Implementasi Intrusion Detection System Dalam Upaya Pencegahan Cyber Attack

1st Sendi Ahmad Hidayat
Falkutas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
sendiahmadhidayat@student.telkomuniversity.ac.id

2nd Denny Darlis
Falkutas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
denny.darlis@tass.telkomuniversity.ac.id

Abstrak **- Dalam era digital ini, sistem informasi telah menjadi tulang punggung bagi banyak organisasi dan perusahaan. namun sistem informasi tidak terlepas dari serangan siber. Data statistik dari Badan Siber dan Sandi Negara (BSSN) mencatat telah terjadi 370,02 juta serangan siber di Indonesia pada tahun 2022[1]. Agar terhindar dari kerugian materiil dan kerugian immateriil yang diakibatkan oleh serangan siber ,organisasi, perusahaan , badan pemerintahaan dan lain diharukan memiliki suatu sistem yang dapat memantau, menganalisis kerentanan, dan mencegah terhadap serangan siber. Wazuh merupakan platform open source yang berperan sebagai Intrusion Detection System (IDS) atau sebagai sistem deteksi ancaman, pemantauan keamanan dan respons insiden. Mengimplementasikan wazuh dapat menjadi tembok pertahanan dalam sebuah badan organisasi, perusahaan , badan pemerintahaan dan lain sebagainya dalam mengatasi serangan siber. Implementasi wazuh memiliki fungsi untuk Threat prevention , Integrity monitoring ,Incident response ,Compliance dalam server, Deteksi ancaman ,Log Event Management dan Deteksi Celah yang dapat meminimalisir terjadinya serangan siber.**

Kata kunci **- Serangan siber, Sistem informasi, Wazuh, Pemantauan keamanan, Deteksi ancaman**

I. PENDAHULUAN

Dalam era digital ini, sistem informasi telah menjadi tulang punggung bagi banyak organisasi dan perusahaan. Sistem informasi digunakan untuk mengelola data, memfasilitasi komunikasi internal dan eksternal, menjalankan proses bisnis, dan menyediakan layanan kepada pengguna. namun penggunaan sistem informasi tidak terlepas terhadap serangan siber yang merugikan.

Data statistik dari Badan Siber dan Sandi Negara (BSSN) mencatat telah terjadi 370,02 juta serangan siber di Indonesia pada tahun 2022 Dibandigkan dengan tahun 2021 terjadi 266,74 juta serangan siber, yang dimana jumlah ini meningkat sebesar 38,72% [1]. ketika suatu badan organisasi, perusahaan , badan pemerintahaan dan lain sebagainya, terkena serangan siber tentunya akan menyebapkan berbagai masalah seperti, Gangguan operasional, Kerusakan reputasi, Hilangnya data pelanggan, Hilangnya data rahasia, Kehilangan bisnis, Kerugian material,Bocornya informasi perusahaan dan lain sebagainya. Berdasarkan website kompas, data Otoritas Jasa Keuangan (OJK), selama periode Semester I-2020 hingga Semester I-2021 saja, serangan siber membuat perbankan mengalami kerugian senilai Rp 246,5 miliar. Bahkan, secara global, Dana Moneter Internasional atau International Monetary Fund (IMF) memperkirakan angkanya mencapai Rp 1.420 triliun per tahun [2].

Agar terhindar dari kerugian materiil dan kerugian immateriil yang diakibatkan oleh serangan siber ,organisasi, perusahaan , badan pemerintahaan dan lain diharukan memiliki suatu sistem yang dapat memantau, menganalisis kerentanan, dan mencegah terhadap serangan siber.sistem pemantauan, analisis kerentanan, dan mencegah terhapat serangan siber ini dapat berupa Intrusion Detection System (IDS) yang dapat mendeteksi dan mencegah serangan siber.

Wazuh merupakan platform open source yang berperan sebagai Intrusion Detection System (IDS) atau sebagai sistem deteksi ancaman, pemantauan keamanan dan respons insiden. Mengimplementasikan wazuh dapat menjadi tembok pertahanan dalam sebuah badan organisasi, perusahaan , badan pemerintahaan dan lain sebagainya dalam mengatasi serangan siber. Implementasi wazuh memiliki fungsi untuk Threat prevention , Integrity monitoring ,Incident response ,Compliance dalam server, Deteksi ancaman ,Log Event Management dan Deteksi Celah yang dapat meminimalisir terjadinya serangan siber.

II. KAJIAN TEORI

Kajian teori dalam penelitian ini meliputi beberapa konsep dan tools yang digunakan dalam implementasi *intrusion detection system*.

A. Intrusion detection system

Intrusion Detection System (IDS) Merupakan sebuah perangkat atau aplikasi perangkat lunak yang memonitor jaringan atau sistem komputer untuk aktivitas mencurigakan atau pelanggaran kebijakan keamanan. IDS dapat mendeteksi berbagai jenis serangan dan anomali dengan memeriksa log data, lalu lintas jaringan, atau aktivitas pengguna.

B. Fungsi Intrusion Detection System

Intrusion Detection System memiliki 3 fungsi utama yaitu sebagai deteksi serangan, monitoring aktivitas, dan pemberitahuan (Alerting). Berikut penjelasan lebih rinci mengenai ke-3 fungsi Intrusion Detection System.

1. Deteksi Serangan

Intrusion Detection System akan mengidentifikasi upaya penyerangan terhadap jaringan atau sistem komputer, seperti serangan DoS (Denial of Service), intrusi berbasis malware, dan lain-lain.

2. Monitoring Aktivitas

Memonitor aktivitas pengguna dan lalu lintas jaringan untuk menemukan pola-pola yang mencurigakan.

3. Pemberitahuan (Alerting)

Memberikan notifikasi kepada administrator sistem ketika ditemukan aktivitas mencurigakan.

C. Komponen intrusion detection system

Secara umum intrusion detection system memiliki 3 komponen yaitu sensor, analyzer, dan user interface. Setiap komponen intrusion detection system tersebut akan saling bekerja sama untuk mendeteksi trafik yang mencurigakan dan kerentanan keamanan. Berikut penjelasan yang lebih rinci mengenai 3 komponen tersebut.

1. Sensor

Sensor akan mengumpulkan data dari jaringan atau host yang dipantau.

2. Analyzer

Analyzer akan menganalisis data yang dikumpulkan untuk mendeteksi aktivitas mencurigakan.

3. User Interface

User interface menyediakan antarmuka bagi administrator untuk melihat hasil deteksi dan mengelola IDS.

D. Wazuh

Wazuh adalah sebuah platform keamanan dan manajemen log sumber terbuka, sehingga dapat digunakan dan dimodifikasi sesuai kebutuhan organisasi tanpa biaya lisensi perangkat lunak. Wazuh memiliki kemampuan untuk pemantauan keamanan, deteksi ancaman, dan respons insiden. Platform ini dirancang untuk membantu organisasi melindungi infrastruktur IT mereka dari berbagai ancaman keamanan.

E. Fungsi wazuh

Wazuh berperan penting dalam mengatasi serangan siber. Fungsi utama wazuh yaitu sebagai pemantau keamanan, deteksi ancaman dan respons insiden. Namun karena wazuh ini bersifat open source yang berati kita bisa memodifikasi wazuh agar dapat menjalakan fungsi lainya di luar fungsi utama wazuh itu sendiri.

F. Typhoon

Typhoon merupakan sebuah mesin virtual (VM) yang dirancang sebagai tantangan dalam pengujian keamanan siber dan pelatihan. VulnHub adalah platform yang menyediakan berbagai mesin virtual yang dirancang khusus untuk menguji dan mengembangkan keterampilan di bidang keamanan informasi dan hacking.

G. Ubuntu

Ubuntu adalah distribusi Linux yang populer dan user-friendly, yang dikembangkan oleh Canonical Ltd. Ubuntu menjadi OS yang penulis pilih untuk server yang nantinya menjalankan wazuh.

H. Kali Linux

Kali Linux adalah distribusi Linux berbasis Debian yang dirancang khusus untuk keamanan informasi, pengujian penetrasi (penetration testing), dan forensik digital. Penulis menggunakan kali linux untuk melakan serangan brute force attack terhadap agen wazuh dan memastikan brute force attack tersebut dapat terdeteksi oleh wazuh.

I. Hydra

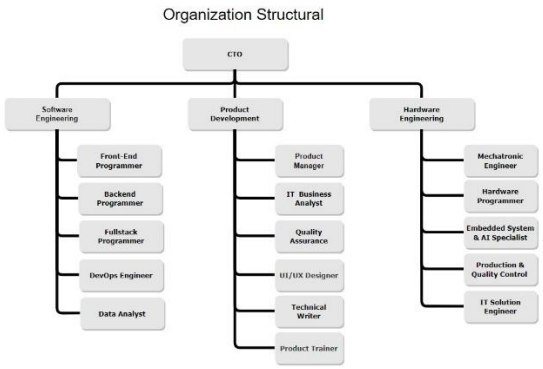
Hydra adalah alat keamanan yang digunakan untuk melakukan serangan brute force pada berbagai jenis layanan otentikasi. Hydra memiliki kemampuan untuk mencoba berbagai kombinasi username dan password untuk mendapatkan akses sistem target. Penulis mengunakan hydra untuk melakukan serangan brute force ssh terhadap agen wazuh dan memastikan wazuh dapat mendekteksi dan memblokir serangan tersebut.

J. Gambarana Umum Institusi

Sebagai TransTrack. TransTrack (PT. Indo Trans Teknologi) adalah perusahaan startup teknologi yang menyediakan solusi end-to-end untuk industri logistik dan transportasi. Ini bertujuan untuk menjadi pengoptimal operasi armada nomor satu dan integrator rantai pasokan di industri untuk membantu bisnis mengoptimalkan operasi mereka dengan mengurangi biaya, meningkatkan efisiensi, memaksimalkan produktivitas, dan meningkatkan keberlanjutan bisnis.

Dengan solusi Fleet Operation Optimizer milik , TransTRACK menyediakan proses pengiriman yang efisien, yang memfokuskan ke pembelian pelanggan berulang kali. Fleet Management System TransTRACK akan melakukan remote pada armada, pengemudi, dan kargo. Transportation Management TransTRACK akan merampingkan proses pengiriman dan memastikan pengiriman tepat waktu, dan Truck Appointment System TransTRACK akan menyelesaikan masalah kemacetan truk dan waktu bongkar/muat yang kurang lancar.

Secara garis besar Struktur organisasi dalam Perusahaan TransTrack terbagi menjadi 3 bagian yaitu Software Engineering, Product Development dan hardware engineering. Software Engineering bertangung jawab untuk mendalami seluruh sistem, program dan perangkat lunak dalam Perusahaan TransTrack. Product Development bertangung jawab terhadap pengembangan produk dari sebuh ide atau konsep sehingga produk dalam Perusahaan TransTrack dapat berkembang. Hardware Engineering bertangung jawat dalam meneliti, merancang, mengembangkan, dan menguji hardware. Dapat mengawasi pembuatan dan pemasangan hardware atau perangkat yang berkaitan dengan komputer dan teknologi.



GAMBAR 1
Struktur Organisasi TransTrack

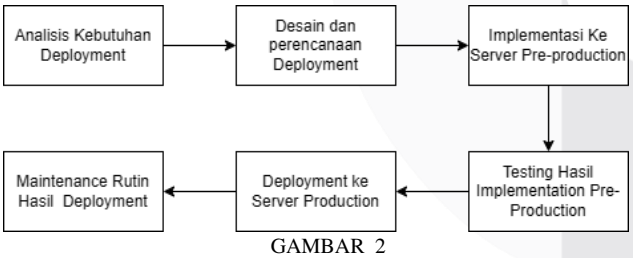
K. Divisi Kerja

Secara umum divisi DevOps bertangung jawab terhadap otomasisasi deployment aplikasi terhadap server production, bertangung jawab terhadap management infrastruktur IT, memantau kinerja aplikasi, infrastruktur dan layanan secara terus menerus, memperkuat aspek security terhadap seluruh service yang ada dalam sebuah Perusahaan dan masih banyak lagi.

III. METODE

A. Deskrisi alur pekerjaan

Tugas utama DevOps adalah mengintegrasikan proses pengembangan (Development) dengan operasi (Operations). Pada proses kolaborasi tersebut dimulai dari perencanaan hingga aplikasi tersebut di-delivery ke pengguna. tujuan kolaborasi terebut yaitu untuk meningkatkan frekuensi Deployment, meningkatkan waktu pemasaran, menurunkan tingkat kegagalan pada rilisan terbaru, dan mempersingkat waktu perbaikan. Dikarenakan terbatasnya sumber daya manusia di TransTrack, untuk tugas tim operasi menjadi tugas tambahan untuk tim DevOps di TransTrack. Untuk lebih jelasnya berikut alur kerja secara yang dilakukan oleh tim DevOps di TransTrack.



GAMBAR 2
Alur Pekerjaan DevOps

B. Analisis sistem

Pada alur pekerjaan yang ada pada tim DevOps di perusahaan TransTrack, terdapat tahapan maintenance rutin. Tahapan ini dapat berupa maintenance rutin, monitoring uptime, security monitoring, defensif cyber attack, vulnerability test, dan upgrade aplikasi. Pada tahapan security monitoring, defensif cyber attack, dan vulnerability test tim DevOps biasanya melakukannya secara manual, yang dilakukan secara rutin setiap bulan.

Namun Tim DevOps menilai untuk proses security monitoring, defensif cyber attack, dan vulnerability test secara manual ini dinilai tidak terlalu efektif dalam mengatasi serangan siber, dan dinilai cukup memakan banyak waktu. Karna itu tim DevOps memutuskan untuk meng-implementasikan wazuh sebagai intrusion detection system yang akan memonitoring security secara terus menerus, melakukan defensif cyber attack terhadap trafik yang mencurigakan, dan vulnerability test berkala secara otomatis. Dengan meng-implementasi wazuh ini dinilai dapat mempermudah proses kerja tim DevOps dalam tahapan maintenance rutin.

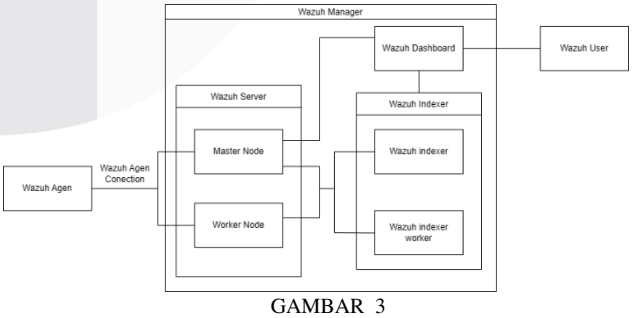
C. Pengembangan Sistem

Agar pada proses maintenance dapat dilakukan secara otomatis dan berlanjutan, maka tim DevOps di transtrack berencana untuk meng-implementasikan wazuh sebagai intrusion detection system yang akan melakukan security monitoring secara terus menerus, vulnerability test secara otomatis dengan waktu berkala, dan melakukan defensif terhadap cyber attack secara otomatis. Karna itu kami setuju untuk menerapkan wazuh sebagai intrusion detection system dalam Upaya meminimalisir serang siber dengan memonitoring aktifitas seluruh sistem.

D. Deployment wazuh

Dalam mengimplementasikan wazuh sebagai intrusion detection system perlu mempersiapkan beberapa rencana. Tahapan tesebut dapat berupa persiapan kebutuhan deploy wazuh, Desain dan perencanaan deploy wazuh, instalasi komponen wazuh server, penambahan agen wazuh, mengaktifkan fitur vulnerability test, perbandingan hasil vulnerability test wazuh dengan vulnerability test lainya, menambahkan active respons untuk mengatasi brute force SSH, pembuatan wazuh custum dashboard, implementasi pada ruang monitoring control.Semua tahapan tersebut perlu dilakukan untuk mestikan wazuh dapat berfungsi pada semestinya

Pengistalan wazuh manager dapat mengunakan 2 metode yaitu, single node dan multiple node. Untuk penginstalan dengan metode multiple node memiliki performa yang lebih baik dan high availability. Penginstalan multiple node digunakan untuk wazuh manager yang menangani banyak agen wazuh lebih dari 100. Dikarenakan untuk agen di TransTrack tidak lebih dari itu maka diputuskan untuk mengistal wazuh dengan metode single node. Untuk desainya kurang lebih seperti pada gambar di bawah.



GAMBAR 3
Infrastruktur Wazuh

E. Persiapan instalasi komponen wazuh manager

Sebelum melakukan pengistalan komponen-komponen wazuh, perlu membuat file konfigurasi untuk setiap komponen-komponen wazuh. pertama *download file konfigurasi* dari wazuh dengan perintah sebagai berikut.

lalu edit file config.yml untuk mengatur node wazuh. atur file config.yml menjadi seperti dibawah.

Gambar 4
Config.yml

Dari konfigurasi di atas dapat dilihat untuk setiap komponen wazuh diatur dengan ip yang sama yang berati setiap komponen wazuh di install pada server yang sama. Dengan setiap komponen yang hanya memiliki 1 node saja yang berati pengistalan dengan metode single node.

Selanjutnya meng-generate file konfigurasi diatas untuk digunakan dalam pengistalan wazuh indexer, wazuh server , dan wazuh dashboard. Untuk men-generate file konfigurasi gunakan perintah berikut.

```
bash wazuh-install.sh --generate-config-files
```

F. Pengistalan wazuh indexer

Komponen yang pertama di install adalah *wazuh indexer*. *Wazuh indexer* ini berfungsi untuk mengelola data log yang diterima dari *wazuh server.* Pengelolaan tersebut bertujuan untuk menganalisa setiap data log yang di terima dari wazuh server untuk mencari kerentanan dan sebagai pengindeksan. Untuk penginstalan *wazuh indexer* dilakukan pada *direktori wazuh indexer* yang sebelumnya dibuat, dan pastikan file *wazuh-install-file.jar* ada pada direktori tersebut. Pertama download file instalasi wazuh indexer terlebih dahulu dengan perintah seperti di bawah.

```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
```

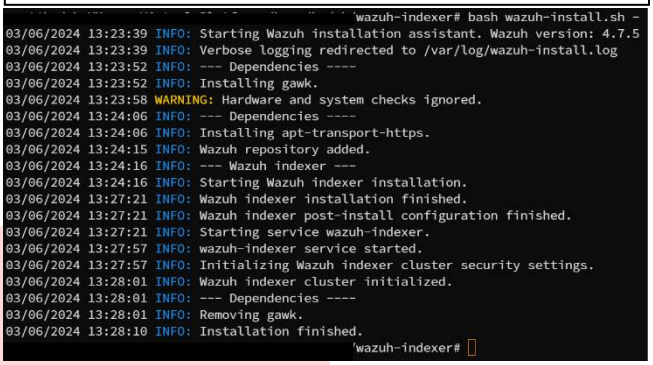
Perintah diatas akan men-*download* file instalasi pada website wazuh. selanjutnya jalankan file instalasi yang telah di-*download* sebelumnya, dengan menggunakan perintah dibawah.

```
bash wazuh-install.sh --wazuh-indexer node-1
```

```
bash wazuh-install.sh --wazuh-dashboard node-1
```

```
curl -sO https://packages.wazuh.com/4.7/config.yml
```

```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
```



GAMBAR 5
Proses instalasi wazuh indexer

G. Pengistalan Wazuh server

Wazuh server berfungsi untuk menganalisis data yang diterima dari semua agen yang terdaftar, hasil analisa data tersebut dapat dijadikan pemicu peringatan ketika suatu peristiwa yang bertentangan aturan. Untuk pengistalan *wazuh server* lakukan pada *direktori wazuh server* yang sebelumnya di buat, dan pastikan *file wazuh-install-file.jar* ada pada *direktori* tersebut. Selanjutnya *download* file instalasi yang dibutuhkan dalam mengistal *wazuh server* dengan perintah seperti berikut.

Perintah diatas akan men-*download* file instalasi pada website wazuh. selanjutnya jalankan file instalasi yang telah di-*download* sebelumnya, dengan menggunakan perintah dibawah.

```
bash wazuh-install.sh --wazuh-server node-1
```

GAMBAR 6
Proses instalasi wazih server

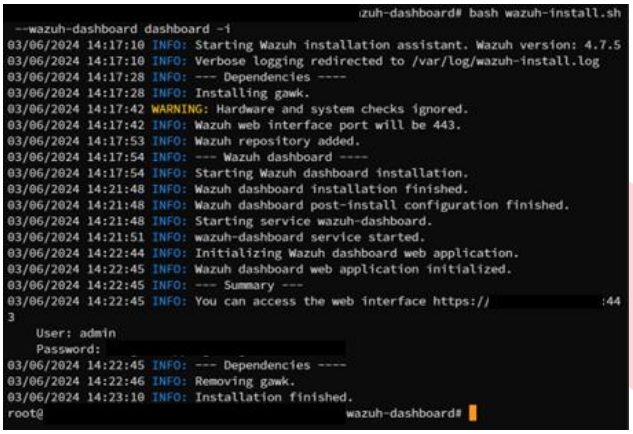
H. Pengistalan wazuh dashboard

Wazuh Dashboard berfungsi sebagai antarmuka web untuk visualisasi dan analisis data yang digunakan oleh *user wazuh* dalam menganalisa data yang diolah oleh wazuh. Untuk pengistalan *wazuh dashboard* lakukan pada *direktori wazuh dashboard* yang sebelumnya di buat, dan pastikan *file*

wazuh-install-file.jar ada pada *direktori* tersebut. Selanjutnya *download* file instalasi yang dibutuhkan dalam mengistal *wazuh dashboard* dengan perintah seperti berikut.

```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
```

Perintah diatas akan men-*download* file instalasi pada website wazuh. selanjutnya jalankan file instalasi yang telah di-*download* sebelumnya, dengan menggunakan perintah dibawah.



GAMBAR 7
Proses instalasi wazuh dashboard

I. Ubah user password

Sebelum mengakses wazuh, sebelumnya perlu melakukan pengubahan user dan password yang diperlukan untuk mengakses wazuh.pertama *download file wazuh-passwords-tool.sh* dengan perintah seperti berikut.

```
curl -so wazuh-passwords-tool.sh
https://packages.wazuh.com/4.7/wazuh-passwords-
tool.sh
```

Lalu jalankan *file wazuh-passwords-tool.sh* dengan perintah sepeti berikut. dengan opsi -u untuk *user* dan -p untuk *password.*

```
bash wazuh-passwords-tool.sh -u admin -p (password)
```

J. Penambahan agen wazuh

Agen wazuh merupakan server yang akan mengirimkan berbagi data kepada wazuh manager, data tersebut akan di amati dan di kumpulkan oleh wazuh manager. Penambahan agen wazuh dapat dilakukan pada berbagai os seperti Linux, Windows, macOS, Solaris, AIX dan lainya. untuk penambahan agen wazuh pada linux jalankan perintah seperti dibawah.

```
wget
https://packages.wazuh.com/4.x/apt/pool/main/w/wazu
h-agent/wazuh-agent_4.7.4-1_amd64.deb && sudo
WAZUH_MANAGER='(ip_wazuh_manager)'
WAZUH_AGENT_GROUP='(agent_group)'
WAZUH_AGENT_NAME='(agent_name)' dpkg -i
./wazuh-agent_4.7.4-1_amd64.deb
```

Perintah diatas akan mengistal *packages* yang dibutuhkan oleh agen wazuh pada website wazuh. lalu akan meng-*konfigurasi* berbagai kebutuhan agen wazuh seperti *IP wazuh manager, agen group dan agent name.*

H. Mengaktifkan Fitur Vulnerability Test

Secara default fitur vulnerability test pada wazuh tidak aktif, karna itu perlu mengaktifkan fitur vulnerability test pada wazuh secara manual. Konfigurasi vulnerability test harus dilakukan pada server wazuh manager dan server wazuh agen. Untuk konfigurasi vulnerability test pada server wazuh manager berada pada file ossec.conf yang berada pada direktori "/var/ossec/etc/" lalu pada tag "system inventory" ubah menjadi seperi berikut.

GAMBAR 8
Ossec file agent wazuh

Ada beberapa hal yang perlu diperhatikan dalam konfigurasi tersebut. Pertama ada "interval" yang menyatakan seberapa seringa vulnerability test akan dilakukan. Lalu ada "scan_on_start" yang menyatakan scan akan dilakukan setelah agen wazuh dijalankan. Setelah itu lakukan konfigurasi pada file "ossec.conf" pada server wazuh manager yang berada pada direktory "/var/ossec/etc/" pada tag "sca, vulnerability-detector dan debian os vulnerability"seperti dibawah.

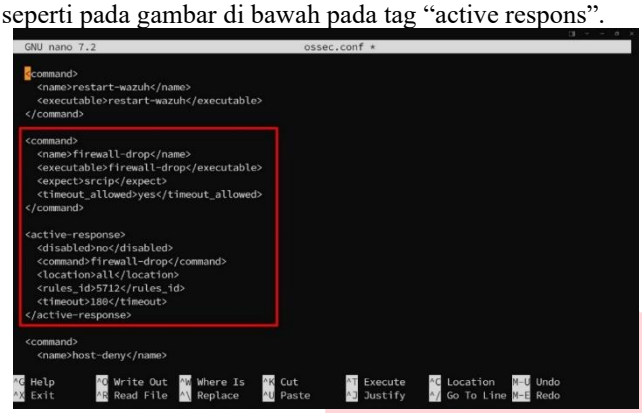
GAMBAR 9
Ossec file wazuh manager

I. Menambahkan Active Respons Untuk Mengatasi Brute Force SSH

active respons dalam wazuh befungsi sebagai tindakan yang akan diambil ketika terjadi kejadian dengan ide rule tertentu. Kali ini penulis akan membuat active response untuk mengatasi serangan brute force SSH.

active respons ini di buat untuk memblokir IP sementara penyerang yang melakukan brute force SSH. Pemblokiran IP

sementara ini dinilai efektif dalam mengatasi brute force SSH, karena dengan memblokir sementara IP penyerang akan membatasi penyerangan yang dilakukan. Penambahan active respons ini di lakukan pada server wazuh manager pada file ossec.conf yang berada pada direktori "/var/ossec/etc/" dengan menambahkan beberapa perintah seperti pada gambar di bawah pada tag "active respons".



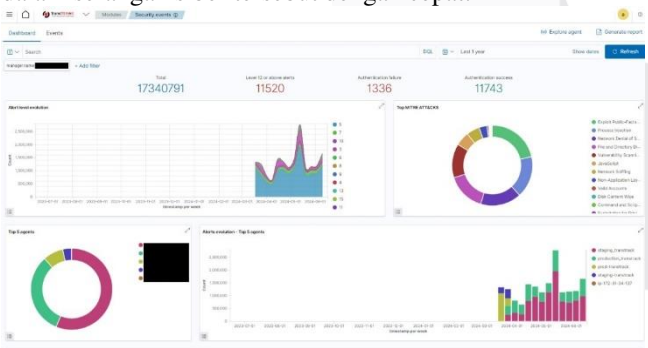
GAMBAR 10
Active respons brute force SSH

IV. HASIL DAN PEMBAHASAN

Wazuh adalah sebuah platform open-source yang berfungsi sebagai sistem deteksi intrusi (IDS), manajemen keamanan, dan monitoring. dengan wazuh memungkinkan kita untuk memonitoring seluruh aktifitas seluruh server yang dapat meningkatkan kemanan infrastruktur IT. Berikut hasil dari implementasi wazuh di TransTrack.

A. Security Log Analysis

Security Log Analysis menggunakan aplikasi open source Wazuh ini akan mengumpulkan, mengagregasi, mengindeks, dan menganalisis data keamanan, membantu seorang security admin mendeteksi intrusi, ancaman, dan anomali perilaku. karena serangan siber ini sekarang cukup bervariatif dan cepat, karna itu penting untuk mengamankan infrastruktur IT dalam serangan siber tersebut dengan cepat.

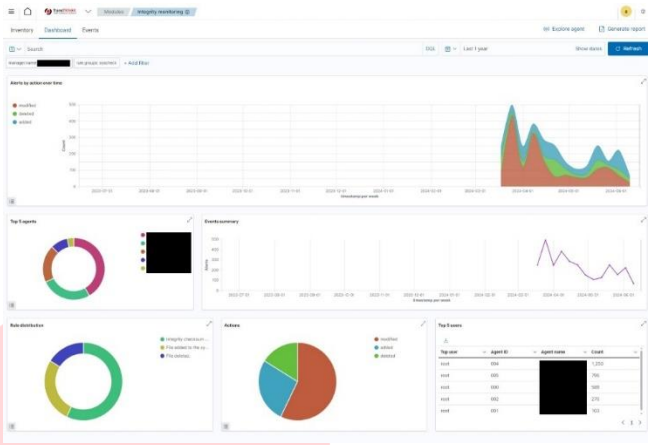


GAMBAR 11
Security Log Analysis

Pada gambar diatas merupakan modules wazuh yang menampilkan security logs analisis. Pada modules tersebut dapat dilihat beberapa aktifitas yang mencurigakan, tindakan wazuh dalam mengatasi serangan dan authentication failure dan authentication success. Dari data tersebut dapat dimanfaatkan oleh admin security untuk tindakan cepat terhadap aktifitas yang mencurigakan.

B. File Integrity Monitoring

Wazuh akan memantau file sistem dengan mengidentifikasi perubahan konten, user access, dan atribut file. Dan juga secara realtime mengidentifikasi pengguna dan aplikasi yang digunakan untuk membuat atau memodifikasi file.



GAMBAR 12
File integrity monitoring

File Integrity Monitoring ini dapat menganalisis setiap perubahan file yang terjadi pada server secara realtime. File Integrity Monitoring dapat digunakan untuk mengidentifikasi ancaman atau host yang disusupi. Dengan ini dapat diketahui kerusakan yang diakibatkan dari serangan siber yang terjadi dan dapat segera mungkin mengamankan file tersebut.

C. Vulnerability Detection

Wazuh akan menarik beberapa data perangkat lunak atau aplikasi dan mengirimkan informasi ini, informasi tersebut akan dikorelasikan dengan basis data CVE (Common Vulnerabilities and Exposure) dengan sumber yang sebelumnya telah diatur dan akan terus diperbarui, penkorelasian tersebut bertujuan untuk menilai dan mengindentifikasi suatu kerentanan yang ada. Penilaian kerentanan otomatis ini bertujuan untuk mencari titik lemah dalam aset yang dianggap penting dan dapat mengambil tindakan cepat sebelum penyerang mengeksploitasinya.

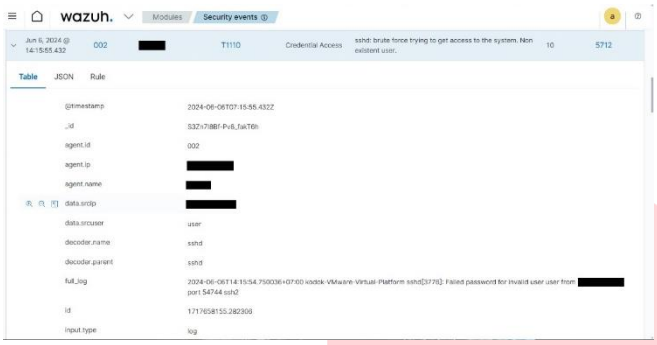
GAMBAR 13
Vulnerability detection

Pada gambar diatas menampilkan wazuh yang melakukan vulnerability detection, hasil yang akan ditampilkan berupa jumlah vulnerability yang terdeteksi dan detail dari vulnerability yang berhasil terdekteksi.

D. Wazuh mengatasi brute force SSH dengan active respons

Active respons pada wazuh merupakan tindakan cepat yang dilkukan wazuh ketika mendapati aktifitas yang mencurigakan. *Active respons* kali ini akan mem-*blokir* akses dari IP yang melakukan percobaan *login* SSH secara tidak wajar (*brute force ssh).*

ketika wazuh mendeteksi *brute force SSH* pada *security event* akan terdapat log seperti dibawah yang mendeteksi *brute force SSH* dengan *id rule 5712.*



GAMBAR 14
Active respons brute force SSH

Setelah wazuh mendeteksi brute force SSH, dengan active respons yang telah dibuat wazuh akan memblokir IP dari penyerang sementara waktu. Ketika active respons tersebut aktif akan menambahkan log pada security events pada wazuh seperti gambar dibawah.

GAMBAR 15
Log Active respons

V. KESIMPULAN

Implementasi intrusion detection system dalam upaya pencegahan cyber attack ini bertujuan untuk mempersingkat proses kerja tim DevOps pada alur maintenance yang sebelumnya monitoring server, vulnerability test , dan memperbaiki keamanan suatu server yang sebelumnya dilakukan secara manual setiap bulannya. Implementasi intrusion detection system dalam upaya pencegahan cyber attack ini betujuan agar mempermudah monitoring server karena semua server dapat dimonitoring dalam satu web site, vulnerability test berjalan secara otomatis, dan perbaikan kemanan suatu server dapat berjalan secara otomatis.

implementasi intruksion detection system ini menggunakan platform open yaitu wazuh. proses mplementasi wazuh sebagai intruksion detection system ini melewati beberapa proses dengan tujuan agar wazuh ini dapat berfungsi pada semestinya yaitu membatu proses tim DevOps dalam proses maintenance server.

REFERENSI

[1] “Jenis-Jenis Serangan Siber di Era Digital,” bpptik kominfo, 15 5 2023. [Online]. Available: https://bpptik.kominfo.go.id/Publikasi/detail/jenis-jenis-serangan-siber-di-era-digital. [Diakses 12 5 2024].

[2] “Serangan Siber, Perbankan Rugi Ratusan Miliar,” [Online]. Available: https://kompas100.kompas.id/berita-ekonomi/serangan-siber-perbankan-rugi-ratusan-miliar/. [Diakses 12 5 2024].

[3] M. D. Pratama, F. Nova dan D. Prayama, “Wazuh sebagai Log Event Management dan Deteksi Celah,” Jurnal Ilmiah Teknologi Sistem Informasi (Jitsi), vol. 3, pp. 1-7, 2022.

[4] “Architecture,” Wazuh Inc., 2024. [Online]. Available: https://documentation.wazuh.com/current/getting-started/architecture.html#architecture. [Diakses 16 5 2024].

[5] “Required ports,” Wazuh Inc., 2024. [Online]. Available: https://documentation.wazuh.com/current/getting-started/architecture.html#required-ports. [Diakses 16 5 2024].

[6] “Requirements Hardware,” Wazuh Inc,, 2024. [Online]. Available: https://documentation.wazuh.com/current/quickstart.html#hardware. [Diakses 16 5 2024].

[7] H. Khotimah, F. Bimantoro, R. S. Kabanga dan I. B. K. Widiartha, “IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) PADA APLIKASI SMS CENTER PEMERINTAH DAERAH PROVINSI NUSA TENGGARA BARAT,” JBegaTI, vol. 3, pp. 1-7, 2022.

[8] A. Shafiyyah, G. F. Nama dan R. A. Pradipta, “IMPLEMENTASI WAZUH MENGGUNAKAN METODE PPDIOO DI SISTEM KEAMANAN JARINGAN PSDKU UNIVERSITAS LAMPUNG WAYKANAN SEBAGAI DETEKSI DAN RESPON SERANGAN SIBER,” JITET (Jurnal Informatika dan Teknik Elektro Terapan) , vol. 12, pp. 970-982, 2024.