**Available online at JKTE Website :** http://journal.uta45jakarta.ac.id/index.php/JKTE

**JURNAL KAJIAN TEKNIK ELEKTRO**
**EISSN : 2502-8464**

# Implementasi Pendeteksian Serangan pada Server Menggunakan Opensource Crowdsec

*Parlindungan Tampubolon[1], silvia Agustina Wulan Sari[2], Panji Wijonarko[3], EE Lailatul Putri[4]*

*[1,2,3,4]Faculty of Engineering and Informatics Universitas 17 Agustus 1945 Jakarta, Jl Sunter Permai Raya, DKI Jakarta, Indonesia*

INFORMASI ARTIKEL

Received: June 19, 2023
Revised: July 25, 2023
Available online: August 29, 2023

CORRESPONDENCE

E-mail:

[1] *Parlindungan.tampubolon@uta45jakarta.ac.id*

**A B S T R A K**

*Server web* umumnya digunakan untuk keperluan aplikasi atau portal yang berkaitan dengan informasi perusahaan atau instansi tertentu. Informasi pada portal berbasis *web* sangat bermanfaat karena memudahkan akses langsung terkait instansi atau perusahaan tersebut. Namun, kemudahan akses ini sering dimanfaatkan oleh peretas untuk melakukan serangan, baik sebagai uji coba kemampuan IT mereka, dengan tujuan merusak, atau untuk mencuri data-data dari sistem yang telah dipublikasikan. Akibatnya, reputasi instansi tersebut dapat terancam, dan sistem keamanan yang telah dibangun dapat hancur total.

Dengan banyaknya alat *open-source* di internet, kita sebenarnya dapat memitigasi serangan-serangan tersebut, baik secara manual maupun otomatis. Peluncuran secara manual akan membuat *administrator* bekerja lebih keras karena harus memeriksa log satu per satu. Namun, jika kita mampu memaksimalkan penggunaan alat *open-source* yang ada di internet, kita dapat dengan mudah memblokir setiap akses yang mengarah pada serangan terhadap *server*, *seperti SQL Injection*, *Defacing*, *Brute Force*, atau serangan yang dapat dideteksi sebelumnya, sehingga setiap akses dan prosesnya dapat diblokir. Penulisan jurnal ini bertujuan untuk membahas proses bagaimana sebuah server diserang, bagaimana kita mengenali proses serangan tersebut, dan bagaimana melakukan pemblokiran secara otomatisKata

Kata kunci: : *server web*, serangan, Peretasan ,crodwsec,

**A B S T R A C T**

Web-related servers are usually used for application or portal needs related to information on certain companies or agencies. Information on the portal using the web is very useful because it will provide general convenience to get direct information related to the agency or company. However, this ease of access is widely used as a forum for attacks by hackers. Either as their test to try their IT skills, aiming to damage, or aiming to retrieve data on a system that has been published. Which results in the reputation of the agency will fall and make the security system that has been built can be completely damaged. With the existence of many open-source tools on the internet, we can mitigate these attacks, whether technically we do the rollout manually or automatically. Manual rollout will make sure that the administrator in charge will work harder because it requires checking the logs one by one. However, if we can maximize opensource tools on the internet, then we can easily block any access that leads to attacks on the server. such as SQL Injection, Defacing, Brute Force, or attacks that can be indicated in advance, so that every access and process can be blocked. Writing this journal, aims to discuss the process of how a server is attacked, and how we can recognize the attack process, and do the blocking automatically.

Keywords: webserver, attacks, Hacking, crodwsec

## I. PENDAHULUAN

Di era sekarang ini, penggunaan web begitu pesat. Informasi yang berkaitan dengan perusahaan, biodata, sekolah atau badan-badan tertentu, semua dapat disajikan dalam bentuk halaman web. Banyaknya tools dan framework yang dapat memberikan kemudahan, membuat orang lebih cepat dalam memberikan informasi kepada publik. Namun, kemudahan ini juga memiliki kekurangan. Framework website yang dapat digunakan dengan cepat, biasanya tidak sepenuhnya aman. Terutama yang gratis, karena proses keamanan perpustakaan di dalamnya biasanya tidak selalu diperbarui. Kelebihan produk berbayar dan tidak berbayar mungkin salah satunya adalah tanggung jawab dalam mengupdate aplikasi. Seperti yang kita ketahui, WordPress merupakan sebuah framework CMS yang sangat mudah untuk dapat menyajikan informasi dalam bentuk website. Keberadaan plugin juga dapat membuat tampilan kita menjadi lebih menarik, tanpa perlu mendalami atau memiliki kemampuan yang berhubungan dengan aplikasi CSS.

Berdasarkan data dari portal Sucuri yang dapat digunakan di WordPress itu sendiri, ditemukan bahwa 4,3% situs web WordPress yang dipindai dengan Site Check (pemindai

keamanan situs web yang populer) pada tahun 2022 telah diretas (terinfeksi). Itu berarti sekitar 1 dari setiap 25 situs web. Oleh karena itu, jika kita telah berhasil menerapkan aplikasi berbasis web, kita juga harus bisa memelihara sistem setelah itu. Masalahnya, proses pemeliharaan tersebut membutuhkan keahlian baik dari sisi aplikasi maupun server yang menjalankannya. System administrator adalah profesi dalam menjaga keamanan di tingkat sistem operasi. Oleh karena itu, kita juga harus bisa memahami lebih dalam bagaimana sistem operasi bekerja dan berintegrasi dengan aplikasi-aplikasi webnya. Jika kita hanya mengelola 1 atau 10 server, kita mungkin bisa memonitor setiap serangan secara manual. Namun, yang menjadi masalah adalah ketika kita diberikan tanggung jawab untuk mengelola server yang jumlahnya lebih dari 100. Oleh karena itu, dengan adanya aplikasi firewall yang mampu mendeteksi bentuk-bentuk serangan, maka akan dapat meminimalisir bentuk serangan tersebut, dan pada penelitian ini, penulis mencoba melakukan tindakan preventif dengan menggunakan tools crowdsec agar dapat mengenali bentuk-bentuk serangan terhadap aplikasi atau server, dan langsung memblokir alamat IP komputer yang mencoba melakukan penyerangan. Penelitian mengenai pendeteksian serangan hacking telah banyak dilakukan.[1] mengembangkan sistem deteksi intrusi menggunakan algoritma machine learning yang menunjukkan hasil akurasi tinggi dalam mengidentifikasi serangan.[2]memanfaatkan teknik honeypot untuk menangkap aktivitas berbahaya dan mempelajari pola serangan hacker. Sementara itu, penelitian oleh Jones dan Brown menyoroti pentingnya integrasi sistem deteksi serangan dengan firewall dan alat keamanan lainnya untuk respons yang lebih cepat.[3]

### 1.1 Maksud dan Tujuan

Maksud dan tujuan dari implementasi penggunaan crowdsec adalah

1. Mengetahui kinerja dari tools crowdsec, dalam mendeteksi serangan pada server
2. Menganalisis perbandingan kinerja tools crowdsec dan tools lainnya dalam mendeteksi serangan.
3. Mengetahui bagaimana kinerja server ketika dilakukan instalasi tools crowdsec

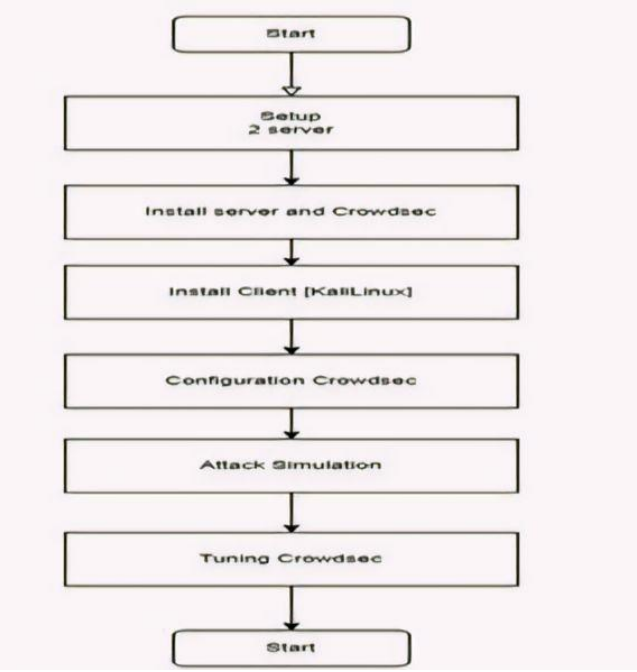
### 1.2 Metode Serangan

Berdasarkan data dari OWASP, sebuah organisasi nirlaba yang berfokus pada keamanan aplikasi web. Berikut adalah metode serangan yang sering dilakukan

1. Injeksi
   Serangan injeksi SQL biasanya terjadi ketika data yang tidak dipercaya dikirimkan ke penerjemah kode melalui formulir input atau cara lain untuk memasukkan data ke dalam situs web. Sebagai contoh, seorang peretas dapat memasukkan kode SQL ke dalam formulir yang sebenarnya hanya meminta data teks biasa. Jika formulir input ini tidak diamankan dengan benar, kode SQL tersebut dapat dieksekusi, sehingga memungkinkan peretas untuk melakukan tindakan berbahaya seperti mengambil data atau merusak basis data. Serangan semacam ini disebut dengan injeksi SQL, dan dapat dicegah dengan teknik seperti penggunaan prepared statements, validasi input yang ketat, dan hak akses minimal pada basis data. serta mencegah serangan injeksi SQL.[4] melakukan pemeriksaan statis terhadap query yang dihasilkan secara dinamis dalam aplikasi basis data.[5] mengembangkan AMNESIA, sebuah alat yang menganalisis dan memonitor serangan injeksi SQL. Selain itu, [6] mengevaluasi keamanan aplikasi web melalui injeksi kesalahan dan pemantauan perilaku
2. Kelemahan system otentikasi
   Kelemahan pada sistem login dapat memberikan peretas akses ke akun pengguna. Tidak hanya itu, mereka dapat mengendalikan seluruh sistem dengan meretas akun admin. Untuk mengurangi kelemahan autentikasi, Anda dapat menggunakan autentikasi 2-faktor (2FA) [7].
3. Data sensitif
   Jika sebuah situs web menyimpan data sensitif penggunanya, akan berbahaya jika mereka tidak menjaganya dengan aman. Untuk mengurangi kemungkinan pencurian data, Anda dapat mengenkripsi data sensitif. Pengembang juga harus memastikan bahwa situs web tidak menyimpan data sensitif yang sebenarnya tidak diperlukan.
4. Serangan XML
   Ini adalah serangan terhadap situs web dan aplikasi yang menganalisis input XML. Masukan ini dapat merujuk pada entitas eksternal untuk mengidentifikasi kelemahan dalam masukan XML. Entitas eksternal yang dimaksud di sini biasanya adalah unit penyimpanan, seperti hard drive. Menganalisis input XML dapat membuatnya terlihat seperti mengirim data ke entitas eksternal yang tidak dipercaya, di mana mereka dapat mengirim data sensitif langsung ke peretas [8].
5. Broken Access Control
   Kontrol akses pada poin ini mengacu pada sistem kontrol yang mengakses informasi dan fungsionalitas. Kontrol akses yang rusak memungkinkan penyerang untuk mem-bypass proses otorisasi dan melakukan hal-hal yang biasanya hanya dapat dilakukan oleh admin [9].
6. Kesalahan konfigurasi Keamanan
   Kesalahan konfigurasi keamanan adalah cacat yang paling umum di antara yang lain dalam daftar ini. Biasanya terjadi ketika Anda hanya menggunakan konfigurasi default tanpa melihat kebutuhan situs web.
7. Cross Site Scripting
   Kelemahan cross site scripting akan terjadi pada aplikasi web jika aplikasi web mengizinkan pengguna untuk menambahkan kode khusus ke jalur URL atau ke situs web yang dilihat oleh pengguna lain. Kelemahan ini biasanya digunakan untuk menjalankan kode JavaScript berbahaya pada browser korban [10].
8. Desersi yang tidak aman
   Untuk memahami masalah dengan kelemahan ini, pertama-tama kita harus memahami apa arti serialisasi dan deserialisasi. Serialisasi adalah proses di mana objek diambil dari kode aplikasi dan dikonversi ke format lain sehingga dapat digunakan untuk tujuan lain, seperti menyimpan data ke disk. Deserialisasi berarti kebalikannya; mengubah data yang

diserialisasikan kembali ke objek yang digunakan oleh aplikasi. Deserialisasi yang tidak aman dapat diserang dengan menggunakan data dari sumber yang tidak terpercaya. Hal ini dapat menyebabkan serangan DDoS. Untuk mencegah hal ini terjadi, Anda perlu melarang deserialisasi data yang tidak dipercaya.

9. Komponen
   Menggunakan Komponen dengan Kerentanan yang Telah Diketahui Sebagian besar pengembang web menggunakan komponen seperti pustaka dan kerangka kerja dalam aplikasi web mereka. Komponen-komponen ini merupakan kumpulan perangkat lunak yang membantu pengembang untuk bekerja lebih efisien.
10. Pemantuan log yang tidak memadai
    Sebagian besar aplikasi web tidak mengambil langkah yang cukup untuk mendeteksi pelanggaran data. Rata-rata orang baru menyadari adanya pelanggaran pada situs web mereka setelah 200 hari. Hal ini memberikan banyak waktu bagi penyerang untuk melancarkan serangan.



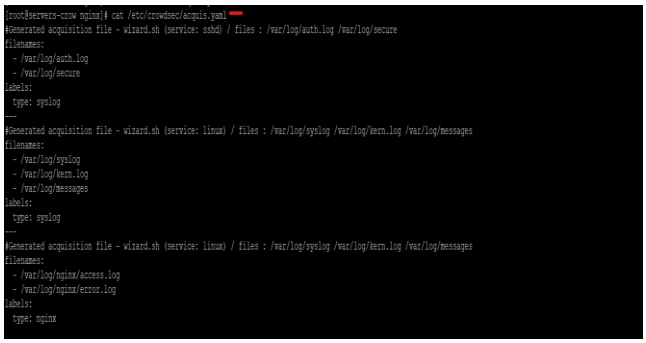

**Gambar 1.** Desain pengujian

## II. Metode dan Desain

Langkah-langkah yang akan dilakukan untuk menguji sistem keamanan pada web server dengan menggunakan tools crowdsec adalah sebagai berikut:

1. Menyiapkan 2 buah server dengan menggunakan Virtual Machine, dimana server pertama diinstall menggunakan Ubuntu server dan server kedua bertujuan sebagai hacker dengan menggunakan kali linux.
2. Melakukan instalasi dan konfigurasi sistem operasi dan sistem crowdsec tools.
3. Install dan konfigurasikan sistem operasi VM hacker agar dapat terhubung ke server tujuan.
4. Lakukan uji konektivitas menggunakan telnet ke port httpd untuk memastikan client dapat mengakses layanan WEB.
5. Lakukan uji coba serangan
6. Mengambil data log sistem pada kedua web server

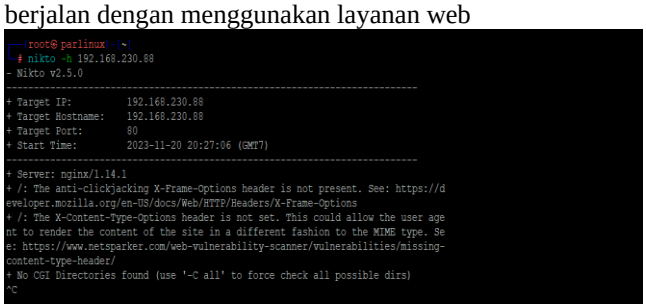
VM dan memasukkan data hasil pengujian ke dalam aplikasi pengolah data untuk dilakukan analisis hasil penelitian sesuai dengan parameter pengujian yang telah ditentukan.




**Gambar 2**. konfig nginx

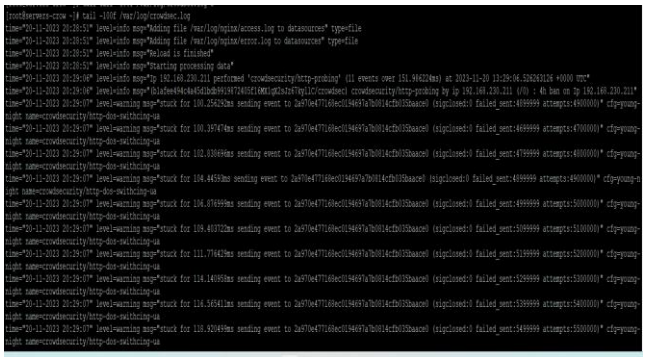
Pada baris terakhir, kita menambahkan lokasi jalur layanan nginx.

Setelah server dikonfigurasi, kita akan mencoba mensimulasikan serangan terhadap server yang sedang berjalan dengan menggunakan layanan web



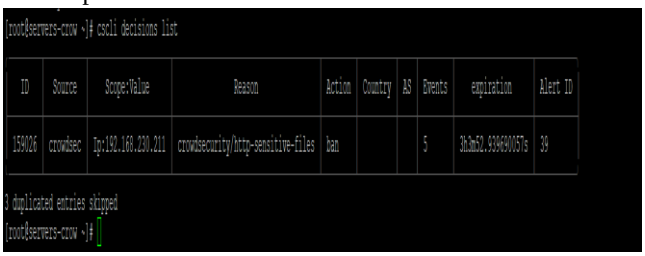

**Gambar 3**. Scan menggunakan Nikto

Dari sisi server, saat pemindaian dilakukan. Crowdsec akan mendeteksi setiap aktivitas yang mengarah ke peretasan. Oleh karena itu, ketika proses tersebut dilakukan sebanyak 5 kali berturut-turut, maka secara otomatis IP yang melakukan peretasan akan diblokir.




**Gambar 4**. Identifikasi serangan

Kemudian service crowdsec akan melakukan pemblokan terhadap server.




**Gambar 5**. List server di block

Secara kinerja, crowdsec sebenarnya melakukan parsing terhadap log yang masuk ke */var/log/nginx/access.log*, karena metode scanning dari client mengindikasikan adanya peretasan maka crowdsec mengkategorikan ke dalam tahap 3 yaitu s02-enrich, metode yang digunakan masuk dalam kategori http-logs dan geoip-enrich rules. Sehingga pada tahap terakhir di langkah skenario, crowdsec secara otomatis melakukan pemblokiran. Berikut adalah detail lognya. log: 2023/11/20 20:29:09 [error] 9686#0: *177 open() "/usr/share/nginx/html/xI5on490.pt-br" failed (2: No such file or directory), client: 192.168.230.211, server: _, request: "GET /xI5on490.pt-br HTTP/1.1", host: "192.168.230.88It enters the first stage s00-raw

Kemudian dari crowdsec akan melakukan pemisahan terhadap setiap line log tersebut menggunakan service berikut:

- *crowdsecurity/dateparse-enrich* proses ini melakukan tagging terhadap waktu setiap log yang akan maksud
- *crowdsecurity/geoip-enrich* log event yang menginformasikan tentang posisi IP yang melakukan serangan
- crowdsecurity/http-logs Proses melakukan pemisahan terhadap log httpd, seperti penandaan statis dari sumber IP, kemudian melakukan pemecahan agar dapat di kategorikan
- crowdsecurity/whitelists proses melakukan whitelist terhadap akses yang normal dan log yang mengancam system
- crowdsecurity/http-crawl-non_statics memastikan ip yang statis melakukan serangan akan di blok permanent
- crowdsecurity/http-probing ini adalah permintaan HTTP 4XX yang tidak menargetkan sumber daya statis

Kita dapat menyesuaikan log mana yang akan dimonitor pada sistem itu sendiri. Sehingga layanan ini tidak hanya mengenali program yang umum saja, tetapi kita mencoba untuk dapat melakukan kustomisasi dan berkontribusi pada forum open source. Karena peneliti percaya, tool ini dapat membantu para administrator sistem dalam melakukan pemeliharaan sistem yang digunakan baik dalam skala kecil maupun skala enterprise.

## IV. Penutup

Kelebihan dari crowdsec yang bisa dibilang tools open source lainnya, adalah database yang terkait dengan bentuk serangan selalu diupdate, sehingga jika ada metode serangan baru, akan lebih mudah untuk dicegah ketika ingin menyerang sistem yang kita gunakan. Akan tetapi dalam proses pemeliharaan tools, seorang system administrator harus mampu mengenali pola serangan yang terbaru, agar dapat melakukan improvement terkait log baru yang diindikasi sebagai bentuk serang terhadap system.

## V. Daftar Pustaka

[1] Y. Almutairi, B. Alhazmi, and A. Munshi, “Network Intrusion Detection Using Machine Learning Techniques,” *Advances in Science and Technology Research Journal*, vol. 16, no. 3, pp. 193–206, Jul. 2022, doi: 10.12913/22998624/149934.

[2] A. M.R. and V. P., “Review of Cyber Attack Detection: Honeypot System,” *Webology*, vol. 19, no. 1, pp. 5497–5514, Jan. 2022, doi: 10.14704/WEB/V19I1/WEB19370.

[3] L. Sama, H. Wang, and P. Watters, “Enhancing System Security by Intrusion Detection Using Deep Learning BT - Databases Theory and Applications,” W. Hua, H. Wang, and L. Li, Eds., Cham: Springer International Publishing, 2022, pp. 169–176.

[4] G. Wassermann and Z. Su, “An Analysis Framework for Security in Web Applications.”

[5] W. G. J. Halfond and A. Orso, “AMNESIA,” in *Proceedings of the 20th IEEE/ACM International Conference on Automated Software Engineering*, New York, NY, USA: ACM, Nov. 2005, pp. 174–183. doi: 10.1145/1101908.1101935.

[6] Y.-W. Huang, S.-K. Huang, T.-P. Lin, and C.-H. Tsai, “Web application security assessment by fault injection and behavior monitoring,” in *Proceedings of the twelfth international conference on World Wide Web - WWW ’03*, New York, New York, USA: ACM Press, 2003, p. 148. doi: 10.1145/775152.775174.

[7] T. Aprilia, B. S. Pitoyo, A. Fauzi, R. G. Ramadhanti, and R. Dwi, “2024 Madani : Jurnal Ilmiah Multidisipline Pengaruh Keamanan Two Factor Authentication Terhadap Pencurian Data ( Cyber Crime ) Pada Media Sosial 2024 Madani : Jurnal Ilmiah Multidisipline,” vol. 2, no. 5, pp. 449–458, 2024.

[8] S. Jan, C. D. Nguyen, and L. C. Briand, “Automated and effective testing of web services for XML injection attacks,” *ISSTA 2016 - Proceedings of the 25th International Symposium on Software Testing and Analysis*, pp. 12–23, 2016, doi: 10.1145/2931037.2931042.

[9] A. F. Hasibuan and D. Handoko, “Analisis Keretanan Website Dengan Aplikasi Owasp Zap,” *Jurnal Ilmu Komputer dan Sistem Informasi*, vol. 2, no. 2, pp. 257–270, 2023, [Online]. Available: https://jurnal.unity-academy.sch.id/index.php/jirsi/article/view/51

[10] Y. Putra, Y. Yuhandri, and S. Sumijan, “Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting,” *Jurnal Sistim Informasi dan Teknologi*, vol. 3, pp. 56–63, 2021, doi: 10.37034/jsisfotek.v3i2.44.