LAPORAN KERJA PRAKTEK

DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KABUPATEN BENGKALIS

IMPLEMENTASI *THREAT HUNTING* DAN PEMANTAUAN *FILE INTEGRITY MONITORING* MENGGUNAKAN *WAZUH* DI DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN BENGKALIS

Rimba Dirgantara
6404211035

PROGRAM STUDI
SARJANA TERAPAN KEAMANAN SISTEM INFORMASI
JURUSAN TEKNIK INFORMATIKA
POLITEKNIK NEGERI BENGKALIS
BENGKALIS
2025

LEMBAR PENGESAHAN
LAPORAN KERJA PRAKTEK
DINAS KOMUNIKASI INFORMATIKA DAN STATISTIK
KABUPATEN BENGKALIS

Ditulis sebagai salah satu syarat untuk menyelesaikan Kerja Praktek

Rimba Dirgantara
6404211035

Bengkalis, 27 Juni 2025

Kepala Seksi Aplikasi
Dinas Komunikasi, Informatika
dan Statistik Bengkalis

Andi Setiawan, S.T
NIP. 19[illegible]20100111014

Dosen Pembimbing
Program Studi Keamanan
Sistem Informasi

Mansur, M.Kom
NIP. 198209192021211003

Disetujui
Ka. Prodi Keamanan Sistem Informasi

Nurmi Hidayasari, ST., M.Kom
NIP. 199109012022032006

KATA PENGHANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa yang telah memberikan rahmat dan karunia-Nya sehingga penulis menyelesaikan laporan kerja praktek ini. Laporan Kerja Praktek ini berjudul Perancangan dan "Impementasi *Threat Hunting* dan Pemantauan *File Integrity Monitoring* Menggunakan *Wazuh* Di Dinas Komunikasi Dan Informatika Kabupaten Bengkalis". Laporan ini disusun untuk memenuhi salah satu persyaratan dalam menyelesaikan kerja praktek. Ini telah penulis laksanakan di Kantor Dinas Komunikasi, Informatika dan Statistik Kabupaten Bengkalis, yang beralamat di Jl. Kartini, Bengkalis Kota, Kecamatan Bengkalis Riau 28711.

Pada kesempatan ini, penulis mengucapkan terima kasih kepada kedua orang tua yang telah membantu penulis berupa finansial serta doa yang diberikan dari awal hingga selesainya laporan ini. Selanjutnya tidak lupa penulis ucapkan terima kasih terhadap pihak-pihak yang membantu penulis dalam mendukung menyelesaikan laporan kerja praktek ini, antara lain:

1. Tuhan Yang Maha Esa telah memberikan nikmat dan hidayah-Nya.
2. Bapak Johny Custer, ST., M.T., selaku Direktur Politeknik Negeri Bengkalis.
3. Bapak Kasmawi, M.Kom., selaku Ketua Jurusan Teknik Informatika Politeknik Negeri Bengkalis.
4. Ibu Nurmi Hidayasari, ST., M.Kom., Selaku Kepala Program Studi Sarjana Terapan Keamanan Sistem Informasi, Politeknik Negeri Bengkalis.
5. Ibu Rezki Kurniawati, M. Kom., Selaku Koordinator Kerja Praktek dari Prodi Keamanan Sistem Informasi.
6. Bapak Mansur, M.Kom., selaku Dosen Pembimbing saya, saya mengucapkan terima kasih atas kesediaan membagi ilmu, memberikan arahan dan meluangkan waktu dalam membimbing saya selama proses penyusunan laporan kerja praktek ini.

7. Seluruh Bapak dan Ibu Dosen di Jurusan Teknik Informatika Politeknik Negeri Bengkalis yang telah memberikan dukungan selama saya melaksanakan Kerja Praktek.
8. Bapak Dr. H. Suwarto, S.Pd., M.Pd., selaku Kepala Dinas Komunikasi Informatika dan Statistik Kabupaten Bengkalis.
9. Bapak Zulkifli, ST., selaku Kepala Bidang PBE Dinas Komunikasi Informatika dan Statistik Kabupaten Bengkalis.
10. Bapak Andri Irawan, ST., selaku Kepala Seksi Insfrastruktur dan Teknologi serta Pembimbing Lapangan Dinas Komunikasi Informatika dan Statistik Kabupaten Bengkalis.
11. Bapak Wibowo, Agus, Heri, Boy, Udin dan Ibu Laili sebagai senior dan rekan yang membantu selama kerja di lapangan.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang Pemikiran KP

Di era globalisasi dan perkembangan teknologi informasi yang semakin pesat, kebutuhan akan sumber daya manusia yang terampil dan kompeten menjadi sangat penting. Pendidikan tinggi, khususnya di lembaga pendidikan kejuruan, memiliki peran strategis dalam mempersiapkan mahasiswa untuk menghadapi tantangan di dunia kerja. Salah satu cara untuk mencapai tujuan tersebut adalah melalui kegiatan Kerja Praktek (KP), yang memberikan kesempatan bagi mahasiswa untuk menerapkan teori yang telah dipelajari dalam situasi nyata [1].

Kerja Praktek merupakan bagian integral dari kurikulum yang dirancang untuk memberikan pengalaman praktis kepada mahasiswa. Melalui kegiatan ini, mahasiswa tidak hanya memperoleh wawasan mengenai dunia industri, tetapi juga meningkatkan keterampilan dan kemampuan memecahkan masalah yang diperlukan dalam lingkungan kerja [2]. Dalam konteks ini, penulis melaksanakan Kerja Praktek di Dinas Komunikasi Informasi dan Statistik (Diskominfo) Bengkalis.

Permasalahan yang terjadi di bidang sistem keamanan informasi adalah belum optimalnya penerapan langkah-langkah keamanan siber terhadap aset digital instansi, khususnya pada *subdomain* yang dimiliki. Berdasarkan hasil observasi dan uji keamanan (*penetration testing*) yang dilakukan, ditemukan bahwa beberapa *subdomain* belum memiliki perlindungan yang memadai terhadap berbagai potensi serangan, seperti serangan injeksi, pengungkapan informasi sensitif, hingga kerentanan terhadap teknik enumerasi. Hal ini disebabkan oleh kurangnya proses audit keamanan secara berkala dan tidak adanya sistem monitoring yang terpusat. Akibatnya, *subdomain-subdomain* tersebut menjadi titik lemah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mengakses sistem internal secara ilegal, mencuri data, maupun melakukan sabotase. Kondisi ini berisiko mengganggu integritas dan kerahasiaan informasi yang dikelola oleh

instansi, serta berdampak pada menurunnya kepercayaan publik terhadap sistem layanan pemerintahan berbasis digital.

1.2 Tujuan dan Manfaat KP

Pelaksanaan Kerja Praktek (KP) memiliki beberapa tujuan dan manfaat penting bagi mahasiswa dalam mengembangkan kompetensi akademik maupun profesional.

Tujuan:

1. Mengaplikasikan Ilmu yang Telah Dipelajari

   Memberikan kesempatan kepada mahasiswa untuk menerapkan teori dan pengetahuan yang telah diperoleh selama perkuliahan ke dalam situasi nyata di dunia kerja.
2. Mengenal Dunia Kerja Secara Langsung

   Memperkenalkan mahasiswa pada lingkungan kerja profesional serta memahami struktur organisasi, budaya kerja dan sistem kerja yang berlaku di instansi atau perusahaan.
3. Meningkatkan Kompetensi Profesional

   Melatih mahasiswa untuk menyelesaikan permasalahan teknis di lapangan, mengambil keputusan dan bertanggung jawab terhadap tugas yang diberikan.

Manfaat:

1. Pengembangan Keterampilan

   Membantu mahasiswa mengembangkan keterampilan teknis (*hard skills*) dan keterampilan interpersonal (*soft skills*), seperti komunikasi, manajemen waktu dan pemecahan masalah.
2. Pengalaman Kerja

   Memberikan pengalaman langsung mengenai cara kerja di dunia instansi pemerintahan, serta meningkatkan kesiapan mahasiswa dalam memasuki dunia kerja setelah lulus.

3. Wawasan dan Jaringan Profesional

   Menambah wawasan mengenai tantangan dan peluang di bidang studi yang ditekuni, serta membuka peluang untuk membangun jaringan profesional dengan praktisi di lapangan.

1.3 Luaran Proyek Kerja Praktek

Luaran dari proyek kerja praktik ini merupakan hasil nyata dari proses implementasi sistem keamanan menggunakan *Wazuh* yang akan diserahkan kepada instansi tempat kerja praktik untuk dimanfaatkan lebih lanjut. Adapun luaran proyek yang dihasilkan adalah sebagai berikut:

1. Implementasi *Wazuh Server* dan *agent*

   Telah berhasil diterapkan sistem *Wazuh* pada lingkungan *server* dan *endpoint* yang ditentukan, mencakup instalasi, konfigurasi awal, serta pengujian fungsi dasar.
2. Pemantauan Keamanan Sistem (*Threat Hunting*)

   Konfigurasi dasar untuk mendeteksi aktivitas berisiko seperti serangan *brute force SSH*, *SQL injection*, dan *XSS* melalui integrasi dengan *log* sistem.
3. *File Integrity Monitoring* (*FIM*)

   Konfigurasi modul FIM untuk memantau perubahan pada *file* sensitif di *server*, guna mendeteksi adanya modifikasi yang mencurigakan.
4. Dokumentasi konfigurasi dan panduan penggunaan *Wazuh*

   Berisi langkah-langkah instalasi, konfigurasi, serta panduan penggunaan *Wazuh*, yang dapat digunakan oleh tim teknis instansi sebagai referensi.

BAB II
GAMBARAN UMUM DINAS KOMUNIKASI DAN INFORMATIKA BENGKALIS

2.1 Sejarah Singkat Dinas Komunikasi Dan Informatika Bengkalis

Dinas Komunikasi Informasi dan Statistik (Dinas Komunikasi Dan Informatika) merupakan lembaga yang memiliki peran penting dalam pengelolaan komunikasi dan informasi di Kabupaten Bengkalis. Sebelumnya, urusan komunikasi dan informasi ini berada di bawah Dinas Perhubungan. Namun, berdasarkan Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah, serta Peraturan Menteri Komunikasi dan Informatika Nomor 14 Tahun 2016 tentang Pedoman Nomenklatur Perangkat Daerah di Bidang Komunikasi dan Informatika, Dinas Komunikasi Dan Informatika kini berdiri sendiri [2].

Keberadaan Dinas Komunikasi Dan Informatika diperkuat oleh Peraturan Bupati Bengkalis Nomor 51 Tahun 2016, yang mengatur kedudukan, susunan organisasi, eselonering, tugas dan tata kerja. Saat ini, kantor Dinas Komunikasi Dan Informatika berlokasi di gedung eks Dinas Pasar dan Kebersihan.

Setelah penggabungan, Dinas Pasar dan Kebersihan melebur dengan Dinas Perdagangan dan Perindustrian untuk urusan pasar, sedangkan urusan kebersihan bergabung dengan Dinas Lingkungan Hidup. Dengan perubahan ini, Dinas Komunikasi Dan Informatika memiliki cakupan tugas dan fungsi yang lebih luas, termasuk penambahan urusan statistik. Bagian Pengelolaan Data Elektronik (PDE) yang sebelumnya berada di Sekretariat Daerah kini menjadi bagian dari Dinas Komunikasi Dan Informatika, bersama dengan urusan *public relations* yang ditangani oleh Humas Sekretariat Daerah.

Pada tahun 2018, terjadi perubahan dalam susunan organisasi Dinas Komunikasi Dan Informatika, di mana Layanan Pengadaan Secara Elektronik (LPSE) tidak lagi menjadi salah satu tugas dan fungsi Dinas ini. Perubahan ini diatur dalam Peraturan Bupati Nomor 58 Tahun 2018, yang mengubah Peraturan Bupati Bengkalis Nomor 52 Tahun 2016 mengenai Kebutuhan Susunan Organisasi,

Eselonering, Tugas, Fungsi dan Uraian Tugas serta Tata Kerja. Dengan perkembangan yang terus berlanjut, Dinas Komunikasi Dan Informatika berkomitmen untuk meningkatkan pelayanan publik melalui pengelolaan informasi dan komunikasi yang efektif, serta mendukung pembangunan daerah yang lebih baik.

2.2 Visi dan Misi Dinas Komunikasi Dan Informatika Bengkalis

2.2.1 Visi

Terwujudnya Kabupaten Bengkalis yang Bermarwah, Maju dan Sejahtera.

2.2.2 Misi

1. Pengelolaan Potensi Keuangan dan Sumber Daya: Mewujudkan pengelolaan potensi keuangan daerah, sumber daya alam dan sumber daya manusia yang efektif untuk memajukan perekonomian Kabupaten Bengkalis.
2. Reformasi Birokrasi dan Penguatan Nilai: Mewujudkan reformasi birokrasi serta penguatan nilai-nilai agama dan budaya Melayu menuju tata kelola pemerintahan yang baik dan masyarakat yang berkarakter.
3. Penyediaan Infrastruktur Berkualitas: Mewujudkan penyediaan infrastruktur yang berkualitas dan mengembangkan potensi wilayah perbatasan untuk kesejahteraan rakyat.

2.3 Struktur Organisasi Dinas Komunikasi Dan Informatika Bengkalis

Struktur organisasi pada Dinas Komunikasi Dan Informatika Kabupaten Bengkalis disusun sesuai dengan ketentuan yang berlaku, dengan memperhatikan fungsi, kewajiban dan tanggung jawab dari masing-masing bagian di setiap bidang. Hal ini bertujuan untuk memastikan efektivitas dan efisiensi dalam pelaksanaan tugas dan fungsi Dinas. Berikut ini adalah struktur organisasi Dinas Komunikasi Dan Informatika bengkalis.

Gambar 2. 1 Struktur Organisasi Dinas Komunikasi Dan Informatika Bengkalis

2.4 Ruang Lingkup Dinas Komunikasi Dan Informatika Kabupaten Bengkalis

Dinas Komunikasi dan Informatika Kabupaten Bengkalis adalah instansi yang berfokus pada bidang komunikasi, statistik, dan informatika. Salah satu bidang yang ada di dalamnya adalah Pengelolaan Berbasis Elektronik (*PBE*), yang menyediakan pelayanan publik melalui pengadaan layanan elektronik. Bidang *PBE* juga bertanggung jawab atas pengembangan aplikasi untuk dinas, sekolah dan organisasi lainnya. Berikut adalah produk-produk yang telah dihasilkan:

1. Aplikasi zonasi sekolah berbasis *web*

   Aplikasi ini mendukung sistem zonasi sekolah, di mana calon peserta didik diwajibkan mendaftar di sekolah terdekat dari domisili mereka. Masyarakat Kabupaten Bengkalis dapat mengakses informasi dan melakukan pendaftaran secara *online*.
2. Aplikasi informasi bapokting berbasis *web* dan *android*

   Aplikasi Informasi Bahan Pokok dan Bahan Penting ini memberikan layanan informasi harga barang pokok dan kebutuhan lainnya kepada masyarakat. Dengan aplikasi ini, pengguna dapat dengan mudah

mendapatkan informasi terkait fluktuasi harga. Aplikasi ini dapat diakses di bapokting.bengkaliskab.go.id dan versi Android dapat diunduh melalui *Google Play Store*.

3. *WebGIS*

   Aplikasi pemetaan digital ini memanfaatkan internet untuk menyediakan informasi dalam bentuk teks dan peta. *WebGIS* menyajikan informasi mengenai tempat wisata, *SKPD*, transportasi, penginapan, *WiFi* gratis, kuliner, *UMKM*, RS & Puskesmas, sekolah, SPBU, dan *CCTV*.

4. *KIM* (Kelompok Informasi Masyarakat)

   Website resmi ini menyediakan informasi publik melalui berbagai media, termasuk *website*, *email* dan faksimili. Informasi yang tersedia meliputi berita terkini, data KIM dan informasi wisata.

5. *Website* Bengkalis

   Website ini berfungsi sebagai fasilitas pelayanan publik, memudahkan masyarakat dalam mengakses informasi berita, pengumuman dan kegiatan pemerintahan Kabupaten Bengkalis. *Website* ini dapat diakses di https://www.bengkaliskab.go.id.

6. *E-office*

   Sistem aplikasi ini membantu tata kelola keuangan berbasis elektronik, khususnya dalam pembuatan laporan keuangan di Dinas Komunikasi, Informasi dan Statistik Kabupaten Bengkalis.

7. *CCTV* penyebrangan Bengkalis - Sungai Selari

   Aplikasi ini menyediakan informasi antrian kendaraan di Pelabuhan *Roro* Bengkalis dan Pelabuhan *Roro* Pakning. *CCTV* ini dapat diakses di https://cctv.bengkaliskab.go.id.

BAB III
BIDANG PEKERJAAN SELAMA KP

3.1 Uji Keamanan Sistem Informasi

Tugas selanjutnya dalam kegiatan kerja praktek adalah melaksanakan proses uji keamanan atau penetration testing terhadap 50 *subdomain* yang telah ditentukan sebelumnya. Kegiatan ini bertujuan untuk mengidentifikasi potensi celah keamanan (*vulnerabilities*) yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan serangan siber, seperti *SQL Injection*, pemaparan direktori sensitif dan manipulasi permintaan *HTTP*. Proses pengujian dilakukan secara bertahap dengan menggunakan lima alat utama, yaitu *Firefox Browser*, *BurpSuite* (*Community Edition*), *SQLMap* dan FFUF (*Fuzz Faster U Fool*) dan *Wazuh*.
Berikut merupakan penjelasan rinci dari masing-masing alat yang digunakan:

1. *Firefox browser*

   Firefox digunakan sebagai salah satu media utama untuk melakukan eksplorasi awal terhadap antarmuka pengguna (*user interface*) dari setiap *subdomain* yang diuji. Dengan memanfaatkan *browser* ini, saya dapat memastikan bahwa halaman *web* dapat dimuat dengan benar serta mengamati struktur dasar dari aplikasi *web*, seperti parameter yang digunakan dalam *URL*, bentuk *input form* dan *cookie* yang aktif. Selain itu, penggunaan *Firefox* juga memungkinkan integrasi dengan berbagai *developer tools* dan ekstensi keamanan tambahan yang berguna untuk analisis lebih lanjut [3].

Gambar 3. 1 *Firefox*

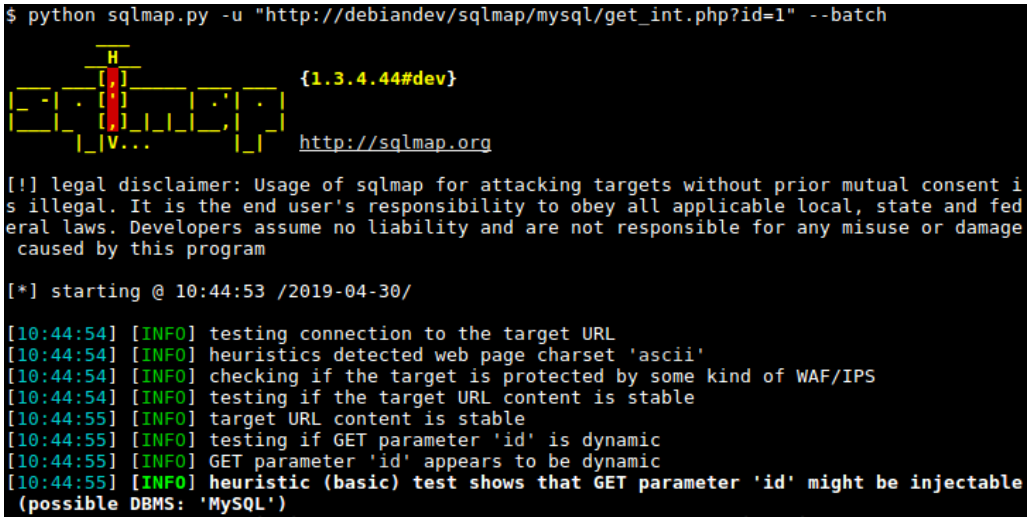
2. *BurpSuite (Community Edition)*

   BurpSuite merupakan salah satu alat penting dalam proses *penetration testing* karena mampu bertindak sebagai *intercepting proxy* antara *browser* dan *web server*. Dengan menggunakan *BurpSuite*, saya dapat menganalisis, memodifikasi dan memanipulasi permintaan *HTTP* dan *respons* yang diterima dari *server*. Hal ini sangat berguna dalam proses pengujian parameter *input* untuk mendeteksi adanya kerentanan seperti *SQL Injeciton*, *XSS* atau manipulasi otentikasi. Selain itu, *BurpSuite* juga dilengkapi fitur *Repeater*, *Intruder* dan *Decoder* yang mempermudah eksplorasi lebih dalam terhadap respons sistem [4].

Gambar 3. 2 *BurpSuite*

3. *SQLMap*

   SQLMap adalah alat *open-source* yang sangat efektif dan efisien dalam mengidentifikasi serta mengeksploitasi kerentanan *SQL Injection* pada aplikasi *web*. Alat ini ditulis menggunakan bahasa pemrograman *Python*, sehingga dapat dijalankan pada berbagai sistem operasi yang telah terinstal *interpreter python*. Dalam konteks tugas ini, *SQLMap* digunakan untuk melakukan serangkaian pengujian otomatis terhadap parameter *input* yang rentan, serta memungkinkan proses ekstraksi data dari basis data jika ditemukan celah yang dapat dimanfaatkan. *SQLMap* juga mendukung pembuatan laporan dalam format seperti *CSV* dan *JSON*, sehingga memudahkan dokumentasi hasil pengujian [4].



Gambar 3. 3 *SQLMAP*

4. *FFuF*

   FFUF adalah alat berbasis *command-line* yang dirancang untuk melakukan *fuzzing* atau *brute-forcing* terhadap direktori, *file* atau parameter tersembunyi dalam suatu aplikasi *web*. Dalam pengujian ini, *FFUF* digunakan untuk mengirimkan sejumlah besar permintaan dengan variasi *path* berdasarkan *wordlist* tertentu dengan tujuan menemukan jalur atau *file* yang tidak terindeks oleh sistem tetapi dapat diakses secara langsung. Informasi ini penting untuk mengidentifikasi potensi kebocoran data atau titik masuk (*entry point*) yang tidak diinginkan [5].

Setelah seluruh proses pengujian keamanan selesai dilakukan, saya menyusun hasil temuan dalam bentuk tabel rekap yang berisi informasi dari setiap *subdomain*. Informasi tersebut mencakup nama *subdomain*, status keamanan yang ditemukan. Dokumentasi ini bertujuan untuk memberikan gambaran singkat mengenai kondisi keamanan sistem serta menjadi dasar dalam perencanaan tindak lanjut perbaikan dan penguatan keamanan informasi di lingkungan instansi.

Tabel 3. 1 Rekap Hasil *Penetration Testing*

No	Domain	Status
1	bengkaliskab.go.id	Tidak Memiliki Celah
2	absensiuat.bengkaliskab.go.id	Tidak Memiliki Celah
3	api-simpel.dukcapil.bengkaliskab.go.id	Tidak Memiliki Celah
4	balitbang.bengkaliskab.go.id	Tidak Memiliki Celah
5	bapenda.bengkaliskab.go.id	Tidak Memiliki Celah
6	bapokting.bengkaliskab.go.id	Tidak Memiliki Celah
7	bappeda.bengkaliskab.go.id	Tidak Memiliki Celah
8	bestie.bengkaliskab.go.id	Tidak Memiliki Celah
9	bkpp.bengkaliskab.go.id	Tidak Memiliki Celah
10	bpbd.bengkaliskab.go.id	Memiliki Celah
11	bpkad.bengkaliskab.go.id	Tidak Memiliki Celah
12	camatbandarlaksamana.bengkaliskab.go.id	Memiliki Celah
13	camatbantan.bengkaliskab.go.id	Tidak Memiliki Celah
14	camatbathinsolapan.bengkaliskab.go.id	Tidak Memiliki Celah
15	camatbengkalis.bengkaliskab.go.id	Tidak Memiliki Celah
16	camatbukitbatu.bengkaliskab.go.id	Tidak Memiliki Celah
17	camatmandau.bengkaliskab.go.id	Tidak Memiliki Celah
18	camatpinggir.bengkaliskab.go.id	Tidak Memiliki Celah
19	camatrupat.bengkaliskab.go.id	Tidak Memiliki Celah
20	camatrupatutara.bengkaliskab.go.id	Memiliki Celah
21	camatsiakkecil.bengkaliskab.go.id	Memiliki Celah
22	camattalangmuandau.bengkaliskab.go.id	Tidak Memiliki Celah
23	cctv.bengkaliskab.go.id	Tidak Memiliki Celah
24	corona.bengkaliskab.go.id	Tidak Memiliki Celah
25	cpanel2.bengkaliskab.go.id	Tidak Memiliki Celah
26	damkar.bengkaliskab.go.id	Tidak Memiliki Celah
27	dashboard.bengkaliskab.go.id	Tidak Memiliki Celah
28	desaku.bengkaliskab.go.id	Tidak Memiliki Celah
29	dinkes.bengkaliskab.go.id	Tidak Memiliki Celah
30	disperindag.bengkaliskab.go.id	Tidak Memiliki Celah
31	dishub.bengkaliskab.go.id	Tidak Memiliki Celah
32	diskominfotik.bengkaliskab.go.id	Memiliki Celah
33	dlh.bengkaliskab.go.id	Tidak Memiliki Celah
34	dprd.bengkaliskab.go.id	Tidak Memiliki Celah

No	Domain	Status
35	e-antrian.bengkaliskab.go.id	Tidak Memiliki Celah
36	e-mtq.bengkaliskab.go.id	Memiliki Celah
37	epinter.bengkaliskab.go.id	Memiliki Celah
38	inspektorat.bengkaliskab.go.id	Tidak Memiliki Celah
39	jdih.bengkaliskab.go.id	Memiliki Celah
40	kesbangpol.bengkaliskab.go.id	Tidak Memiliki Celah
41	kemenag.bengkaliskab.go.id	Tidak Memiliki Celah
42	koperasiukm.bengkaliskab.go.id	Tidak Memiliki Celah
43	mikoumkm.bengkaliskab.go.id	Tidak Memiliki Celah
44	ppdb.bengkaliskab.go.id	Tidak Memiliki Celah
45	prokopim.bengkaliskab.go.id	Memiliki Celah
46	pupr.bengkaliskab.go.id	Tidak Memiliki Celah
47	puskesmasdurikota.bengkaliskab.go.id	Tidak Memiliki Celah
48	puskesmasmuarabasung.bengkaliskab.go.id	Tidak Memiliki Celah
49	puskesmasdurikota.bengkaliskab.go.id	Tidak Memiliki Celah
50	puskesmasmuarabasung.bengkaliskab.go.id	Tidak Memiliki Celah

Dari lima puluh *subdomain* terdapat sembilan *subdomain* yang miliki kerentanan, kerentanan tersebut terdiri dari *SQL Injection*, *IDOR*, *Sensitive Data Exposure*. Oleh karena itu, sangat dibutuhkan adanya monitoring keamanan terpusat untuk memantau secara *real-time* potensi serangan, mendeteksi aktivitas mencurigakan, serta memberikan peringatan dini agar tindakan mitigasi dapat dilakukan dengan cepat dan efektif. Sistem monitoring ini juga akan membantu tim keamanan dalam melakukan audit, investigasi insiden dan pemeliharaan terhadap sistem yang rentan.

5. *Wazuh*

   Wazuh merupakan sebuah *platform* keamanan berbasis *open-source* yang dirancang untuk melakukan pemantauan (*monitoring*), deteksi ancaman (*threat detection*), respon insiden (*incident response*), serta analisis keamanan secara *real-time*. *Platform* ini banyak digunakan oleh profesional di bidang keamanan siber karena fleksibilitas dan skalabilitasnya dalam mengelola dan menganalisis data *log* dari berbagai sistem dan perangkat jaringan [6]. Beberapa fitur unggulan yang dimiliki oleh *Wazuh* meliputi:

1. *File integrity monitoring* (FIM)

   Memantau perubahan pada *file* sistem, fitur ini penting untuk mendeteksi potensi modifikasi berbahaya.

2. *Log data analysis*

   Mengumpulkan dan menganalisis data *log* dari berbagai sumber untuk mendeteksi aktivitas mencurigakan.

3. *Intrusion detection system*

   Mendeteksi tanda-tanda serangan seperti *brute force*, *port scanning* dan aktivitas mencurigakan lainnya.

4. *Agent-based monitoring*

   Menggunakan *agent* yang dipasang di *endpoint* untuk mengirimkan *data* ke *server Wazuh* secara aman dan terenskripsi.

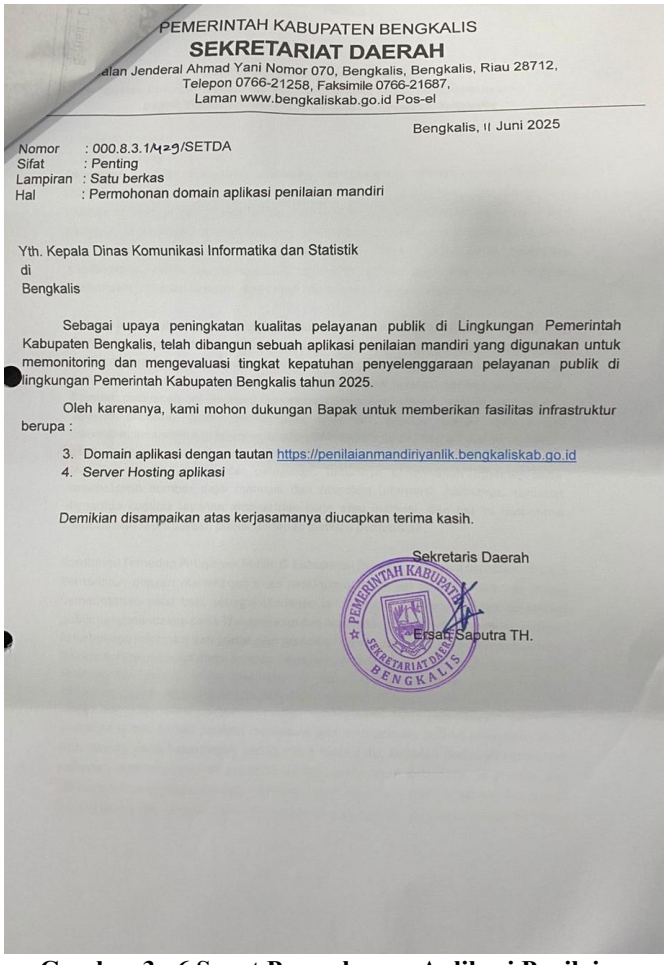
Gambar 3. 4 *Wazuh*

3.2 *Scan* Dokumen

Saya bertanggung jawab untuk melakukan proses pemindaian dokumen ke dalam format *.pdf* sesuai dengan permintaan dengan menggunakan perangkat pemindai *Brother* (*Brother scanner*) untuk memastikan hasil *scan* berkualitas dan sesuai standar yang dibutuhkan.

Gambar 3. 5 *Scanner*

Beberapa surat yang saya *scanning* dengan alat *Brother Scanner*.



PEMERINTAH KABUPATEN BENGKALIS
SEKRETARIAT DAERAH
Jalan Jenderal Ahmad Yani Nomor 070, Bengkalis, Bengkalis, Riau 28712,
Telepon 0766-21258, Faksimile 0766-21687,
Laman www.bengkaliskab.go.id Pos-el

Bengkalis, 11 Juni 2025

Nomor : 000.8.3.1/429/SETDA
Sifat : Penting
Lampiran : Satu berkas
Hal : Permohonan domain aplikasi penilaian mandiri

Yth. Kepala Dinas Komunikasi Informatika dan Statistik
di
Bengkalis

Sebagai upaya peningkatan kualitas pelayanan publik di Lingkungan Pemerintah Kabupaten Bengkalis, telah dibangun sebuah aplikasi penilaian mandiri yang digunakan untuk memonitoring dan mengevaluasi tingkat kepatuhan penyelenggaraan pelayanan publik di lingkungan Pemerintah Kabupaten Bengkalis tahun 2025.

Oleh karenanya, kami mohon dukungan Bapak untuk memberikan fasilitas *infrastruktur* berupa :

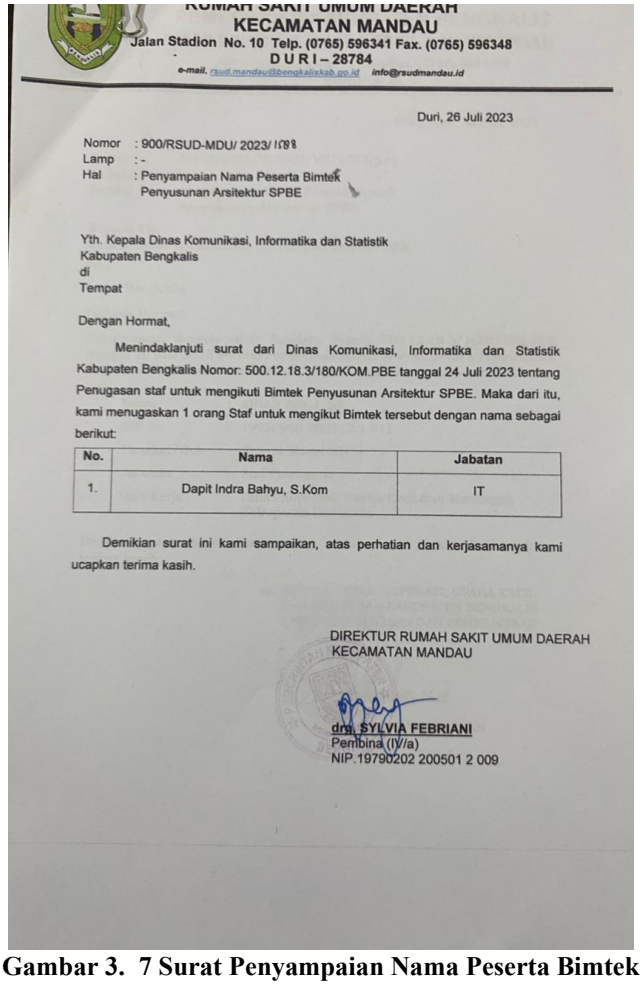
3. Domain aplikasi dengan tautan https://penilaianmandiriyanlik.bengkaliskab.go.id
4. *Server Hosting aplikasi*

Demikian disampaikan atas kerjasamanya diucapkan terima kasih.

Sekretaris Daerah

Ersan Saputra TH.

Gambar 3. 6 Surat Permohonan Aplikasi Penilaian Mandiri



RUMAH SAKIT UMUM DAERAH
KECAMATAN MANDAU
Jalan Stadion No. 10 Telp. (0765) 596341 Fax. (0765) 596348
D U R I – 28784
e-mail. rsud.mandau@bengkaliskab.go.id info@rsudmandau.id

Duri, 26 Juli 2023

Nomor : 900/RSUD-MDU/ 2023/ 1088
Lamp : -
Hal : Penyampaian Nama Peserta Bimtek Penyusunan Arsitektur SPBE

Yth. Kepala Dinas Komunikasi, Informatika dan Statistik
Kabupaten Bengkalis
di
Tempat

Dengan Hormat,

Menindaklanjuti surat dari Dinas Komunikasi, Informatika dan Statistik Kabupaten Bengkalis Nomor: 500.12.18.3/180/KOM.PBE tanggal 24 Juli 2023 tentang Penugasan staf untuk mengikuti Bimtek Penyusunan Arsitektur SPBE. Maka dari itu, kami menugaskan 1 orang Staf untuk mengikut Bimtek tersebut dengan nama sebagai berikut:

No.	Nama	Jabatan
1.	Dapit Indra Bahyu, S.Kom	IT

Demikian surat ini kami sampaikan, atas perhatian dan kerjasamanya kami ucapkan terima kasih.

DIREKTUR RUMAH SAKIT UMUM DAERAH
KECAMATAN MANDAU

drs. SYLVIA FEBRIANI
Pembina (IV/a)
NIP.19790202 200501 2 009

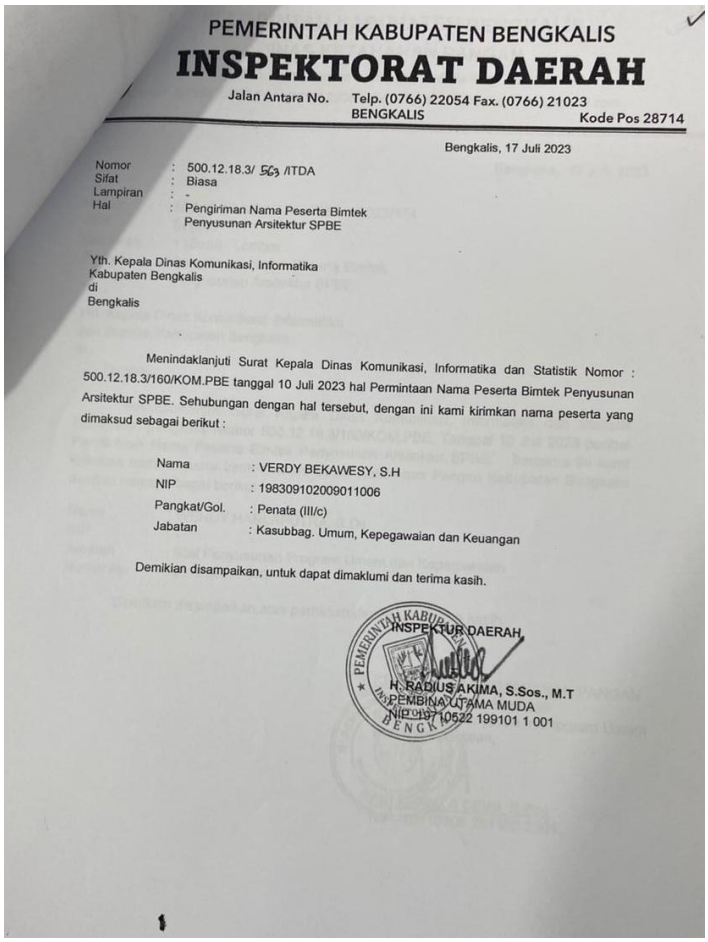
Gambar 3. 7 Surat Penyampaian Nama Peserta Bimtek Penyusunan Arsitektur SPBE

3.3 *Fotocopy*

Saya bertanggung jawab untuk melakukan fotokopi dokumen sesuai permintaan, serta memastikan hasil salinan memiliki kualitas yang baik, tersusun rapi dan sesuai dengan jumlah yang dibutuhkan.

Gambar 3. 8 Mesin *Fotocopy*

Surat yang saya *Fotocopy*.



PEMERINTAH KABUPATEN BENGKALIS

INSPEKTORAT DAERAH

Jalan Antara No. Telp. (0766) 22054 Fax. (0766) 21023
BENGKALIS Kode Pos 28714

Bengkalis, 17 Juli 2023

Nomor : 500.12.18.3/ 563 /ITDA
Sifat : Biasa
Lampiran : -
Hal : Pengiriman Nama Peserta Bimtek Penyusunan Arsitektur SPBE

Yth. Kepala Dinas Komunikasi, Informatika
Kabupaten Bengkalis
di
Bengkalis

Menindaklanjuti Surat Kepala Dinas Komunikasi, Informatika dan Statistik Nomor : 500.12.18.3/160/KOM.PBE tanggal 10 Juli 2023 hal Permintaan Nama Peserta Bimtek Penyusunan Arsitektur SPBE. Sehubungan dengan hal tersebut, dengan ini kami kirimkan nama peserta yang dimaksud sebagai berikut :

Nama : VERDY BEKAWESY, S.H
NIP : 198309102009011006
Pangkat/Gol. : Penata (III/c)
Jabatan : Kasubbag. Umum, Kepegawaian dan Keuangan

Demikian disampaikan, untuk dapat dimaklumi dan terima kasih.

INSPEKTUR DAERAH,

H. RADIUS AKIMA, S.Sos., M.T
PEMBINA UTAMA MUDA
NIP 19[illegible]10522 199101 1 001

1

Gambar 3. 9 Surat Pengiriman Nama Peserta Bimtek Penyusunan Arsitektur SPBE

BAB IV
IMPLEMENTASI *THREAT HUNTING* DAN PEMANTAUAN *FILE INTEGRITY MONITORING* MENGGUNAKAN WAZUH DI DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN BENGKALIS

4.1 Metodologi

4.1.1 Prosedur Pembuatan Sistem

Proyek kerja praktik ini berfokus pada implementasi sistem monitoring keamanan informasi menggunakan *platform open-source Wazuh*. Sistem ini dirancang untuk menyediakan fungsi *Threat Hunting* dan *File Integrity Monitoring* (FIM) yang mampu mendeteksi berbagai ancaman keamanan secara *real-time* serta memantau integritas *file* sistem yang sensitif. Adapun prosedur pembuatan sistem dilakukan melalui beberapa tahapan teknis sebagai berikut:

1. Persiapan lingkungan sistem

   Tahap awal dimulai dengan membangun infrastruktur *virtual* untuk mendukung proses pengujian dan *monitoring*. Lingkungan ini terdiri dari:

   a. Satu *server* utama yang bertindak sebagai *Wazuh Server* (*Monitoring Center*).
   b. Satu *server* target yang berfungsi sebagai objek *monitoring* dan simulasi serangan.

2. Instalasi *Wazuh All In One Development*

   Instalasi *Wazuh* dilakukan pada *server* utama menggunakan skema *All-in-One Development* yang mencakup komponen penting seperti *Wazuh Manager*, *Filebeat*, *Wazuh Indexer* dan *Kibana*. Instalasi ini memanfaatkan skrip resmi dari dokumentasi *Wazuh* yang disesuaikan untuk kebutuhan pengembangan dan pengujian internal.

3. Instalasi dan konfigurasi *Wazuh agent*

   Pada *server* target, dilakukan pemasangan *Wazuh Agent* yang berfungsi untuk mengirimkan data *log* ke *server* pusat. Konfigurasi dilakukan melalui *file ossec.conf* untuk mengatur jenis *log* yang dikirimkan, seperti *log* sistem, *log* aplikasi, serta perubahan *file* pada direktori tertentu.
4. Konfigurasi fitur *file integrity monitoring* (FIM)

   Fitur FIM dikonfigurasi dengan menentukan *path* atau direktori yang ingin dipantau, misalnya direktori tempat *file* konfigurasi penting atau *file* aplikasi disimpan. Setiap perubahan, penghapusan atau penambahan *file* di direktori tersebut akan dicatat dan dikirimkan ke *Wazuh Manager*.
5. Konfigurasi fitur *threat hunting*

   Untuk mendukung fitur *Threat Hunting*, dikonfigurasi dengan menambahkan *log webserver* pada file konfigurasi sehingga *agent* akan mengirimkan *data log* ke *Wazuh manager*.
6. Simulasi dan pengujian sistem

   Setelah sistem aktif dan berjalan, dilakukan simulasi serangan untuk menguji kemampuan deteksi *Wazuh*. Jenis simulasi meliputi:
   a. Serangan *SQL Injection* pada aplikasi *web*.
   b. *Brute-force login* terhadap layanan *SSH*.
   c. *Cross-Site Scripting* (*XSS*).
   d. Perubahan konten *file* pada direktori yang telah ditentukan.

4.1.2 Metode Pengumpulan Data

Metodologi pengumpulan *data* dalam implementasi sistem *monitoring* ini dilakukan dengan pendekatan teknis yang sesuai dengan karakteristik sistem keamanan informasi. Terdapat tiga teknik yang digunakan:

1. Observasi

   Penulis melakukan observasi terhadap aktivitas sistem secara langsung melalui *dashboard Wazuh* (*Kibana*). Observasi ini bertujuan untuk memantau *log*

aktivitas, mendeteksi perubahan *file*, serta meneliti setiap *event* atau peringatan keamanan yang muncul.

2. Simulasi

   Untuk mengukur efektivitas dan akurasi sistem, dilakukan beberapa simulasi serangan umum, seperti:

   a. Simulasi *brute-force login SSH* dengan mencoba *login* secara berulang menggunakan kredensial acak.
   b. Simulasi *SQL Injection* dan *XSS* terhadap aplikasi *web* aplikasi.
   c. Simulasi penambahan, perubahan *file* pada direktori yang telah dikonfigurasi dalam modul *FIM*.

   Simulasi ini dirancang untuk memicu sistem deteksi dan mengevaluasi apakah sistem mampu mencatat dan memberikan peringatan yang sesuai.

Metode ini memberikan bukti konkret yang mendukung validitas sistem yang telah dibangun serta menunjukkan efektivitasnya dalam mendeteksi ancaman.

4.1.3 Proses Perancangan

Proses perancangan sistem *monitoring* keamanan berbasis *Wazuh* dimulai dengan tahap perencanaan infrastruktur, penentuan skenario pengujian, hingga implementasi teknis dan dokumentasi. Rangkaian langkah-langkahnya meliputi:

1. Persiapan lingkungan

   Lingkungan uji coba dirancang dengan konfigurasi minimal dua *server*:

   a. Satu sebagai *Wazuh Server* (*Monitoring Center*)
   b. Satu sebagai *Target Server* (*endpoint* yang dipantau)
      Topologi ini memungkinkan proses pemantauan dilakukan secara terpisah agar skenario simulasi serangan tidak mengganggu sistem monitoring itu sendiri.

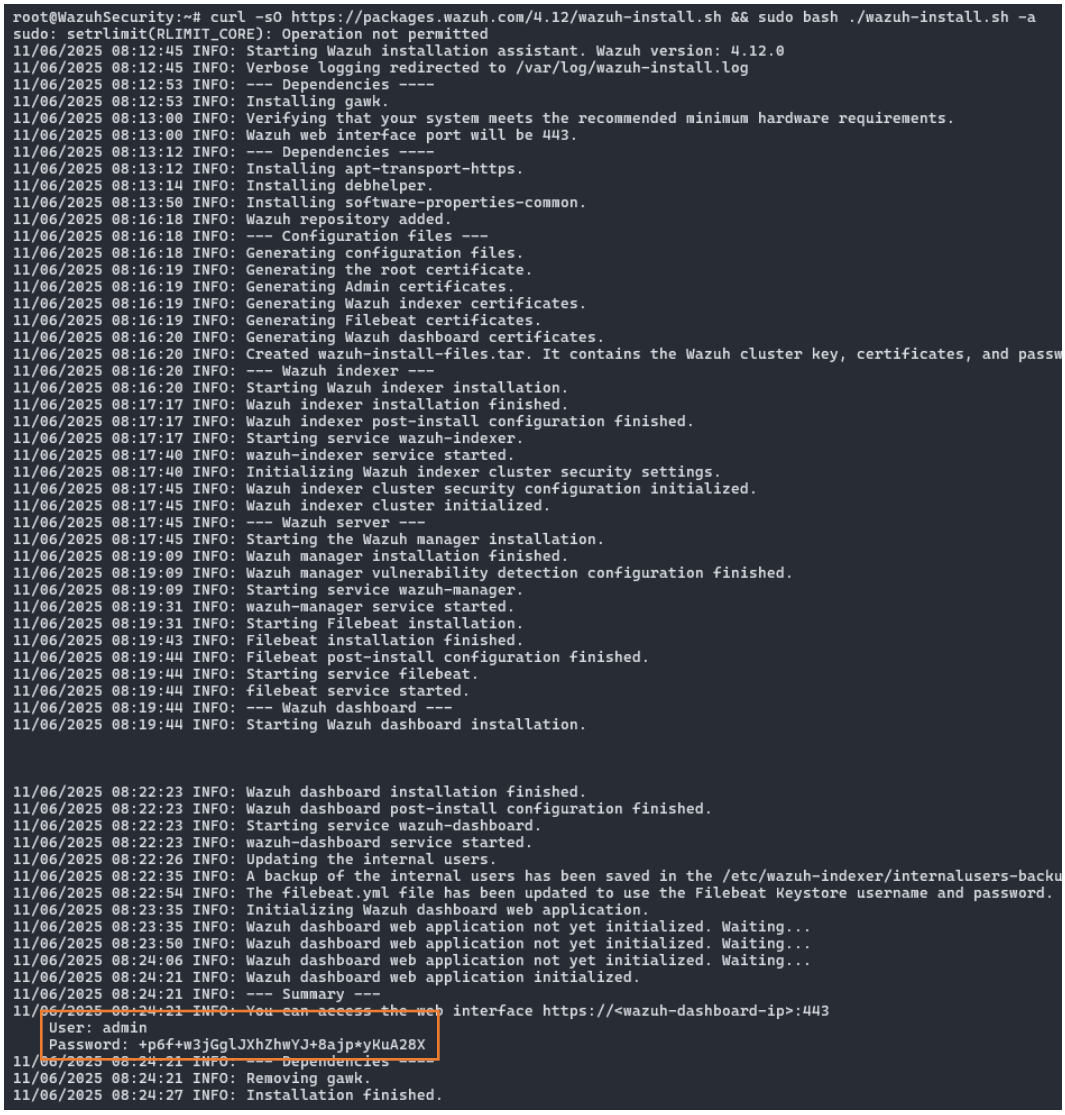
2. Instalasi *Wazuh all-in-one development*

   Untuk mempercepat proses implementasi dan mempermudah integrasi antar komponen, penulis memilih metode instalasi *Wazuh All-in-One Development*.

Metode ini memungkinkan seluruh komponen penting seperti *Wazuh Manager*, *Wazuh Indexer*, *Filebeat* dan *Kibana* terinstal secara otomatis dalam satu *server* melalui skrip resmi dari *Wazuh*. Pendekatan ini efisien digunakan dalam konteks pengujian dan penelitian, karena tidak memerlukan konfigurasi yang kompleks antar *node*. Untuk melakukan instalasi *Wazuh All-in-One Development*, digunakan perintah berikut:

```
curl -sO https://packages.Wazuh.com/4.12/Wazuh-install.sh && sudo bash ./Wazuh-install.sh -a
```

Dengan menggunakan perintah ini, proses instalasi dijalankan secara otomatis tanpa perlu konfigurasi manual pada setiap komponen. Skrip tersebut akan mengunduh dan mengeksekusi instalasi semua komponen utama *Wazuh* seperti *Wazuh Manager*, *Wazuh Indexer*, *Filebeat* dan *Kibana* dalam satu langkah. Pendekatan ini sangat efektif karena meminimalkan risiko kesalahan konfigurasi serta mempercepat proses implementasi sistem monitoring keamanan, khususnya dalam lingkungan pengujian atau pengembangan. Selain itu, metode ini memungkinkan integrasi antar komponen terjadi secara lancar, sehingga sistem siap digunakan untuk melakukan *monitoring log*, deteksi ancaman, serta visualisasi *data* keamanan melalui antarmuka *kibana*. Pada gambar 4.1 merupakan proses pemasangan *Wazuh all-in-one development*.

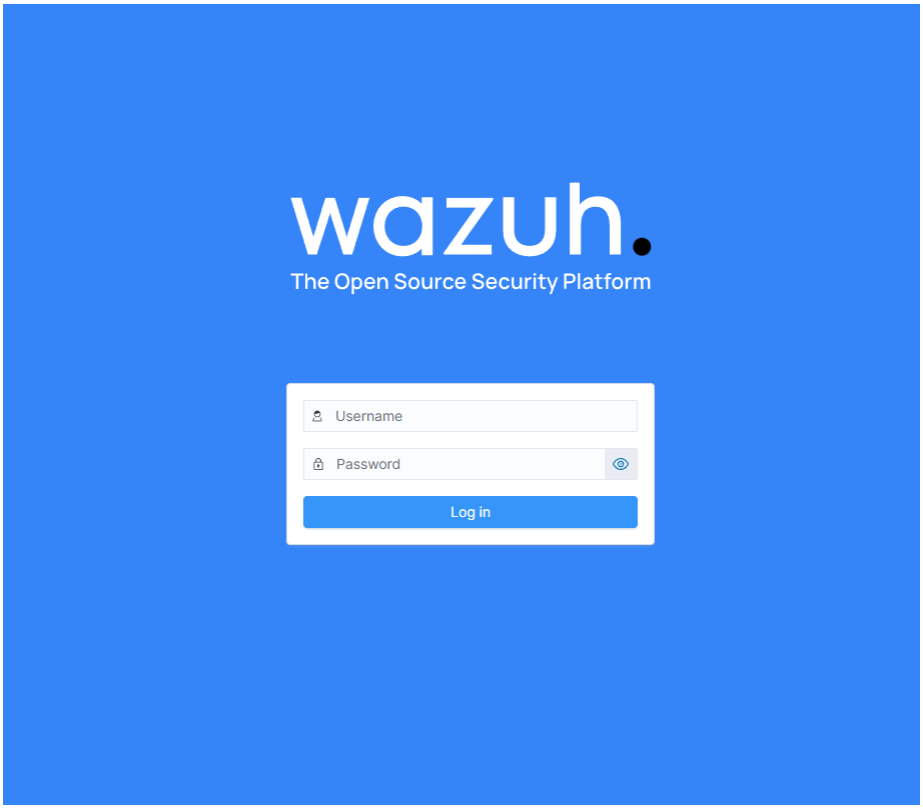


Gambar 4. 1 Instalasi *Wazuh Server*

Setelah instalasi selesai, *Wazuh dashboard* dapat langsung di akses melalui *browser* dengan kredensial:

Tabel 4. 1 Kredensial *Wazuh Dashboard*

Username	Password
admin	+p6Efw3jGqLJXhzHvJ+8ajpywKuA28X

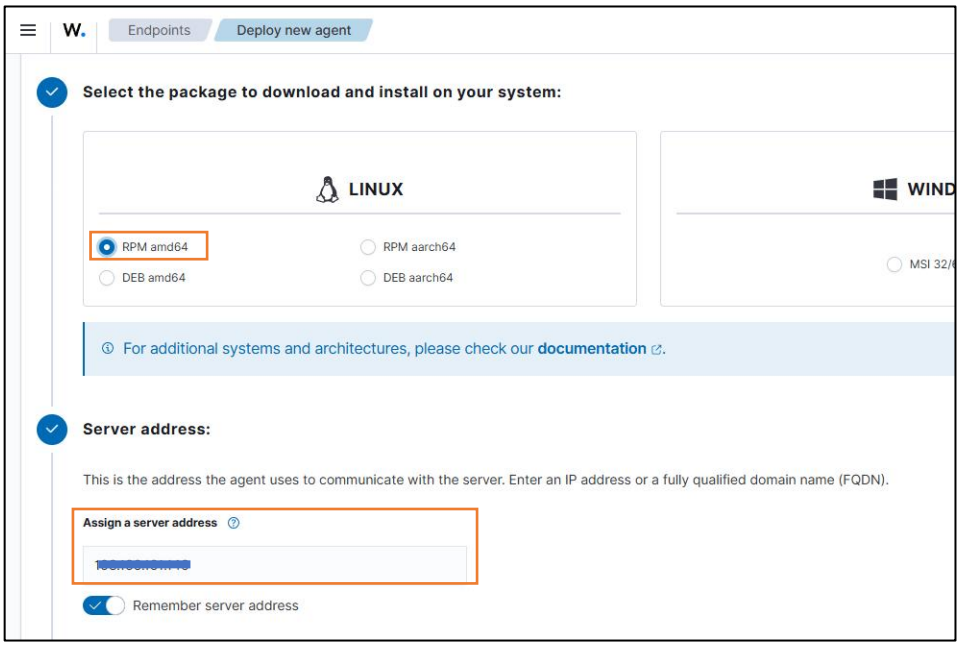


Gambar 4. 2 Halaman *Login Wazuh Server*

3. Instalasi dan konfigurasi *Wazuh agent*

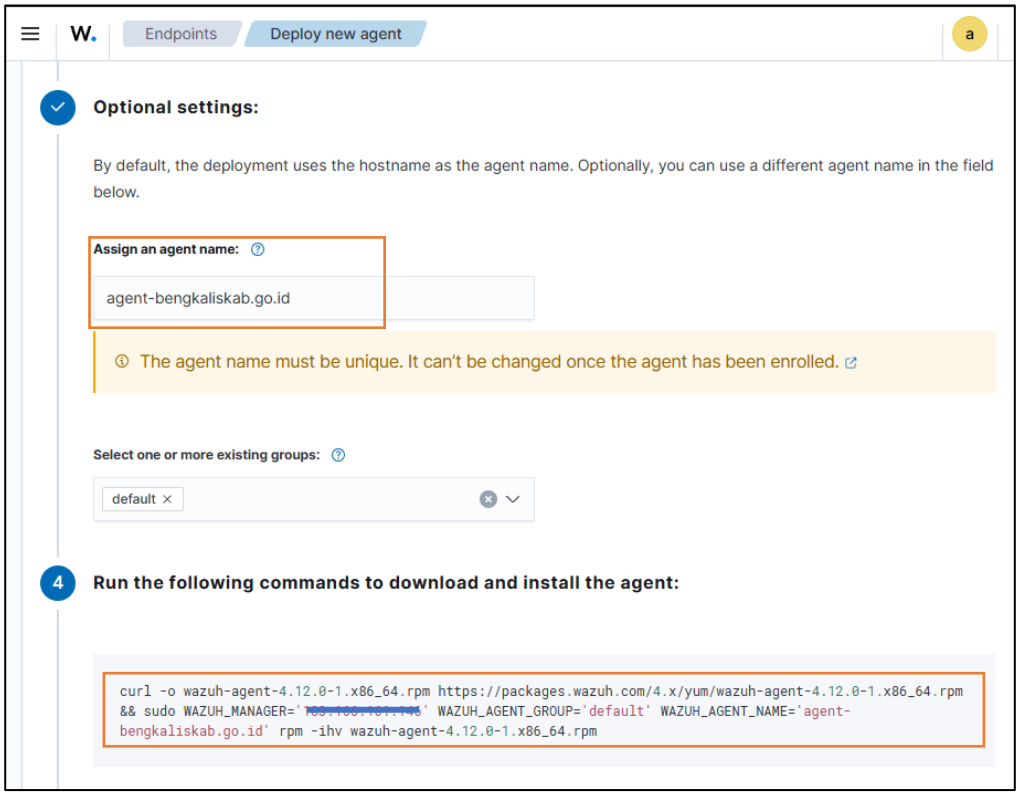
   Setelah *Wazuh Server* berhasil di instal dan dikonfigurasi, langkah selanjutnya adalah melakukan instalasi dan konfigurasi *Wazuh Agent* pada *server* target yang akan dimonitor. *Agent* ini berfungsi sebagai komponen klien yang bertugas mengirimkan *log*, informasi sistem dan data keamanan dari *endpoint* menuju *Wazuh Manager* untuk dianalisis. Pada *Wazuh Dashboard* (*Kibana*) tersedia fitur bernama *Deploy Agent*, yaitu sebuah menu interaktif yang memudahkan *administrator* untuk menambahkan *endpoint* atau sistem target yang ingin dipantau. Dengan konfigurasi yang tepat, *agent* akan secara otomatis mulai mengirimkan data ke *Wazuh Server* setelah layanan dijalankan. *Data* yang diterima selanjutnya akan dianalisis dan divisualisasikan melalui *dashboard*, memungkinkan *administrator* untuk melakukan deteksi dini terhadap aktivitas yang mencurigakan atau serangan siber. Tahap-tahap *deploy* sebagai berikut:

1. *Deploy agent* baru



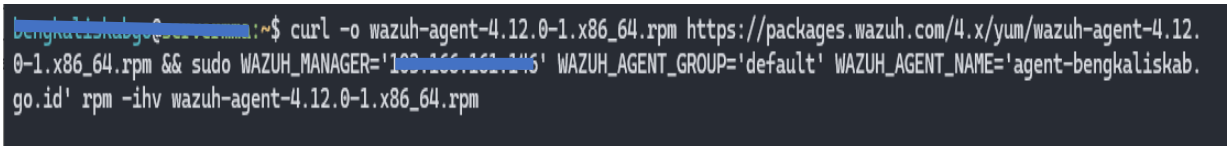
Gambar 4. 3 *Deploy Agent*

Dikarenakan *agent* yang ingin di *install* merupakan *Centos Linux*, maka *package* yang digunakan adalah *RPM* (*Red Hat Package Manager*), kemudian *server address* disesuaikan dengan alamat *IP server Wazuh*. Setelah itu dibutuhkan nama *agent* pada langkah ”*Option Settings”*, nama ini diwajibkan unik agar tidak salah dalam menganalisis nantinya,



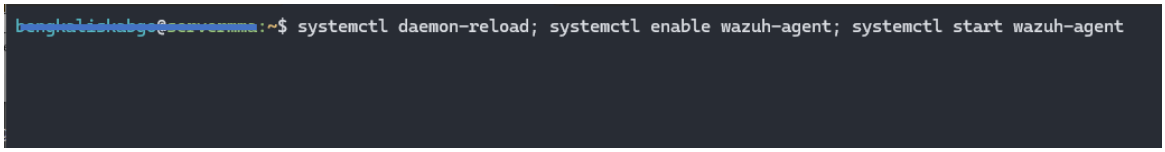
Gambar 4. 4 *Deploy Agent*

kemudian pada *step* ke empat, perintah tersebut di *copy* dan di *paste* pada *terminal server agent* sehingga *server agent* melakukan instalasi *Wazuh agent* secara otomatis.



Gambar 4. 5 Menjalakan Perintah *Install Wazuh Agent*

Setelah perintah pada gambar 4.5 dijalankan sangat diwajibkan untuk melakukan *restart daemon*, *enable Wazuh-agent* dan *start Wazuh agent* agar *service agent* dapat berjalan dengan lancar.

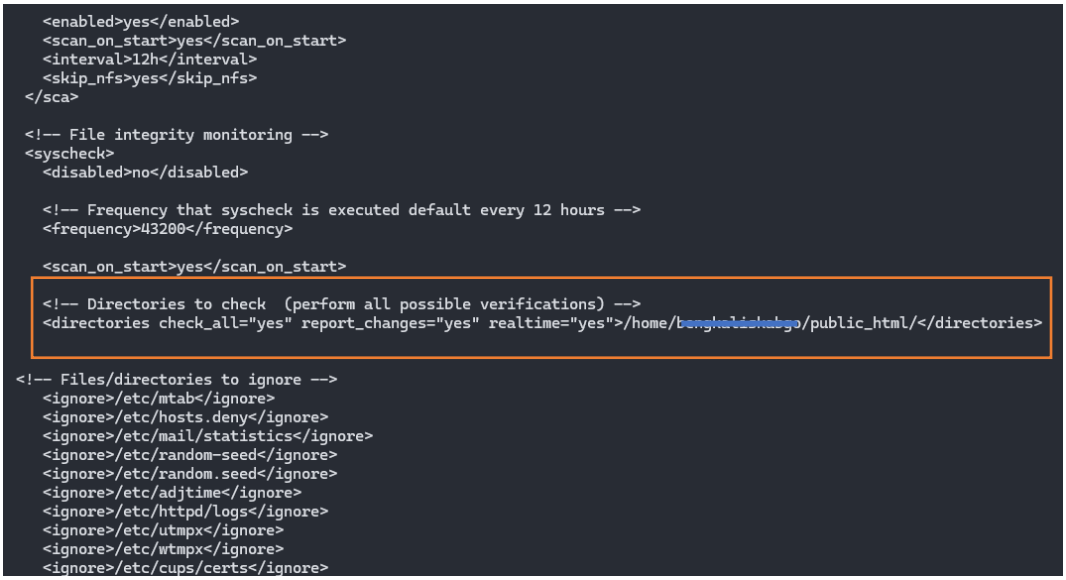


Gambar 4. 6 *Restart* Layanan *Wazuh Agent*

4. Konfigurasi fitur *integrity Monitoring* (*FIM*)

   Konfigurasi fitur *File Integrity Monitoring* (*FIM*) dilakukan pada sisi *agent*, karena *agent* mengirimkan *data* perubahan *file* secara langsung pada *Wazuh manager*. Fitur *FIM* sangat penting dalam konteks keamanan sistem karena memungkinkan *administrator* mendeteksi perubahan yang mencurigakan atau tidak sah terhadap *file-file* penting yang dapat menjadi indikator awal dari serangan atau kompromi sistem. Namun, perlu diperhatikan bahwa *Wazuh* memiliki batasan dalam jumlah *file* yang dapat dipantau, yaitu sebanyak 100.000 *file* per *agent*. Oleh karena itu, agar pemantauan tetap optimal dan tidak membebani sistem, maka hanya direktori yang berkaitan langsung dengan aplikasi-aplikasi dan direktori bawaan konfigurasi yang dianggap penting dan rawan perubahan yang dimasukkan ke dalam daftar pemantauan. Konfigurasi dilakukan melalui *file ossec.conf* yang terletak pada direktori */var/ossec/etc/*. Pada *file* ini, ditambahkan blok konfigurasi dalam format *XML* sebagai berikut:

```
<directories check_all="yes" report_changes="yes" realtime="yes">
    /home/bxxxxliskxbgo/public_html/
</directories>
```



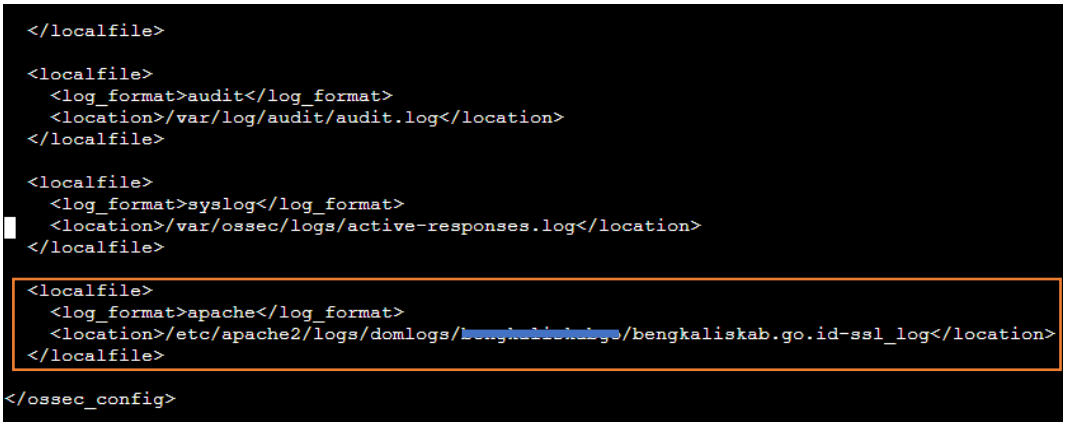
Gambar 4. 7 Konfigurasi *File ossec.conf*

Konfigurasi tersebut bertujuan agar *Wazuh Agent* mencatat seluruh aktivitas perubahan terhadap *file* pada direktori yang telah ditentukan, seperti penambahan, penghapusan atau modifikasi *file*. Dengan opsi *realtime="yes"*, maka sistem akan mendeteksi dan mengirimkan informasi perubahan secara langsung (*real-time*) ke *Wazuh Manager*, tanpa harus menunggu interval tertentu. Parameter *check_all="yes"* dan *report_changes="yes"* juga berperan penting, karena memastikan bahwa semua *file* dalam direktori tersebut diperiksa secara menyeluruh dan perubahan isinya dilaporkan secara detail, termasuk isi *file* jika memungkinkan. *Data* ini kemudian akan dianalisis dan divisualisasikan melalui *dashboard* untuk kepentingan *audit* serta *incident response*. Dengan adanya fitur *FIM* ini, sistem mampu memberikan *early warning* apabila terdapat aktivitas yang tidak biasa pada *file* aplikasi, seperti modifikasi *file* oleh pihak tidak berwenang yang sering menjadi ciri khas serangan berbasis *web* seperti *webshell* atau *deface attack*.

5. Konfigurasi Fitur *Threat Hunting*

Konfigurasi fitur *threat hunting* pada *Wazuh* dilakukan di sisi *agent*, yakni pada *server* yang akan dipantau. Fokus utama dari konfigurasi ini adalah memungkinkan *agent* untuk mengirimkan data *log* dari aplikasi atau layanan tertentu dalam hal ini *web server* ke *Wazuh Manager* untuk dianalisis lebih lanjut. Langkah awal dalam mengaktifkan fitur ini adalah dengan menambahkan direktori *lokasi file log web server* ke dalam *file* konfigurasi *ossec.conf* yang terletak di direktori */var/ossec/etc/*. Konfigurasi dilakukan dengan menambahkan blok *XML* berikut:

```
<localfile>
    <log_format>apache</log_format>
     <location>/etc/apache2/logs/domlogs/bxxxxliskxbgo/bengkaliskab.g
o.id-ssl_log</location>
</localfile>
```



Gambar 4. 8 Konfigurasi *File ossec.conf*

Pada gambar 4.8 *tag log_format* disesuaikan dengan jenis *log* yang digunakan oleh *webserver*, dalam hal ini adalah *Apache WebServer*. Sedangkan *tag location* menunjukkan *path* atau jalur direktori tempat *file log* disimpan. Setelah konfigurasi ini diterapkan, *Wazuh agent* akan secara

aktif membaca *file log* tersebut dan mengirimkannya ke *Wazuh Server*. Di sisi *server*, *log* yang diterima akan diproses oleh komponen *decoder*, yaitu modul yang bertugas untuk melakukan *parsing* terhadap *log* mentah dan mengubahnya menjadi informasi terstruktur dan mudah dibaca. Informasi yang telah didekodekan kemudian akan dicocokkan dengan *ruleset* deteksi ancaman (*threat detection rules*), sehingga setiap pola aktivitas mencurigakan atau indikasi serangan dapat teridentifikasi. Fitur ini sangat penting dalam kegiatan *threat hunting* yaitu proses proaktif untuk mencari dan menganalisis potensi ancaman siber yang mungkin belum terdeteksi oleh sistem keamanan konvensional. Dengan adanya data *log* yang terstruktur dan terpantau secara *real-time*, *administrator* dapat melakukan analisis forensik lebih mendalam terhadap insiden keamanan, sekaligus meningkatkan kemampuan deteksi dini terhadap serangan.

4.1.4 Tahapan Dan Jadwal Pelaksanaan

Tahapan dan jadwal pelaksanaan kerja praktik ini dilakukan secara terstruktur, dimulai dari tahap persiapan lingkungan sistem, instalasi, konfigurasi, hingga dokumentasi dan penulisan laporan. Berikut ini adalah uraian jadwal kegiatan berdasarkan waktu pelaksanaan:

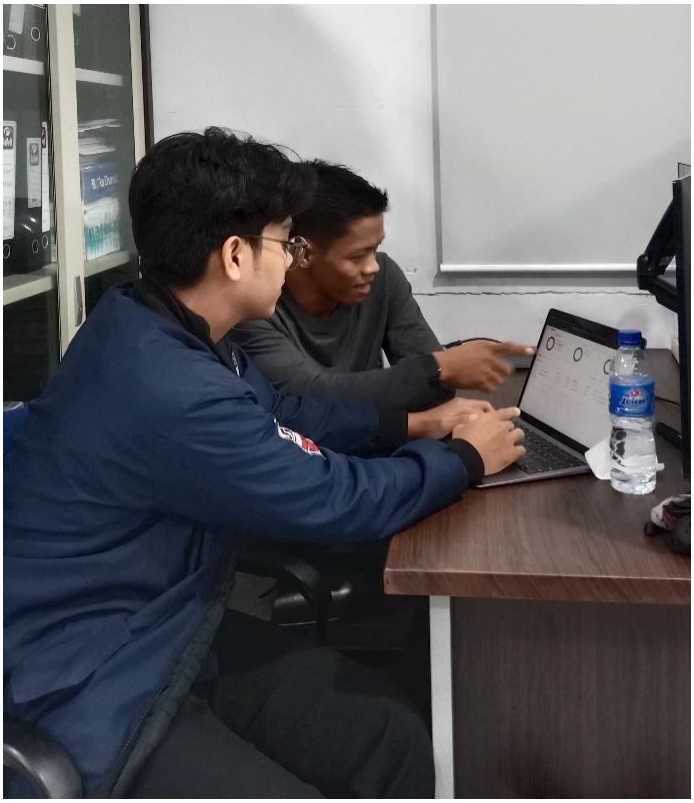
Tabel 4. 2 Tahapan Dan Perancangan Jadwal Pelaksanaan

Tanggal	Kegiatan
12 Juni 2025	Instalasi dan konfigurasi awal *Wazuh All-in-One* (*Wazuh Manager*, *Wazuh Indexer*, *Kibana*) dan pemasangan *Wazuh Agent* di *server* objek.
13 Juni 2025	Konfigurasi lanjutan *Wazuh Server* dan *Wazuh Agent*, termasuk aktivasi fitur *File Integrity Monitoring* (*FIM*) dan *Threat Hunting*.

14 Juni – 09 Juli 2025	Dokumentasi hasil implementasi, pengambilan gambar *dashboard Wazuh*, analisis hasil *monitoring* dan penyusunan laporan kerja praktik.

Rangkaian kegiatan tersebut bertujuan untuk memastikan sistem monitoring dapat berjalan dengan optimal serta menghasilkan dokumentasi yang dapat digunakan dalam keamanan sistem *server* di lingkungan Dinas Komunikasi dan Informatika Kabupaten Bengkalis.

4.2 Perancangan Dan Implementasi



Gambar 4. 9 Installasi Dan Konfigurasi *Wazuh* Bersama *Admin Server*

4.2.1 Analisis *Data*

Analisis *data* dilakukan untuk mengevaluasi hasil pengumpulan data yang diperoleh dari proses simulasi serangan pada *server agent*. Pengambilan *data*

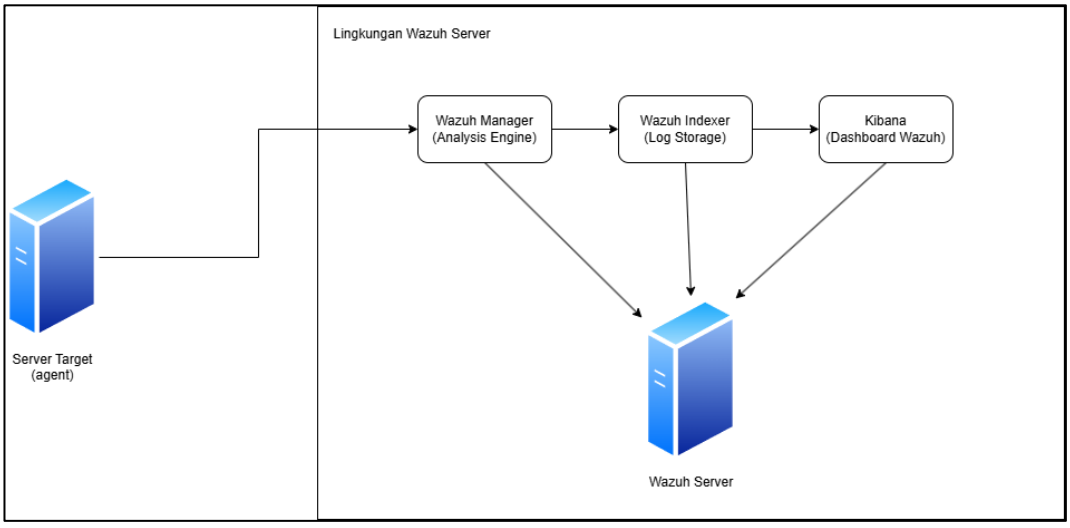
dilakukan pada dua modul fungsional, yaitu *File Integrity Monitoring* (*FIM*) dan *Threat Hunting* yang terintegrasi dalam sistem secara keseluruhan. Data yang dianalisis meliputi:

1. *Event* perubahan *file* (*File Integrity Monitoring*)

   Sistem mencatat setiap perubahan yang terjadi di direktori yang telah dikonfigurasi dalam *Wazuh agent*. Ketika ada seseorang melakukan penambahan, penghapusan atau modifikasi *file* melalui aplikasi atau *terminal*, *log* tersebut akan dikirim secara *real-time* ke *Wazuh server*. Contohnya, jika ada satu *file* ditambahkan atau diubah, *event* tersebut langsung terdeteksi dan ditampilkan di *dashboard Kibana* lengkap dengan nama *file*, waktu, *ID* dan tingkat aturan yang dipicu.
2. *Event webserver* dan *journald* (*Threat Hunting*)

   Log webserver pada direktori */etc/apache2/logs/domlogs/bxxxxliskxbgo* dianalisis untuk mendeteksi serangan seperti *XSS*, *SQL Injection* dan *brute force ssh* pada komponen *journald*. Log diproses oleh *Wazuh Manager* menggunakan *ruleset* dan hasilnya ditampilkan dalam bentuk *alert* melalui *dashboard Kibana* sebagai bagian dari aktivitas *threat hunting*.

4.2.2 Rancangan Sistem



Gambar 4. 10 Rancangan Sistem

Sistem monitoring keamanan yang dirancang dalam proyek kerja praktik ini mengadopsi arsitektur *client-server*, setiap *server* target (*endpoint*) dipasang *Wazuh agent* yang bertugas mengumpulkan dan mengirimkan *data log* secara *real-time* ke pusat pengolahan, yaitu *Wazuh Server*. *Data log* yang dikirimkan mencakup aktivitas sistem, perubahan integritas *file*, serta *log web server* yang berguna dalam proses *Threat Detection* dan *Incident Response*. Selanjutnya *data* ini akan dianalisis, disimpan dan divisualisasikan melalui *dashboard kibana*. Penjelasan gambar 4.10:

1. *Server* target (*agent*)

   Merupakan perangkat atau sistem *endpoint* yang menjadi objek pemantauan. Di dalamnya di *install Wazuh agent* yang bertugas untuk:

   a. Mengumpulkan *log* aktivitas sistem.
   b. Melakukan pemantauan perubahan *file* (*File Integrity Monitoring*).
   c. Mengambil *file log web server* dan *log journald* untuk keperluan *threat hunting.*

2. *Wazuh Manager* (*Analysis engine*)

   Komponen inti yang berfungsi sebagai pusat analisis, *Wazuh Manager* menerima *data log* dari *agent* dan melakukan proses:

   1. *Decoding* dan *parsing data log*.
   2. Menganalisis *data* berdasarkan *ruleset* yang telah dikonfigurasi (misalnya deteksi *brute force*, *file modification* dan *suspicious access*).
   3. Menghasilkan *event* keamanan jika ditemukan aktivitas yang mencurigakan atau menyimpang dari kebiasaan normal sistem.

3. *Wazuh Indexer* (*Log storage*)

   Dulunya dikenal sebagai *Elasticsearch*, *Wazuh Indexer* berfungsi sebagai tempat penyimpanan utama bagi seluruh *log* dan *security events* yang telah dianalisis. *Data* disimpan dalam format terstruktur yang memungkinkan pencarian cepat dan efisien. Komponen ini sangat krusial karena menjadi dasar dari proses visualisasi dan pelaporan *data log* melalui antarmuka *dashboard*.

4. *Kibana* (*Dashboard Wazuh*)

   Kibana merupakan antarmuka berbasis *web* yang digunakan untuk menampilkan hasil *monitoring* secara visual dan interaktif. Melalui *Kibana*, *administrator* atau analis keamanan dapat:

   1. Melihat status terkini dari semua *agent* yang dipantau.
   2. Menganalisis *alert* dan *event* keamanan berdasarkan waktu, deskripsi, jenis serangan.
   3. Membuat visualisasi dalam bentuk grafik, tabel untuk mempercepat proses investigasi insiden.

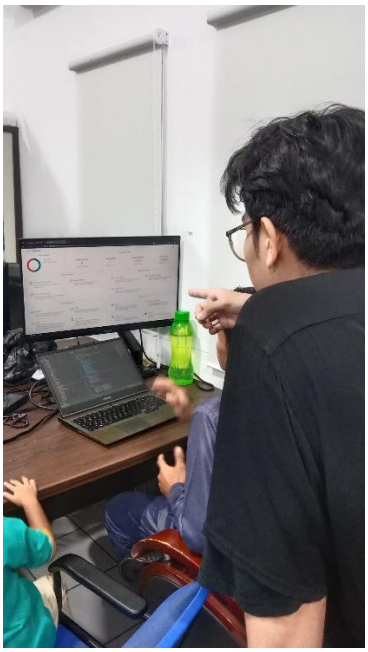
Cara kerja sistem dari sistem monitoring *Wazuh*:

1. *Wazuh Agent* yang terpasang pada *server* target mengirimkan berbagai jenis *log* (aktivitas sistem, log web server, perubahan *file*) ke *Wazuh Manager*.
2. *Wazuh Manager* melakukan analisis *data* menggunakan *ruleset* yang telah disusun sebelumnya, seperti untuk mendeteksi perubahan *file*, *brute force ssh*, *SQL Injection* dan *XSS*.
3. Hasil analisis tersebut kemudian dikirimkan ke *Wazuh Indexer*, tempat *log* disimpan secara terstruktur untuk keperluan pencarian dan penyimpanan jangka panjang.
4. *Kibana* kemudian mengambil *data* dari *indexer* dan menampilkannya dalam bentuk visual, sehingga memudahkan tim keamanan dalam memantau, menginvestigasi dan mengambil keputusan terhadap ancaman yang terdeteksi.

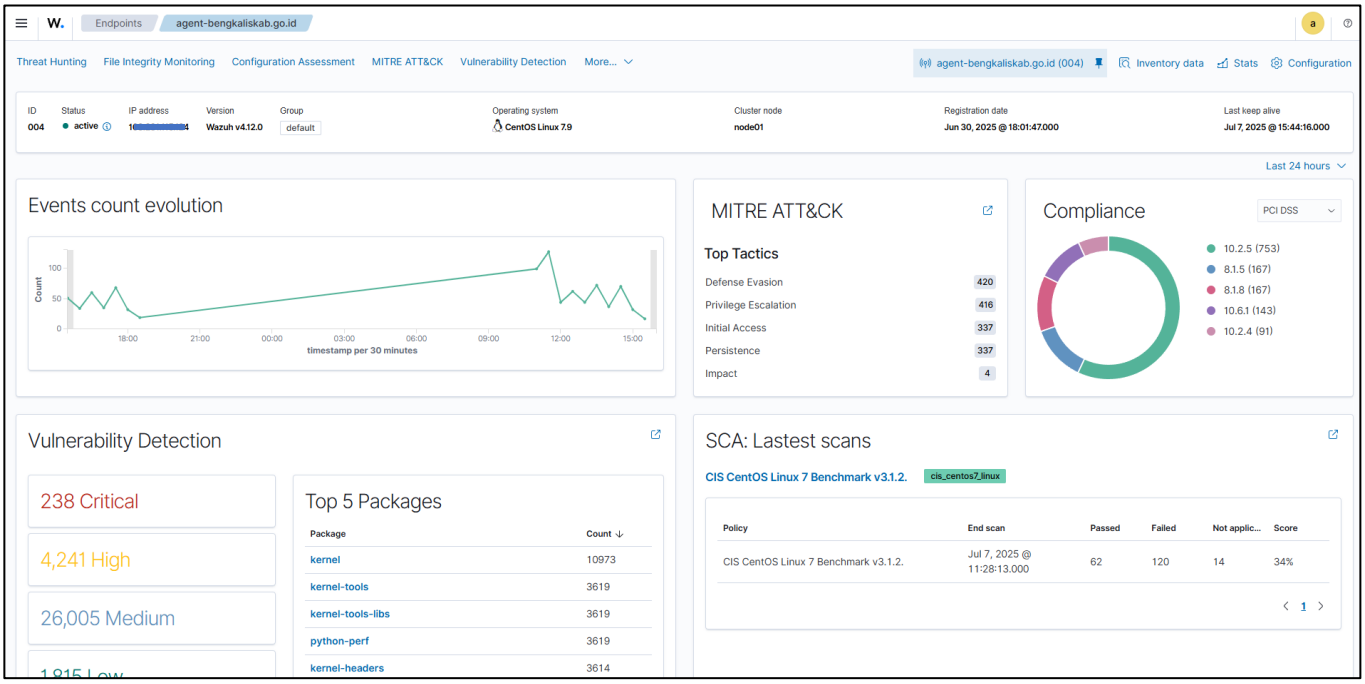
4.2.3 Implementasi Sistem

Gambar 4. 11 Pelatihan Penggunaan *Wazuh*

Gambar 4. 12 Pelatihan Penggunaan Fitur *File Integrity Monitoring*



Gambar 4. 13 Pelatihan Penggunaan Fitur *Threat Hunting*



Gambar 4. 14 Halaman *Dashboard Agent*

Penjelasan komponen *dashboard*:

Tabel 4. 3 Penjelasan Komponen *Dashboard*

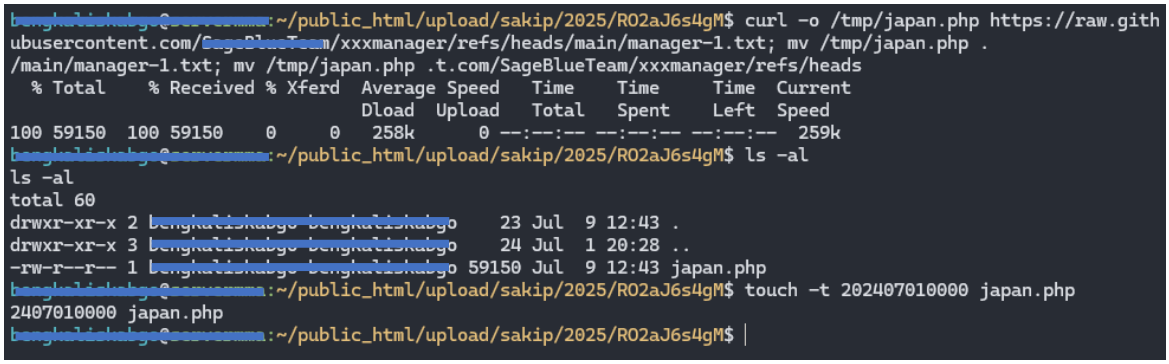
Komponen	Penjelasan
Informasi Umum *Agent*	*Dashboard* menampilkan identitas *agent* yang aktif, termasuk nama *host* (agent-bengkaliskab.go.id), alamat *IP*, status aktif, versi *Wazuh* (v4.12.0), serta sistem operasi yang digunakan (*CentOS Linux 7.9*). Informasi ini digunakan untuk mengidentifikasi sumber data keamanan yang dimonitor oleh *Wazuh*.
Events Count Evolution	Grafik ini menggambarkan evolusi jumlah *event* keamanan yang terdeteksi dalam interval waktu 30 menit selama 24 jam terakhir. Peningkatan atau penurunan jumlah *event* dapat menunjukkan aktivitas mencurigakan, serangan, atau anomali pada sistem.
MITRE ATT&CK Tactics	Panel ini mengelompokkan *event* berdasarkan taktik *MITRE ATT&CK*, yaitu kerangka kerja standar yang digunakan untuk memahami metode dan tujuan serangan. Taktik utama yang terdeteksi antara lain: • ***Defense Evasion***: Upaya penyerang untuk menghindari deteksi. • ***Privilege Escalation***: Usaha memperoleh hak akses yang lebih tinggi. • ***Initial Access***: Langkah awal masuk ke dalam sistem target. • ***Persistence***: Usaha untuk mempertahankan akses jangka panjang.

	• ***Impact***: Dampak yang dihasilkan terhadap sistem korban.
Compliance	Panel ini menunjukkan tingkat kepatuhan sistem terhadap standar *PCI DSS*. Visualisasi *pie chart* mengelompokkan skor *audit* berdasarkan kategori tertentu. Skor yang tinggi menunjukkan ketidaksesuaian terhadap standar keamanan dan perlu segera ditindaklanjuti untuk menurunkan risiko.
Vulnerability Detection	Sistem mengidentifikasi kerentanan perangkat lunak berdasarkan tingkat keparahan: • ***Critical***: Risiko sangat tinggi yang dapat dimanfaatkan dengan mudah. • ***High***: Risiko tinggi yang berdampak signifikan. • ***Medium*** dan ***Low***: Risiko sedang hingga rendah. Klasifikasi ini membantu prioritisasi penanganan kerentanan pada sistem.
Top 5 Packages with Vulnerabilities	Paket perangkat lunak yang memiliki jumlah kerentanan tertinggi ditampilkan dalam daftar ini. Sebagian besar berasal dari komponen kernel *Linux*, yang merupakan target utama karena posisinya yang krusial dalam sistem operasi.
Security Configuration Assessment (SCA)	Komponen ini menunjukkan hasil *audit* konfigurasi keamanan sistem berdasarkan *benchmark CIS CentOS Linux 7 v3.1.2*. Hasil *audit* dibagi menjadi: • ***Passed***: Konfigurasi sesuai dengan standar. • ***Failed***: Konfigurasi tidak sesuai. • ***Not Applicable***: Pemeriksaan tidak relevan dengan sistem. Skor keseluruhan (34%) menunjukkan tingkat kepatuhan sistem terhadap standar best practice keamanan.

Selanjutnya, proses implementasi dilakukan pada *server virtual* yang berjalan di atas *server* fisik menggunakan *platform Proxmox*. *Server* fisik tersebut memiliki kemampuan untuk membagi sumber daya nya menjadi beberapa bagian (virtualisasi), sehingga memungkinkan instalasi dan pengoperasian beberapa *server virtual* secara simultan.

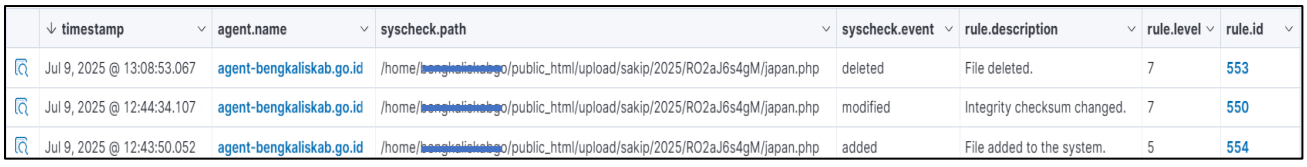
1. Implementasi Fitur *File Integrity Management*

   Pada FIM *event*, *Wazuh agent* sudah dikonfigurasikan untuk melihat perubah pada isi direktori tertentu, pada saat ada yang melakukan perubahan pada direktori tertentu, *Wazuh agent* akan mencatat perubahan tersebut kemudian mengirimkan *data* tersebut ke *Wazuh Server*. Pada gambar 4.15 ditambahkan sebuah *file* dan diubah *datetime* nya melalui *terminal*.



Gambar 4. 15 Menambahkan Dan Memanipulasi *File*

Pada gambar 4.16, *Wazuh* telah menghasilkan sebuah *data event* bahwa telah terjadi perubahan isi direktori seperti pada gambar 4.15. Terdapat tiga *event* yang terjadi.



timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Jul 9, 2025 @ 13:08:53.067	agent-bengkaliskab.go.id	/home/[redacted]/public_html/upload/sakip/2025/RO2aJ6s4gM/japan.php	deleted	File deleted.	7	553
Jul 9, 2025 @ 12:44:34.107	agent-bengkaliskab.go.id	/home/[redacted]/public_html/upload/sakip/2025/RO2aJ6s4gM/japan.php	modified	Integrity checksum changed.	7	550
Jul 9, 2025 @ 12:43:50.052	agent-bengkaliskab.go.id	/home/[redacted]/public_html/upload/sakip/2025/RO2aJ6s4gM/japan.php	added	File added to the system.	5	554

Gambar 4. 16 *FIM Event*

Pada gambar 4.16 yang ditampilkan hasil pemantauan fitur *File Integrity Monitoring* (FIM) pada *Wazuh Dashboard*, sistem berhasil mendeteksi penambahan, perubahan dan penghapusan *file* pada direktori yang telah dikonfigurasikan. Penjelasan ketiga *event:*

a. *Event* 1

Tabel 4. 4 *Event Deleted*

Waktu	09 Juli 2025, 13:08 *WIB*
Status	*Deleted*
Lokasi *File*	/home/bxxxxliskxbgo/public_html/upload/sakip/2025/RO2aJ6s4gM/japan.php
Keterangan *File*	Pada waktu ini, *file japan.php* terdeteksi telah dihapus dari sistem.

b. *Event 2*

Tabel 4. 5 *Event Modified*

Waktu	09 Juni 2025, 12:44 *WIB*
Status	*Modified*
Lokasi File	/home/bxxxxliskxbgo/public_html/upload/sakip/2025/RO2aJ6s4gM/japan.php.
Keterangan File	Sistem mendeteksi bahwa isi *file japan.php* telah diubah. Hal ini diketahui dari perubahan *checksum* yang menunjukkan bahwa *datetime file* telah dimanipulasi.

c. *Event 3*

Tabel 4. 6 *Event Added*

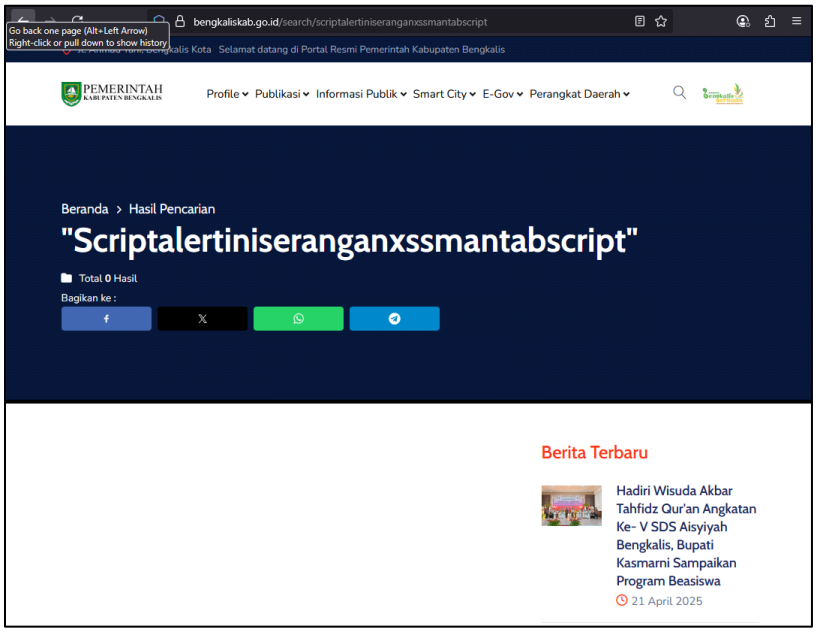
Waktu	09 Juli 2025, 12:44 *WIB*
Status	*Added*

Lokasi File	/home/bxxxxliskxbgo/public_html/upload/sakip/2025/RO2aJ6s4gM/japan.php
Keterangan File	*Japan.php* ditambahkan ke dalam direktori sebuah aplikasi *web*. Dari tempat *file* tersebut ditambahkan, mengindikasikan kemungkinan *file webshell* atau skrip jahat, sehingga keberadaannya patut dicurigai sebagai bagian dari aktivitas eksploitasi atau *backdoor access*

2. Implementasi Fitur *Threat Hunting*

a. Uji Deteksi Serangan XSS

Uji coba serangan *XSS* dilakukan dengan menyisipkan skrip *javascript* ke *URL*. Skrip ini bertujuan untuk memicu *pop-up* dengan tulisan ”iniSeranganXSSMantab” jika *input* tidak di sanitasi dengan benar, tetapi jika *input* telah disanitasi dengan benar maka karakter khusus akan ditiadakan.



Gambar 4. 17 Uji Coba Serangan *XSS*

Hasil dari serangan tersebut adalah sebuah *event* yang cukup jelas informasinya pada gambar 4.18.

	timestamp	agent.name	rule.description	rule.level	rule.id
	Jul 9, 2025 @ 15:45:26.307	agent-bengkaliskab.go.id	XSS (Cross Site Scripting) attempt.	6	31105

Gambar 4. 18 *XSS Event*

Pada tanggal 09 Juli 2025 pukul 15:45:26.307, sistem *Wazuh* mendeteksi sebuah upaya serangan *XSS* (*Cross Site Scripting*) pada *agent* bernama *agent-bengkaliskab.go.id*. Deteksi ini tercatat dengan *Rule ID 31105* dan memiliki tingkat keparahan *level* 6, yang mengindikasikan ancaman tingkat menengah.

b. Uji Deteksi Serangan *SQL Injection*

Uji coba serangan *SQL Injection* dilakukan dengan menyisipkan *query SQL '+UNION SELECT 1,2,3--+-* ke *URL*, tujuan nya adalah untuk memicu *event* pada *threat hunting*.

Gambar 4. 19 Uji oba Serangan *SQL Injection*

Hasil dari serangan tersebut adalah sebuah *event* yang cukup jelas informasinya pada gambar 4.20.

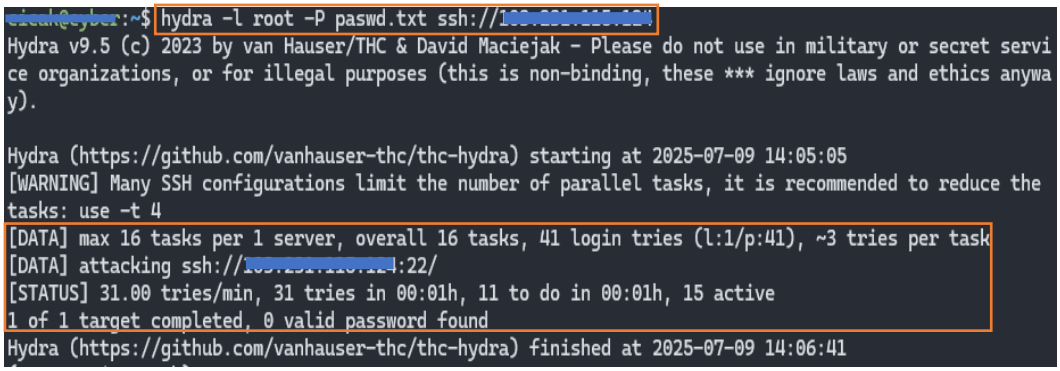
	timestamp	agent.name	rule.description	rule.level	rule.id
	Jul 9, 2025 @ 16:02:56.349	agent-bengkaliskab.go.id	SQL injection attempt.	6	31164

Gambar 4. 20 *SQL Injection Event*

Pada 09 Juli 2025 pukul 16:02:56, sistem *Wazuh* mendeteksi upaya serangan *SQL Injection* pada *agent agent-bengkaliskab.go.id* dengan *Rule ID 31164* dan tingkat keparahan *level* 6. Serangan ini merupakan percobaan penyisipan perintah *SQL* berbahaya melalui *input* aplikasi *web* dengan tujuan mengakses atau memanipulasi basis data secara ilegal.

c. Uji Deteksi Serangan *Bruteforce SSH*

Uji coba serangan *bruteforce ssh* dilakukan dengan alat *hydra* dengan kredensial pengguna *root* dan menggunakan *password list* dari *file paswd.txt*.



```
:~$ hydra -l root -P paswd.txt ssh://
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-09 14:05:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41 login tries (l:1/p:41), ~3 tries per task
[DATA] attacking ssh://                :22/
[STATUS] 31.00 tries/min, 31 tries in 00:01h, 11 to do in 00:01h, 15 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-09 14:06:41
```

Gambar 4. 21 Uji Coba Serangan *Bruteforce SSH*

	timestamp	agent.name	rule.description	rule.level	rule.id
	Jul 9, 2025 @ 14:05:09.262	agent-bengkaliskab.go.id	sshd: authentication failed.	5	5760
	Jul 9, 2025 @ 14:05:09.262	agent-bengkaliskab.go.id	sshd: authentication failed.	5	5760
	Jul 9, 2025 @ 14:05:09.262	agent-bengkaliskab.go.id	sshd: authentication failed.	5	5760
	Jul 9, 2025 @ 14:05:09.262	agent-bengkaliskab.go.id	sshd: authentication failed.	5	5760
	Jul 9, 2025 @ 14:05:09.262	agent-bengkaliskab.go.id	sshd: brute force trying to get access to the system. Authentication failed.	10	5763
	Jul 9, 2025 @ 14:05:09.247	agent-bengkaliskab.go.id	sshd: authentication failed.	5	5760
	Jul 9, 2025 @ 14:05:07.334	agent-bengkaliskab.go.id	PAM: User login failed.	5	5503
	Jul 9, 2025 @ 14:05:07.333	agent-bengkaliskab.go.id	PAM: User login failed.	5	5503
	Jul 9, 2025 @ 14:05:07.333	agent-bengkaliskab.go.id	PAM: User login failed.	5	5503
	Jul 9, 2025 @ 14:05:07.326	agent-bengkaliskab.go.id	PAM: User login failed.	5	5503
	Jul 9, 2025 @ 14:05:07.326	agent-bengkaliskab.go.id	PAM: User login failed.	5	5503
	Jul 9, 2025 @ 14:05:07.306	agent-bengkaliskab.go.id	PAM: Multiple failed logins in a small period of time.	10	5551
	Jul 9, 2025 @ 14:05:07.306	agent-bengkaliskab.go.id	PAM: User login failed.	5	5503
	Jul 9, 2025 @ 14:05:07.306	agent-bengkaliskab.go.id	PAM: User login failed.	5	5503
	Jul 9, 2025 @ 14:05:07.305	agent-bengkaliskab.go.id	PAM: User login failed.	5	5503
	Jul 9, 2025 @ 14:05:07.305	agent-bengkaliskab.go.id	PAM: User login failed.	5	5503
	Jul 9, 2025 @ 14:05:07.305	agent-bengkaliskab.go.id	PAM: User login failed.	5	5503
	Jul 9, 2025 @ 14:05:07.305	agent-bengkaliskab.go.id	PAM: User login failed.	5	5503
	Jul 9, 2025 @ 14:05:07.305	agent-bengkaliskab.go.id	PAM: User login failed.	5	5503
	Jul 9, 2025 @ 14:05:07.305	agent-bengkaliskab.go.id	PAM: User login failed.	5	5503

Gambar 4. 22 *Event SSH Bruteforce*

Pada 09 Juli 2025 pukul 14:05, *Wazuh* mendeteksi sejumlah besar kegagalan *login SSH* dan *PAM* pada *agent agent-bengkaliskab.go.id*. *Log* menunjukkan percobaan *login* yang terus-menerus gagal dalam waktu singkat, termasuk deteksi *brute force* dengan *level* keparahan 10 (*Rule ID 5763*), serta beberapa autentikasi gagal dengan *rule ID 5503, 5504, 5551* dan *5760* pada *level* 5. Aktivitas ini mengindikasikan adanya serangan *brute force SSH* yang mencoba menebak kredensial sistem secara berulang.

4.2.4 Dampak Implementasi Sistem

Implementasi sistem *monitoring* keamanan menggunakan *Wazuh* memberikan dampak yang signifikan, baik terhadap instansi tempat kerja praktik maupun terhadap penulis sebagai mahasiswa yang terlibat langsung dalam proses instalasi, konfigurasi dan pengujian sistem. Dampak terhadap Instansi:

1. Kemampuan deteksi ancaman secara *real-time*

   Dengan diaktifkannya fitur *Threat Hunting* dan *File Integrity Monitoring* (FIM), instansi kini dapat mengetahui adanya aktivitas mencurigakan seperti

brute force ssh login, *SQL Injection*, *XSS,* maupun perubahan *file* sistem secara langsung saat kejadian. Hal ini memungkinkan tim teknis mengambil langkah mitigasi lebih cepat sebelum serangan berkembang lebih jauh.

2. Pemantauan sistem lebih terpusat dan efisien
   Seluruh *log* dan *alert* dari *server* yang dipantau terkumpul dan divisualisasikan di *dashboard Wazuh* (*Kibana*). Hal ini membuat proses monitoring menjadi lebih efisien, tidak perlu lagi melakukan pengecekan manual pada tiap sistem. Tim dapat dengan mudah melihat riwayat aktivitas, pola serangan, serta potensi celah keamanan dalam satu tampilan terpadu.

Dampak terhadap Mahasiswa (Penulis):

1. Peningkatan *Skill Blue Team*
   Melalui proyek ini, penulis mendapatkan pengalaman langsung dalam membangun dan mengoperasikan sistem keamanan dari sudut pandang *blue team*, termasuk bagaimana melakukan analisis *log*, mendeteksi serangan.
2. Pemahaman *tools SIEM open-source*
   Penulis juga memperoleh pemahaman mendalam mengenai penggunaan SIEM (*Security Information and Event Management*) berbasis *open-source*, khususnya *Wazuh*, ini merupakan keahlian yang sangat relevan dalam industri keamanan siber saat ini.

Secara keseluruhan, sistem yang diimplementasikan tidak hanya memberikan manfaat teknis dan operasional bagi instansi, tetapi juga menjadi sarana belajar yang praktis dan berharga bagi penulis dalam mempersiapkan diri menghadapi tantangan di dunia kerja profesional, khususnya di bidang keamanan informasi.

BAB V
PENUTUP

5.1 Kesimpulan

Selama melaksanakan kerja praktik di Dinas Komunikasi dan Informatika Kabupaten Bengkalis, penulis memperoleh pengalaman dan manfaat yang sangat berharga, baik dari segi teknis maupun non-teknis. Secara teknis, penulis terlibat langsung dalam berbagai kegiatan yang relevan dengan bidang keamanan informasi, antara lain melakukan pengujian penetrasi (*penetration testing*) terhadap 50 *subdomain* milik instansi, menyusun laporan hasil uji keamanan secara sistematis, serta mengimplementasikan sistem monitoring keamanan berbasis *open-source security platform Wazuh*. Implementasi ini mencakup proses instalasi, konfigurasi, hingga pengujian fungsi *monitoring* terhadap aktivitas berpotensi ancaman seperti upaya eksploitasi celah keamanan aplikasi *web*. Selain peningkatan keterampilan teknis, kerja praktik ini juga memberikan kesempatan kepada penulis untuk membangun jejaring profesional dengan para pegawai di lingkungan instansi yang sangat berguna dalam pengembangan karier ke depan. Dari sisi *soft skill*, penulis dilatih untuk bekerja secara disiplin, profesional, serta tepat waktu dalam menyelesaikan tugas-tugas yang diberikan oleh pembimbing lapangan. Secara keseluruhan, rangkaian kegiatan selama kerja praktik ini tidak hanya memperkaya wawasan dan keterampilan penulis dalam bidang keamanan informasi, tetapi juga memperkuat pemahaman terhadap penerapan praktik keamanan siber dalam konteks nyata di lingkungan pemerintahan.

5.2 Saran

Berdasarkan hasil kerja praktik yang telah dilaksanakan, penulis menyampaikan beberapa saran yang diharapkan dapat menjadi masukan konstruktif bagi pengembangan sistem, instansi dan mahasiswa di masa mendatang.

5.2.1 Saran Untuk Pengembangan Tugas

Sistem monitoring keamanan menggunakan *Wazuh* yang telah diimplementasikan masih memiliki ruang pengembangan. Disarankan untuk menambahkan fitur notifikasi *real-time* melalui *Telegram*, *email* atau web *dashboard* guna meningkatkan respons terhadap insiden. Selain itu, pengembangan analisis korelasi *log* dari berbagai sumber akan memperkuat kemampuan deteksi terhadap serangan kompleks.

5.2.2 Saran Pengembangan Projek Sebagai Topik Skripsi

Project ini dapat dikembangkan menjadi topik skripsi yang relevan, seperti: "Analisis Efektivitas *Wazuh* sebagai *Platform SIEM* dalam Mendeteksi Ancaman Siber di Lingkungan Pemerintahan."
Topik ini dapat mencakup pengujian berbagai jenis serangan, pembuatan custom rules, serta evaluasi performa dibandingkan dengan platform SIEM lainnya.

5.2.3 Saran Untuk Instansi

Dinas Kominfo Bengkalis disarankan untuk terus mendukung penggunaan teknologi *open source* dalam keamanan informasi. Penyusunan dokumentasi teknis yang rapi dan pelatihan internal yang rutin akan sangat membantu dalam meningkatkan kesiapan dan kapasitas tim IT.

5.2.4 Saran Untuk Mahasiswa Selanjutnya

Mahasiswa yang akan melaksanakan kerja praktik disarankan untuk memiliki pemahaman dasar tentang *Linux*, jaringan komputer, serta keamanan siber. Kemampuan membaca dan menganalisis *log*, memahami sistem monitoring, serta menulis laporan teknis akan sangat menunjang keberhasilan. Selain itu, sikap proaktif dan komunikasi yang baik dengan pembimbing sangat penting untuk mendukung kelancaran magang.

DAFTAR PUSTAKA

[1] H. R. A. Nurul Aulia Dewi, “LAPORAN PRAKTEK KERJA LAPANGAN DISKOMINFO PROV. KALTIM DI BIDANG APTIKA (APLIKASI INFORMATIKA),” 2024.

[2] Anggun Fitriyani, “LAPORAN KERJA PRAKTEK DINAS KOMUNIKASI INFORMATIKA DAN STATISTIK PROVINSI RIAU,” 2024.

[3] M. Dody Firmansyah, “Perancangan Web E-Commerce Berbasis Website pada Toko Ida Shoes,” 2023.

[4] M. Reddy Basireddy, “Investigations into Security Testing Techniques, Tools, and Methodologies for Identifying and Mitigating Security Vulnerabilities A B S T R A C T Journal of Artificial Intelligence, Machine Learning and Data Science,” *J Artif Intell Mach Learn & Data Sci*, vol. 2024, no. 1, p. 626, 2024, doi: 10.51219/JAIMLD/maheswara.

[5] M. Mattsson, “A comparison of FFUF and Wfuzz for fuzz testing web applications.”

[6] M. Rizky, R. Pahlevi, C. Umam, and L. B. Handoko, “Deteksi dan Pencegahan Web Defacing Judi Online dengan Wazuh SIEM dan Snort IDS Berbasis Signature”, doi: 10.33364/algoritma/v.22-1.2220.

LAMPIRAN

Lampiran 1 Surat Pengajuan Kerja Praktek

KEMENTERIAN PENDIDIKAN TINGGI, SAINS DAN TEKNOLOGI
POLITEKNIK NEGERI BENGKALIS
Jalan Bathin Alam, Sungai Alam, Bengkalis, Riau 28711
Telepon: (+62766) 24566, Fax: (+62766) 800 1000
Laman: http.://www.polbeng.ac.id, E-mail: polbeng@polbeng.ac.id

Nomor : 374/PL31/TU/2024 10 Januari 2025
Hal : **Permohonan Kerja Praktek (KP)**

Yth. Kepala Dinas Komunikasi Informatika dan Statistik Kabupaten Bengkalis
Jl. R. A. Kartini, Bengkalis Kota, Kec. Bengkalis, Kabupaten Bengkalis, Riau 28712

Dengan hormat,

Sehubungan akan dilaksanakannya Kerja Praktek untuk Mahasiswa Politeknik Negeri Bengkalis yang bertujuan untuk meningkatkan pengetahuan dan keterampilan mahasiswa kami di Bidang Teknik Informatika melalui keterlibatan secara langsung dalam berbagai kegiatan di perusahaan, maka kami mengharapkan kesediaan dan kerjasama Bapak/Ibu untuk dapat menerima mahasiswa kami guna melaksanakan Kerja Praktek di Perusahaan yang Bapak/Ibu pimpin. Pelaksanaan Kerja Praktek mahasiswa Politeknik Negeri Bengkalis akan dimulai pada bulan 24 Februari sd 27 Juni 2025, adapun nama mahasiswa sebagai berikut:

No	Nama	NIM	PROGRAM STUDI
1	Aryanto Winata	6404211029	D-IV Keamanan Sistem Informasi
2	Rimba Dirgantara	6404211035	D-IV Keamanan Sistem Informasi
3	Ayu Wandira	6304211348	D-IV Rekayasa Perangkat Lunak
4	Izatul Fateha	6304211389	D-IV Rekayasa Perangkat Lunak
5	Feri Pratama	6304211366	D-IV Rekayasa Perangkat Lunak

Kami sangat mengharapkan informasi lebih lanjut dari Bapak/Ibu melalui balasan surat atau menghubungi narahubung dalam waktu dekat.

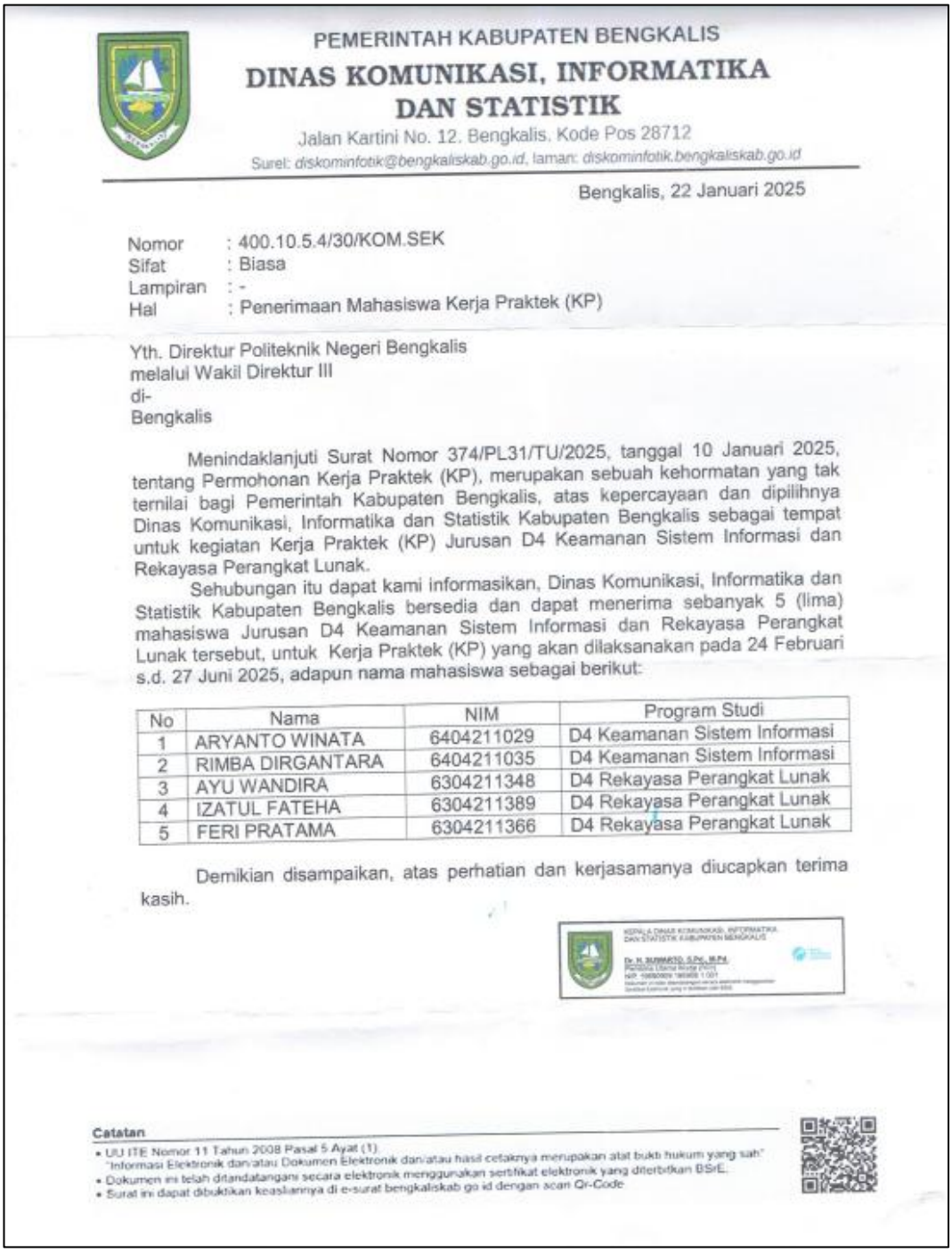
Demikian permohonan ini disampaikan, atas perhatian dan perkenan Bapak/Ibu kami ucapkan terima kasih.

a.n. Direktur,
Wakil Direktur III

Marhadi Sastra., S.T., M.Sc
NIP.198903142015041001

Koordinator KP Keamanan Sistem Informasi :
Rezki Kurniati, M.Kom (085265516425)

Lampiran 2 Surat Balasan Diterima Kerja Praktek



PEMERINTAH KABUPATEN BENGKALIS

DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK

Jalan Kartini No. 12. Bengkalis. Kode Pos 28712

Surel: diskominfotik@bengkaliskab.go.id, laman: diskominfotik.bengkaliskab.go.id

Bengkalis, 22 Januari 2025

Nomor : 400.10.5.4/30/KOM.SEK
Sifat : Biasa
Lampiran : -
Hal : Penerimaan Mahasiswa Kerja Praktek (KP)

Yth. Direktur Politeknik Negeri Bengkalis
melalui Wakil Direktur III
di-
Bengkalis

Menindaklanjuti Surat Nomor 374/PL31/TU/2025, tanggal 10 Januari 2025, tentang Permohonan Kerja Praktek (KP), merupakan sebuah kehormatan yang tak ternilai bagi Pemerintah Kabupaten Bengkalis, atas kepercayaan dan dipilihnya Dinas Komunikasi, Informatika dan Statistik Kabupaten Bengkalis sebagai tempat untuk kegiatan Kerja Praktek (KP) Jurusan D4 Keamanan Sistem Informasi dan Rekayasa Perangkat Lunak.

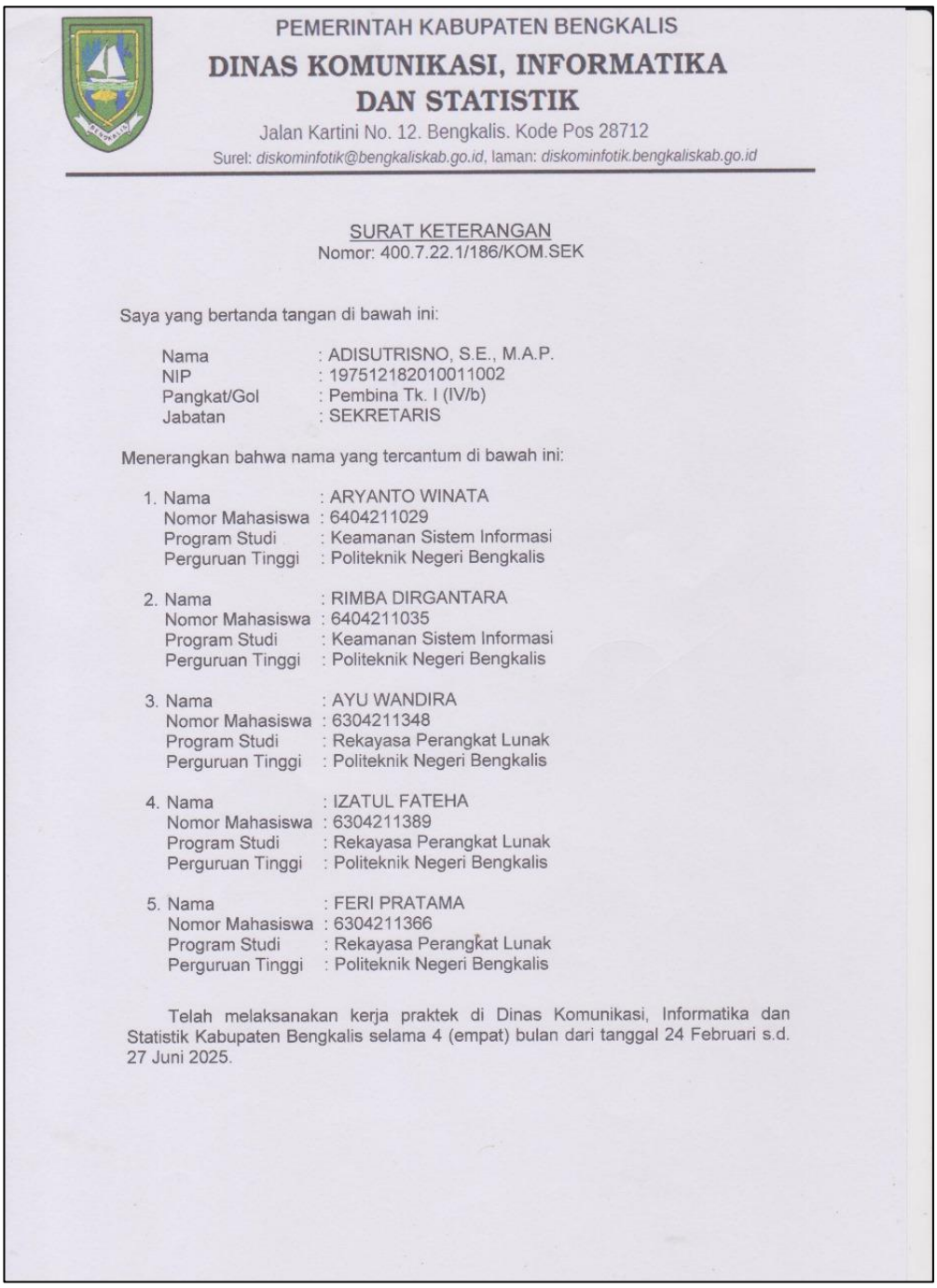
Sehubungan itu dapat kami informasikan, Dinas Komunikasi, Informatika dan Statistik Kabupaten Bengkalis bersedia dan dapat menerima sebanyak 5 (lima) mahasiswa Jurusan D4 Keamanan Sistem Informasi dan Rekayasa Perangkat Lunak tersebut, untuk Kerja Praktek (KP) yang akan dilaksanakan pada 24 Februari s.d. 27 Juni 2025, adapun nama mahasiswa sebagai berikut:

No	Nama	NIM	Program Studi
1	ARYANTO WINATA	6404211029	D4 Keamanan Sistem Informasi
2	RIMBA DIRGANTARA	6404211035	D4 Keamanan Sistem Informasi
3	AYU WANDIRA	6304211348	D4 Rekayasa Perangkat Lunak
4	IZATUL FATEHA	6304211389	D4 Rekayasa Perangkat Lunak
5	FERI PRATAMA	6304211366	D4 Rekayasa Perangkat Lunak

Demikian disampaikan, atas perhatian dan kerjasamanya diucapkan terima kasih.

Catatan
- UU ITE Nomor 11 Tahun 2008 Pasal 5 Ayat (1)
"Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"
- Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSrE.
- Surat ini dapat dibuktikan keasliannya di e-surat bengkaliskab go id dengan scan Qr-Code

Lampiran 3 Surat Keterangan Bahwa Mahasiswa Telah Menyelesaikan Kerja Praktek



PEMERINTAH KABUPATEN BENGKALIS

DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK

Jalan Kartini No. 12. Bengkalis. Kode Pos 28712

Surel: *diskominfotik@bengkaliskab.go.id*, laman: *diskominfotik.bengkaliskab.go.id*

SURAT KETERANGAN
Nomor: 400.7.22.1/186/KOM.SEK

Saya yang bertanda tangan di bawah ini:

Nama	: ADISUTRISNO, S.E., M.A.P.
NIP	: 197512182010011002
Pangkat/Gol	: Pembina Tk. I (IV/b)
Jabatan	: SEKRETARIS

Menerangkan bahwa nama yang tercantum di bawah ini:

1. Nama : ARYANTO WINATA
   Nomor Mahasiswa : 6404211029
   Program Studi : Keamanan Sistem Informasi
   Perguruan Tinggi : Politeknik Negeri Bengkalis

2. Nama : RIMBA DIRGANTARA
   Nomor Mahasiswa : 6404211035
   Program Studi : Keamanan Sistem Informasi
   Perguruan Tinggi : Politeknik Negeri Bengkalis

3. Nama : AYU WANDIRA
   Nomor Mahasiswa : 6304211348
   Program Studi : Rekayasa Perangkat Lunak
   Perguruan Tinggi : Politeknik Negeri Bengkalis

4. Nama : IZATUL FATEHA
   Nomor Mahasiswa : 6304211389
   Program Studi : Rekayasa Perangkat Lunak
   Perguruan Tinggi : Politeknik Negeri Bengkalis

5. Nama : FERI PRATAMA
   Nomor Mahasiswa : 6304211366
   Program Studi : Rekayasa Perangkat Lunak
   Perguruan Tinggi : Politeknik Negeri Bengkalis

Telah melaksanakan kerja praktek di Dinas Komunikasi, Informatika dan Statistik Kabupaten Bengkalis selama 4 (empat) bulan dari tanggal 24 Februari s.d. 27 Juni 2025.

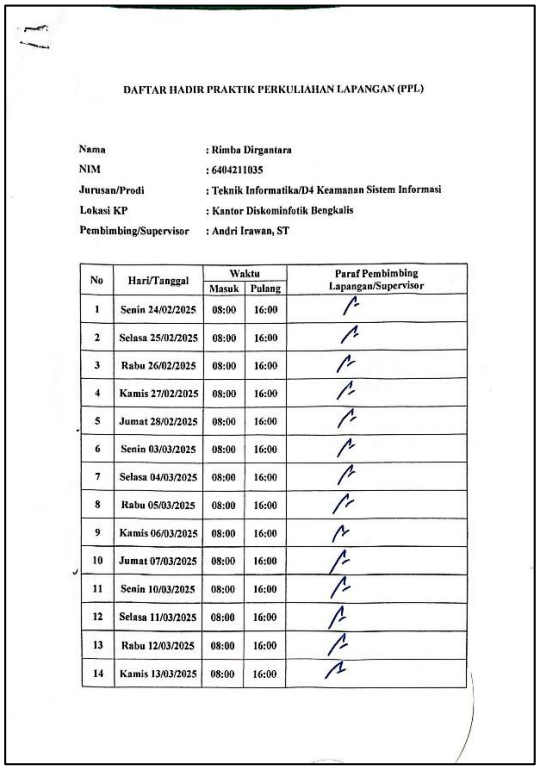
Demikianlah surat keterangan ini dibuat untuk dapat dipergunakan sebagaimana mestinya.

Bengkalis, 18 Juli 2025

a.n. KEPALA DINAS KOMUNIKASI,
INFORMATIKA DAN STATISTIK
KABUPATEN BENGKALIS
SEKRETARIS,

ADISUTRISNO, S.E., M.A.P.
Pembina Tk. I (IV/b)
NIP 19751218 201001 1 002

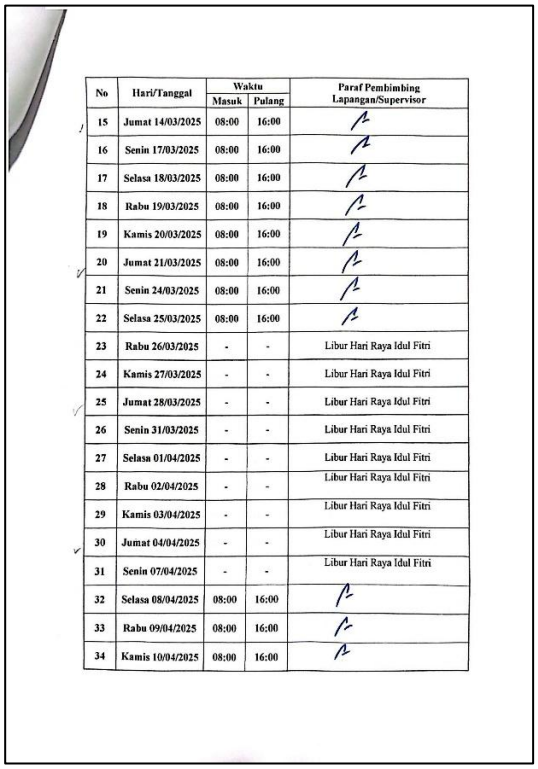
Lampiran 4 Absensi Kerja Praktek



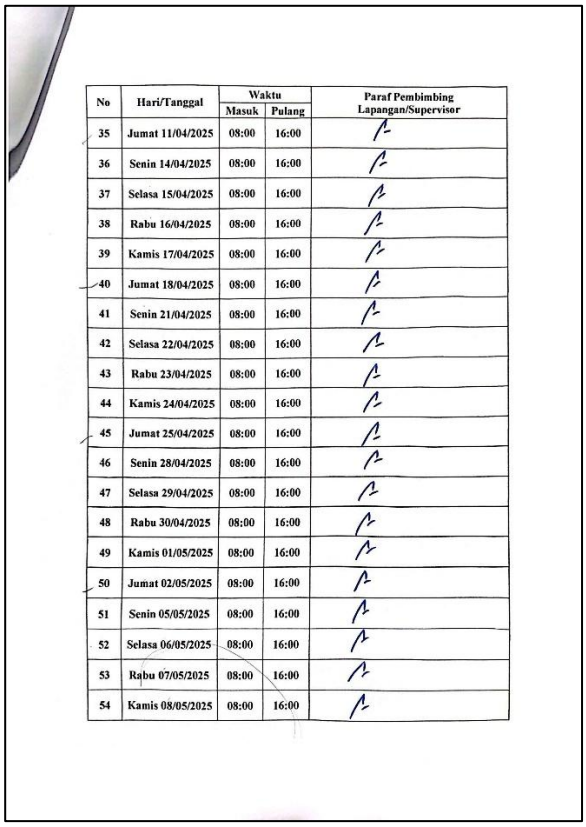
DAFTAR HADIR PRAKTIK PERKULIAHAN LAPANGAN (PPL)

Nama : Rimba Dirgantara
NIM : 6404211035
Jurusan/Prodi : Teknik Informatika/D4 Keamanan Sistem Informasi
Lokasi KP : Kantor Diskominfotik Bengkalis
Pembimbing/Supervisor : Andri Irawan, ST

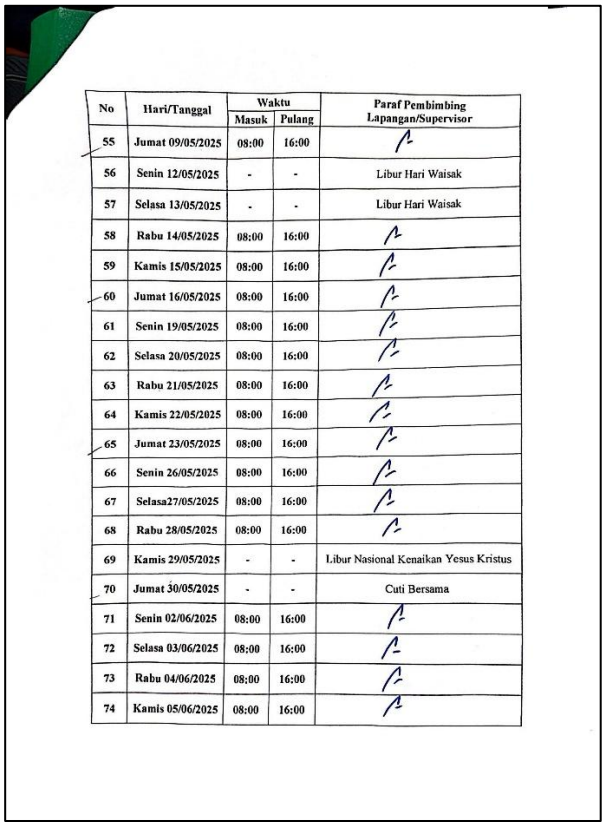
No	Hari/Tanggal	Waktu		Paraf Pembimbing Lapangan/Supervisor
		Masuk	Pulang	
1	Senin 24/02/2025	08:00	16:00	
2	Selasa 25/02/2025	08:00	16:00	
3	Rabu 26/02/2025	08:00	16:00	
4	Kamis 27/02/2025	08:00	16:00	
5	Jumat 28/02/2025	08:00	16:00	
6	Senin 03/03/2025	08:00	16:00	
7	Selasa 04/03/2025	08:00	16:00	
8	Rabu 05/03/2025	08:00	16:00	
9	Kamis 06/03/2025	08:00	16:00	
10	Jumat 07/03/2025	08:00	16:00	
11	Senin 10/03/2025	08:00	16:00	
12	Selasa 11/03/2025	08:00	16:00	
13	Rabu 12/03/2025	08:00	16:00	
14	Kamis 13/03/2025	08:00	16:00	



No	Hari/Tanggal	Waktu		Paraf Pembimbing Lapangan/Supervisor
		Masuk	Pulang	
15	Jumat 14/03/2025	08:00	16:00	
16	Senin 17/03/2025	08:00	16:00	
17	Selasa 18/03/2025	08:00	16:00	
18	Rabu 19/03/2025	08:00	16:00	
19	Kamis 20/03/2025	08:00	16:00	
20	Jumat 21/03/2025	08:00	16:00	
21	Senin 24/03/2025	08:00	16:00	
22	Selasa 25/03/2025	08:00	16:00	
23	Rabu 26/03/2025	-	-	Libur Hari Raya Idul Fitri
24	Kamis 27/03/2025	-	-	Libur Hari Raya Idul Fitri
25	Jumat 28/03/2025	-	-	Libur Hari Raya Idul Fitri
26	Senin 31/03/2025	-	-	Libur Hari Raya Idul Fitri
27	Selasa 01/04/2025	-	-	Libur Hari Raya Idul Fitri
28	Rabu 02/04/2025	-	-	Libur Hari Raya Idul Fitri
29	Kamis 03/04/2025	-	-	Libur Hari Raya Idul Fitri
30	Jumat 04/04/2025	-	-	Libur Hari Raya Idul Fitri
31	Senin 07/04/2025	-	-	Libur Hari Raya Idul Fitri
32	Selasa 08/04/2025	08:00	16:00	
33	Rabu 09/04/2025	08:00	16:00	
34	Kamis 10/04/2025	08:00	16:00	



No	Hari/Tanggal	Waktu		Paraf Pembimbing Lapangan/Supervisor
		Masuk	Pulang	
35	Jumat 11/04/2025	08:00	16:00	
36	Senin 14/04/2025	08:00	16:00	
37	Selasa 15/04/2025	08:00	16:00	
38	Rabu 16/04/2025	08:00	16:00	
39	Kamis 17/04/2025	08:00	16:00	
40	Jumat 18/04/2025	08:00	16:00	
41	Senin 21/04/2025	08:00	16:00	
42	Selasa 22/04/2025	08:00	16:00	
43	Rabu 23/04/2025	08:00	16:00	
44	Kamis 24/04/2025	08:00	16:00	
45	Jumat 25/04/2025	08:00	16:00	
46	Senin 28/04/2025	08:00	16:00	
47	Selasa 29/04/2025	08:00	16:00	
48	Rabu 30/04/2025	08:00	16:00	
49	Kamis 01/05/2025	08:00	16:00	
50	Jumat 02/05/2025	08:00	16:00	
51	Senin 05/05/2025	08:00	16:00	
52	Selasa 06/05/2025	08:00	16:00	
53	Rabu 07/05/2025	08:00	16:00	
54	Kamis 08/05/2025	08:00	16:00	



No	Hari/Tanggal	Waktu		Paraf Pembimbing Lapangan/Supervisor
		Masuk	Pulang	
55	Jumat 09/05/2025	08:00	16:00	
56	Senin 12/05/2025	-	-	Libur Hari Waisak
57	Selasa 13/05/2025	-	-	Libur Hari Waisak
58	Rabu 14/05/2025	08:00	16:00	
59	Kamis 15/05/2025	08:00	16:00	
60	Jumat 16/05/2025	08:00	16:00	
61	Senin 19/05/2025	08:00	16:00	
62	Selasa 20/05/2025	08:00	16:00	
63	Rabu 21/05/2025	08:00	16:00	
64	Kamis 22/05/2025	08:00	16:00	
65	Jumat 23/05/2025	08:00	16:00	
66	Senin 26/05/2025	08:00	16:00	
67	Selasa27/05/2025	08:00	16:00	
68	Rabu 28/05/2025	08:00	16:00	
69	Kamis 29/05/2025	-	-	Libur Nasional Kenaikan Yesus Kristus
70	Jumat 30/05/2025	-	-	Cuti Bersama
71	Senin 02/06/2025	08:00	16:00	
72	Selasa 03/06/2025	08:00	16:00	
73	Rabu 04/06/2025	08:00	16:00	
74	Kamis 05/06/2025	08:00	16:00	

Lampiran 5 *Log* Mingguan

KEGIATAN HARIAN KERJA PRAKTEK (KP)

NAMA : Rimba Dirgantara
NIM : 6404211035
Hari/Tanggal : Senin-Jumat / Mingu I
Tanggal : 24 – 28 februari 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Pengenalan Lingkungan Kerja. 2. Pengenalan Diri Masing-masing. 3. Pengenalan Sama Senior.	Andri Irawan, ST	
Catatan Pembimbing		

Hari/Tanggal : Senin-Jumat / Mingu III
Tanggal : 10 – 14 Maret 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melakukan uji keamanan website pupr.bengkaliskab.go.id 2. Melakukan uji keamanan website pupr.bengkaliskab.go.id 3. Melakukan uji keamanan website prokopim.bengkaliskab.go.id 4. Melakukan uji keamanan website ppdb.bengkaliskab.go.id	Andri Irawan, ST	
Catatan Pembimbing		
Bagus.		

Hari/Tanggal : Senin-Jumat / Mingu III
Tanggal : 10 – 14 Maret 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melakukan uji keamanan website pupr.bengkaliskab.go.id 2. Melakukan uji keamanan website pupr.bengkaliskab.go.id 3. Melakukan uji keamanan website prokopim.bengkaliskab.go.id 4. Melakukan uji keamanan website ppdb.bengkaliskab.go.id	Andri Irawan, ST	
Catatan Pembimbing		
Bagus.		

Hari/Tanggal : Senin-Jumat / Mingu IV
Tanggal : 17 – 21 Maret 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melakukan uji keamanan website ppdb.bengkaliskab.go.id 2. Melakukan uji keamanan website mikoumkm.bengkaliskab.go.id 3. Melakukan uji keamanan website koperasiukm.bengkaliskab.go.id	Andri Irawan, ST	
Catatan Pembimbing		
Bagus.		

Hari/Tanggal : Senin-Jumat / Mingu V

Tanggal : 24 – 28 Maret 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melakukan uji keamanan website kemenag.bengkaliskab.go.id 2. Melakukan uji keamanan website kesbangpol.bengkaliskab.go.id 3. Cuti Hari Raya Idul Fitri	Andri Irawan, ST	
Catatan Pembimbing		
Bagus.		

Hari/Tanggal : Senin-Jumat / Mingu VI

Tanggal : 31 Maret – 04 April 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Cuti Hari Raya Idul Fitri	Andri Irawan, ST	
Catatan Pembimbing		

Hari/Tanggal : Senin-Jumat / Mingu VII

Tanggal : 07 – 11 April 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Cuti Hari Raya Idul Fitri 2. Melakukan uji keamanan website jdih.bengkaliskab.go.id 3. Melakukan uji keamanan website inspektorat.bengkaliskab.go.id 4. Melakukan uji keamanan website epinter.bengkaliskab.go.id 5. Melalukan uji keamanan website dashboard.bengkaliskab.go.id 6. Baraan ke rumah pak sekretaris	Andri Irawan, ST	
Catatan Pembimbing		

GAMBARAN KERJA	KETERANGAN
	Baraan ke rumah pak sekretaris

Hari/Tanggal : Senin-Jumat / Mingu VIII

Tanggal : 14 – 18 April 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melakukan uji keamanan website e-mtq.bengkaliskab.go.id 2. Melakukan uji keamanan website e-antrian.bengkaliskab.go.id 3. Melakukan uji keamanan website dprd.bengkaliskab.go.id 4. Melakukan uji keamanan website dlh.bengkaliskab.go.id 5. Melalukan uji keamanan website diskominfotik.bengkaliskab.go.id	Andri Irawan, ST	
Catatan Pembimbing		
Bagus.		

Hari/Tanggal : Senin-Jumat / Minggu IX

Tanggal : 21 – 25 April 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melakukan uji keamanan website dishub.bengkaliskab.go.id 2. Melakukan uji keamanan website disperindag.bengkaliskab.go.id 3. Melakukan uji keamanan website dinkes.bengkaliskab.go.id 4. Melakukan uji keamanan website desaku.bengkaliskab.go.id 5. Melalukan uji keamanan website diskominfotik.bengkaliskab.go.id	Andri Irawan, ST	
Catatan Pembimbing		
Baik.		

Hari/Tanggal : Senin-Jumat / Minggu X

Tanggal : 28 April – 02 Mei 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melakukan uji keamanan website damkar.bengkaliskab.go.id 2. Melakukan uji keamanan website camattalangmuandau.bengkaliskab.go.id 3. Melakukan uji keamanan website dinkes.bengkaliskab.go.id 4. Melakukan uji keamanan website camatsiakkecil.bengkaliskab.go.id 5. Melalukan uji keamanan website camatrupat.bengkaliskab.go.id	Andri Irawan, ST	
Catatan Pembimbing		
Baik.		

Hari/Tanggal : Senin-Jumat / Minggu XI

Tanggal : 05 - 09 Mei 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melakukan uji keamanan website camatpinggir.bengkaliskab.go.id 2. Melakukan uji keamanan website camatmandau.bengkaliskab.go.id 3. Melakukan uji keamanan website camatbukitbatu.bengkaliskab.go.id 4. Melakukan uji keamanan website camatbengkalis.bengkaliskab.go.id 5. Melalukan uji keamanan website camatbengkalis.bengkaliskab.go.id	Andri Irawan, ST	
Catatan Pembimbing		
Baik.		

Hari/Tanggal : Senin-Jumat / Minggu XII

Tanggal : 12 - 16 Mei 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Libur Waisak 2. Melakukan uji keamanan website camatbathinsolapan.bengkaliskab.go.id 3. Melakukan uji keamanan website camatbantan.bengkaliskab.go.id 4. Melakukan uji keamanan website camatbandarlaksamana.bengkaliskab.go.id 5. Instalasi dan konfigurasi wazuh server dan agent 6. Konfigurasi lanjutan 7. Simulasi	Andri Irawan, ST	
Catatan Pembimbing		

Hari/Tanggal : Senin-Jumat / Minggu XIII

Tanggal : 19 - 23 Mei 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melakukan uji keamanan website bpkad.bengkaliskab.go.id 2. Melakukan uji keamanan website bkpp.bengkaliskab.go.id 3. Melakukan uji keamanan website bestie.bengkaliskab.go.id 4. Melakukan uji keamanan website camatbandarlaksamana.bengkaliskab.go.id	Andri Irawan, ST	
Catatan Pembimbing		
Bagus		

Hari/Tanggal : Senin-Jumat / Minggu XIV

Tanggal : 26 - 30 Mei 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melakukan uji keamanan website bappeda.bengkaliskab.go.id 2. Melakukan uji keamanan website bapokting.bengkaliskab.go.id 3. Cuti Bersama	Andri Irawan, ST	
Catatan Pembimbing		
Bagus .		

Hari/Tanggal : Senin-Jumat / Minggu XV

Tanggal : 02 - 06 Juni 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melakukan uji keamanan website absensiuat.bengkaliskab.go.id 2. Melakukan uji keamanan website website bengkaliskab.go.id 3. Melakukan uji keamanan website prokopim.bengkaliskab.go.id 4. Melakukan uji keamanan website jdih.bengkaliskab.go.id 5. Melakukan uji keamanan website epinter.bengkaliskab.go.id	Andri Irawan, ST	
Catatan Pembimbing		

Hari/Tanggal : Senin-Jumat / Minggu XVI

Tanggal : 09 - 13 Juni 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Cuti Bersama Hari Raya Idul Adha 1446H 2. menulis laporan hasil uji keamanan website diskominfotik.bengkaliskab.go.id dan berkunjung ke ruanga server diskominfo 3. melakukan uji keamanan website desaku.bengkaliskab.go.id 4. melakukan uji keamanan website camatsiakkecil.bengkaliskab.go.id 5. melakukan uji keamanan website camatrupatutara.bengkaliskab.go.id	Andri Irawan, ST	
Catatan Pembimbing		

GAMBARAN KERJA	KETERANGAN
	Berkunjung ke ruangan server

Hari/Tanggal : Senin-Jumat / Mingu XVII

Tanggal : 16 - 20 Juni 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Menulis laporan uji keamanan website camathandarlaksamana.bengkaliskab.go.id 2. Menulis laporan uji keamanan website bpbd.bengkaliskab.go.id 3. Menulis laporan kp bab 1 sampai bab 3 4. Menulis laporan kerja praktek bab 3 sampai bab 4	Andri Irawan, ST	
Catatan Pembimbing		

Hari/Tanggal : Senin-Jumat / Mingu XVII

Tanggal : 23 - 27 Juni 2025

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Menulis laporan kp bab 1 sampai bab 5	Andri Irawan, ST	
Catatan Pembimbing		

Lampiran 6 Formulir Penilaian Dari Instansi

PENILAIAN DARI PERUSAHAAN KERJA PRAKTEK

KANTOR DINAS KOMUNIKASI INFORMASI DAN STATISTIKA

Jl. Kartini No 12 Bengkalis

Nama : Rimba Dirgantara

NIM : 6404211035

Program Studi : D4 Keamanan Sistem Informasi Politeknik Negeri Bengkalis

No.	Aspek Penilaian	Bobot	Nilai
1.	Displin	20%	95
2.	Tanggung Jawab	25%	90
3.	Penyesuaian Diri	10%	90
4.	Hasil Kerja	30%	95
5.	Perilaku Secara Umum	15%	90
	Total Jumlah (1+2+3+4+5)	100%	460

Keterangan :

Nilai : Kriteria

81 – 100 : Istimewa

71 – 80 : Baik Sekali

66 – 70 : Baik

61 – 65 : Cukup Baik

56 – 60 : Cukup

Catatan :

Perbanyak latihan tentang security, analisis dan buku referensi.

Bengkalis, 27 Juni 2025

Andri Irawan, ST

Pembimbing Lapangan

Lampiran 7 Surat Pernyataan Proyek Kerja Praktek

Surat Pernyataan Penyelesaian Proyek Kerja Praktek

Yang bertanda tangan di bawah ini:

Nama	: Andri Irawan, S.T
Jabatan	: Pranata Komputer Ahli Muda
Instansi	: Dinas Komunikasi, Informatika dan Statistik Bengkalis

Dengan ini menyatakan bahwa:

Nama	: Rimba Dirgantara
NIM	: 6404211035
Perguruan Tinggi	: Politeknik Negeri Bengkalis

Telah menyelesaikan proyek praktek dengan judul "Implementasi Threat Hunting Dan Pemantauan File Integrity Monitoring Menggunakan Wazuh Di Dinas Komunikasi Dan Informatika Kabupaten Bengkalis" sesuai dengan tugas yang diberikan selama masa kerja praktek. Wazuh merupakan alat yang dapat membantu dalam mendeteksi serangan siber dan aktifitas mencurigakan pada server aplikasi. Demikian surat ini dibuat untuk digunakan sebagaimana mestinya.

Bengkalis, 26 Juli 2025

PEMERINTAH KABUPATEN BENGKALIS
DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK

Andri Irawan, S.T

Lampiran 8 Sertifikat Magang

SERTIFIKAT

Nomor: 400.10.5.4/184/KOM.SEK

Diberikan kepada:

RIMBA DIRGANTARA

POLITEKNIK NEGERI BENGKALIS

Telah menyelesaikan Kerja Praktek selama 4 (empat) bulan,
terhitung dari tanggal 24 Februari s.d. 27 Juni 2025
pada Dinas Komunikasi, Informatika dan Statistik Kabupaten Bengkalis

Bengkalis, 17 Juli 2025

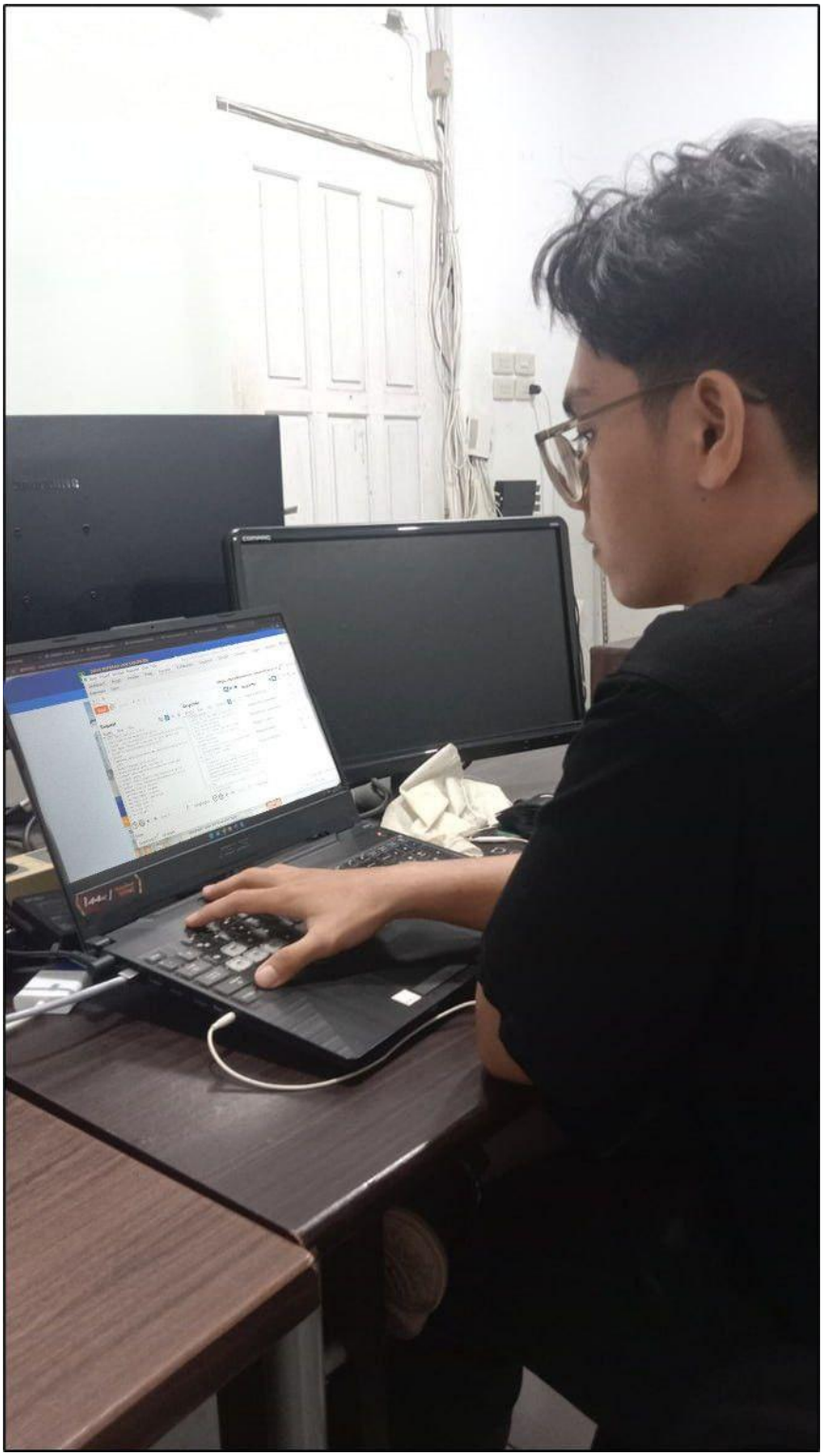
KEPALA DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KABUPATEN BENGKALIS

Dr. H. SYAHRIYO, S.Pd., M.Pd.

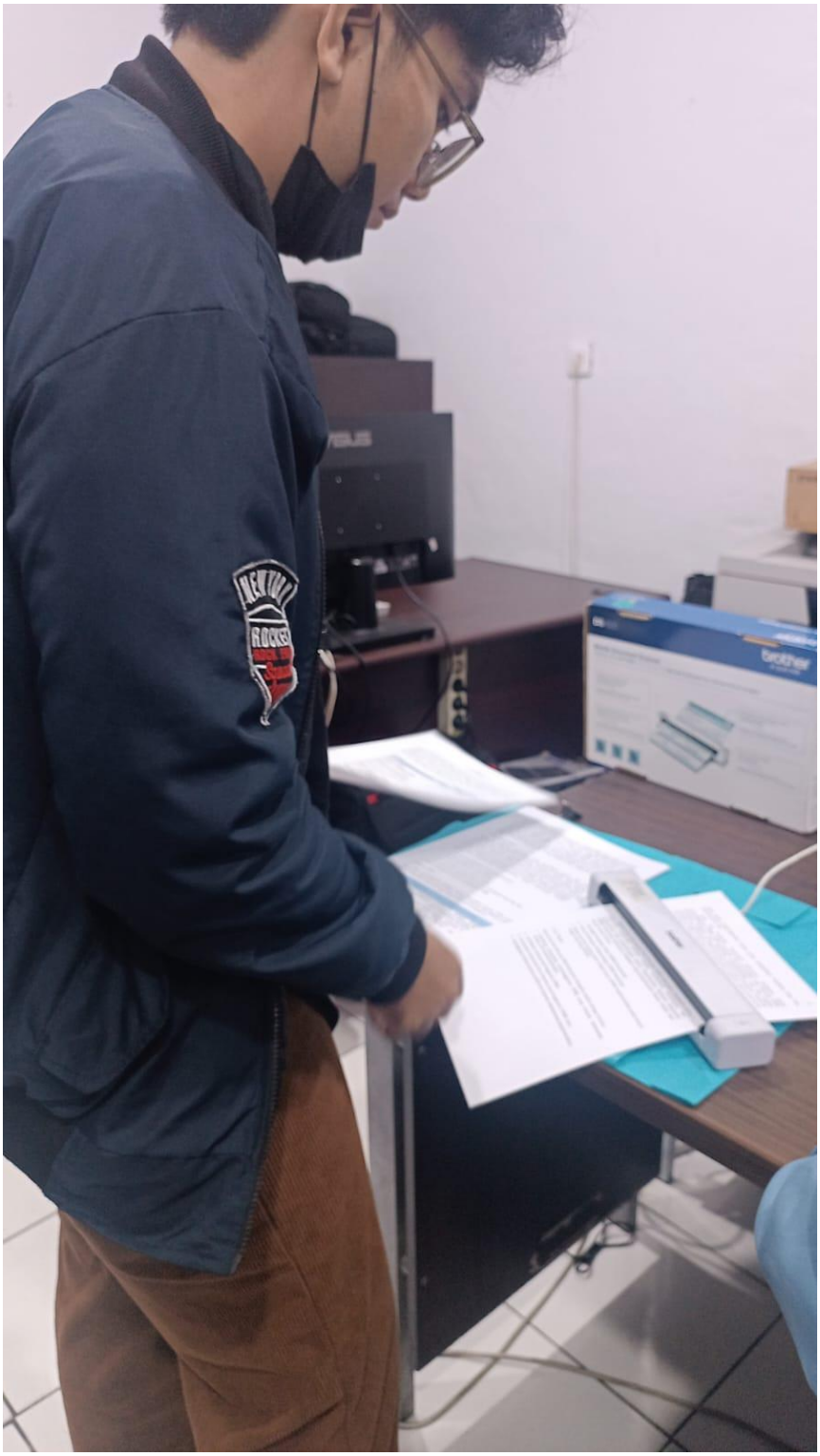
Catatan

- UU ITE Nomor 11 Tahun 2008 Pasal 5 Ayat (1):
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"
- Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSrE.
- Surat ini dapat dibuktikan keasliannya di e-surat bengkaliskab go id dengan *scan Qr-Code*.

Lampiran 9 Kegiatan Uji Keamanan *Website*



Lampiran 10 Kegiatan *Scanning* Dokumen



Lampiran 11 Kegiatan *Fotocopy* Dokumen