Jurnal Minfo Polgan (JMP)
Volume 15, Nomor 1, Maret 2026
DOI : https://doi.org/10.33395/jmp.v15i1.16224
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Pengembangan Sistem Pertahanan Server Cerdas Menggunakan Honeypot Dionaea dan Host-Based Intrusion Detection System (HIDS) dalam Deteksi Serangan Siber

[1*]Fadli Tamrin, [2]Asrul
[1]Politeknik Negeri Ujung Pandang, [2]Universitas Halu Oleo, Indonesia
*Korespondensi : fadlitamri@poltek.a.id

Submit : 16 Jan 2026 | **Diterima** : 15 Feb 2026 | **Terbit** : 19 Feb 2026

ABSTRACT

The increasing intensity and complexity of cyberattacks pose a serious threat to server security. Host-based Intrusion Detection Systems (HIDS) such as Wazuh have limitations in detecting certain types of attacks, particularly at the application and network layers, while honeypots like Dionaea—although effective in capturing attacks—are often used only for passive analysis. This study aims to design, implement, and evaluate an integrated security system that leverages Dionaea as an active sensor to enhance the detection and response capabilities of Wazuh HIDS. The research methodology involved building an architecture within a virtual environment consisting of the Dionaea honeypot, Wazuh server, protected agents, and attacker machines. Attack data captured by Dionaea was processed and forwarded to Wazuh via agents. Custom detection rules were developed in Wazuh to generate alerts, which then triggered active response mechanisms to automatically block attacker IP addresses at the firewall of the protected machines. The system was tested against various attack scenarios, including Port Scanning, Brute Force, and Distributed Denial of Service (DDoS). The results demonstrate that the integration was successful. For application-layer attacks such as Brute Force and Slowloris, the system was able to detect, generate alerts, and automatically block attacker IPs, verified by a 100% connection failure. For network-layer attacks such as SYN Flood and ICMP Flood, although not directly recorded by the honeypot, their impact was detected as anomalies through spikes in CPU resource usage on the host. In conclusion, this integration successfully transformed the honeypot from a passive analysis tool into an active defense sensor, significantly enhancing the visibility and response capability of Wazuh HIDS against diverse cyber threats.

Keywords: *Honeypot, Dionaea, HIDS, Wazuh, Cybersecurity*

ABSTRAK

Meningkatnya intensitas dan kompleksitas serangan siber merupakan ancaman serius bagi keamanan server. Host-based Intrusion Detection System (HIDS) seperti Wazuh memiliki keterbatasan dalam mendeteksi beberapa jenis serangan, terutama pada lapisan aplikasi dan jaringan, sementara honeypot seperti Dionaea yang efektif menangkap serangan seringkali hanya digunakan untuk analisis pasif. Penelitian ini bertujuan untuk merancang, membangun, dan menguji sebuah sistem keamanan terintegrasi yang memanfaatkan honeypot Dionaea sebagai sensor aktif untuk meningkatkan kemampuan deteksi dan respons dari HIDS Wazuh Metodologi penelitian melibatkan pembangunan arsitektur dalam lingkungan virtual yang terdiri dari honeypot Dionaea, server Wazuh, agent yang dilindungi, dan mesin penyerang. Data serangan yang ditangkap oleh Dionaea diolah dan diteruskan ke Wazuh menggunakan agent. Aturan deteksi khusus (custom rules) dikembangkan pada Wazuh untuk menghasilkan peringatan, yang kemudian memicu mekanisme active response untuk memblokir alamat IP penyerang secara otomatis pada firewall di mesin yang dilindungi. Sistem diuji menggunakan berbagai skenario serangan, termasuk Port Scanning, Brute Force, dan Distributed Denial of Service (DDoS). Hasil pengujian menunjukkan bahwa integrasi sistem berhasil. Untuk serangan pada lapisan aplikasi seperti Brute Force dan Slowloris, sistem mampu mendeteksi, menghasilkan peringatan, dan secara otomatis memblokir IP penyerang, yang diverifikasi dengan kegagalan koneksi 100%. Untuk serangan lapisan jaringan seperti SYN Flood dan ICMP

Flood, meskipun tidak tercatat oleh honeypot, dampaknya dapat terdeteksi sebagai anomali melalui lonjakan penggunaan sumber daya CPU pada host. Kesimpulannya, integrasi ini berhasil mengubah honeypot dari alat analisis pasif menjadi sensor pertahanan aktif, yang secara signifikan meningkatkan visibilitas dan kemampuan respons HIDS terhadap berbagai ancaman siber.

Kata Kunci: Honeypot, Dionaea, HIDS, Wazuh, Keamanan Siber

PENDAHULUAN

Perkembangan internet yang sangat pesat telah menjadikan keamanan data dan informasi pada server publik sebagai aspek yang krusial untuk diperhatikan (Hafiz et al., 2020). Di sisi lain, kemajuan ini juga membuka peluang baru sekaligus memunculkan tantangan yang semakin kompleks dalam ranah keamanan siber. Serangan siber, seperti brute force attack, malware, dan eksploitasi layanan, terus meningkat baik dalam skala maupun kompleksitasnya. Menurut (Fiqri et al., 2020) ancaman siber ini dapat merusak penyedia layanan seperti situs web, email, dan cloud melalui retas sistem atau pencurian data pengguna layanan, yang berpotensi merugikan pihak penyedia layanan dan pengguna.

Berdasarkan laporan tahunan 2023 Badan Siber dan Sandi Negara (BSSN), Indonesia mengalami peningkatan signifikan dalam jumlah serangan siber dalam beberapa tahun terakhir. Pada tahun 2023, tercatat sekitar 603.276.807 serangan siber. Ancaman siber yang dihadapi server sangat beragam. Beberapa di antaranya yang menjadi fokus dalam penelitian ini adalah Port Scanning, yaitu teknik pengintaian awal untuk mencari celah keamanan; Brute Force Attack, yaitu upaya menebak kredensial login secara paksa untuk mendapatkan akses tidak sah; serta Distributed Denial of Service (DDoS), yaitu serangan yang bertujuan melumpuhkan layanan dengan membanjiri server menggunakan lalu lintas data dalam jumlah masif. Dokumentasi log internal Unit Penunjang Akademik Teknologi Informasi dan Komunikasi (UPA TIK) Politeknik Negeri Ujung Pandang mencatat adanya insiden serangan siber yang terjadi pada data center Politeknik Negeri Ujung Pandang pada bulam agustus 2024, Serangan ini dapat mengganggu akses publik terhadap situs resmi maupun portal akademik. Sebagai respon dari ancaman ini diperlukan solusi keamanan yang lebih inovatif dan adaptif untuk melindungi server dari berbagai jenis serangan.

Salah satu pendekatan yang dapat digunakan dengan memanfaatkan teknologi Honeypot dan Host-based Intrusion Detection System (HIDS). 1 Honeypot berfungsi sebagai perangkat tiruan yang sengaja dibuat agar terlihat seperti target yang menarik bagi penyerang. Tujuan utamanya adalah untuk mengelabui attacker agar menyerang honeypot, bukan server yang sebenarnya. Namun, data yang dikumpulkan oleh honeypot sering kali hanya dimanfaatkan untuk analisis pasif, tanpa ada tindakan langsung untuk mencegah serangan berikutnya.

Di sisi lain, HIDS (Host-Based Intrusion Detection System) adalah sistem yang dirancang untuk mendeteksi aktivitas mencurigakan atau berbahaya pada perangkat individu (host). Berbagai penelitian terdahulu telah dilakukan untuk meningkatkan keamanan server, antara lain melalui implementasi teknologi honeypot dan sistem deteksi intrusi berbasis host (Host-Based Intrusion Detection System/HIDS). Penelitian oleh Hartinah (2018) yang berjudul "Implementasi Honeypot Dionaea untuk Analisis Malware dan Ransomware" menyoroti kinerja honeypot dalam menjebak malware serta menganalisis cara kerjanya. Sementara itu, penelitian oleh Fathin Abd. Hadi (2018) yang berjudul "Peningkatan Sistem Keamanan Data Center Menggunakan Metode Host-Based Intrusion Detection System (HIDS) dengan Aplikasi Wazuh" menunjukkan bahwa HIDS mampu mendeteksi aktivitas mencurigakan melalui analisis log sistem serta memberikan respons aktif terhadap potensi ancaman. Berdasarkan kedua studi tersebut, penelitian ini bertujuan untuk mengintegrasikan teknologi Honeypot Dionaea dan HIDS guna meningkatkan kemampuan deteksi dan pencegahan terhadap serangan siber, serta memberikan kontribusi nyata dalam pengembangan sistem keamanan server yang lebih adaptif dan proaktif.

METODE PENELITIAN

Penelitian ini menggunakan jenis penelitian eksperimen (experimental research) dengan pendekatan kuantitatif. Penelitian dilakukan melalui proses perancangan, implementasi, dan pengujian sistem pertahanan server berbasis Honeypot Dionaea dan Host-Based Intrusion Detection System (HIDS) untuk mendeteksi berbagai jenis serangan siber pada server.

Pendekatan eksperimen digunakan untuk menguji efektivitas integrasi Honeypot Dionaea dan HIDS dalam:

1. mendeteksi aktivitas serangan siber,
2. mengumpulkan log serangan,
3. memonitor aktivitas host,
4. meningkatkan keamanan server secara real-time.

Lokasi dan Waktu Penelitian

Penelitian dilaksanakan pada lingkungan laboratorium jaringan komputer atau server virtual berbasis Linux. Implementasi sistem dilakukan menggunakan teknologi virtualisasi agar simulasi serangan siber dapat dilakukan secara aman tanpa mengganggu jaringan produksi.

Waktu penelitian dilaksanakan selama ±6 bulan yang meliputi:

1. studi literatur,
2. perancangan sistem,
3. implementasi,
4. pengujian sistem,
5. analisis hasil,
6. penyusunan laporan penelitian.

Objek Penelitian

Objek penelitian adalah sistem keamanan server berbasis:

1. **Honeypot Dionaea** sebagai pendeteksi aktivitas serangan jaringan,
2. **Host-Based Intrusion Detection System (HIDS)** sebagai sistem monitoring aktivitas internal server.

Server yang digunakan berupa sistem operasi Linux Ubuntu Server yang dikonfigurasi sebagai target simulasi serangan siber.

Alat dan Bahan Penelitian

Perangkat Keras

Perangkat keras yang digunakan meliputi:

Tabel 1 Perangkat Keras

No	Perangkat	Spesifikasi
1	Laptop/PC Server	Processor Intel Core i5/Ryzen 5
2	RAM	Minimal 8 GB
3	Harddisk/SSD	Minimal 256 GB
4	Router/Switch	Untuk simulasi jaringan
5	Koneksi Internet	Untuk update repository

Perangkat Lunak

Perangkat lunak yang digunakan meliputi:

Tabel 2 Perangkat Lunak

No	Software	Fungsi
1	Ubuntu Server	Sistem operasi server
2	Dionaea Honeypot	Monitoring dan penangkapan serangan
3	Wazuh/OSSEC	Host-Based Intrusion Detection System
4	VirtualBox/VMware	Virtualisasi server
5	Kali Linux	Simulasi serangan siber
6	Wireshark	Analisis lalu lintas jaringan
7	ELK Stack	Visualisasi log keamanan
8	Nmap	Port scanning
9	Hydra	Simulasi brute force attack

Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui beberapa metode berikut:

1. Studi Literatur

Pengumpulan referensi dilakukan melalui:

a. jurnal ilmiah,
b. prosiding,

c. buku,
d. dokumentasi keamanan siber,
e. artikel penelitian terkait Honeypot dan HIDS.

2. Observasi Sistem

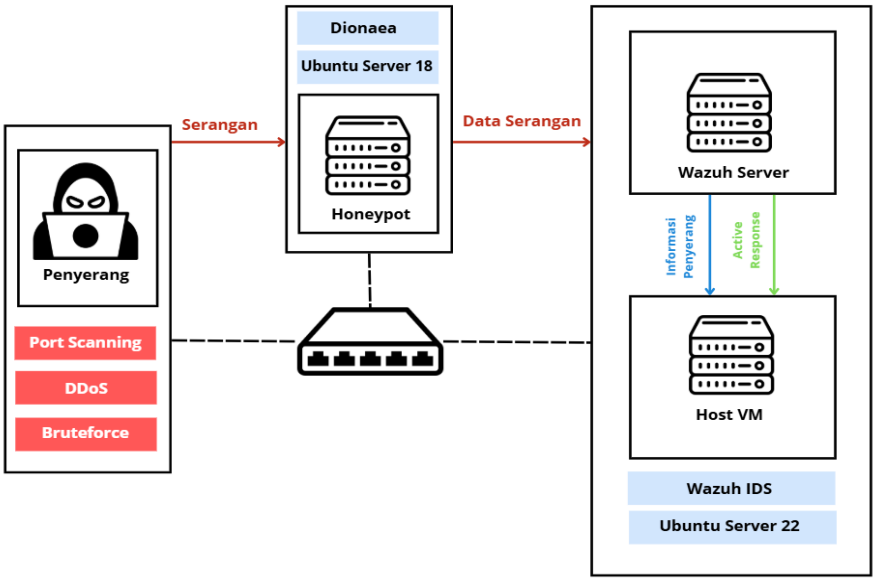
Observasi dilakukan terhadap:

a. aktivitas server,
b. lalu lintas jaringan,
c. log keamanan,
d. aktivitas serangan yang berhasil dideteksi.

HASIL DAN PEMBAHASAN

Perancangan Sistem

Perancangan Sistem Pada tahap ini dilakukan perancangan sistem guna memperoleh gambaran yang jelas mengenai sistem yang akan dikembangkan, sehingga dapat menjadi pedoman dalam pelaksanaan penelitian. Arsitektur sistem yang dirancang diilustrasikan pada Gambar 3.2. Diagram tersebut menunjukkan alur kerja di mana Penyerang melancarkan serangan ke Honeypot. Data serangan yang berhasil ditangkap kemudian dikirim ke Wazuh Server untuk dianalisis. Jika terdeteksi ancaman, Wazuh Server akan mengirimkan perintah Active Response ke Host VM (yang dilindungi oleh Wazuh Agent) untuk memblokir penyerang. 27 Gambar 3. 2 Perancangan Sistem



Gambar 1. Perancangan Sistem

Pembuatan Sistem

Pada tahap ini, dilakukan implementasi sistem berdasarkan perancangan yang telah dibuat sebelumnya. Proses ini mencakup instalasi, konfigurasi, dan integrasi antara honeypot Dionaea, Wazuh HIDS, serta lingkungan virtualisasi Proxmox. Selain itu, dilakukan pengujian terhadap sistem dengan menggunakan alat seperti Metasploit dan hping3 untuk mensimulasikan serangan.

1. Honeypot Dionaea

Proses instalasi honeypot dionaea dilakukan melalui perintah pada console

```
git clone https://github.com/DinoTools/dionaea.git
cd dionaea
```

Gambar 2. Perintah Proses Instalasi Dionaea

Gambar 2 menunjukkan perintah yang digunakan untuk mengunduh honeypot Dionaea dan masuk kedalam direktori dionaea. Selanjutnya akan dilakukan proses penginstallan dependensi yang diperlukan dengan perintah seperti gambar 3

```
apt-get install
    build-essential
    cmake
    check
    cython3 \
    libcurl4-openssl-dev \
    libemu-dev
    libev-dev
    libglib2.0-dev \
    libloudmouth1-dev \
    libnetfilter-queue-dev \
    libnl-3-dev \
    libpcap-dev \
    libssl-dev \
    libtool
    libudns-dev \
    python3 \
    python3-dev \
    python3-bson \
    python3-yaml \
    python3-boto3 \
    fonts-liberation
```

Gambar 3. Perintah Instalasi Dependensi

Selanjutnnya membuat direktori baru dan melakukan konfigurasi untuk Dionaea dapat menjalankan perintah seperti pada gambar 4

```
mkdir build
cd build
cmake -DCMAKE_INSTALL_PREFIX:PATH=/opt/dionaea
make
sudo make install
```

Gambar 4 Konfigurasi Instalasi Dionaea

Untuk melakukan instalasi script DionaeaToJson dapat dilihat pada gambar 5

```
cd/opt/
git clone https://github.com/eval2A/dionaeaToJSON/
cd dionaeaToJSON/
mv dionaeaSqliteToJson.py /opt/
```

Gambar 5 Perintah Instalasi DionaeaToJson

DionaeaToJSON (atau script dionaeaSqliteToJson.py) digunakan untuk mengonversi data log serangan yang tersimpan dalam database SQLite milik Dionaea ke dalam format JSON. Dionaea secara default menyimpan informasi koneksi, serangan, dan aktivitas penyerang dalam sebuah file database dionaea.sqlite. Data tersebut tidak langsung terbaca oleh sistem monitoring seperti Wazuh tanpa proses ekstraksi.

Dengan menggunakan script dionaeaToJSON, informasi seperti alamat IP penyerang, port yang diserang, protokol yang digunakan, serta waktu kejadian akan diambil dari database dan disimpan dalam bentuk file JSON. File JSON ini kemudian

dapat dibaca oleh Wazuh Agent, sehingga sistem Wazuh dapat memantau, memproses, dan memvisualisasikan aktivitas mencurigakan atau serangan yang ditangkap oleh honeypot. Proses ini memungkinkan integrasi yang antara honeypot dan sistem keamanan seperti Wazuh atau ELK Stack, sehingga dapat memperoleh notifikasi serta analisis secara real-time berdasarkan data aktual dari honeypot.

```
# Path of the Dionaea SQLite database file (make sure this is the correct path)
dionaeaSQLite = '/opt/dionaea/var/lib/dionaea/dionaea.sqlite'

# Path to where to store the json log files (optional path)
dionaeaLogPath = '/opt/dionaea/var/lib/dionaea/json'

# Path to binaries captured by Dionaea
dionaeaBinariesPath = '/opt/dionaea/var/lib/dionaea/binaries'
```

Gambar 6 Konfigurasi Path DionaeaToJson

Gambar 6 merupakan bagian dari script dionaeaSqliteToJson.py yang digunakan untuk mengekstrak data dari database SQLite milik Dionaea. Variabel dionaeaSQLite menunjukkan lokasi file database utama yang menyimpan informasi koneksi dan aktivitas yang ditangkap oleh honeypot. Variabel dionaeaLogPath menentukan direktori tujuan untuk menyimpan hasil konversi log ke dalam format JSON, yang memudahkan integrasi dengan sistem pemantauan seperti Wazuh atau ELK Stack. Sedangkan dionaeaBinariesPath merujuk ke direktori tempat Dionaea menyimpan file-file biner (misalnya malware) yang berhasil diunduh atau ditangkap selama proses interaksi dengan penyerang. Ketiga path ini penting untuk memastikan script berjalan dengan benar dan seluruh data hasil penangkapan dapat diolah dan disimpan secara sistematis.

```
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow
# Every minute: dionaeaSqliteToJson
*/1 **** /usr/bin/python3 /opt/dionaeaSqliteToJson.pyl
```

Gambar 7 Konfigurasi Crontab

Konfigurasi crontab yang telihat pada gambar 7 berfungsi untuk menjalankan script Python bernama dionaeaSqliteToJson.py setiap satu menit secara otomatis menggunakan interpreter Python 3 yang berada di direktori /usr/bin/python3. Script ini dijalankan dari direktori /opt/, dan biasanya digunakan untuk mengambil data log serangan dari database SQLite milik Dionaea, lalu mengubahnya menjadi format JSON agar dapat diolah lebih lanjut atau dikirim ke sistem monitoring seperti Wazuh. Dengan adanya penjadwalan ini, proses konversi. log dapat berjalan secara terus-menerus dan real-time tanpa perlu intervensi manual, sehingga sistem keamanan dapat secara konsisten mendapatkan data terbaru untuk dianalisis.

2. Wazuh

Proses instalasi wazuh terbagi menjadi dua bagian yaitu instalasi wazuh manager dan wazuh agent

a. Wazuh Manager

Wazuh Manager merupakan komponen utama dalam arsitektur Wazuh yang bertanggung jawab untuk menerima, menganalisis, dan mengelola data keamanan yang dikirim oleh Wazuh Agent. Pada proses instalasi ini, Wazuh Manager akan diinstal bersamaan dengan komponen pendukung lainnya seperti Wazuh Indexer, Filebeat, dan Dashboard menggunakan metode all-in-one untuk mempermudah proses setup. Seperti yang ditunjukkan pada Gambar 8, proses instalasi diawali dengan mengunduh skrip instalasi resmi dari repositori Wazuh menggunakan perintah curl, yang kemudian dieksekusi dengan hak akses sudo bash dan opsi -a untuk menginstal semua komponen secara otomatis .

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

Gambar 8 Perintah Download dan Install Wazuh Manager

b. Wazuh Agent

Wazuh Agent adalah komponen yang dipasang pada endpoint atau host yang ingin dipantau, berfungsi untuk mengumpulkan log sistem, memantau integritas file, mendeteksi perubahan, serta mengirimkan data tersebut ke Wazuh Manager untuk dianalisis. Instalasi Wazuh Agent dilakukan secara terpisah pada setiap mesin target, dan setelah proses instalasi, agen harus dikonfigurasi agar dapat terhubung ke Wazuh Manager melalui alamat IP dan port yang telah ditentukan.

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH |
gpg --no-default-keyring --keyring
gnupg-ring:/usr/share/keyrings/wazuh.gpg --import
&& chmod 644 /usr/share/keyrings/wazuh.gpg
```

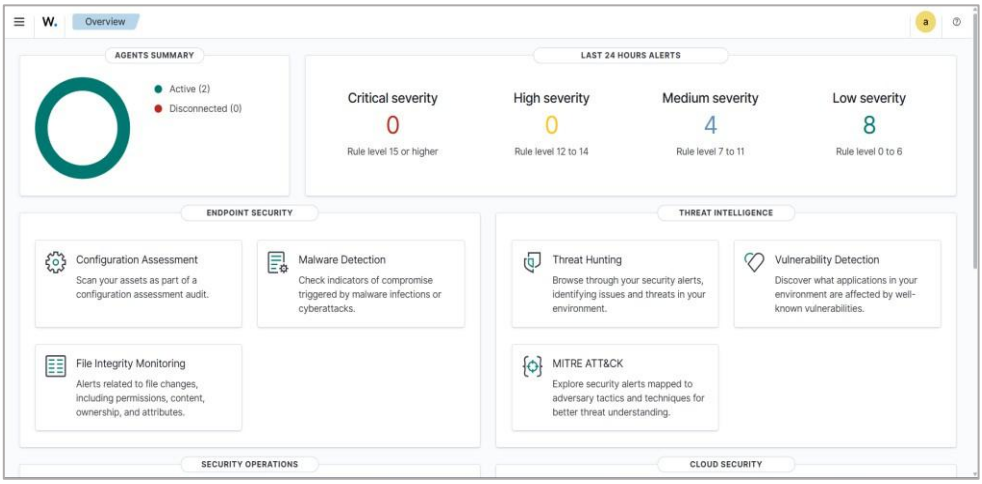
Gambar 9. Perintah Instalasi Wazuh Agent

Gambar 9 menunjukkan perintah yang digunakan untuk mengunduh dan mengimpor kunci GPG resmi dari Wazuh ke sistem, yang diperlukan untuk memverifikasi integritas paket Wazuh selama proses instalasi, serta menetapkan izin akses yang sesuai pada file kunci tersebut.

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg]
https://packages.wazuh.com/4.x/apt/ stable main" |
tee -a /etc/apt/sources.list.d/wazuh.list
```

Gambar 10. Menambahkan Repository Wazuh

Perintah pada gambar 10 digunakan untuk menambahkan repository resmi Wazuh ke dalam sistem APT dan mengaitkannya dengan kunci GPG yang telah diimpor sebelumnya, sehingga memungkinkan sistem untuk mengunduh dan memverifikasi paket Wazuh secara aman selama proses instalasi. Seteleah proses instalasi berhasil antarmuka wazuh *dashboard* akan terlihat seperti pada gambar 11



Gambar 11. Tampilan Awal Wazuh

KESIMPULAN

Berdasarkan hasil penelitian, integrasi antara Honeypot Dionaea dan Host-based Intrusion Detection System (HIDS) Wazuh terbukti berhasil diimplementasikan sebagai sistem keamanan adaptif yang mampu meningkatkan kinerja deteksi dan respons melalui pemrosesan log serta pengembangan aturan deteksi khusus. Pengujian menunjukkan bahwa sistem efektif mendeteksi dan merespons serangan pada lapisan aplikasi, seperti brute force terhadap layanan FTP, dengan kemampuan menghasilkan peringatan sekaligus memblokir alamat IP penyerang secara otomatis. Sementara itu, serangan pada lapisan jaringan seperti SYN Flood dan ICMP Flood, meskipun tidak tercatat oleh Honeypot Dionaea, tetap dapat diidentifikasi sebagai anomali melalui pemantauan lonjakan penggunaan CPU dan memori. Secara keseluruhan, integrasi ini berhasil mengubah honeypot dari alat analisis pasif menjadi sensor pertahanan aktif, sehingga meningkatkan ketahanan server terhadap berbagai ancaman siber dan memperkuat visibilitas serta kemampuan respons HIDS Wazuh.

UCAPAN TERIMA KASIH

Terima kasih kepada tempat mengabdi kami di Politeknik Negeri Ujung Pandang dan Universitas Halu Oleo yang sudah memberikan motivasi terhadap kami dan terima kasih kepada keluarga kami yang paling kami sayangi.

REFERENSI

Asrul, A. (2025). Pengaruh Kebijakan Manajemen Teknologi Terhadap Inovasi Produk Di Industri Kreatif. *Portal Riset Dan Inovasi Sistem Perangkat Lunak*, *3*(1), 21–27. https://doi.org/10.59696/prinsip.v3i1.78

Asrul, A., Sarinah, S., Rijal, M., Said, L. O. A., Makmur, M., Rusudu, N. A., & Ningtyas, C. P. (2025). Pemanfaatan Teknologi Digital untuk Meningkatkan Daya Saing Usaha Mikro Desa Tridana Mulya Kabupaten Konawe Selatan. *Jurnal Ilmiah Pengabdian Multidisiplin*, *1*(1), 44-50.

Asrul, A., Putra, A. ., & Rajab, M. . (2025). Transpormasi Bisnis Di Era Digital: Peluang, Tantangan, Dan Strategi Inovasi. *Jurnal Minfo Polgan*, *13*(2), 2294-2298.

Asrul, A. (2024). Penerapan Strategi Manajemen Teknologi untuk Meningkatkan Daya Saing di Industri 4.0. *INVESTASI : Inovasi Jurnal Ekonomi Dan Akuntansi*, *2*(4), 215–220. https://doi.org/10.59696/investasi.v2i4.71

Adnyana, I. G., Dirgayusari, A. M., & Atmaja, K. J. (2024). Data Visualization for Building a Cyber Attack Monitoring Dashboard Based on Honeypot. *Sinkron: Jurnal Dan Penelitian Teknik Informatika*, *8*(4), 2510–2518.

Adzimi, S. N., Alfasih, H. A., Ramadhan, F. N. G., Neyman, S. N., & Setiawan, A. (2024). Implementasi Konfigurasi Firewall dan Sistem Deteksi Intrusi menggunakan Debian. *Journal of Internet and Software Engineering*, *1*(4), 12.

AL-Hawamleh, A. M. (2023). Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures. *International Journal of Advanced Computer Science and Applications*, *14*(2), 801–809. https://doi.org/10.14569/IJACSA.2023.0140292

Andria. (2020). Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux. *Generation Journal*, *4*(2), 69–76.

Badan Siber dan Sandi Negara (BSSN). (2024). Laporan Tahunan Layanan Honeynet BSSN 2023. Diakses dari https://www.bssn.go.id/honeynet/

Bahodirovich, R. A., Rauf o‘g‘li, H. A., & Ravshan o‘g‘li, T. J. (2024). АНАЛИЗ БЕЗОПАСНОСТИ СИСТЕМ ELASTIC STACK, WAZUH И IDS В СЕТЯХ. *ANALYSIS OF MODERN SCIENCE AND INNOVATION*, *1*(2), 300– 302.

Bensaid, R., Labraoui, N., Ari, A. A. A., Maglaras, L., Saidi, H., AbduLwahhab, A. M., & Benfriha, S. (2024). Toward a Real-Time TCP SYN Flood DDoS Mitigation Using Adaptive Neuro-Fuzzy Classifier and SDN Assistance in Fog Computing. Security and Communication Networks, 2024, 1–20.

Chandra, R., & Sitorus, A. T. (2024). Virtualisasi Server Menggunakan Proxmox Untuk Mengoptimalkan Resource Server Pada SMK Bhakti Persada. *Jurnal Multidisiplin Ilmu Akademik*, *1*(2), 69–80.

Dwi Prasetyo, O., Hari Trisnawan, P., & Bhawiyuga, A. (2023). Uji Kinerja Host-Based Intrution Detection System WAZUH terhadap Serangan Brute Force dan Dos. *Jurnal*

Pengembangan Teknologi Informasi Dan Ilmu Komputer, *7*(6), 2686–2692. http://j-ptiik.ub.ac.id

Faiz, M. N., Somantri, O., Supriyono, A. R., & Muhammad, A. W. (2022b). Impact of feature selection methods on machine learning-based for detecting DDoS attacks: Literature review. *Journal of Informatics and Telecommunication Engineering*, *5*(2), 305–314.

Fiqri, K. G., Hanuranto, A. T., & Setianingsih, C. (2020). Analisis Perbandingan Klasifier Decision Tree, Random Forest, Dan Adaboost Dalam Mendeteksi Serangan Siber. *EProceedings of Engineering*, *7*(1).

Fuada, Z. (2023). *Penerapan Keamanan Jaringan Menggunakan Sistem Snort Dan Honeypot Sebagai Pendeteksi Dan Pencegah Malware Skripsi*. 1–55.

Fortinet. (2025). *Serangan Siber: Arti & Definisi*. Fortinet.Com. https://www.fortinet.com/resources/cyberglossary/what-is-cyber-attack

Goyal, U., Krishna, A., Kumar, A., & Sharma, K. (2022). Detection And Prevention Of Cyber Attacks On Multi-purpose IoT Devices Using Honeypot. *Proceedings of the Advancement in Electronics & Communication Engineering*.

Grover, V. (2020). An Efficient Brute Force Attack Handling Techniques for Server Virtualization. *SSRN Electronic Journal*, 1–4. https://doi.org/10.2139/ssrn.3564447

Hadhiatma, A., Hernawan, A., & Soelistijanto, B. (2024). *Pengembangan Sumber dan Evaluasi Pembelajaran Sekolah Dasar Menggunakan Moodle Berbasis Virtual Machine*. *4*(5).

Hadi, F. A. (2018). Peningkatan sistem keamanan data center menggunakan metode host-based intrusion detection system (HIDS) dengan aplikasi Wazuh

Hafiz, A., Kurniawan, T., Sivi, N. A., Ikhsan, F. K., & Andhika, P. (2020). Analisis Celah Keamanan Jaringan Dan Server Menggunakan Snort Intrusion Detection System. *Jurnal Informasi Dan Komputer*, *8*(2), 55–65.

Hameed Alazawi, S. A., Abdulhameed, A. A., Hassan, G. M., & Hassooni, M. (2024). Comparative Study on Applications of Cybersecurity Tools for Kali Linux Operating System. *AIP Conference Proceedings*, *3207*(1). https://doi.org/10.1063/5.0234136

Hartinah. (2018). Implementasi Honeypot Dionaea untuk Analisis Malware Ransomware.

Holbel, R., Yerby, J., & Smith, W. (2024). Utilizing virtualized honeypots for threat hunting, malware analysis, and reporting. *Issues in Information Systems*, *25*(1).

Ikhwanul Uzlah, L., Adi Saputra, R., & Isnawaty, I. (2024). Deteksi Serangan Siber Pada Jaringan Komputer Menggunakan Metode Random Forest. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(3), 2787–2793. https://doi.org/10.36040/jati.v8i3.8891

Intan Sabila, M., Tahir, M., Dwi Mardania, S., & Ilham Arifin, R. (2025). Implementasi Snort Sebagai Ids Dalam Mendeteksi Serangan Port Scanning Nmap Pada Simulasi Jaringan Virtual. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(4), 6944–6948.

Irfandi, F. R., Hedianto, U. Y. K. S., & Almaarif, A. (2022). Software Security Hardening Pada Virtual Private Server Berdasarkan NIST SP 800-123 di Universitas XYZ. *Journal of Information System Research (JOSH)*, *4*(1), 94–102. https://doi.org/10.47065/josh.v4i1.2299

Iswara, I. B. A. I., & Yasa, I. P. P. K. (2021). Analisis Dan Perbandingan Quality of Service Video Conference Jitsi Dan Bigbluebutton Pada Virtual Private Server. *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, *4*(2), 192–203. https://doi.org/10.31598/jurnalresistor.v4i2.794

Jovanka Daryl Ruindungan, Sherwin R. U. A. Sompie, & Xaverius B. N. Najoan. (2025). Analisis Kerentanan terhadap Serangan Denial of Service pada Website Universitas Sam RatulangiNgrok. 20(1), 39–50.

Kocaogullar, Y., Cetin, O., Arief, B., Brierley, C., Pont, J., & Hernandez-Castro,J. (2025). Hunting High or Low: Evaluating the Effectiveness of High- Interaction and Low-Interaction Honeypots. *Lecture Notes in Computer Science*, *13855 LNCS*, 14–30. https://doi.org/10.1007/978-3-031-83072-3_2

Mispriatin, M., Ginting, J. G. A., & Arifwidodo, B. (2022). Analisis Kinerja Honeypot Dionaea Dan Cowrie Dalam Mendeteksi Serangan. *Prosiding Seminar Nasional Teknoka*, *6*(2502), 170–178. https://doi.org/10.22236/teknoka.v6i1.448

Mitton, N. (2020). *Cyber Incident handling Trend Analysis*.Musa, U. S., Chhabra, M., Ali, A., & Kaur, M. (2020). Intrusion detection system using machine learning techniques: A review. *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, 149–155.

Nas, M., Ulfiah, F., & Putri, U. (2023). Analisis Sistem Security Information and Event Management (SIEM) Aplikasi Wazuh pada Dinas Komunikasi Informatika Statistik dan Persandian Sulawesi Selatan. *Jurnal Teknologi Elekterika*, *20*(2), 92–97.

Yang, X., Yuan, J., Yang, H., Kong, Y., Zhang, H., & Zhao, J. (2023). A highly interactive honeypot-based approach to network threat management. *FutureInternet*, *15*(4), 127.

Zein, M. A., Hediyanto, U. Y. K. S., & Almaarif, A. (2023). Hardening Sistem Operasi Virtual Private Server Fakultas Rekayasa Industri Berdasarkan Nist Sp 800- 123. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *8*(1), 230–241. https://doi.org/10.29100/jipi.v8i1.3438