Vol 3 (2022) No 1

Jitsi Jurnal Ilmiah Teknologi Sistem Informasi

http://jurnal-itsi.org ISSN 2722-4619 (Print) ISSN 2722-4600 (Online)

Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos

Muhammad Dehan Pratama[#], Fitri Nova[#], Deddy Prayama[#]

[#] *Jurusan Teknologi Informasi, Politeknik Negeri Padang, Limau Manis, Padang, 25164, Indonesia*
E-mail: fitrinova@pnp.ac.id, deddy@pnp.ac.id

A B S T R A C T S

Server monitoring is the process of monitoring server system resources such as monitoring server performance also helps identify other performance-related problems such as resource utilization, application downtime, and response time to a service. File Integrity Monitoring (FIM) is the activity of monitoring the integrity of a file to maintain the integrity of a file from unauthorized changes, by utilizing Wazuh as one of the open source applications to monitor has various features to perform monitoring. Computer network security becomes something that needs to be considered as technology develops rapidly. It is the responsibility of a network administrator to monitor system security at any time. Given the various threats that can enter the system at any time, an application is needed that can detect and prevent the threat in real time. The problem raises the idea for the author to utilize one of the applications, namely Suricata in which there is an IDS (Intruction Detection System) method that will serve as an attacker detection. Suricata will display an alert when there is a suspicious package. The resulting alert will be stored in the file log. Then the log will be displayed on the Wazuh web interface. Alerts that appear on Wazuh will be sent to network administrators via e-mail.

K A T A K U N C I

Server,
Wazuh,
Monitoring,
Keamanan,
Suricata ,
IDS,
E-mail

A B S T R A K

Monitoring server merupakan proses pemantauan sumber daya sistem server seperti memantau kinerja server juga membantu mengidentifikasi masalah terkait kinerja lainnya seperti pemanfaatan sumber daya, waktu henti aplikasi, dan waktu respon terhadap suatu service. File Integrity Monitoring (FIM) merupakan aktifitas memonitor integritas sebuah file untuk menjaga keutuhan suatu file dari perubahan yang tidak terotorisasi, dengan memanfaatkan Wazuh sebagai salah satu aplikasi open source untuk melakukan monitoring memiliki berbagai macam fitur untuk melakukan monitoring. Keamanan jaringan komputer menjadi hal yang perlu diperhatikan seiring berkembangnya teknologi yang pesat. Menjadi tanggung jawab bagi seorang administrator jaringan untuk memonitor keamanan sistem sewaktu-waktu. Mengingat adanya berbagai ancaman yang bisa masuk kedalam sistem kapan saja, dibutuhkan aplikasi yang dapat mendeteksi dan mencegah adanya ancaman tersebut secara realtime. Permasalahan tersebut menimbulkan gagasan untuk memanfaatkan salah satu aplikasi, yaitu Suricata yang di dalamnya terdapat metode IDS (Intruction Detection System) yang akan berfungsi sebagai pendeteksi attacker. Suricata akan menampilkan alert ketika ada paket yang mencurigakan. Alert yang dihasilkan akan disimpan didalam log file. Kemudian log tersebut akan ditampilkan pada web interface Wazuh. Alert yang tampil pada Wazuh nantinya akan dikirimkan kepada administrator jaringan melalui e-mail.

1. PENDAHULUAN

Seiring berkembangnya internet, banyak instansi kantor ataupun perusahaan yang menggunakan internet untuk memperlancar arus komunikasi informasi di dalamnya. Data-data perusahaan merupakan informasi yang bersifat rahasia dan harus dijaga keamanannya. Di sisi lain, mudahnya akses untuk mendapat informasi tersebut menyebabkan munculnya masalah baru yaitu dapat dimanfaatkannya informasi atau data penting oleh pihak yang tidak bertanggung jawab demi kepentingannya sendiri.

Adanya Covid-19 yang memaksa setiap orang untuk melakukan segala aktifitasnya dari rumah, baik belajar, bekerja maupun berbelanja. Oleh karena itu, orang dituntut lebih banyak menggunakan akses internet. Kesempatan ini digunakan oleh para penjahat siber untuk melakukan berbagai macam serangan, seperti pengumpulan data, ransomware, penipuan online dan phishing. Federal Bureau of Investigation (FBI) menyatakan bahwa kejahatan dunia maya mengalamai pengingkatan sebanyak 300 persen sejak awal pandemi virus corona ini. Sedangkan BKA Jerman mencatat total 108.474 kasus cyber crime di laporannya pada tahun 2020 silam. Sedangkan data tersebut masih berupa data kotor karena banyak kasus yang tidak sempat dilaporkan. Penyerangan ini bisanya dilakukan pada server dimana data client disimpan. Para penjahat siber bisa saja dengan segaja merusak server dan mengambil data-data penting untuk keperluan pribadi.

Seorang penyerang akan menyerang sistem jaringan dengan maksud guna mengalahkan layanan keamanan pada fasilitas jaringan tersebut. Dengan mempertimbangkan fakta bahwa jaringan public pada awalnya dirancang untuk keterbukaan tanpa mempertimbangkan keamanan, jelas diikuti meningkatnya pula serangan cybercriminals dari tahun ketahuan[1]. Untuk itu perlu sekali dilakukan monitoring server guna memastikan data-data penting yang dianggap rahasia tetap aman dan tidak tidak dirusak maupun dicuri oleh penjahat siber. Maka diperlukan sebuah tools yang dapat memantau perkembangan yang terjadi dalam sebuah server. Diamana akan ada sebuah server yang bertugas melakukan monitoring terhadap suatu server dengan teknologi cloud computing. Cluod computing sendiri sangat tergantung pada teknologi virtualisasi, yaitu konsep pembuatan versi virtual dari sesuatu yang bersifat fisik, misalnya sistem operasi, perangkat storage atau penyimpanan data atau sumber daya jaringan. Teknologi virtualisasi ini juga memiliki tujuan untuk memaksimalkan kinerja server serta menghindari pemborosan. Salah satu tools yang digunakan untuk monitoring adalah Wazuh.

Web server seringkali menjadi target dari berbagai jenis serangan baik yang sifatnya minor maupun major sehingga berakibat fatal. Akan tetapi, adakalanya website dijadikan pintu oleh peretas (hacker) untuk menembus web server. Salah satu contoh eksploitasi pada web server yang sering terjadi adalah serangan DoS[2].

GAMBAR 1. Perbandingan jumlah serangan DoS, Q2 dan Q3 2021, dan Q3 2020

DoS(Denial of Service) adalah serangan ditujukan untuk membanjiri server jaringan dengan permintaan layanan sehingga server mogok dan menolak akses pengguna. Ini dapat menyebabkan gangguan besar bagi organisasi dan bisnis. Serangan semacam itu dapat berlangsung selama beberapa menit atau bahkan beberapa hari. Kemudian ada yang disebut serangan DoS "pintar" ini merupakan serangan lanjutan dari Dos yang awal. Serangan ini lebih canggih dan sering ditargetkan, dan dapat digunakan tidak hanya untuk mengganggu layanan tetapi juga untuk membuat sumber daya tertentu tidak dapat diakses atau mencuri uang. Kedua jenis serangan tersebut meningkat pada Q3 2021. Jika dibandingkan dengan Q3 2020, jumlah total serangan DoS meningkat hampir 24%, dan jumlah total serangan "pintar" meningkat sebesar 31%. Kedua jenis serangan tersebut juga meningkat jika dibandingkan dengan Q2 2021, dengan persentase resource yang diserang terbesar (40,8%) berada di AS, diikuti oleh Hong Kong dan China daratan. Faktanya, pada bulan Agustus, Kaspersky mencatat rekor jumlah serangan DoS dalam satu hari: 8.825[3].

2. METODOLOGI PENELITIAN

Wazuh merupakan perangkat berbasis Open Source yang berfungsi sebaga sistem deteksi intrusi berbasis host (endpoint). Wazuh melakukan analisis log, pemeriksaan integritas, pemantauan registri Windows, deteksi rootkit, peringatan berbasis waktu, dan respons aktif. Wazuh merupakan perangkat yang menyediakan fitur visibilitas keamanan yang lebih dalam ke sebuah infrastruktur dengan memantau host pada sistem operasi dan juga pada tingkat aplikasi. Wazuh terdiri dari 2 (dua) bagian yaitu Wazuh-Server dan Wazuh-Agent. Wazuh server merupakan perangkat yang digunakan sebagai manajemen agen dan dashboard sistem monitoring baik file integrity, intrusion, maupun log. Sedangkan Wazuh agent merupakan perangkat yang diinstall pada perangkat

endpoint untuk melakukan pembacaan sistem, pengumpulan log serta mengirimkan ke Wazuh server. Fitur-fitur yang disediakan oleh Wazuh antara lain:

1. Manajemen dan analisis log: Wazuh agent membaca sistem operasi dan log aplikasi, dan meneruskannya dengan aman ke Wazuh server untuk analisis dan penyimpanan (management).
2. Pemantauan integritas file: Wazuh memonitor sistem file, mengidentifikasi perubahan konten, izin, kepemilikan, dan atribut file yang ada pada sistem;
3. Deteksi intrusi dan anomali: Wazuh agent memindai sistem untuk mencari malware, rootkit, atau anomali yang mencurigakan. agent dapat mendeteksi file tersembunyi, proses terselubung atau pendengar jaringan yang tidak terdaftar, serta inkonsistensi dalam respons panggilan sistem;
4. Pemantauan kebijakan dan kepatuhan: Wazuh memantau file konfigurasi untuk memastikan mereka mematuhi kebijakan keamanan, standar, atau panduan pada sistem sesuai Security Framework. Agent melakukan pemindaian berkala untuk mendeteksi aplikasi yang diketahui rentan,atau tidak dikonfigurasi dengan aman. Rangkaian kemampuan yang beragam ini disediakan dengan mengintegrasikan OSSEC, OpenSCAP dan Elastic Stack,

Sistem monitoring merupakan suatu proses untuk mengumpulkan data dari berbagai sumber daya. Biasanya data yang dikumpulkan merupakan data yang realtime. Secara garis besar tahapan dalam sebuah sistem monitoring terbagi ke dalam tiga proses besar, yaitu:

1. Proses di dalam pengumpulan data monitoring.
2. Proses di dalam analisis data monitoring.
3. Proses di dalam menampilkan data hasil monitoring.

Aksi yang terjadi di antara proses-proses dalam sebuah sistem monitoring adalah berbentuk service, yaitu suatu proses yang terus-menerus berjalan pada interval waktu tertentu. Proses-proses yang terjadi pada suatu sistem monitoring dimulai dari pengumpulan data seperti data dari network traffic, hardware information, dan lain-lain yang kemudian data tersebut di analisis pada proses analisis data dan pada akhirnya data tersebut akan ditampilkan

Management log adalah proses mengumpulkan, menganalisis, dan menyimpan data log. Log adalah catatan aktivitas sistem seperti kesalahan, peristiwa keamanan, dan pola penggunaan. Perangkat lunak logging menangkap log dan menyimpannya untuk analisis di masa mendatang. Management log biasanya terdiri dari komponen:

1. Koleksi: Mengumpulkan berbagai data dari berbagai sumber seperti jaringan, server, aplikasi dan OS.
2. Pemantauan: Alat ini melacak setiap aktivitas yang terjadi di seluruh direktori.
3. Analisis: Manajemen log bekerja pada data yang diterima dan mengubahnya menjadi informasi untuk secara proaktif mengidentifikasi bug, kesalahan, dan peningkatan.
4. Penyimpanan: Alat ini menominasikan berapa lama data harus disimpan dalam file log.
5. Pelaporan: Kemudian membuat audit laporan untuk meningkatkan kinerja operasi, keamanan, dan kepatuhan terhadap peraturan.

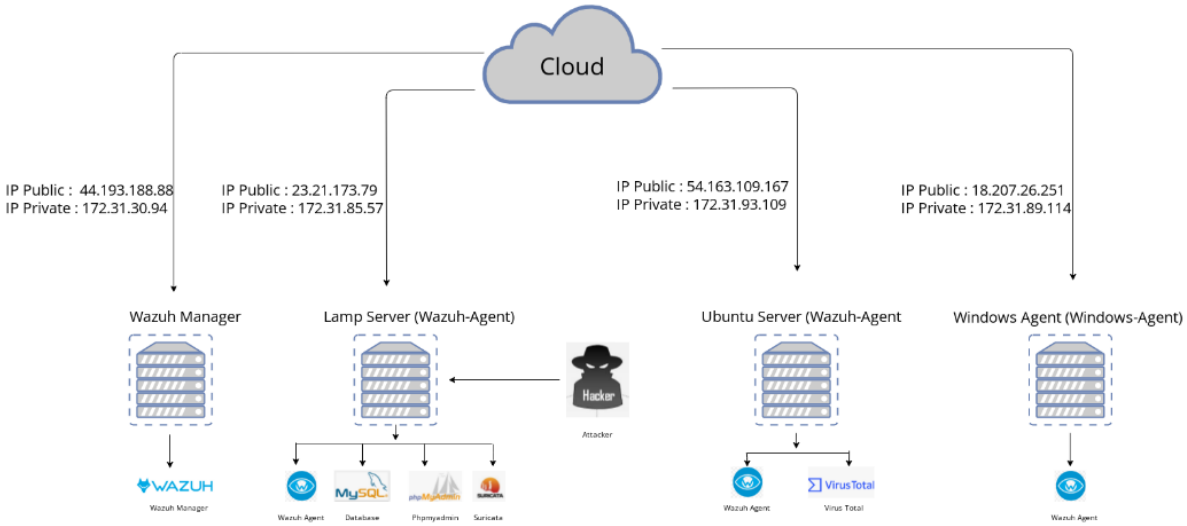
Denial of Service (DOS) attack merupakan sebuah serangan yang bertujuan untuk merusak atau mengacaukan layanan. Serangan DoS bekerja dengan cara menghabiskan sumber daya yang dimiliki server sehingga server tersebut tidak bisa diakses dan tidak dapat menjalankan fungsinya. Biasanya penyerang sering melakukan serangan DoS dengan cara membanjiri trafik dengan banyak paket yang dikirim ke server. Selain itu, teknik yang digunakan untuk melakukan serangan DoS sangat bermacam-macam diantaranya adalah menghabiskan bandwidth, serangan paket SYN, serangan paket ICMP, menyerang keamanan aplikasi, mengirimkan request layanan yang banyak, serangan peer-to-peer atau permanen DoS [7]. Beberapa jenis serangan DoS adalah sebagai berikut [8] :

1. UDP Flooding
   Serangan UDP flooding digunakan untuk mengirimkan paket data secara masif kepada server target dengan menggunakan protokol UDP sebagai akses penyerangan. Akibatnya, komputer target akan kesulitan menangani request data dalam jumlah besar.
2. SYN Flooding
   Serangan SYN flooding dilakukan saat dua komputer akan melakukan sambungan komunikasi. Attacker akan mengirimkan pesan “syn ack” kepada komputer target dalam jumlah besar. target akan merespons dengan sebuah paket SYN/ACK yang ditujukan kepada alamat yang tercantum di dalam SYN Packet yang di terima (yang berarti sistem tersebut tidak ada secara aktual), dan kemudian akan menunggu paket Acknowledgment (ACK) sebagai balasan untuk melengkapi proses pembuatan koneksi. Tetapi, karena alamat sumber dalam paket SYN yang dikirimkan oleh penyerang tidaklah valid, paket ACK tidak akan pernah datang ke target, dan port yang menjadi target serangan akan menunggu hingga waktu pembuatan koneksi "kedaluwarsa" atau timed-out.
3. ACK flood attack
   Ketika penyerang mencoba membebani server dengan paket TCP ACK. Tujuan dari ACK flood adalah untuk menolak layanan ke pengguna lain dengan memperlambat atau menghancurkan target

menggunakan data sampah. Server yang ditargetkan harus memproses setiap paket ACK yang diterima, yang menggunakan begitu banyak daya komputasi sehingga tidak dapat melayani pengguna yang sah.

4. HTTP Flood
   Serangan lapisan aplikasi yang sederhana dimana serangan ini menargetkan server website pada target dan menggunakan banyak permintaan HTTP cepat untuk menjatuhkan server.
5. ICMP flood
   Pada serangan ICMP flood, resource target akan dibanjiri dengan request ICMP secara cepat tanpa menunggu respon dari Anda. Jenis serangan seperti ini semua bandwidth masuk maupun keluar terkena dampaknya dan ini mengakibatkan kelambatan sistem pada server milik korban.

Sistem yang akan dibuat dengan metode Cloud computing pada platform AWS(Amazon Web service) menggunakan empat server untuk keperluan Wazuh manager dan Wazuh agent. Nantinya tiga dari empat server tersebut akan menggunakan sistem operasi Ubuntu server 20.40 dan satu menggunakan sistem operasi Microsoft Windows Server 2019 Base. Pada Wazuh manager akan menggunakan sistem operasi Ubuntu server 20.04.



GAMBAR 2. Topologi sistem

TABEL 1. Spesifikasi Kebutuhan Perangkat Lunak

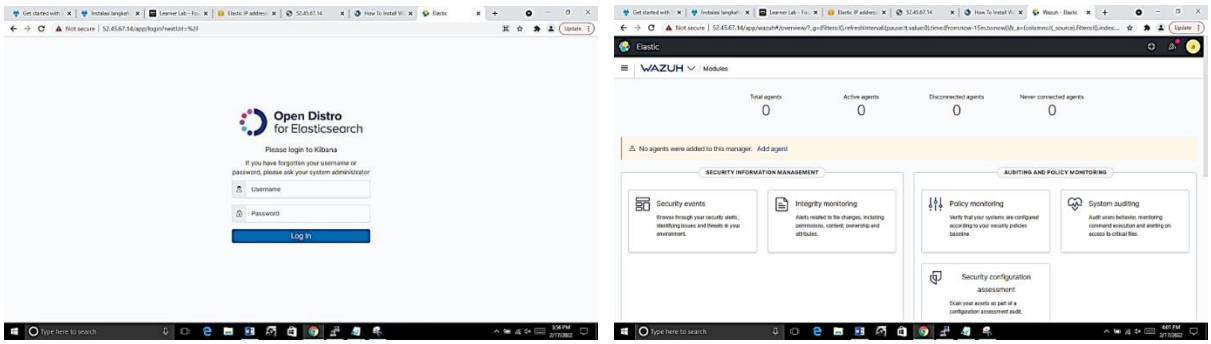
Nama	Versi	Fungsi
Ubuntu Server	20.04 LTS	Sistem operasi *server* Wazuh *manager*
Windows *Server*	2019 Base	Sistem operasi *server* Wazuh *agent*
Wazuh *Manager*	v4.2.1	Aplikasi *Network* Monitoring
*File*beat	v.7.10.2	Mengirim data *log* ke Elaticsearch
Elastic Stack	v.7.10.2	Elasticsearch berkemampuan dalam pencarian dan analisis data secara realtime.
Kibana	v.7.10.2	Kibana memvisualisasikan data yang tersimpan pada Elasticsearch.
Wazuh agent	v4.2.1	Agent yang akan dimonitoring oleh Wazuh manager
Suricata	V5.3.0	Aplikasi yang digunakan untuk mendeteksi adanya sengan Dos

Berdasarkan Gambar 1, gambaran topologi yang dibangun kita dapat mengetahui alur bagaimana Wazuh manager bisa bekerja sama dengan Wazuh agent. Bedasarkan gambar di atas, kita mengetahui bahwa semua server kita akses melalui Cloud. pada server Wazuh manager juga akan dilakukan instalasi Kibana, Filebeat, dan Elasticsearch yang nantinya akan berguna sebagai web interface Wazuh manager dan Wazuh agent. maka ada beberapa hal yang harus dipersiapkan terlebih dahulu. Hal yang perlu dilakukan adalah menentukan apa saja yang terdapat dalam sistem yang kita bangun. Perancangan sistem yang akan dibangun terdiri dari Hardware dan Sorftware.. maka untuk kebutuhan Ssitem Operasi dan Perangkat Lunaknya dapat dilihat pada Tabel 1. Khusus pada agent Lamp server merupakan server yang akan kita uji nantinya dengan menggunakan metode serangan dos. Untuk melihat apakah server dapat mendetksi adanya serangan dos dan mengirimkan log tersebut pada Wazuh manager nantinya. Untuk Wazuh agent akan didaftarkan pada Wazuh manager, konfigurasi tersebut dilakukan dengan cara remote access menggunakan aplikasi PuTTY. Setelah Wazuh manager dan Wazuh agent saling terhung, maka aktifitas yang dilakukan oleh Wazuh agent dapat diketahui oleh Wazuh manager.

5. Melakukan instalasi suricata pada Wazuh agent Lamp.
6. Melakukan instalasi Hping3 pada Kali Linux yang berfungsi sebagai tools untuk melakukan serangan Dos.
7. Melakukan pengujian deteksi celah keamanan pada Wazuh agent dengan melakukan serangan Dos menggunakan Hping3.

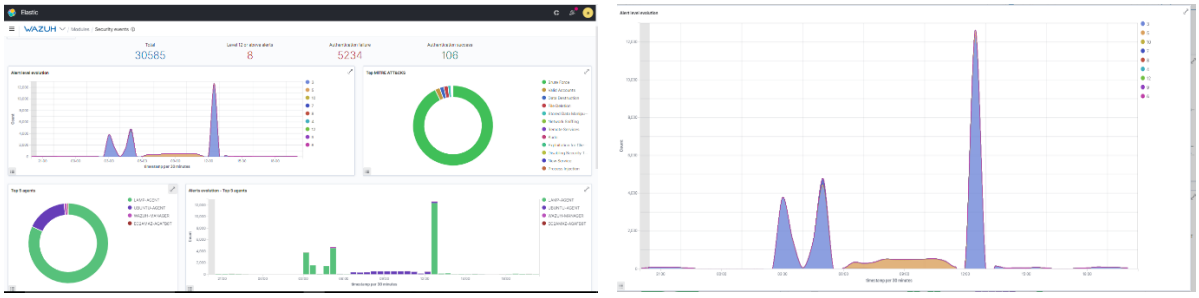
Perintah mngunduh repository Wazuh

```
#aptinstall curl apt-transport-https unzip wget libcap2-bin software-
properties-common lsb-release gnupg

#curl -s https://packages.wazuh.com/key/GPG- KEY-WAZUH | apt-key add

#echo "deb https://packages.wazuh.com/4.x/apt/stable main" | tee -a
/etc/apt/sources.list.d/wazuh.list

#apt-get update
```



GAMBAR 3. Tampilan Wazuh

Pada Gambar 4 dapat terlihat informasi mengenai aktivitas apa saja yang dilakuakan oleh semua agent dalam rentang waktu 24 jam terakhir. Data yang ditampilkan pada web interface Wazuh sudah berupa grafik, sehingga mudah dipahami oleh administrator jika ingin melakukan monitoring. Pada dashboard tersebut juga dapat dilihat tentang berapa banyak serangan yang masuk, agent mana yang paling sering aktif dan jenis serangan apa saja yang paling banyak dilakukan terhadap agent Wazuh



GAMBAR 4. Dashboard Security Event dan Alert level

TABEL 3. Pengujian Deteksi Terhadap Serangan DoS

No	Metode Serangan	Keterangan
1	SYN Flood	Berhasil Terdeteksi
2	ICMP Flood	Berhasil Terdeteksi
3	ACK Flood	Gagal Terdeteksi
4	UDP Flood	Gagal Terdeteksi

System monitoring ini kita harus benar-benar mencermati user mana saja yang melakukanaktifitas pada server dan apa saja yang dilakukan user tersebut ketika melakukan aktifitas pada server. Monitoring seperti ini sangat berguna untuk mengantisipasi pencurian data oleh pihak yang tidak bertanggung jawab. Pada sisi kemanan kita berhasil melakukan integrase dengan platform Virus Total sehingga jika user tidak sengaja mengunduh file yang didalamnya terdapat malware.

Wazuh manager akan mengeluarkan peringatan bahwa file tersebut berbahaya. Sehingga administrator dapat menghapus file tersebut sebelum menginfeksi komputer. Pada Tabel 3 dapat kita lihat bahwa dari lima percobaan, hanya dua yang berhasil. Hal ini disebabkan oleh AWS Amazon sudah memiliki firewall tersendiri, yang otomatis didapatkan jika kita menggunakan server cloud computing AWS. Sehingga paket serangan DoS yang kita kirimkan terhadap Lamp – agent banyak yang sudah berhasil ditangani oleh AWS. Hal inilah yang membuat Lamp – agent tidak mendeteksi adanya serangan. Mengacu pada hasil pengujian monitoring dan pendeteksian serangan Dos di atas, walaupun belum semua pendeteksian serangan Dos berrhasil dilakukan. Dapat kita simpulkan bahwa implementasi Wazuh sebagai log event management dan deteksi celah keamanan pada server dari serangan DoS sudah berhasil dilakukan.

4. KESIMPULAN

Administrator tidak perlu lagi mengakses komputer server secara fisik. Karena aktivitas monitoring dapat dilakukan secara rutin menggunakan Wazuh. Wazuh manager mendapat informasi berupa log mengenai aktivitas yang dilakukan oleh agent. Kemudian log tersebut dapat divisualisasikan oleh Wazuh dengan beragam bentuk statistik agar mudah dipahami. Pada menu integrity monitoring menampilkan log dari aktivitas berupa membuat,memodifikasi dan menghapus file. Untuk mendeteksi adanya malware berbahaya, diperlukan integrasi antara Wazuh manager dan VirusTotal. Suricata dapat mendeteksi adanya serangan DoS. Kemudian alert dari suricata tersebut diteruskanWazuh agar ditampilkan pada web interface Wazuh. Alert dari Wazuh akan dikirmkan kepada administrator melalu e-mail..

REFERENSI

[1] M. Arman, “Metode Pertahanan Web Server Terhadap Distributed Slow HTTP DoS Attack,” JATISI (Jurnal Tek. Inform. dan Sist. Informasi), vol. 7, no. 1, pp. 56–70, 2020, doi: 10.35957/jatisi.v7i1.284.

[2] H. Juliansyah, “Analisa dan Perancangan Sistem Keamanan Jaringan Webserver dari Serangan Denial of Service (DoS) Dengan Menggunakan Metode Penetration,” pp. 1–6, 2015.

[3] Kaspersky. (2021). DDoS attacks in Q3 grow by 24%, become more sophisticated. Dari https://www.kaspersky.com/about/press- releases/2021_ddos-attacks-in-q3-grow-by-24-become-more-sophisticated Diakses pada 27 Desember 2021.

[4] I. Amazon Web Service, Cloud Platform. Dari https://aws.amazon.com/what-is- aws/?nc1=h_ls. Diakses pada 20 Januari 2022.

[5] I. Efendi, (2015), “Apa Yang di Maksud Dengan Server ?”. Dari https://www.it- jurnal.com/apa-yang-di-maksud-dengan-server/. Diakses pada 23 Januari 2022.

[6] BSSN, (2021), “Tutorial instalasi wazuh 4.0 endpoint security pada centOS7”. Dari https://govcsirt.bssn.go.id/tutorial-instalasi-wazuh-4-0-endpoint-security- padacentos7/# :~:text=Wazuh%20merupakan%20perangkat%20berbasis%20Op en,berbasis%20 waktu%2C%20 dan %20respons% 20aktif. Diakses 21 Januari 2022.

[7] A. S. Fadhlillah, A. I. Irawan, F. T. Elektro, U. Telkom, and K. Jaringan, “Analisis Performansi Ids Menggunakan Metode Deteksi Anomaly- Based Terhadap Serangan Dos Ids Performance Analysis Using Anomaly-Based Detection Methods,” e-Proceeding Eng., vol. 6, no. 2, pp. 3398–3405, 2019.

[8] N. Febrianto (2019), “Macam – macam serangan DDoS Dan Cara Mengantisipasinya,”. Dari https:// www.tagar.id/macammacam-serangan-ddos- dan-cara-mengantisipasinya. Diakses pada 21 Januari 2022.

[9] S. Sanplippo, “Hping.” http://www.hping.org/ (accessed Jan. 23, 2022).

[10] M. Azmi, C. Foozy, K. Sukri, N. Abdullah, I. Hamid, & H. Amnur "Feature Selection Approach to Detect DDoS Attack Using Machine Learning Algorithms," JOIV : International Journal on Informatics Visualization, vol. 5, no. 4, , pp. 395-401, Dec. 2021. https://doi.org/10.30630/joiv.5.4.734

[11] Die.net, “hping3(8) - Linux man page,” linux.die.net. Dari https://linux.die.net/man/8/hping3. Diakses pada 21 Januari 2022