stmikplk.ac.id) untuk memantau aktivitas jaringan secara real-time serta mengenali pola trafik yang normal dan anomali. Setelah berfungsi, dilaksanakan ekseperimen bentuk simulasi trafik normal dan trafik anomali untuk mengamati bagaimana wazuh merespons setiap aktivitas yang muncul, termasuk kemampuannya untuk memberikan peringatan otomatis saat deteksi anomali. Data log yang diperoleh dari wazuh kemudian dianalisis secara deskriptif bersamaan dengan hasil wawancara dengan pengelola jaringan untuk menggambarkan perbedaan yang jelas antara trafik normal dan anomali, sekaligus mengevaluasi efektivitas sistem dalam mendeteksi aktivitas mencurigakan. Berdasarkan hasil analisis ini, penelitian menyususn

Kesimpulan tentang kondisi keamanan jaringan website STMIK Palangkaraya dan memberikan rekomendasi yang dapat diterapkan untuk memperbaiki keamanan serta memperkuat proses pemantauan jaringan kedepannya.

3.4 Instrumen Penelitian

Penelitian ini digunakan untuk membantu penelitian dalam pengumpulan data yang dibutuhkan, baik secara teknis maupun kualitatif. Dalam, penelitian ini, instrumen yang digunakan meliputi:

a. Studi Pustaka

Pada tahap ini penulis melakukan studi Pustaka untuk mengumpulkan teori dan referensi yang relevan dan bersumber dari jurnal, artikel atau buku, dengan penelitian yang berjudul Analisis Jaringan Website E-Journal STMIK Menggunakan Wazuh Untuk Deteksi Trafik dan Anomali.

b. Wawancara

Wawancara dilakukan untuk mengumpulkan informasi yang lebih rinci mengenai keadaan sebenarnya dari jaringan website E-journal STMIK Palangkaraya, termasuk permasalahan keamanan yang sering muncul dan langkah-langkah pencegahan yang telah diambil. Berdasarkan hasil wawancara dengan administrator jaringan, diketahui bahwa website E-Journal sering mengalami masalah berupa spam pada from dan komentar, serta ditemukan tautan yang mengarah kesitus judi online atau iklan yang mengindikasikan adanya potensi percobaan akses tidak sah terhadap terhadap sistem OJS. Informasi ini menjadi bahan penting dalam penelitian karena menunjukkan adanya ancaman trafik dan pemantauan log yang lebih mendalam menggunakan wazuh.



Gambar 3. 2 Wawancara bersama administrator STMIK Palangkaraya

c. Studi Dokumen

Tahapan ini dilakukan dengan meninjau berbagai dokumen terkait sistem jaringan dan website E-Journal STMIK Palangkaraya, seperti struktur jaringan, konfigurasi server, serta data log aktivitas website. Studi dokumen membantu peneliti memahami kondisi awal sistem yang akan di analisis dan menjadi dasar dalam proses penerapan Wazuh.

3.5 Analisis Kebutuhan

Pada tahap ini penulis melakukan analisis untuk menentukan komponen komponen yang diperlukan dalam penerapan sistem Wazuh sebagai alat bantu dalam menganalisis trafik jaringan pada website E-Journal STMIK Palangkaraya. Analisis kebutuhan ini bertujuan agar proses pemantauan, pengumpulan log, dan deteksi aktivitas anomali dapat berjalan secara optimal. Kebutuhan penelitian meliput aspek perangkat keras, perangkat lunak, informasi, dan pengguna, yang dijelaskan sebagai berikut:

a. Kebutuhan perangkat keras (Hardware)

1. Menggunakan laptop atau server dengan prosesor Intel 3.
2. Memiliki kapasitas RAM minimal 4 GB.
3. Menggunakan SSD minimal 256 GB.
4. Koneksi jaringan internet yang stabil.

Perangkat keras digunakan untuk menjalankan sistem Wazuh dan mendukung aktivitas pemantaun jaringan.

b. Kebutuhan perangkat lunak (Software)

Perangkat lunak digunakan untuk menjalankan sistem pemantauan dan melakukan analisis log. Berikut Tabel 3.1 kebutuhan pada perangkat lunak Sofware

Tabel 3. 1 Kebutuhan Perangkat Lunak

Perangkat Lunak	Keterangan
Ubuntu Server	Tempat wazuh server di instal
Wazuh Agent	Sebuah komponen yang dipasang pada perangkat endpoint seperti linux, Windows, dan sistem operasi lainnya, untuk mendeteksi dan mengumpulkan informasi keamanan pada suatu sistem lalu mengirimkannya ke Wazuh-server (Punta Dewa 2024)
Wazuh Server	Komponen dari wazuh yang bertugas menganalisis data yang diterima dari wazuh agent dan memberikan peringatan jika terjadi perubahan pada file (Punta Dewa 2024)
Wazuh Indexer	Mesin pencari yang digunakan untuk mengindeks dan menyimpan peringatan yang dihasilkan oleh wazuh server (punta dewa 2024)
Wazuh Dasshboard	Antarmuka web yang menampilkan dan memvisualisasikan informasi

Perangkat Lunak	Keterangan
	keamanan yang berguna seperti pemantauan integritas file, indikator ancaman, log aktivitas sistem, dan laporan keamanan (Punta Dewa 2024)
VirtualBox	digunakan sebagai platform virtualisasi untuk menjalankan Ubuntu Server dan seluruh komponen Wazuh tanpa mengubah konfigurasi sistem fisik.

c. Kebutuhan informasi

Informasi yang diperlukan dalam penelitian ini meliputi:

1. Data log aktivitas jaringan yang dikumpulkan dari server website STMIK Palangkaray melalui Wazuh Agent.
2. Data hasil wawancara dengan pengelola jaringan dan administrator website sebagai sumber informasi kualitatif mengenai kondisi keamanan jaringan dan permasalahan yang sering muncul.

d. Kebutuhan pengguna (user)

Pengguna berperan penting dalam proses pengumpulan, pemantauan, dan analisis data.

1. Administrator sistem, bertanggung jawab dalam proses instalasi, konfigurasi, dan pemantauan hasil log di dashboard Wazuh.
2. Peneliti, berperan dalam melakukan eksperimen, mencatat hasil pengamatan, serta menganalisis data log dan hasil wawancara untuk memperoleh kesimpulan penelitian.

3.5.1 Analisis Data

Data yang dianalisis dalam penelitian ini adalah data log dari aktivitas website E-Journal STMIK Palangkaraya yang dikumpulkan secara otomatis oleh sistem melalui Wazuh Agent yang terinstal diserver. Data log merupakan sebuah catatan sistem yang merekam semua kegiatan yang terjadi pada situs, baik yang dilakukan oleh pengguna maupun oleh sistem itu sendiri. Log ini berfungsi sebagai sumber utama untuk menganalisis pola trafik jaringan yang muncul selama operasional situs web.

Secara umum, data log menyimpan informasi mengenai waktu terjadinya suatu aktivitas (timestamp), alamat IP alamat IP pengguna yang mengakses, jenis aktivitas yang dilakukan, serta tanggapan yang diberikan oleh server. Waktu akses berguna untuk menentukan kapan sebuah aktivitas terjadi, sementara alamat IP berfungsi untuk mengidentifikasi sumber akses, baik dari pengguna biasa maupun dari sumber yang dianggap mencurigakan. Jenis aktivitas yang tercatat dalam log mencakup akses halaman situs web, proses login oleh pengguna, upaya login yang tidak berhasil, unggahan berkas, serta kegiatan sistem lain yang terkait dengan operasi E-Journal.

Selain mencatat aktivitas dasar, data log juga memuat informasi mengenai status respon server, seperti apakah suatu permintaan berhasil diproses atau mengalami kegagalan. Informasi ini membantu peneliti dalam melihat apakah suatu aktivitas berjalan secara normal atau menunjukkan adanya gangguan. Aktivitas autentikasi juga tercatat secara detail, termasuk jumlah percobaan login dalam

rentang waktu tertentu, yang dapat digunakan untuk mengidentifikasi pola akses yang tidak wajar.

Data log yang telah dikumpulkan kemudian diproses oleh sistem Wazuh untuk dianalisis lebih lanjut. Wazuh melakukan pemantauan terhadap pola aktivitas yang muncul dan menghasilkan peringatan (alert) apabila ditemukan aktivitas yang menyimpang dari pola normal. Contoh aktivitas yang dapat memicu peringatan antara lain percobaan login berulang dalam waktu singkat dari satu alamat IP, akses otomatis oleh bot, serta aktivitas unggah berkas yang tidak sesuai dengan pola penggunaan normal website E-Journal.

Hasil dari pemantauan dan notifikasi peringatan yang dihasilkan oleh Wazuh dapat dilihat melalui Wazuh Dashboard dalam format data log, grafik aktivitas, dan notifikasi peringatan. Informasi yang ditampilkan tersebut kemudian di analisis secara deskriptif untuk menggambarkan perbedaan karakteristik antara trafik normal dan trafik anomali. Trafik normal ditandai dengan pola akses yang wajar dan sesuai dengan aktivitas pengguna website, sedangkan trafik anomali ditandai dengan aktivitas yang tidak biasa, berulang, atau berpotensi mengganggu sistem.

Dalam penelitian ini, analisis terhadap data dilakukan tidak dengan perhitungan statistik atau pengujian spesifik, tetapi melalui interpretasi dan deskripsi dari log data serta pemberitahuan yang muncul. Metode ini diterapkan untuk mendapatkan pemahaman yang jelas mengensi keadaan jaringan trafik jaringan di website E-Journal STMIK Palangkaraya dan bagaimana sistem Wazuh

merekam serta memvisualisasikan aktivitas normal dan yang tidak bisa selama periode pengawasan.

3.5.2 Analisis Proses

Pada tahap ini penulis menjelaskan proses analisis yang diterapkan dalam studi untuk mengidentifikasi dan membedakan trafik normal (antara lalu lintas biasa) dan trafik anomali (lalu lintas tidak biasa) pada situs web utama STMIK Palangkaraya. Pelaksanaan penelitian ini memanfaatkan sistem Wazuh sebagai instrumen utama dalam pengumpulan serta analisis data log. Proses alur analisis dijelaskan sebagai berikut:

a. Pengumpulan Log (*Data Collection*)

Agen Wazuh yang sudah terpasang diserver situs E-Journal Stmik Palangkaraya bertugas mengumpulkan catatan aktivitas jaringan, mencakup permintaan pengguna, alamat IP, dan waktu akses. Informasi log menunjukkan aktivitas lalu lintas jaringan secara real-time.

b. Pengiriman Data ke Wazuh Server

Data yang dikumpulkan oleh Wazuh Agent secara otomatis dikirim keserver Wazuh untuk dianalisis lebih dalam. Tahapan ini mencakup pengiriman data yang terenkripsi agar keamanan log tetap terjaga.

c. Analisis log dan Deteksi Aktivitas

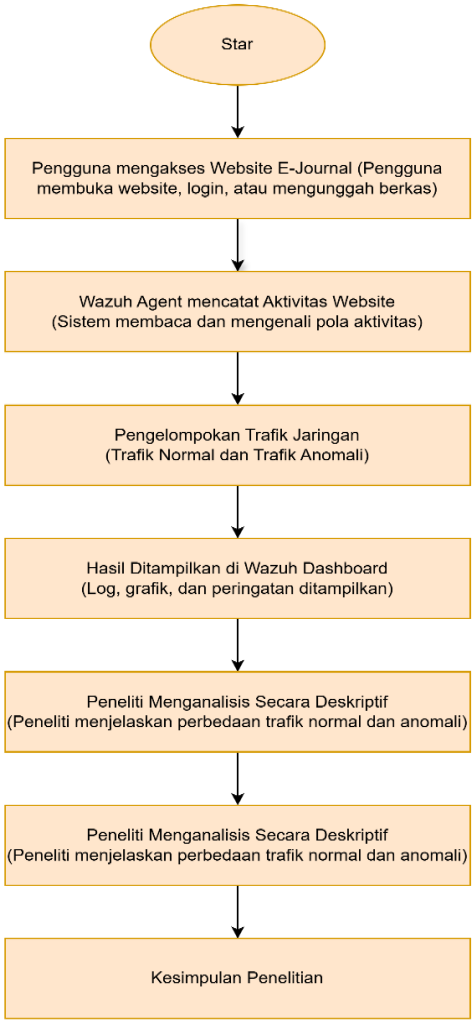
Server Wazuh memeriksa log dengan memanfaatkan aturan standar SIEM untuk mengenali pola perilaku yang mencurigakan, seperti usaha login berulang kali, peningkatan lalu lintas, atau permohonan akses yang tidak biasa.

d. Klasifikasi Trafik

Berdasarkan hasil analisis yang dilakukan, aktivitas didalam jaringan dibagi menjadi dua kategori, yaitu trafik yang normal (akses yang wajar dari pengguna) dan trafik yang tidak biasa (aktivitas yang mencurigakan atau yang berpotensi menjadi serangan).

e. Visualisasi dan Notifikasi

Hasil analisis ditampilkan melalui Wazuh Dashboard dalam bentuk grafik, daftar log, serta notifikasi (peringatan) yang muncul secara langsung. Penyajian visual ini mempermudah peneliti untuk mengenali pola lalu lintas dan memastikan akurasi dari hasil eksperimen sederhana yang telah dilakukan. Jadi proses analisis pada poin a sampai e merupakan tahapan yang saling berkaitan dan divisualisasikan berikut pada gambar 3.3 yang menggambarkan alur analisis Proses.



Gambar 3. 3 gambaran alur analisis proses

Gambar tersebut merupakan alur analisis proses trafik jaringan pada website E-Journal STMIK Palangkaraya menggunakan Wazuh. Proses dimulai ketika pengguna mengakses website E-Journal, baik untuk membuka halaman, melakukan login, maupun mengunggah berkas. Setiap aktivitas yang dilakukan pengguna secara otomatis dicatat oleh Wazuh Agent yang terpasang pada server website sebagai data log aktivitas. Data log tersebut kemudian diproses oleh sistem Wazuh untuk mengenali pola aktivitas jaringan yang terjadi. Berdasarkan hasil pemrosesan

tersebut, trafik jaringan dikelompokkan menjadi dua kategori, yaitu trafik normal yang menunjukkan aktivitas wajar pengguna dan trafik anomali yang menunjukkan aktivitas tidak biasa atau mencurigakan. Hasil pengelompokan trafik selanjutnya ditampilkan melalui Wazuh Dashboard dalam bentuk data log, grafik aktivitas, serta peringatan (alert) apabila terdeteksi aktivitas anomali. Data dan informasi yang ditampilkan pada dashboard kemudian dianalisis secara deskriptif oleh peneliti dengan menjelaskan perbedaan karakteristik antara trafik normal dan trafik anomali. Berdasarkan hasil analisis deskriptif tersebut, peneliti menyusun kesimpulan penelitian mengenai kondisi trafik jaringan pada website E-Journal STMIK Palangkaraya selama proses pengamatan.

3.6 Desain

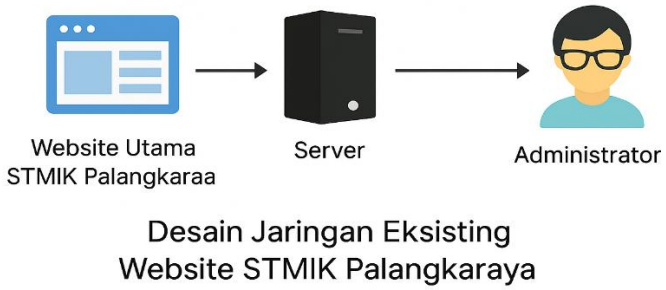
Bagian ini merupakan dari desain sistem. Beberapa hal yang diperlukan dalam desain sistem disertakan gambar dan penjelasan sebagai penunjang terkait gambar yang disajikan.

3.6.1 Desain Jaringan Eksisting STMIK Palangkaraya

Desain jaringan eksisting pada website E-Journal STMIK Palangkaraya menunjukan alur layanan masih berjalan secara sederhana, yaitu dimulai dari pengguna yang mengakses web E-Journal melalui browser. Kemudian permintaan tersebut diproses oleh server ojs yang menjadi pusat seluruh aktivitas sistem. Server ini menangani berbagai proses seperti akses artikel, login author, unggah berkas naskah, hingga aktivitas yang terjadi didalam sistem sebenarnya sudah tersimpan dalam log server, namun pemantauan masih dilakukan secara manual oleh pihak administrator STMIK.

Dalam kondisi saat ini, pengelola baru mengetahui adanya masalah setelah mendapatkan laporan dari pengguna atau setelah melakukan pemeriksaan rutin pada server. Saat ini belum ada sistem pemantauan otomatis yang bisa membaca log secara real-time, mendeteksi anomali, atau memberikan peringatan ketika ada aktivitas yang mencurigakan. Hal ini mengakibatkan beberapa ancaman potensial sulit dideteksi sejak awal, seperti adanya spam pada fomulir tertentu, munculnya tautan berbahaya seperti link yang mengarah ke judi online, pinjaman online dan iklan yang disisipan secara illegal, hingga upaya login berulang dari Alamat IP yang tidak dikenal. Selain itu trafik normal atau Tindakan bot yang berusaha mengakses halaman tertentu secara berlebihan juga tidak teridentifikasi sejak awal.

Keterbatasan ini menunjukan bahwa sistem E-Journal masih sangat bergantung pada pemantaun manual tanpa dukungan alat analisis keamanan yang terintegrasi. Oleh karena itu, keadaan eksisting ini memperkuat urgensi penerapan sistem monitoring seperti wazuh untuk membantu menganalisis trafik, memeriksa log secara otomatis, serta memberikan notifikasi saat terdeteksi aktivitas yang dapat mengancam, sehingga keamanan dan keandalan layanan publikasi ilmiah dikampus dapat diperkuat. Berikut pada Gambar 3.3 adalah menggambarkan alur hubungan antara website, server, dan administrator.

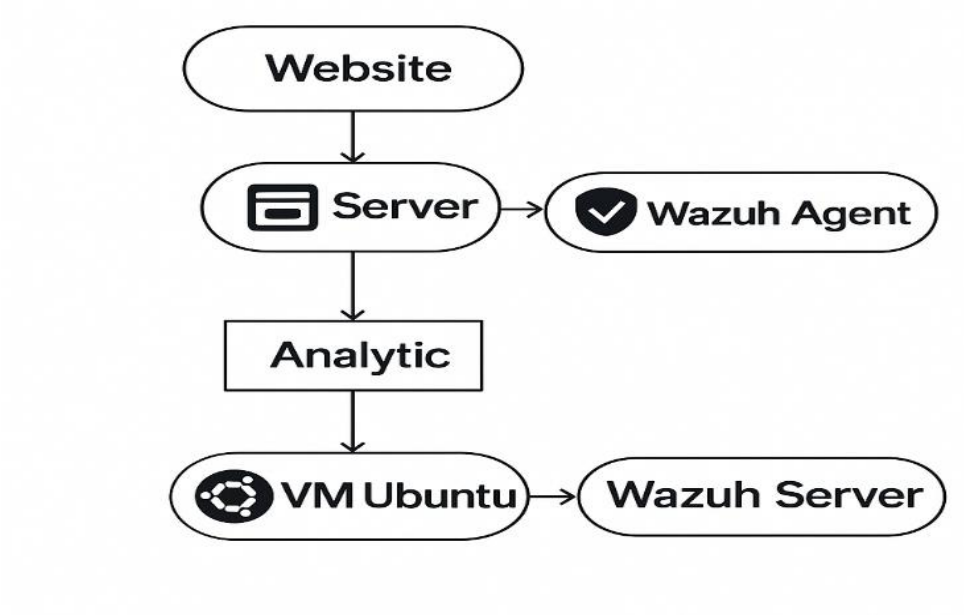


Gambar 3. 4 Desain Jaringan Eksisting STMIK Palangkaraya

3.6.2 Desain Eksisting Yang Dikaitkan Dengan Penelitian

Pada desain eksisting ini yang dikaitkan dengan penelitian struktur jaringan website STMIK tetap dipertahankan, namun ditambahkan dengan sistem pemantaun keamanan yang berbasis Wazuh untuk membantu analisis lalu lintas yang normal dan anomali. Dalam Penelitan ini Wazuh Agent dipasang pada server website untuk mengumpulkan seluruh log aktivitas, seperti permintaan *HTTP/HTTPS,* aktivitas login, kesalahan server, dan pola akses pengguna. Selanjutnya, log tersebut dikirimkan ke sistem Wazuh yang dijalankan pada lingkungan virtualisasi Ubuntu menggunakan VirtualBox. Mesin virtual ubuntu berfungsi sebagai pusat analisis melalui komponen Wazuh server yang memproses catatan, mendeteksi pola yang mencurigakan, dan mengelompokkan aktivitas menjadi trafik normal dan trafik anomali. Hasil analisis di tampilkan di Wazuh Dashboard agar administrator atau peneliti dapat memantau grafik lalu lintas, tipe ancaman, sumber IP, dan tingkat keparahan secara rieal-time. Dengan integrasi ini jaringan eksisting STMIK tidak diubah, tetapi diperkuat dengan sistem analisis

keamanan sehingga proses deteksi dini dapat dilakukan lebih cepat akurat dibandingkan pemantauan manual sebelumnya. Berikut pada Gambar 3.4 adalah desain eksisting yang dikaitkan dengan penelitian, yang menggambarkan penambahan sistem Wazuh pada jaringan website E-Journal STMIK Palangkaraya



Gambar 3. 5 Desain Eksisting Yang Dikaitkan Dengan Penelitian

3.7 Jadwal Penelitian

Jadwal penelitian ditunjutkkan dalam bentuk tabel yang berisi tahapan dalam penelitian dengan contoh seperti Tabel 3.1 dengan penyesuaian tahapan dari penelitian mahasiswa. Jadwal penelitian dapat dirincikan dengan menyertakan tahapan, tahun, bulan, dan minggu.

Tabel 3. 2 Jadwal Penelitian

No.	Tahapan	September 2025				Oktober 2025				November 2025				Desember 2025				Januari 2026				February 2026			
		I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV
1.	Pengumpulan Data (wawancara & log wazuh)																								
2.	Penerapan dan pemantauan Wazuh trafik website																								
3.	Eksperimen trafik normal dan anomali (uji respon Wazuh)																								
4.	Analisis Data																								
5.	Kesimpulan dan Rekomendasi																								

DAFTAR PUSTAKA

Abdullah, M., Jayaraman, K. & Kamal, S.B.M, 2016 A Conceptual Model of Interactive Hotel Website: The Role of Perceived Website Interactivity and Customer Perceived Value Toward Website Revisit Intention. *Procedia Economics and Finance*, 37, 370–375.

Azzah, N., Rahmadhan, D., & Sari, A., 2024. Implementasi Wazuh Menggunakan Metode PPDIOO di Sistem Keamanan Jaringan PSDKU Universitas Lampung Waykanan. *Jurnal Informatika dan Teknik Elektro Terapan*, 12(2), 4074–4085.

Buana, R., Rachdian, A., & Santoso, H., 2013. Jaringan Komputer dan Komunikasi Data*. (Buku). Jakarta: Penerbit Informatika.*

Encep, R., Suryana, A., & Fathurrahman, M., 2024. Ubuntu dan Sistem Operasi Open Source. *(Buku). Bandung: Tekno Mandiri Press.*

Faruq, A., Dharmawan, T.R., & Rustianto, A., 2024. Implementasi Wazuh SIEM untuk Manajemen Log Event di Pesantren Teknologi Informasi dan Komunikasi Jombang. *Jurnal Informatika Terpadu,* 10(2), *146-155.*

Gede Parama, I., & Rachmawati, I.D.A., 2024. Implementasi dan Analisis Wazuh sebagai Intrusion Detection System (IDS) dan Platform Monitoring. *Jurnal Informasi, Sains dan Teknologi, 7(2), 290-303.*

Indriani, A., 2018. Pembuatan Website struktur, Desain, dan Fungsi. *Jakarta: Deepublish.*

Khirdany, E.N., 2024. Efektivitas Penggunaan Website di Desa Sebagai Layanan Informasi untuk Masyarakat. *Journal of Economic and Business*, 1(1), 1–10.

Mardhiyah, L., Nugraha, B., & Setiawan, A., 2023. Analisis Sistem SIEM Aplikasi Wazuh pada Dinas Kominfo Sulawesi Selatan. *Jurnal Sistem Informasi dan Keamanan*, 5(3), 55–64.

Nugraha, H., Wijaya, S., & Kurniawan, R., 2025. Penerapan SIEM dalam Sistem Pendidikan untuk Peningkatan Deteksi Ancaman. *Jurnal Keamanan Siber*, 9(1), 12–20.

Nursi, A., Ramli, F., & Syahputra, A., 2025. *Analisis Sistem Jaringan, Konsep dan Studi Kasus*. Bandung: Informatika.

Pratama, E., 2022. Analisis Trafik Jaringan untuk Deteksi Anomali. *Jurnal Teknologi Jaringan*, 4(2), 101–110.

Punta Dewa, P., & Windarto, A., 2024. Konsep Wazuh Agent dan Komponen SIEM. *Jurnal Keamanan Sistem Informasi*, 8(1), 45–53.

Racmawati, S., 2024. Deteksi Serangan DoS dan HTTP Flood Menggunakan Wazuh. *Jurnal Siber Indonesia*, 7(2), 77–88.

Saputra, A., Dharmawan, R., & Rustianto, B. 2024. Penerapan Wazuh sebagai SIEM di Lingkungan Pendidikan. *Jurnal Informatika Terpadu*, 10(2), 146–155.

Salsabilah, A.R., Panjaitan, R.L., & Ismail, A., 2025 Pengaruh Metode Pembelajaran Eksperimen terhadap peningkatan kemampuan: *Jurnal Ilmiah Pendidikan Dasar*, 10(3), 232–247.

Kusnadi, D. 2021. Pendekatan Metode Deskriptif dalam Penelitian Pendidikan**.** *Edudikara: Jurnal Pendidikan dan Pembelajaran*, 6(1), 32–41

Yuliani, R., & Supriatna , A. 2023. *Metode Penelitian Kualitatif*. Bandung: Alfabeta

LAMPIRAN

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangka Raya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

SURAT TUGAS PEMBIMBING TUGAS AKHIR

NO. 242/STMIK-3.C.2/AU/IX/2025

Ketua Program Studi Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya menugaskan nama-nama tersebut di bawah ini :

1. Nama : Ir. Abdul Hadi, S.T., M.Kom
   NIK : 198505102021101
   Sebagai Pembimbing I dalam **PEMBUATAN PROGRAM**
2. Nama : Herkules, S.Kom., M.Cs
   NIK : 198510042010106
   Sebagai Pembimbing II dalam **PENULISAN TUGAS AKHIR**

Untuk membimbing Tugas Akhir mahasiswa :

Nama	:	RHEMA SHELVIA PUTRI
NIM	:	C2255201004
Program Studi	:	TEKNIK INFORMATIKA (55201)
Tanggal Daftar	:	19/09/2025
Judul Tugas Akhir	:	Analisis Jaringan Website STIMIK menggunakan Wazuh untuk deteksi Trafik normal dan anomali

Demikian surat ini dibuat agar dapat dipergunakan sebagaimana mestinya, dan dilaksanakan dengan penuh tanggung jawab.

Palangka Raya, 03 Oktober 2025

Ketua Program Studi,

3 Oktober 2025

Ir. Abdul Hadi, S.T., M.Kom
NIK. 198505102021101

TEMBUSAN :
1. Pembimbing I dan II
2. Mahasiswa yang bersangkutan
3. Arsip Prodi TI

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangkaraya
email : humas@stmikpik.ac.id - website : www.stmikpik.ac.id

KARTU KEGIATAN KONSULTASI TUGAS AKHIR

Nama Mahasiswa : RHEMA SHELVIA PUTRI
NIM : C2255201004
Tanggal Persetujuan Judul :
Judul Tugas Akhir : ANALISIS JARINGAN MENGGUNAKAN WAZUH UNTUK DETEKSI TRAFIK NORMAL DAN ANOMALI

No.	Tanggal Konsultasi		Uraian	Tanda Tangan
	Terima	Kembali		
1	03/10/2025		Paragraf kedua latar belakang bagian kondisi indikator adanya gangguan atau upaya penretasan ditambah atau (sitasi). Paragraf ke empat perbaikan solusi pendekatan nator monotoring < SIEM dan sitasi memper kuat latar belakang, Paragraf 6 Perbaiki penulisan, kumusan masah diperbaiki penulisan, Batas masalah a.	
2	21/11/2025		Revisi tambahkan nama gambar sebelum kemunculan gambar.	
	21/11/2025		Bab 2 tambahkan virtualisasi (virtualbox atau VM ware)	
3	23/11/2025		Desain Penelitian dibuat Flowchat dan digelarkan alur desain penelitian. dan instrument penelitian, studi dokumen (isi: hasil log wazuh yang diambil dari server Stmik, wawancara, studi pustaka	
4.	25/11/2025		Di desain Jaringan website dibagi menjadi 2 yaitu desain eksisting (Jaringan Stmik saat ini) dan desain eksisting yang dikaitkan dengan penelitian.	
5.	26/11/2025		Revisi untuk nama gambar yang sehara dibahwa gambar pada Gambar 3.2 wawancara bersama administrator Stmik Palangkaya.	

No.	Tanggal Konsultasi		Uraian	Tanda Tangan
	Terima	Kembali		
	3/12/25		ACC Seminar	
6.	12/10/2025		Revisi penulisan, typo (salah ketik) Paragraf yang tidak sesuai pedoman Stmik.	
7.	23/11/2025		beberapa kutipan belum muncul didalam daftar pustaka	
8.	24/11/2025		Revisi nama gambar sebelum kemunculan gambar, seperti berikut Gambar 2i Arsitektur	
9.	26/11/2025		Revisi daftar pustaka untuk menyesuaikan dengan pedoman Stmik.	

Menyetujui :

Dosen Pembimbing I,

.....

Dosen Pembimbing II,

.....

NASKAH WAWANCARA PENELITIAN

ANALISIS JARINGAN WEBSITE E-JOURNAL STMIK PALANGKARAYA MENGGUNAKAN WAZUH UNTUK DETEKSI TRAFIK NORMAL DAN ANOMALI

Pewawancara

Nama : Rhema Shelvia Putri

Nim : C2255201004

Program Studi : Teknik Informatika

Narasumber

Nama : Dedy Yusman, S.Kom

Jabatan : Kasbag Data dan Sistem Informasi

Instansi : STMIK Palangkaraya

Tanggal Wawancara : 07 September 2025

Daftar Pertanyaan Wawancara

1. Di STMIK Palangkaraya ada beberapa website yang membantu akses mahasiswa dan dosen untuk mengetahui informasi atau kegiatan akademik pak, nah website apa saja yang sering diakses pak?

Jawab : Masing-masing website itu fungsinya berbeda-berbeda ya, tapi yang paling sering diakses itu Website Stmikplk.ac.id, SMART Campus, Informasi Penerima Mahasiswa baru dan e-Journal.

2. Kalau soal keamanan dari beberapa website STMIK itu, ada gak yang bapak rasa paling rawan atau perlu dijaga ekstra?

Jawab : Menurut Saya yang cukup rentan keamanan nya sekarang website Stmikplk.ac.id dan e-Journal karna cukup sering mengalami masalah berupa lemot waktu di akses, bisa error karna spam pada from dan komentar serta sering ditemukan tautan yang mengarah kesitus judi online atau iklan yang mengindikasi adanya potensi akses tidak sah dan juga itu sering ada IP yang mencoba login secara berulang terhadap sistem. Menurut hal itu bisa sangat berpontesi membahayakan keamanan sistem website.

3. Biasanya kalau ada masalah disalah satu website biasanya bapak tahu nya dari laporan orang atau dari pemantauan sistem dan cara penanganannya gimana pak?

Jawab : Dari pemantauan sistem dicek rutin dan juga laporan. Kalau penanganannya itu diblok IP dan Injection Kode lalu cek dilog aktivitas.

4. Menurut Bapak website yang cocok untuk saya melakukan penelitian dalam TA saya dengan topik menganalisis jaringan website STMIK menggunakan Wazuh sebagai tools untuk deteksi trafik normal dan anomali, kira kira website yang mana ya pak?

Jawab : Menurut saya ada dua ya, stmikplk.ac.id website utama dan e-Journal tapi mungkin bisa dicoba website di e-Journal (ojs.stmikplk.ac.id).

5. Ada alat khusus kah pak yang bisa dipakai buat dilihat aktivitas atau trafik pengunjung nya di website?

Jawab : Ada Dibagian pengunjung.

Palangkaraya 07 September 2025

Kasbag Data & Sistem Informasi

Dedy Yusman, S.Kom

Lampiran Dokumentasi



Wawancara dengan Kasbag Data dan Sistem Informasi

Bapak Dedy Yusman, S.Kom