Vol 3 (2022) No 1

Jitsi Jurnal Ilmiah Teknologi Sistem Informasi

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

Deteksi Ancaman Keamanan Pada Server dan Jaringan Menggunakan OSSEC

Yarmis Yuliana[#], Hanriyawan Adnan Mooduto[#], Ronal Hadi [#]

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

ABSTRACTS

Cyber crimes can attack computer networks, infiltrate the network, retrieve confidential data and paralyze computer network systems. In overcoming the crimes that will occur, a system equipped with a firewall and an Intrusion Detection System (IDS) is needed. Firewall and IDS as network security features that can protect servers, networks, and block attacks. Firewall and IDS features can be implemented in OSSEC Tools. OSSEC is an open-source host-based intrusion detection system (HIDS) capable of performing log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerts, and active responses. OSSEC is capable of monitoring a single server or thousands of servers in server/agent mode.

KATA KUNCI

OSSEC,
Open Source,
HIDS,
Server

ABSTRAK

Kejahatan cyber dapat menyerang jaringan komputer, menyusup kedalam jaringan mengambil data-data rahasia dan melumpuhkan sistem jaringan komputer. Dalam mengatasi kejahatan yang akan terjadi, dibutuhkan sistem yang dilengkapi firewall dan Intrusion Detection System (IDS). Firewall dan IDS sebagai fitur keamanan jaringan yang dapat melindungi server, jaringan, dan memblok serangan. Fitur firewall dan IDS dapat diterapkan dalam Tools OSSEC. OSSEC merupakan IDS berbasis open-source (host-based intrusion detection system/HIDS) yang mampu melakukan analisis log, pengecekan integritas, pemantauan registri Windows, deteksi rootkit, peringatan berbasis waktu, dan respons aktif. OSSEC mampu memantau satu server atau ribuan server dalam mode server/agent.

1. PENDAHULUAN

Dewasa ini, dengan adanya internet membuat komunikasi dan informasi sangat mudah didapatkan. Kemudahan ini menyebabkan terjadinya kejahatan di dunia maya. Kejahatan cyber dapat menyerang jaringan komputer, menyusup kedalam jaringan mengambil data-data rahasia dan melumpuhkan sistem jaringan komputer. Dalam mengatasi kejahatan yang akan terjadi, dibutuhkan sistem yang dilengkapi firewall dan Intrusion Detection System (IDS). Firewall dan IDS sebagai fitur keamanan jaringan yang dapat melindungi server, jaringan, dan memblok serangan. Fitur firewall dan IDS dapat diterapkan dalam Tools OSSEC. OSSEC merupakan IDS berbasis open-source (host-based intrusion detection system/HIDS) yang mampu melakukan analisis log, pengecekan integritas, pemantauan registri Windows, deteksi rootkit, peringatan berbasis waktu, dan respons aktif. OSSEC mampu memantau satu server atau ribuan server dalam mode server/agent.

Dari tahun ke tahun, jumlah serangan siber di Indonesia terus mengalami peningkatan. Berdasarkan data Badan Siber dan Sandi Negara (BSSN) periode Januari- Mei 2021, jumlah kasus serangan siber di Indonesia mencapai 448 juta kasus. Kepala BSSN, Hinsa Siburian mengungkapkan bahwa tingginya tingkat pemanfaatan teknologi informasi komunikasi berbanding lurus dengan risiko dan ancaman keamanan. Malware menjadi bentuk serangan siber yang paling banyak terjadi di Indonesia. Lalu, diikuti dengan serangan aktivitas Trojan,

serta inforamsi leak atau kebocoran informasi. Total kasus serangan pada Mei 2021 mencapai 177 juta kasus. Adapun, jumlah tersebut naik cukup signifikan dari bulan sebelumnya, yakni April, sebanyak 115 juta kasus. Menurut Hinsa, tingginya serangan siber di Indonesia turut mempengaruhi peningkatan implementasi layanan pemerintah berbasis elektronik. Salah satu kasus serangan siber yang baru-baru ini menarik perhatian publik, yakni kebocoran data pribadi dari server BPJS Kesehatan.[1].

2. METODOLOGI PENELITIAN

OSSEC adalah HIDS open source yang dikembangkan oleh Daniel B. Cid yang menjual proyek ke Trend Micro pada tahun 2008 tetapi proyek tersebut terus berlanjut gratis dan sumber terbuka. Rilis stabil saat ini adalah 2.9.3. Terdiri dari banyak layanan dan modul yang masing-masing menyediakan fitur uniknya sendiri dalam hal Deteksi gangguan. HIDS memiliki banyak aspek dan OSSEC menggabungkan semuanya yang di pengembalian memberikan beberapa manfaat mendasar seperti:

1. Manfaat: OSSEC memenuhi persyaratan kepatuhan keamanan, Ini multi platform dan fleksibel, OSSEC menyediakan pemantauan dan peringatan waktu nyata, terintegrasi dengan banyak alat untuk memberikan fungsionalitas tambahan, dapat dikelola secara terpusat yang memfasilitasi administrasi.
2. Fitur: OSSEC mampu memantau dan menganalisis log, OSSEC sering melakukan pemeriksaan Integritas file (Syscheck), OSSEC dapat mendeteksi perangkat lunak berbahaya seperti malware, OSSEC dapat dikonfigurasi untuk secara aktif menanggapi aktivitas tertentu.[2].
3. Modul :

TABEL 1. Modul OSSEC

Modul	Keterangan
ossec-authd	Daemon yang menambahkan agen ke manajer
ossec-agentlessd	Daemon yang menangani komunikasi tanpa agen
ossec-analysisd	Daemon yang membuat peringatan dengan menganalisis log
ossec-csyslogd	Daemon yang meneruskan peringatan menggunakan syslog
ossec-dbd	Daemon yang menyimpan log peringatan dalam database yang dikonfigurasi
ossec-execd	Daemon yang menjalankan skrip respons aktif
ossec-maild	Daemon yang mengirimkan peringatan email
ossec-monitored	Daemon yang memantau konektivitas agen
ossec-remoted	Daemon yang menangani komunikasi agen
ossec-reportd	Daemon yang membuat log peringatan
ossec-syscheckd	Daemon yang memeriksa file untuk setiap perubahan
agent-auth	Alat yang digunakan dengan ossec-authd untuk menambahkan agen ke manajer
ossec-control	Alat untuk mengontrol semua layanan OSSEC
ossec-logcollector	Alat untuk mengumpulkan log tertentu
ossec-logtest	Alat untuk menguji log untuk membantu pemecahan masalah
ossec-makelists	Alat untuk mengkompilasi ulang yang sudah ketinggalan zaman
ossec-regex	Alat untuk membaca ekspresi regex
verify-agent-conf	Alat untuk memverifikasi file konfigurasi agen
clear_stats	Alat untuk menghapus statistik acara
list_agents	Alat untuk membuat daftar agen yang tersedia terhubung ke manajer
agent_control	Alat untuk mengontrol agen dan mendapatkan informasi mereka
manage_agents	Alat untuk mengelola kunci otentikasi agen
syscheck_control	Alat untuk mengelola database pemeriksaan integritas
syscheck_update	Alat untuk memperbarui database pemeriksaan integritas
rootcheck_control	Alat untuk mengelola database audit
util.sh	Alat untuk menambahkan file yang akan dipantau oleh ossec-logcollector

4. Rulest Classification
   Aturan ini digunakan oleh sistem untuk mendeteksi serangan, intrusi, penyalahgunaan perangkat lunak, masalah konfigurasi, kesalahan aplikasi, malware, rootkit, anomali sistem, atau pelanggaran kebijakan keamanan. OSSEC menyediakan seperangkat aturan out-of-the-box yang diperbarui dan diperluas, untuk meningkatkan kemampuan pendeteksiannya. Aturan diklasifikasikan dalam beberapa level, dari yang terendah (0) hingga maksimum (16). Beberapa level tidak digunakan saat ini. Tabel berikut menjelaskan masing-masing, yang dapat berguna untuk memahami tingkat keparahan setiap lansiran yang dipicu atau membuat aturan khusus.[9] :

TABEL 2. Rulest Classification

Tingkat	Judul	Keterangan
0	Diabaikan	Tidak ada tindakan yang diambil. Digunakan untuk menghindari positif palsu. Aturan-aturan ini dipindai sebelum yang lainnya. Termasuk acara tanpa relevansi keamanan.
2	Pemberitahuan prioritas rendah sistem	Pemberitahuan sistem atau pesan status. Mereka tidak memiliki relevansi keamanan
3	Acara yang berhasil/Diotorisasi	Termasuk upaya login yang berhasil, firewall mengizinkan acara, dll.
4	Kesalahan prioritas rendah sistem	Kesalahan terkait dengan konfigurasi yang buruk atau perangkat/aplikasi yang tidak digunakan. Hal yang tidak memiliki relevansi keamanan dan biasanya disebabkan oleh instalasi default atau pengujian perangkat lunak
5	Kesalahan yang dibuat pengguna	Termasuk kata sandi yang tidak terjawab, tindakan yang ditolak, dll. Dengan sendirinya mereka tidak memiliki relevansi keamanan.
6	Serangan relevansi rendah	Hal yang menunjukkan worm atau virus yang tidak mempengaruhi sistem (seperti kode merah untuk server apache, dll). Mereka juga termasuk events IDS dan sering terjadi kesalahan.
7	Pencocokan "kata buruk"	Hal itu termasuk kata-kata seperti "buruk", "kesalahan", dll. Peristiwa ini sebagian besar waktu tidak diklasifikasikan dan mungkin memiliki beberapa relevansi keamanan
8	Pertama kali dilihat	Sertakan events yang pertama kali dilihat. Pertama kali peristiwa IDS dipicu atau pertama kali pengguna masuk. Ini juga mencakup tindakan yang relevan dengan keamanan (seperti memulai sniffer atau semacamnya).
9	Kesalahan dari sumber yang tidak valid	Sertakan upaya untuk masuk sebagai pengguna yang tidak dikenal atau dari sumber yang tidak valid. Mungkin memiliki relevansi keamanan (khususnya jika diulang). Mereka juga menyertakan kesalahan terkait akun "admin" (root).
10	Beberapa kesalahan yang dibuat pengguna	Hal itu termasuk beberapa kata sandi yang buruk, beberapa login yang gagal, dll. Mereka mungkin menunjukkan serangan atau mungkin saja pengguna lupa kredensialnya
11	Peringatan pemeriksaan integritas	Hal itu termasuk pesan mengenai modifikasi binari atau keberadaan rootkit (oleh Rootcheck). Hal itu mungkin menunjukkan serangan yang berhasil. Juga termasuk event IDS yang akan diabaikan (jumlah pengulangan yang tinggi).
12	Event yang sangat penting	Hal itu termasuk pesan kesalahan atau peringatan dari sistem, kernel, dll. Mereka mungkin menunjukkan serangan terhadap aplikasi tertentu.
13	Kesalahan yang tidak biasa (sangat penting)	Sebagian besar waktu itu cocok dengan pola serangan umum.
14	Acara keamanan yang sangat penting	Sebagian besar waktu dilakukan dengan korelasi dan itu menunjukkan serangan.
15	Serangan parah	Tidak ada kemungkinan positif palsu. Perhatian segera diperlukan.

Dalam pembangunan server OSSEC untuk deteksi ancaman keamanan pada server dan jaringan perlu dipersiapkan sebuah rancangan topologi. Topologi ini nantinya akan menjelaskan gambaran fisik dari sistem yang akan dibangun. Gambar 1 di bawah ini merupakan topologi yang akan digunakan dalam membangun deteksi ancaman keamanan menggunakan OSSEC sehingga lebih mudah dipahami.

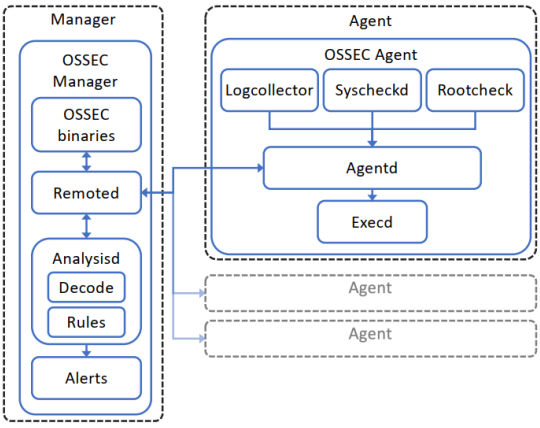
GAMBAR 1. Tapologi Sistem

TABEL 3. Sistem Operasi dan Software yang digunakan

Nama	Versi	Fungsi
Ubuntu Server	20.04 LTS	OSSEC *Manager*
Ubuntu Server	20.04 LTS	OSSEC *Agent*
RedHat Server	8	OSSEC *Agent*
Ubuntu Server	20.04 LTS	Penyerang
OSSEC Manager	3.6.0	Aplikasi *Network* Monitoring
OSSEC Agent	3.6.0	*Agent* yang akan dimonitoring oleh OSSEC *manager*
OSSEC-WUI	0.8	*Web-Based Monitoring OSSEC*

Dalam rancangan yang akan dibangun, server yang digunakan sebagai server OSSEC manager menggunakan sistem operasi Ubuntu 20.04. mulanya, AWS akan memberikan IP public yang akan berganti secara berkala pada masing-masing server yang telah dibangun di EC2. Jaringan cloud computing yang terhubung dengan server OSSEC akan memperoleh IP address yang nantinya akan digunakan pada saat melakukan konfigurasi dan remote access untuk instalasi server OSSEC. Saat melakukan konfigurasi akan dilakukan remote ssh melalui aplikasi Putty dengan menggunakan IP address yang telah diberikan secara otomatis oleh AWS.

Pada server OSSEC manager juga akan dilakukan instalasi OSSEC web UI yang akan berguna sebagai web interface user antara OSSEC manager dan OSSEC agent. Untuk mengakses OSSEC manager ini pada web interface di browser nantinya akan menggunakan IP Public dengan alamat http://ip-addres/ossec-wui/ IP yang digunakan ialah IP milik server OSSEC manager yang didapatkan secara otomatis dari AWS. Untuk konfigurasi OSSEC agent dilakukan pada server RedHat 8 dan Ubuntu 20.04. Konfigurasi dilakukan melalui remote ssh dengan aplikasi Putty. Setiap OSSEC agent akan didaftarkan ke OSSEC manager untuk dilakukan monitoring dan deteksi keamanan pada OSSEC agent. Sehingga nantinya informasi yang didapatkan dari client akan mudah dilihat pada OSSEC manager melalui OSSEC WUI. OSSEC agent Ubuntu akan diinstalkan rootkit untuk uji coba pendeteksiannya. Notifikasi alert akan dikirim ke Ossec Web UI serta ke Gmail. Selanjutnya untuk server penyerang menggunakan sistem operasi ubuntu 20.04 yang akan diinstalkan hping3 untuk melakukan serangan ke OSSEC agent, kemudian OSSEC agent akan memberi tahu kepada OSSEC manager lalu OSSEC manager mengirim alert ke OSSEC WUI serta notifikasi ke Gmail.



GAMBAR 2. Diagram Sistem

Penyebaran OSSEC dasar terdiri dari serangkaian layanan yang berjalan di agent, yang terus-menerus mengumpulkan log yang disimpan secara lokal dan dikirim ke manager. Dekoder yang telah ditentukan sebelumnya dan aturan yang dikonfigurasi diperiksa terhadap semua log agent menurut pengaturan yang ditentukan maka suatu tindakan akan diterapkan. Pada gambar 3.3 di atas mengilustrasikan blok fungsional penyebaran OSSEC di manager (dengan OSSEC manager dalam satu atau beberapa agent) dengan OSSEC agent. OSSEC manager ditempatkan di manager dan berisi OSSEC binaries yang mewakili file biner dari layanan OSSEC manager. Remoted membuat koneksi dengan setiap agent untuk menerima lognya atau mengirim tindakan.

Ketika Log agent diterima oleh Remoted, log diterjemahkan dalam blok Decode serta mencocokkan Rules dalam blok Rules, Analysisd memberi sinyal peristiwa ke Alert dan mengirimkan tindakan yang telah ditentukan sebelumnya ke Remoted. OSSEC agent yang ditempatkan di setiap Agen memahami Logcollector, Syscheckd dan Blok rootcheckd, yang memiliki fungsi memperoleh log dan melakukan analisis keamanan yang lebih dalam pada sistem lokal. Ketiga blok ini mengirimkan log mereka ke agentd, yang pada gilirannya, mengirimkan data ke manager OSSEC. Jika Manajer OSSEC memiliki tindakan yang dikonfigurasi untuk log tertentu, Agentd menerima instruksi dan mengeksekusi tindakan menggunakan Execd.

3. HASIL DAN PEMBAHASAN

Adapun langkah-langkah yang dilakukan dalam penelitian ini adalah:

1. Membangun server cloud computing di AWS.
2. Melakukan instalasi sistem operasi Ubuntu 20.04 dan RedHat 8 pada AWS.
3. Melakukan instalasi dan konfigurasi server OSSEC manager pada OS Ubuntu 20.04 yang sudah di-install sebelumnya.
4. Melakukan instalasi OSSEC-WUI pada OSSEC manager
5. Melakukan instalasi OSSEC agent pada server Ubuntu 20.04 dan RedHat 8.
6. Melakukan konfigurasi OSSEC agent agar terdaftar pada server OSSEC manager.
7. Melakukan percobaan serangan pada OSSEC agent

Log in pada akun AWS yang sudah dimiliki, kemudian siapkan server yang dibutuhkan menggunakan EC2 Instance. EC2 (Elastic Computer Cloud) merupakan salah satu service yang tersedia di Amazon Web Service. Server yang telah di-install sebelumnya, salah satunya digunakan sebagai server OSSEC, dan yang lainnya digunakan sebagai OSSEC agent serta penyerang. Langkah pertama yang harus dilakukan instalasi OS dengan melakukan remote SSH ke instance dengan menggunakan aplikasi Putty dengan cara memasukkan IP Public dan private key yang sudah dirubah sebelumnya.

Setelah itu, unduh kode source OSSEC terbaru yaitu 3.6.0 versi rilis stabil terbaru pada saat ini dengan perintah:

```
#wget https://github.com/ossec/ossec- hids/archive/3.6.0.tar.gz
```

Kemudian ekstrak OSSEC yang telah diunduh tadi untuk dilakukan proses instalasi. Untuk instalasi OSSEC-WUI pada OSSES Manager, Masuk ke direktori /tmp untuk menginstall OSSEC-WUI dengan perintah

```
#git clone https://github.com/ossec/ossec-wui.git
```

Lakukan instalasi pada tiga server yang sudah dibangun di AWS sebelumnya. Agar agent bisa berkomunikasi dengan manager maka agent harus ditambahkan ke server OSSEC. Buka OSSEC manager lalu ketikkan perintah:

```
/var/ossec/bin/manage_agents
```

kemudian pilih A menambahkan agent. Masukkan nama, ip address, dan id dari agent lalu konfirmasi dengan mengetikkan y dan enter.

Pengumpulan data log adalah proses real-time untuk memahami catatan yang dihasilkan oleh server atau perangkat. Komponen ini dapat menerima log melalui file teks atau log peristiwa. Untuk mengaktifkan log data collection pada OSSEC, harus dilakukan konfigurasi pada OSSEC manager atau OSSE agent. Masuk ke /var/ossec/etc/ossec.conf. Lalu tambahkan lokasi log yang ingin di monitoring. Setelah ditambahkan pastikan untuk merestart kembali OSSEC manager. Untuk masuk ke file konfigurasi OSSEC manager, jalankan perintah berikut:

```
#nano /var/ossec/etc/ossec.conf
```

Sistem File Integriry Monitoring (FIM) pada OSSEC mengawasi file yang dipilih dan memicu peringatan ketika file-file ini dimodifikasi. Komponen yang bertanggung jawab untuk tugas ini disebut syscheck. Modul FIM terletak di agent OSSEC. Modul mencari modifikasi dengan membandingkan checksum file baru dengan checksum lama. Semua perubahan yang terdeteksi dilaporkan ke manager OSSEC. Untuk konfigurasi FIM, masuk ke file konfigurasi ossec.conf. Tentukan direktori mana yang ingin dilakukan monitoring. Kemudian aktifkan FIM.

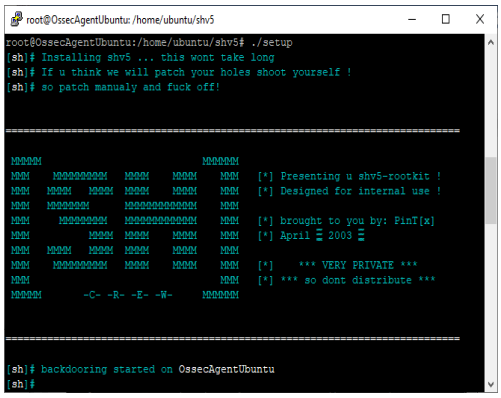
Untuk notifikasi e-mail, disini saya menggunakan layanan dari SMTP dari g-mail. Langkah pertama yang harus dilakukan adalah masuk ke pengaturan e-mail yang digunakan, lalu aktifkan verifikasi dua langkah. Selanjutnya, aktifkan sandi aplikasi pada e-mail, beri nama Postfix serta simpan password yang ditampilkan. Lakukan instalasi Postfix pada OSSEC manager agar server SMTP dapat terkoneksi dengan OSSEC manager. perintahnya ialah

```
#sudo apt-get install libsasl2-modules postfix
```

Pengujian dilakukan untuk hal-hal yang telah dikonfigurasi sebelumnya menggunakan OSSEC manager dan OSSEC agent yang dipasang pada server Ubuntu dan RedHat pastikan seluruh agent sudah aktif dan status OSSEC agent pada masing- masing server dalam kondisi running. Berikut ini hal-hal yang akan diujikan pada sistem ini, yaitu:

1. Koneksi antara OSSEC manager dan OSSEC agent
2. Koneksi antara OSSEC manager dan OSSEC agent pada OSSEC-WUI
3. Pengujian Log Data Collection pada OSSEC agent seperti web server
4. Pengujian File Integrity Monitoring pada OSSEC agent
5. Pengujian notifikasi alert melalui e-mail
6. Pengujian deteksi Rootkit pada OSSEC agent
7. Pengujian deteksi attack pada OSSEC agent

GAMBAR 3. DDoS-Ripper



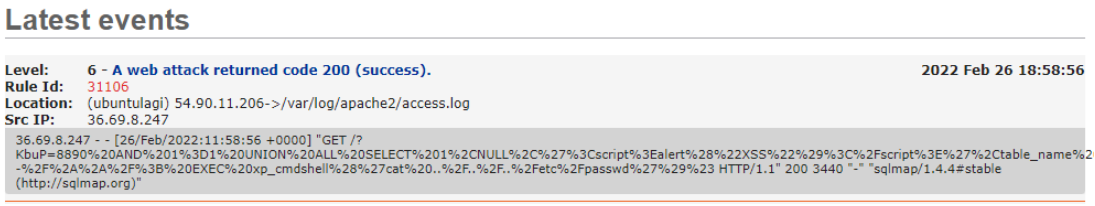
GAMBAR 4. Rootkit

Berdasarkan hasil pengujian yang diperoleh dari deteksi ancaman keamanan server dan jaringan menggunakan OSSEC yang dibangun pada cloud computing AWS, server yang dibangun pada AWS adalah Ubuntu 20.04 LTS yang digunakan sebagai OSSEC manager sedangkan server untuk OSSEC agent menggunakan RedHat 8 dan Ubuntu 20.04 LTS. OSSEC manager diinstal pada server Ubuntu 20.04 LTS sekaligus menginstal OSSEC-WUI untuk mempermudah pemantauan dari OSSEC agent yang telah terkoneksi ke OSSEC manager. Jika server beroperasi dan jaringan internet stabil, maka informasi log akan dikirim secara real-time.

Seluruh aktivitas yang telah diujikan sebelumnya dapat diterima oleh user melalui notifikasi e-mail. Pada OSSEC manager diinstal Postfix yang berfungsi untuk manajemen e-mail dan dengan menggunakan SMPT server dari g-mail. Event atau alert dari masing-masing agent akan diperoleh melalui notifikasi e-mail. Jika user hanya menginginkan notifikasi untuk hal-hal yang bersifat penting, maka diatur level e-mail alert pada OSSEC manager. Serangan yang dilakukan pada OSSEC agent oleh server penyerang berhasil dideteksi oleh OSSEC manager yang kemudian mengirimkan alert ke OSSEC-WUI serta notifikasi g-mail sehingga admin dapat melihat dan megambil tindakan lebih lanjut. Dari hasil pengujian fungsionalitas server OSSEC yang dibangun pada AWS, server tersebut telah bekerja sebagaimana mestinya sesuai dengan rancangan. Hal ini dibuktikan dengan berjalannya semua fungsi pada OSSEC baik server maupun agent serta adanya laporan dan peringatan yang dikirim oleh server OSSEC terhadap serangan DDoS serta SQL Injection, server OSSEC juga bekerja dengan baik.

Hasil pengujian SQL Injection.

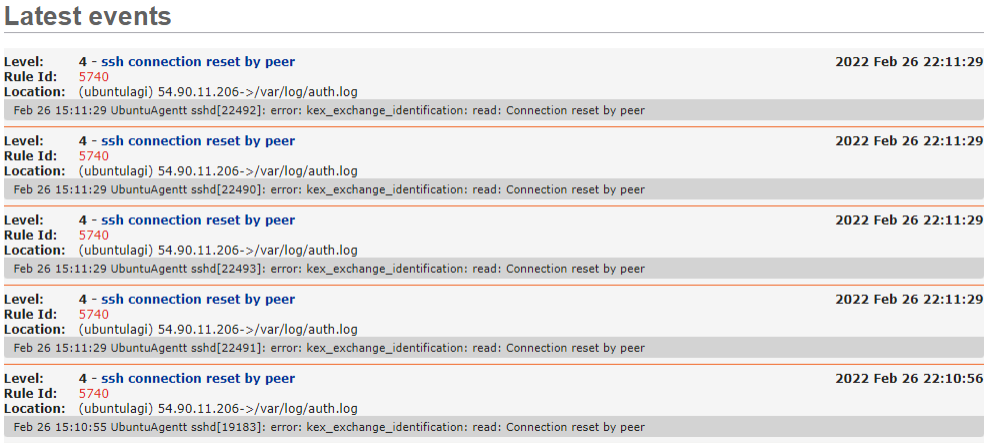
Setelah melakukan SQL Injection dari device lain menuju OSSEC agent, maka manager akan mendeteksi bahwa adanya serangan sehingga menampilkan alert seperti pada gambar



GAMBAR 5. Alert SQL Injection

Hasil pengujian DDoS Ripper pada port 22

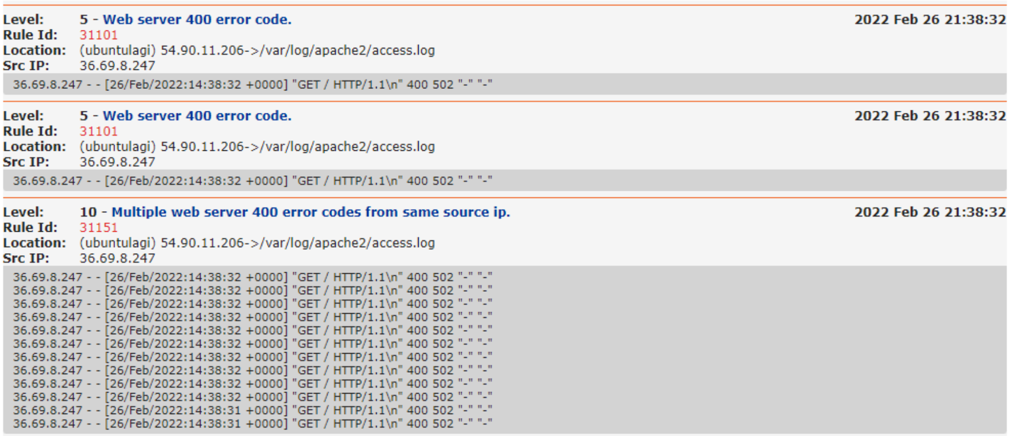
Pada gambar 6. merupakan alert saat melakukan penyerangan DDoS-Ripper dari server penyerang menuju port 22 SSH.



GAMBAR 6. Alert DDos-Ripper Port 22

Hasil pengujian DdoS Ripper pada port 80

Pada gambar 5 merupakan alert saat melakukan penyerangan DDoS-Ripper dari server penyerang menuju port 80 HTTP. Pada gambar di atas tertera ip sumber yang merupakan ip dari server penyerang.



GAMBAR 7. Alert DDos-Ripper Port 80

4. KESIMPULAN

OSSEC manager akan memonitoring setiap agent yang terdaftar pada OSSEC manager. Pada pengujian fungsionalitas OSSEC server, fungsi-fungsi yang ada berjalan sesuai dengan rancangan yang telah dibangun. File Integrity Monitoring merupakan hal-hal yang berhubungan dengan tindakan terhadap suatu file, mengubah isi file, serta menghapus file. Pada pengujian OSSEC server terhadap serangan, server mampu mendeteksi serangan yang muncul serta menampilkan alert kepada admin. Saat melakukan serangan, OSSEC server tidak selalu memberikan alert secara real-time karena disebabkan koneksi yang tidak stabil serta tempat pengimplementasian yang memang telah dijaga dari serangan DDoS. OSSEC server mampu mendeteksi serangan berbentuk rootkit jenis shv5 yang diinstalkan pada salah satu OSSEC agent. Alert dan event bisa diatur oleh admin yang melalui notifikasi e-mail dan OSSEC-WUI sesuai dengan kebutuhan dan informasi yang ingin diperoleh oleh admin..

REFERENSI

[1] P. Ananda, “Serangan Siber di RI Terus Meningkat, Capai 448 Juta Kasus.” https://mediaindonesia.com (accessed Oct. 28, 2021).

[2] A. Anafcheh, “Intrusion Detection with OSSEC,” 2018.

[3] M. Syani, “Analisis Dan Implementasi Network Security System Menggunakan Teknik Host-Based Intrusion Detection System (Hids) Berbasis Cloud Computing,” no. Selisik, 2019, doi: 10.31227/osf.io/6t7us.

[4] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, “Building an efficient intrusion detection system based on feature selection and ensemble classifier,” Comput. Networks, vol. 174, 2020, doi: 10.1016/j.comnet.2020.107247.

[5] D. Teixeira, L. Assunção, T. Pereira, S. Malta, and P. Pinto, “OSSEC IDS extension to improve log analysis and override false positive or negative detections,” J. Sens. Actuator Networks, vol. 8, no. 3, 2019, doi: 10.3390/jsan8030046.

[6] M. Syafrizal and U. A. Yogyakarta, Pengantar Jaringan Komputer. Penerbit Andi, 2020.

[7] M. A. Anas, Y. Soepriyanto, and S. Susilaningsih, “Pengembangan multimedia tutorial topologi jaringan untuk smk kelas x teknik komputer dan jaringan,” J. Kaji. Teknol. Pendidik., vol. 1, no. 4, pp. 307–314, 2019.

[8] A. Hadi, Administrasi Jaringan Komputer, 1st ed. Jakarta: Kencana Prenada Media Group, 2016.

[9] OSSEC, “Rules Classification.” https://www.ossec.net/docs/manual/rules- decoders/rule-levels.html (accessed Feb. 18, 2022).

[10] C. Zoho, “Server Monitoring Tools.” https://www.manageengine.com (accessed Oct. 27, 2021).

[11] M. Azmi, C. Foozy, K. Sukri, N. Abdullah, I. Hamid, & Hidra 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

[12] H. Malallah et al., "A Comprehensive Study of Kernel (Issues and Concepts) in Different Operating Systems," Asian J. Comput. Sci. Inf. Technol., vol. 8, pp. 16–31, 2021, doi: 10.9734/AJRCOS/2021/v8i330201.

[13] W. S. Bintara, "Pengertian Ubuntu, Definisi, Sejarah, Jenis, Kelebihan," 2021. https://dianisa.com/pengertian-ubuntu/ (accessed Dec. 23, 2021).

[14] A. Vardi, "Linux For Beginners: The Ultimate Guide To The Linux OperatingSystem & Linux Commands," 2016.

[15] T. Alam, "Cloud Computing and its role in the Information Technology," IAIC Trans. Sustain. Digit. Innov., vol. 1, pp. 108–115, 2021.

[16] A. W. S. Inc, "Komputasi Cloud dengan AWS," 2021. https://aws.amazon.com/id/what-is-aws/ (accessed Nov. 25, 2021)..