

## PKM Pengembangan Sistem Monitoring Keamanan Server Aplikasi SIMLP2M UNM Menggunakan Wazuh

<sup>1\*</sup>Abdul Wahid, <sup>2</sup>Muhammad Agung, <sup>3</sup>Jumadi Mabe Parenreng, <sup>4</sup>Fatimah Hidayahni Amin,  
<sup>5</sup>Seny Luhriyani

<sup>1,4,5</sup>Jurusan Bahasa Inggris, Fakultas Bahasa dan Sastra, Universitas Negeri Makassar

<sup>2</sup>Jurusan Pendidikan Teknik Mesin, Fakultas Teknik, Universitas Negeri Makassar

<sup>3</sup>Jurusan Teknik Informatika dan Komputer, Fakultas Teknik, Universitas Negeri Makassar

Email: wahid@unm.ac.id<sup>1</sup>, agung@unm.ac.id<sup>2</sup>, jparenreng@unm.ac.id<sup>3</sup>, fatimah.hidayahni@unm.ac.id<sup>4</sup>,  
senyluhriyanifbs@unm.ac.id<sup>5</sup>

\*Corresponding author: wahid@unm.ac.id

Received : 13 September 2024

Accepted : 15 Oktober 2024

Published : 21 Oktober 2024

### ABSTRAK

Aplikasi SIMLP2M Universitas Negeri Makassar merupakan sistem yang mengelola data penting terkait penelitian dan pengabdian kepada masyarakat yang dilakukan oleh dosen dan peneliti. Mengingat sensitivitas data yang dikelola, keamanan server aplikasi ini menjadi prioritas. Belum adanya sistem monitoring keamanan yang efektif membuat server ini rentan terhadap serangan siber. PKM ini bertujuan untuk meningkatkan keamanan server SIMLP2M melalui pengembangan sistem monitoring berbasis Wazuh, sebuah perangkat lunak open-source yang mampu mendeteksi dan mencegah ancaman siber secara real-time. PKM ini dilaksanakan dalam beberapa tahapan, yaitu survei dan analisis kebutuhan, desain topologi keamanan, instalasi dan konfigurasi Wazuh, pelatihan admin server, evaluasi sistem, serta pendampingan teknis. Hasil implementasi menunjukkan bahwa Wazuh berhasil mendeteksi ancaman potensial dan meningkatkan kemampuan admin server dalam merespon insiden keamanan. Selain itu, melalui pelatihan dan alih teknologi, admin server kini lebih kompeten dalam memantau dan melindungi server dari serangan siber. Dengan demikian, pengembangan sistem monitoring keamanan berbasis Wazuh ini telah memberikan kontribusi signifikan dalam meningkatkan keamanan aplikasi yang dikelola oleh UNM

**Kata Kunci:** SIMLP2M, Keamanan Siber, Wazuh, Monitoring, Server.

### ABSTRACT

The SIMLP2M at Universitas Negeri Makassar is a system that manages critical data related to research and community service conducted by lecturers and researchers. Given the sensitivity of the data, securing the SIMLP2M application server is a priority. However, the absence of an effective security monitoring system has made the server vulnerable to cyberattacks. This Community Service Program (PKM) aims to enhance the security of the SIMLP2M server by developing a monitoring system based on Wazuh, an open-source software capable of detecting and preventing cyber threats in real-time. The PKM was implemented in several stages, including needs analysis, security topology design, Wazuh installation and configuration, server admin training, system evaluation, and technical assistance. The results of the implementation showed that Wazuh successfully detected potential threats and improved the ability of the server admins to respond to security incidents. Additionally, through training and technology transfer, the admins have become more proficient in monitoring and protecting the server from cyberattacks. Thus, the development of the Wazuh-based security monitoring system has made a significant contribution to improving the security of the systems managed by UNM.

**Keywords:** SIMLP2M, Cybersecurity, Wazuh, Monitoring, Server.

*This is an open access article under the CC BY-SA license*



## 1. PENDAHULUAN

Universitas Negeri Makassar (UNM) memiliki aplikasi Sistem Informasi Manajemen Lembaga Penelitian dan Pengabdian Masyarakat (SIMLP2M) yang berfungsi untuk mengelola data dan informasi terkait kegiatan penelitian serta pengabdian masyarakat oleh dosen dan peneliti. Aplikasi ini memainkan peran penting dalam mendukung proses administrasi mulai dari pengajuan proposal, penilaian oleh reviewer, hingga pelaporan kemajuan dan hasil akhir penelitian maupun pengabdian (Wahid et al., 2021).

Namun, di tengah maraknya kejahatan siber, keamanan data yang tersimpan dalam SIMLP2M menjadi perhatian serius. Serangan siber yang menargetkan aplikasi dan sistem informasi semakin meningkat, baik dalam bentuk peretasan data, pencurian informasi, penyebaran malware, maupun serangan lainnya yang dapat mengakibatkan kerugian finansial, reputasi, dan gangguan operasional bagi organisasi. Mengingat pentingnya data yang dikelola, seperti data dosen, peneliti, serta staf pengabdian UNM, sistem ini menjadi target potensial bagi pelaku kejahatan siber (Wahid & Parenreng, 2020).

Saat ini, keamanan server aplikasi SIMLP2M UNM masih memerlukan peningkatan. Belum ada sistem monitoring yang mampu memantau secara real-time dan memberikan informasi yang akurat kepada admin server untuk mendeteksi dan mencegah serangan siber sejak dini. Akibatnya, admin server menghadapi kesulitan dalam menangani potensi ancaman, yang dapat berdampak pada terganggunya operasional dan keamanan data yang dikelola oleh aplikasi ini.

Potensi dampak negatif dari serangan siber terhadap server aplikasi SIMLP2M (Parulian et al., 2021) meliputi:

- Gangguan operasional: Ketidakmampuan mengakses server yang menghambat proses penelitian dan pengabdian.
- Kehilangan data: Risiko pencurian atau penghapusan data yang dapat merusak reputasi dan membawa kerugian finansial bagi UNM.
- Pelanggaran privasi: Pelanggaran privasi data dosen dan peneliti yang berpotensi menimbulkan kecemasan bagi sivitas akademika.

Untuk menghadapi ancaman ini, diperlukan sistem monitoring keamanan yang andal, yang mampu mendeteksi dan mencegah serangan siber secara real-time serta memberikan peringatan dini kepada admin untuk mengambil tindakan pencegahan. Salah satu solusi yang efektif adalah penggunaan Wazuh, sebuah perangkat lunak open-source yang dapat memonitor keamanan server dan jaringan dengan berbagai fitur, termasuk pemantauan aktivitas endpoint, analisis log, deteksi ancaman, pemindaian kerentanan, dan deteksi intrusi.

Pengembangan sistem monitoring keamanan menggunakan Wazuh diharapkan dapat meningkatkan keamanan server aplikasi SIMLP2M UNM, melindungi data sivitas akademika dari potensi serangan siber, serta meningkatkan kesadaran tentang pentingnya keamanan siber di kalangan pengelola server.

Sebagai bagian dari solusi yang ditawarkan dalam program Pengabdian kepada Masyarakat (PKM) ini, proses instalasi dan konfigurasi Wazuh di server SIMLP2M UNM menjadi langkah awal yang sangat penting. Proses ini melibatkan instalasi Wazuh secara terpusat di server SIMLP2M serta konfigurasi agen-agen di server dan endpoint yang terkait. Dengan fitur-fitur yang tersedia, Wazuh akan dikonfigurasi untuk memantau secara otomatis setiap aktivitas jaringan dan sistem, serta memberikan laporan secara berkala kepada admin.

Selain itu, pelatihan intensif akan diberikan kepada para admin server SIMLP2M UNM agar mereka mampu memahami dan memanfaatkan seluruh fitur Wazuh dengan maksimal. Pelatihan ini meliputi penggunaan antarmuka dashboard Wazuh untuk memantau aktivitas keamanan, cara membaca dan menafsirkan hasil analisis log serta laporan ancaman, dan metode untuk merespon potensi serangan secara efektif. Pelatihan ini bertujuan untuk meningkatkan keterampilan teknis admin dalam mendeteksi anomali dan serangan siber, serta membantu mereka dalam mengambil tindakan pencegahan atau mitigasi yang tepat (Nugraha et al., 2024; Rangga Aditya et al., 2024; Stanković et al., 2022).

Proses instalasi dan pelatihan ini merupakan bagian integral dari PKM, karena tanpa adanya implementasi teknis yang baik dan pengetahuan yang memadai di kalangan admin, sistem monitoring yang dirancang tidak akan mampu berjalan optimal. Dengan adanya pelatihan, diharapkan para admin dapat beroperasi secara mandiri dalam menjaga keamanan server dan mengantisipasi serangan siber, serta mampu memperbarui konfigurasi sistem sesuai dengan perkembangan ancaman yang ada.

Pengembangan sistem monitoring keamanan menggunakan Wazuh diharapkan dapat meningkatkan keamanan server aplikasi SIMLP2M UNM, melindungi data sivitas akademika dari potensi serangan siber, serta meningkatkan kesadaran tentang pentingnya keamanan siber di kalangan pengelola server. Program Pengabdian kepada Masyarakat ini juga memiliki relevansi yang tinggi dengan tantangan keamanan siber yang semakin meningkat di lingkungan pendidikan.

Dengan demikian, program PKM ini tidak hanya menyediakan solusi teknis untuk meningkatkan keamanan siber di UNM, tetapi juga menciptakan basis pengetahuan yang berkelanjutan bagi tim admin server dalam menghadapi tantangan keamanan siber di masa mendatang.

## **2. METODE PELAKSANAAN**

Pelaksanaan program Pengabdian kepada Masyarakat ini dilaksanakan melalui beberapa tahapan yang sistematis, dimulai dari survei kebutuhan hingga pendampingan implementasi sistem. Tahapan-tahapan ini dirancang agar solusi yang diberikan tidak hanya efektif dalam meningkatkan keamanan server SIMLP2M UNM, tetapi juga memberikan pengetahuan dan keterampilan yang berkelanjutan bagi admin server. Berikut ini adalah rincian setiap tahap.

### **2.1. Survei dan Analisis Kebutuhan**

Tahap awal pelaksanaan PKM adalah melakukan survei dan analisis kebutuhan terhadap sistem yang ada di server aplikasi SIMLP2M. Tujuan dari tahap ini adalah untuk:

- Mengidentifikasi kondisi infrastruktur server saat ini, termasuk spesifikasi hardware, software, dan arsitektur jaringan yang digunakan.
- Menganalisis potensi risiko keamanan dan serangan siber yang mungkin mengancam server SIMLP2M.
- Menggali kebutuhan teknis yang diperlukan oleh admin server dalam memonitor dan mengamankan sistem.
- Melakukan wawancara dan diskusi dengan admin server dan pengelola LP2M UNM untuk memahami tantangan dan kendala yang mereka hadapi dalam aspek keamanan server.

Hasil dari survei dan analisis ini akan digunakan untuk menyusun perencanaan yang lebih detail pada tahapan berikutnya.

### **2.2. Proses Desain Topologi Jaringan dan Keamanan**

Setelah analisis kebutuhan selesai, tim PKM akan merancang topologi jaringan dan arsitektur keamanan yang optimal untuk implementasi Wazuh. Proses ini meliputi:

- Mendesain topologi server dan endpoint yang akan dipantau oleh Wazuh, termasuk integrasi dengan server aplikasi SIMLP2M.
- Merancang aturan keamanan yang diperlukan, seperti konfigurasi firewall, intrusion detection system (IDS), dan pengaturan pemantauan log server.
- Menyusun skenario pemantauan berbasis real-time yang dapat mendeteksi anomali atau serangan siber di server SIMLP2M secara cepat dan akurat.

Desain ini akan menjadi panduan teknis dalam tahap instalasi dan konfigurasi Wazuh.

### **2.3. Proses Instalasi dan Konfigurasi Wazuh**

Tahap selanjutnya adalah instalasi dan konfigurasi perangkat lunak Wazuh pada server SIMLP2M UNM. Proses ini dilakukan dengan langkah-langkah berikut:

- Instalasi Wazuh Manager di server utama yang akan menjadi pusat pengelolaan keamanan.
- Instalasi Wazuh Agents di server SIMLP2M dan endpoint lain yang terhubung untuk memantau seluruh aktivitas di jaringan.
- Konfigurasi Wazuh Manager agar sesuai dengan topologi yang telah dirancang, termasuk pengaturan monitoring log server, analisis ancaman, dan notifikasi peringatan.
- Uji coba sistem monitoring untuk memastikan bahwa Wazuh berjalan dengan baik dan dapat mendeteksi serta melaporkan ancaman keamanan secara real-time.

Tahap ini penting untuk memastikan bahwa sistem Wazuh terinstal dan terkonfigurasi dengan baik sehingga siap digunakan untuk monitoring keamanan.

### **2.4. Proses Pelatihan dan Alih Teknologi**

Setelah sistem Wazuh terpasang, tim PKM akan memberikan pelatihan dan alih teknologi kepada para admin server SIMLP2M UNM. Pelatihan ini mencakup:

- Pengenalan dasar tentang cara kerja Wazuh dan pentingnya monitoring keamanan.
- Pelatihan penggunaan dashboard Wazuh untuk memantau aktivitas keamanan secara real-time.
- Cara menganalisis laporan yang dihasilkan oleh Wazuh, seperti log aktivitas, deteksi ancaman, dan kerentanan sistem.
- Metode respons terhadap ancaman yang terdeteksi, seperti mitigasi ancaman, penanganan serangan, dan pemulihan data.
- Peningkatan pemahaman tentang prosedur keamanan siber yang harus diterapkan secara berkelanjutan.

Alih teknologi ini bertujuan untuk membekali admin server dengan keterampilan yang diperlukan untuk mengoperasikan dan memelihara sistem monitoring keamanan secara mandiri.

### 2.5. Proses Evaluasi Sistem

- Setelah pelatihan selesai dan sistem mulai beroperasi, evaluasi terhadap performa sistem akan dilakukan secara berkala. Tahap ini meliputi:
- Monitoring kinerja Wazuh dalam mendeteksi dan mencegah potensi ancaman selama periode uji coba.
- Pengumpulan umpan balik dari admin server mengenai kemudahan penggunaan, keandalan sistem, dan efektifitas Wazuh dalam meningkatkan keamanan.
- Evaluasi apakah sistem telah sesuai dengan kebutuhan yang telah diidentifikasi pada tahap survei awal.

Berdasarkan hasil evaluasi, tim PKM akan melakukan penyesuaian atau pengoptimalan sistem jika diperlukan, seperti penambahan fitur atau pengaturan ulang konfigurasi keamanan.

### 2.6. Proses Pendampingan

Untuk memastikan keberlanjutan dan keberhasilan implementasi sistem monitoring, tim PKM akan melakukan pendampingan selama beberapa waktu setelah sistem dioperasikan. Pendampingan ini bertujuan untuk:

- Membantu admin server dalam mengatasi masalah teknis yang mungkin muncul selama implementasi awal sistem.
- Memberikan bimbingan tambahan jika diperlukan terkait dengan pengaturan lanjutan atau pemecahan masalah teknis.
- Menyediakan panduan untuk update atau perawatan berkala sistem keamanan, termasuk rekomendasi untuk menghadapi ancaman baru yang mungkin muncul di masa depan.

Pendampingan ini merupakan komponen penting untuk memastikan bahwa admin server SIMLP2M UNM mampu mengelola sistem secara mandiri dan menjaga keberlanjutan pengamanan server.

## 3. HASIL DAN PEMBAHASAN

Bagian ini menjelaskan hasil yang dicapai selama pelaksanaan program PKM "Pengembangan Sistem Monitoring Keamanan Server Aplikasi SIMLP2M UNM Menggunakan Wazuh." Setiap tahapan implementasi akan dipaparkan dengan detail, disertai dokumentasi gambar sebagai bukti pencapaian dan penjelasan lebih lanjut.

### 3.1. Hasil Survei dan Analisis Kebutuhan

Survei dan analisis kebutuhan yang dilakukan di awal program berhasil mengidentifikasi beberapa aspek penting terkait infrastruktur dan risiko keamanan pada server SIMLP2M UNM. Beberapa hasil yang dicapai dari tahapan ini adalah:

- Kondisi infrastruktur: Server SIMLP2M menggunakan teknologi virtualisasi dengan konfigurasi hardware yang memadai, tetapi belum dilengkapi dengan sistem monitoring yang komprehensif. Gambar 1 berikut adalah kondisi infrastruktur fisik server UNM.



Gambar 1. Survey kondisi Infrastruktur Server UNM

- Analisis risiko: Ditemukan potensi risiko berupa serangan brute force, malware, dan pencurian data yang dapat mengganggu operasional server.
- Kebutuhan keamanan: Dibutuhkan sistem monitoring yang dapat memantau log secara real-time, mendeteksi anomali, dan mengirimkan notifikasi peringatan dini. Gambar 2 berikut ini menunjukkan kegiatan focus discussion group (FGD) dalam analisis resiko dan kebutuhan system untuk keamanan.



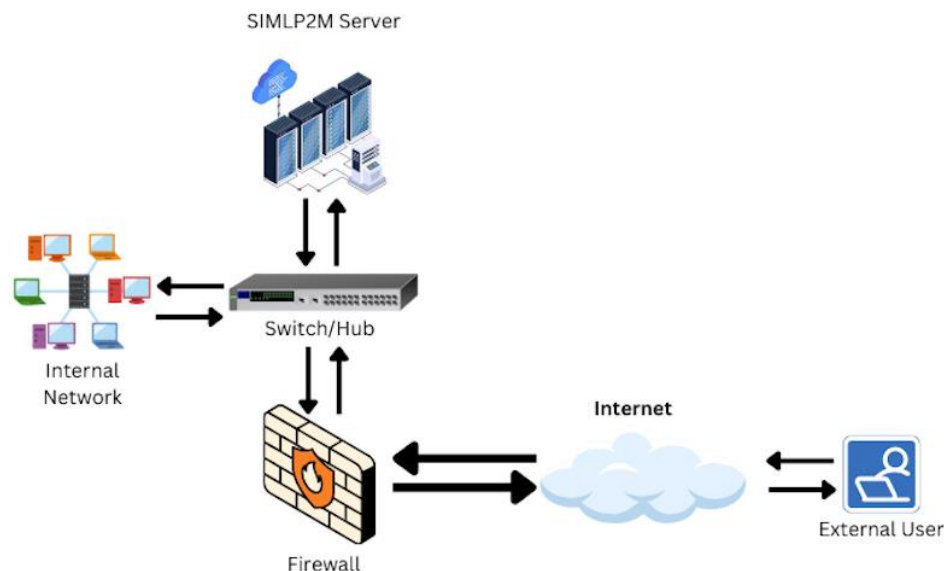
Gambar 2. FGD Survey dan analisis kebutuhan sistem.

### 3.2. Desain Topologi Jaringan dan Keamanan

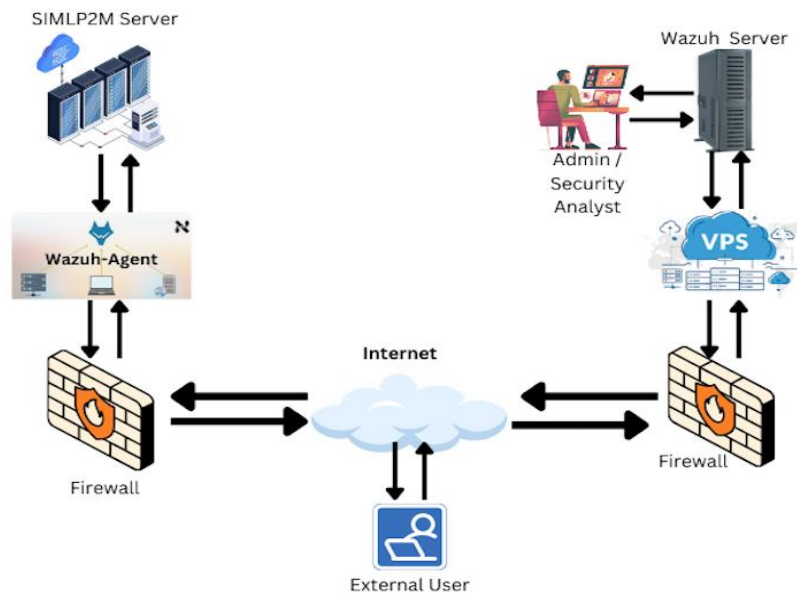
Berdasarkan hasil survei, dilakukan perancangan topologi jaringan dan keamanan untuk implementasi Wazuh. Topologi ini mencakup:

- Server SIMLP2M sebagai Wazuh Agent: Server ini akan menjadi endpoint yang diawasi oleh Wazuh.
- Pemasangan Wazuh Manager di server pusat: Berfungsi untuk mengumpulkan dan menganalisis log dari semua agen di jaringan.
- Endpoint tambahan: Beberapa perangkat endpoint lain seperti komputer admin dan pengguna juga dimasukkan ke dalam pemantauan.

Gambar 3. adalah topologi jaringan ke server aplikasi SIMLP2M sebelum instalasi dan konfigurasi Wazuh, sedangkan Gambar 4. adalah desain topologi jaringan setelah implementasi Wazuh sebagai sistem monitoring keamanan server.



Gambar 3. Topologi Jaringan Sebelum Instalasi Wazuh



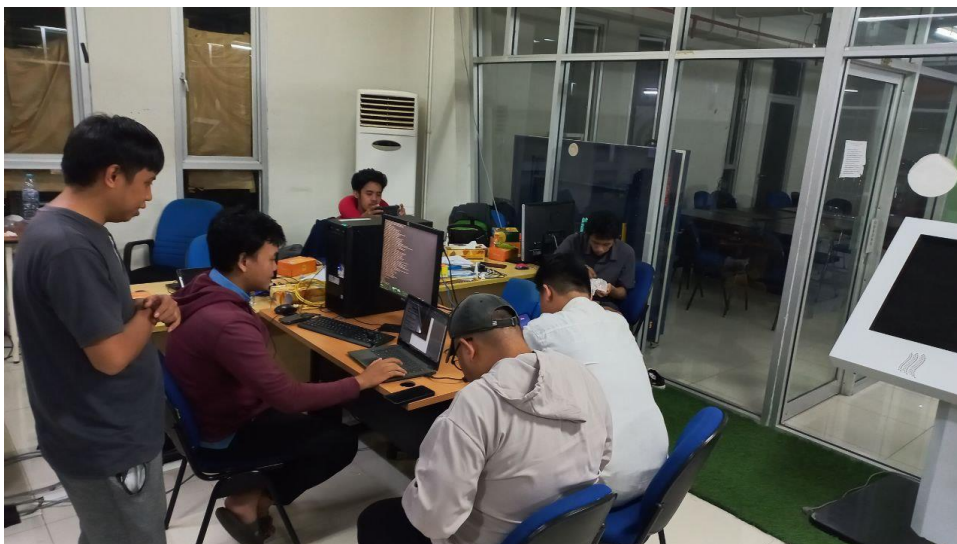
Gambar 4. Topologi Jaringan Sesudah Instalasi Wazuh

### 3.3. Instalasi dan Konfigurasi Wazuh

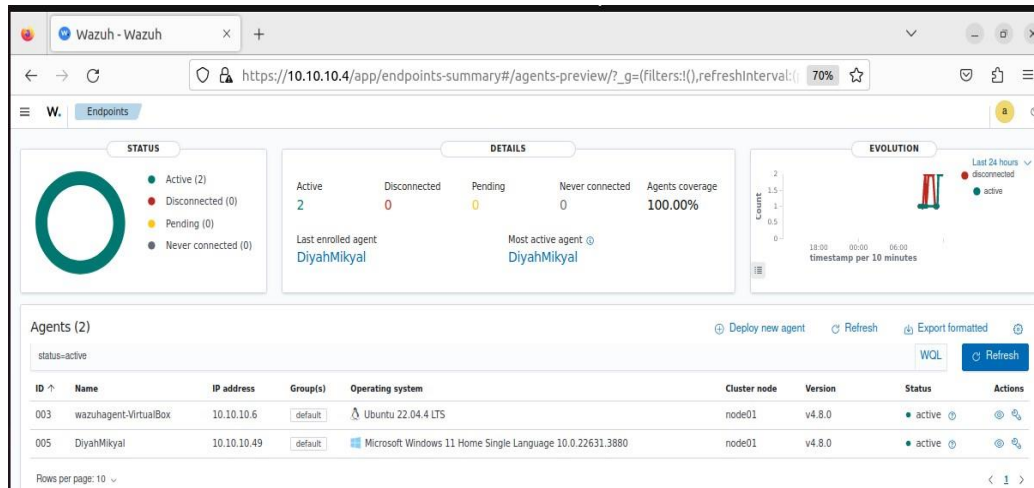
Proses instalasi dan konfigurasi Wazuh dilakukan dalam beberapa tahapan, mulai dari instalasi Wazuh Manager, Wazuh Agent, hingga konfigurasi monitoring. Hasil yang dicapai dari tahap ini adalah:

- Instalasi Wazuh Manager: Sukses dilakukan pada server pusat, di mana Wazuh Manager siap mengumpulkan log dari semua agen.
- Instalasi Wazuh Agent: Agen Wazuh berhasil diinstal pada server SIMLP2M dan beberapa endpoint lain yang relevan.
- Konfigurasi monitoring: Sistem Wazuh dikonfigurasi untuk melakukan monitoring secara real-time terhadap aktivitas jaringan, mencakup pemantauan log, deteksi anomali, dan pengiriman notifikasi ancaman.

Gambar 5. Menunjukkan proses Instalasi dan Konfigurasi Wazuh Agent dan Wazuh Server (Dashboard). Wazuh Agent diinstall menempel pada server aplikasi SIMLP2M, sedangkan wazuh dashboard di install pada satu server virtual tersendiri sebagai pusat monitoring serangan yang mengarah ke server aplikasi SIMLP2M. Sementara gambar 6. Menampilkan dashboard wazuh dalam keadaan normal setelah proses instalasi dan konfigurasi dilakukan.



Gambar 5. Proses Instalasi Wazuh



**Gambar 6.** Dashboard Wazuh

### 3.4. Pelatihan dan Alih Teknologi

Setelah sistem Wazuh terpasang, pelatihan dilakukan untuk admin server SIMLP2M. Beberapa hasil yang dicapai dari pelatihan ini adalah:

- Penguasaan antarmuka dashboard Wazuh: Admin dapat memahami dan menggunakan dashboard untuk memantau aktivitas dan anomali yang terdeteksi.
- Analisis log: Admin mampu menafsirkan log yang dihasilkan oleh Wazuh untuk mendeteksi aktivitas mencurigakan.
- Tindakan pencegahan dan mitigasi: Admin dilatih untuk merespon ancaman dengan tindakan pencegahan yang tepat, seperti memperbarui firewall atau mengisolasi perangkat yang terancam.



**Gambar 7.** Sesi Pelatihan bagi Admin Server

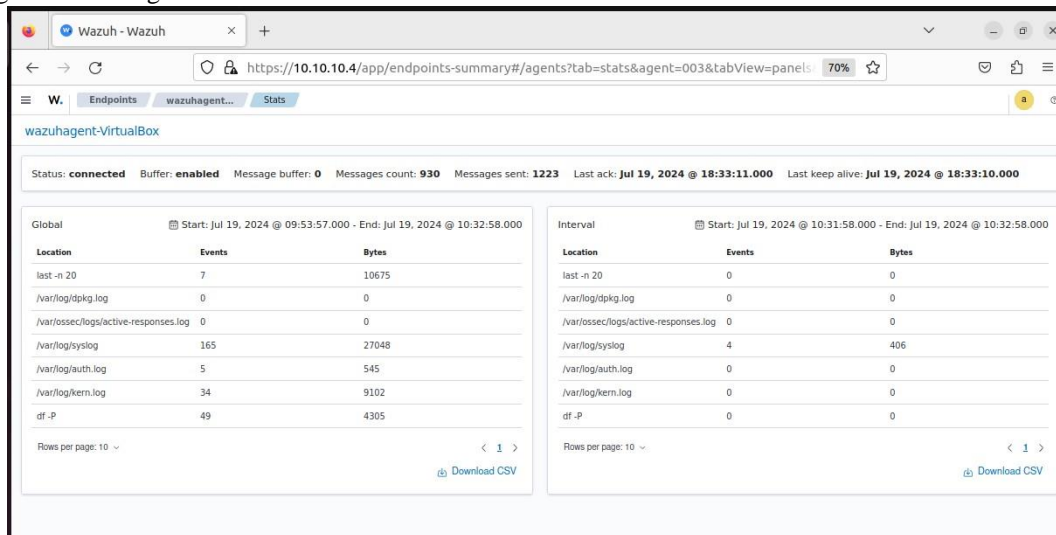
### 3.5. Evaluasi Sistem

Setelah sistem diimplementasikan dan digunakan selama beberapa waktu, evaluasi dilakukan untuk menilai efektivitas sistem. Hasil evaluasi menunjukkan:

- Peningkatan deteksi ancaman: Sistem berhasil mendeteksi beberapa aktivitas mencurigakan yang sebelumnya tidak terdeteksi, seperti upaya akses tidak sah (unauthorized access) dan anomali di jaringan.

- Respon cepat terhadap ancaman: Admin server mampu merespon ancaman dengan cepat berdasarkan notifikasi yang diberikan oleh Wazuh, sehingga serangan dapat dicegah sebelum berdampak.
- Keandalan sistem: Wazuh menunjukkan performa yang stabil dan mampu bekerja dengan baik dalam lingkungan server SIMLP2M.

Gambar 8. berikut menunjukkan hasil monitoring Wazuh dengan melakukan simulasi serangan DOS/DDOS menggunakan HPing sebesar 500.000.



The screenshot shows the Wazuh monitoring interface with two tables displaying log data for a simulated attack. The status is 'connected' and the message buffer is 'enabled'. The message count is 930 and messages sent are 1223. The last acknowledgment is from Jul 19, 2024 @ 18:33:11.000 and the last keep-alive is from Jul 19, 2024 @ 18:33:10.000.

Global			Interval		
Start: Jul 19, 2024 @ 09:53:57.000 - End: Jul 19, 2024 @ 10:32:58.000			Start: Jul 19, 2024 @ 10:31:58.000 - End: Jul 19, 2024 @ 10:32:58.000		
Location	Events	Bytes	Location	Events	Bytes
last-n 20	7	10675	last-n 20	0	0
/var/log/dpkg.log	0	0	/var/log/dpkg.log	0	0
/var/ossec/logs/active-responses.log	0	0	/var/ossec/logs/active-responses.log	0	0
/var/log/syslog	165	27048	/var/log/syslog	4	406
/var/log/auth.log	5	545	/var/log/auth.log	0	0
/var/log/kern.log	34	9102	/var/log/kern.log	0	0
df -P	49	4305	df -P	0	0

**Gambar 8.** Tampilan Monitoring Wazuh dengan Simulasi Serangan HPing 500000

### 3.6. Pendampingan

Tahap pendampingan dilakukan setelah sistem mulai beroperasi. Tim PKM tetap mendampingi admin server selama beberapa waktu untuk memastikan kelancaran operasional sistem monitoring. Beberapa hasil dari tahap pendampingan meliputi:

- Peningkatan keterampilan admin: Admin server semakin mahir dalam menggunakan Wazuh untuk memantau dan melindungi server.
- Penyelesaian masalah teknis: Beberapa masalah kecil yang muncul selama implementasi berhasil diselesaikan, seperti penyesuaian konfigurasi log dan pengaturan notifikasi.



**Gambar 9.** Sesi Pendampingan dan Diskusi



#### 4. KESIMPULAN DAN SARAN

Program Pengabdian kepada Masyarakat (PKM) dengan judul "Pengembangan Sistem Monitoring Keamanan Server Aplikasi SIMLP2M UNM Menggunakan Wazuh" telah dilaksanakan dengan sukses dan mencapai tujuan yang diharapkan. Berdasarkan hasil pelaksanaan program, dapat ditarik beberapa kesimpulan penting:

1. Peningkatan Keamanan Server Aplikasi SIMLP2M; Implementasi Wazuh sebagai sistem monitoring keamanan telah terbukti efektif dalam meningkatkan keamanan server aplikasi SIMLP2M UNM. Dengan fitur-fitur seperti pemantauan real-time, analisis log, deteksi ancaman, dan notifikasi peringatan dini, Wazuh berhasil mendeteksi potensi serangan siber dan ancaman lainnya yang sebelumnya tidak terdeteksi oleh sistem keamanan yang ada.
2. Penguasaan Teknologi oleh Admin Server; Melalui pelatihan dan alih teknologi yang diberikan, admin server SIMLP2M kini memiliki keterampilan yang lebih baik dalam mengoperasikan dan memelihara sistem monitoring keamanan. Mereka dapat menggunakan dashboard Wazuh untuk memantau aktivitas keamanan secara mandiri, menganalisis log ancaman, dan merespon insiden dengan cepat dan tepat. Hal ini menunjukkan peningkatan kapasitas teknis yang signifikan bagi admin server dalam mengelola keamanan siber.
3. Keandalan Sistem Wazuh dalam Pemantauan Keamanan; Selama masa evaluasi, Wazuh menunjukkan performa yang stabil dan andal dalam memantau keamanan server SIMLP2M. Sistem ini mampu bekerja dengan baik dalam mendeteksi berbagai bentuk ancaman siber, seperti serangan brute force, akses tidak sah, dan anomali dalam jaringan. Hal ini membuktikan bahwa Wazuh merupakan solusi open-source yang efektif untuk meningkatkan keamanan jaringan dan server.
4. Kesenambungan Solusi Keamanan Siber di UNM; Dengan adanya sistem monitoring keamanan berbasis Wazuh yang sudah terinstal dan berjalan, UNM kini memiliki solusi keamanan siber yang berkelanjutan. Tim PKM juga telah memberikan pendampingan teknis agar admin server dapat mengelola sistem ini secara mandiri di masa mendatang. Hal ini diharapkan dapat memberikan perlindungan jangka panjang bagi data dan informasi penting yang tersimpan di server aplikasi SIMLP2M.

Secara keseluruhan, kegiatan PKM ini telah berhasil memberikan kontribusi signifikan dalam meningkatkan keamanan siber di lingkungan UNM, khususnya dalam melindungi server aplikasi SIMLP2M dari potensi serangan siber. Sistem monitoring yang telah dikembangkan melalui program ini diharapkan mampu menjaga kelangsungan operasional aplikasi SIMLP2M dan memberikan rasa aman bagi seluruh sivitas akademika UNM dalam menggunakan layanan tersebut.

#### 5. UCAPAN TERIMA KASIH

Ucapan Terimakasih kepada Universitas Negeri Makassar yang telah memberikan hibah pengabdian PNPB. Selanjutnya ucapan terimakasih kepada Ketua Lembaga Penelitian UNM dan Kepala UPT. TIK UNM beserta jajaran UPT. TIK UNM yang telah menjadi pusat pelaksanaan PKM ini.

#### REFERENSI

- Nugraha, A., Muhyidin, Y., & Kurniawan, I. (2024). Implementasi Wazuh Dashboard pada Server untuk Monitoring Serangan DDOS terhadap Web XYZ. *Jurnal Ilmiah Sains dan Teknologi (Scientica)*, 2(11), 215–228.
- Parulian, S., Pratiwi, D. A., & Yustina, M. C. (2021). Ancaman dan Solusi Serangan Siber di Indonesia. *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)*, 1(2), 85–92.
- Rangga Aditya, Yusuf Muhyidin, & Dayan Singasatia. (2024). Implementasi Security Information And Event Management (SIEM) Untuk Monitoring Keamanan Server Menggunakan Wazuh. *Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika*, 2(5), 137–144. <https://doi.org/10.61132/merkurius.v2i5.289>

- Stanković, S., Gajin, S., & Petrović, R. (2022). A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis. *PROCEEDINGS IX INTERNATIONAL CONFERENCE IcETAN*, 6-9 June 2022.
- Wahid, A., & Parenreng, J. M. (2020). Pengelolaan Aplikasi Sistem Informasi Lembaga Penelitian dan Pengabdian Masyarakat (SIMLP2M) Universitas Negeri Makassar. *Prosiding Seminar Nasional "Peluang dan tantangan pengabdian kepada masyarakat yang inovatif di era kebiasaan baru."* SEMINAR NASIONAL HASIL PENGABDIAN KEPADA MASYARAKAT LP2M UNM, Makassar, Indonesia.
- Wahid, A., Parenreng, J. M., & Agung, M. (2021). PKM Pengembangan dan Tata Kelola Modul Reviewer pada Aplikasi SIMLP2M Universitas Negeri Makassar. *Prosiding Semnas Hasil Pengabdian 2021 "Penguatan Riset, Inovasi, dan Kreativitas Peneliti di Era Pandemi Covid-19."* Seminar Nasional Hasil Pengabdian 2021 LP2M UNM, Makassar, Indonesia.