Jurnal Informasi, Sains dan Teknologi
Vol. 7 No. 2 Tahun 2024
ISSN: 2829-2758, ISSN: 2828-7207, Hal 290-303
DOI: https://doi.org/10.55606/isaintek.v7i2.301

Implementasi dan Analisis *Wazuh* Sebagai *Intrusion Detection System (IDS)* dan *Platform Monitoring*

Gede Parama Antara[1], Ika Dyah Agustia Rachmawati[2]
[1,2] Universitas Bina Nusantara

Abstract. *Attacks on web applications (web application attacks) can compromise data security in hospitals which are exploited by attackers by using weaknesses in the web application code. However, there are still many developers who are less alert to attacks on web applications. To improve the security side of the web server so that it detects suspicious attacks in website network traffic, namely by using wazuh as an Intrusion Detection System (IDS) and monitoring platform. The evaluation results show that the implementation of wazuh as an Intrusion Detection System (IDS) and monitoring platform can detect attacks by closing security gaps so that attackers cannot attack in the same way.*

Keywords: *Intrusion Detection System, Platform Monitoring, Wazuh*

Abstrak. Serangan terhadap aplikasi web (web application attack) dapat membahayakan keamanan data di Rumah Sakit yang dimanfaatkan oleh attacker dengan menggunakan kelemahan pada web application code. Namun, masih banyak developer kurang waspada terhadap serangan pada aplikasi web. Untuk meningkatkan sisi keamanan pada web server agar mengetahui adanya serangan yang mencurigakan dalam traffic jaringan website, yaitu dengan menggunakan wazuh sebagai Intrusion Detection System (IDS) dan platform monitoring. Hasil evaluasi menunjukkan bahwa implementasi wazuh sebagai Intrusion Detection System (IDS) dan platform monitoring dapat mendeteksi serangan dengan menutup celah keamanan tersebut supaya attacker tidak dapat menyerang dengan cara yang sama.

Kata Kunci : Intrusion Detection System, Platform Monitoring, Wazuh

1. PENDAHULUAN

Kemajuan Ilmu Pengetahuan dan Teknologi (IPTEK) semakin pesat setiap tahunnya dan pengguna internet di didunia dan di Indonesia juga terus bertambah. Jumlah pengguna internet di dunia pada bulan April tahun 2024, yaitu mencapai angka 5,44 miliar atau setara dengan 67,1% populasi global (Arhami, 2024). Sedangkan jumlah pengguna internet di Indonesia pada bulan Januari 2024 mencapai angka 185 juta individu atau setara dengan 66,6% dari total populasi nasional yang berjumlah 278,7 juta orang (Arhami, 2024). Penggunaan teknologi internet dalam dunia kesehatan merupakan bagian dari konsep teknologi kesehatan yang membawa manusia memasuki kehidupan yang berdampingan dengan informasi dan teknologi itu sendiri. Hal ini juga berdampak pada kegiatan di rumah sakit dengan perkembangan proses penelusuran informasi yang juga membutuhkan teknologi internet. Dengan teknologi internet yang berkembang saat ini di rumah sakit, dapat meningkatkan kualitas pelayanan di rumah sakit dan pengelolaan informasi dapat dilakukan secara lebih aktual dan optimal.

Dengan adanya penggunaan internet dan teknologi dalam bidang kesehatan, menimbulkan risiko terhadap kejahatan dunia maya, khususnya dalam keamanan jaringan. Keamanan jaringan komputer kini dipandang sebagai salah satu tugas dan masalah penting

Received: Oktober 21, 2024; Revised: November 15, 2024; Accepted: December 25, 2024; Published: December 30, 2024

yang harus diberikan solusinya untuk melindungi aset-aset dan berbagai informasi. Sistem keamanan jaringan adalah sebuah sistem yang digunakan untuk mencegah serta mendeteksi dan mengidentifikasi sesuatu yang tidak sah, serta yang mencurigakan pada sebuah jaringan komputer (Albar & Putra, 2022). Sistem keamanan jaringan komputer adalah sebuah integritas sistem yang digunakan untuk menjaga semua sumber daya dan unsur-unsur yang terdapat pada suatu jaringan komputer, bentuk pengamanannya bisa berupa hardware maupun software yang telah diberikan fasilitas untuk suatu pengamanan jaringan (Sukaridhoto, 2021).

Menurut data dari Badan Siber dan Sandi Negara (BSSN) tahun 2022 tentang Laporan Bulanan Publik Hasil Monitoring Keamanan Siber menjelaskan insiden serangan siber di Indonesia yaitu mencapai angka 976.429.996, sedangkan tahun 2023 mencapai angka 990.357.998, dengan anomali trafik paling banyak berasal dari aktivitas Web Application attack (serangan LFI dan XXE) mencapai angka 477.023.076 (tahun 2022) dan 489.371.276 (2023), dan diikuti oleh serangan siber Denial of Service (DoS) mencapai angka 386.231.332 (tahun 2022) dan 398.445.675 (tahun 2023), yang merupakan serangan dari perangkat lunak yang dirancang mampu merusak sistem komputer atau jaringan komputer, sehingga membahayakan pemilik perangkat (Badan Siber dan Sandi Negara, 2023). Di sektor Kesehatan, termasuk di Rumah Sakit, trend kasus peretasan di Indonesia tahun 2022, yaitu mencapai angka 523 (nomor dua terbanyak setelah sektor pemerintah), sedangkan tahun 2023 mencapai angka 657 (nomor dua terbanyak setelah sektor pemerintah) (Badan Siber dan Sandi Negara, 2023). Dan, pada sektor Kesehatan (termasuk Rumah Sakit), anomali trafik dengan klasifikasi anomali Web application attack (serangan LFI dan XXE) pada tahun 2022 sebanyak 3.856.123 dan pada tahun 2023 sebanyak 4.926.876. Selain itu, jenis sumber anomali lainnya disektor Kesehatan (termasuk Rumah Sakit) pada tahun 2022, yaitu Denial of Service (DoS) dengan capaian angka 949.716 dan pada tahun 2023 mencapai angka 989.600 (Badan Siber dan Sandi Negara, 2023). Dari data yang diuraikan diatas, dapat dinyatakan bahwa insiden serangan siber di indonesia setiap tahun meningkat, terutama di sektor kesehatan, khususnya di Rumah Sakit. Berdasarkan data BSSN diatas, bahwa sektor kesehatan (termasuk Rumah Sakit) paling banyak jenis serangan dengan anomali trafik, yaitu LFI, XXE dan DoS, dan hal ini penting untuk dilakukan tindakan upaya pencegahan terhadap serangan siber untuk menjaga data pasien dirumah sakit dan sistem pelayanan kesehatan di rumah sakit, sehingga keselamatan pasien dan mutu pelayanan di rumah sakit menjadi baik.

Serangan terhadap aplikasi web (web application attack) yang dapat terjadi di Rumah Sakit seperti serangan Denial of Service (DoS), Local File Inclusion (LFI) dan XML External Entity (XXE) yang dapat membahayakan data rekam medis pasien dan data pelayanan

kesehatan lainnya di Rumah Sakit (Badan Siber dan Sandi Negara, 2023). Hal inilah yang dijadikan sasaran utama yang dimanfaatkan oleh para peretas / hacker dengan memanfaatkan kelemahan pada web application code dan kecerobohan para developer situs yang tidak mengikuti pedoman dalam pembuatan web application.

File Inclusion yang merupakan salah satu celah keamanan yang memiliki dampak cukup besar terhadap website dan server di Rumah Sakit. File Inclusion sendiri terdiri dari Local File Inclusion (LFI) dan Remote File Inclusion (RFI) (Koprawi, 2020). Celah keamanan ini terjadi pada Rumah Sakit salah satunya karena kurangnya kesadaran terhadap secure programming atau bagaimana menuliskan kode program dengan cara yang aman. Penggunaan IDS sebagai platform monitoring bisa dilakukan untuk keamanan data rumah sakit.

Kegiatan di Rumah Sakit banyak dilakukan melalui aplikasi web, sehinga diperlukan sistem keamanan yang baik (Hasan et al, 2018). Saat ini, kerentanan Local File Inclusion (LFI) umumnya ditemukan di beberapa aplikasi web yang menyebabkan eksekusi kode jarak jauh di server host. Deteksi kerentanan LFI menjadi perhatian yang sangat penting bagi pemilik web Rumah Sakit untuk mengambil tindakan efektif memitigasi risikonya. Pada penelitian ini mengusulkan model deteksi kerentanan LFI otomatis dengan tingkat pencapaian akurasi 88%, sehingga data pasien dan data pelayanan kesehatan di Rumah Sakit menjadi aman dari berbagai serangan web application (web application attack), seperti LFI.

Rumah Sakit yang menggunakan teknologi perangkat lunak wordpress sebagai framework pengembangan website, sangat rentan terhadap serangan LFI atau XXE (Aziz, 2021). Hal ini membuat semakin banyak laporan insiden keamanan informasi berupa web application attack, seperti LFI dan XXE, yaitu berupa pencurian informasi di Rumah Sakit, terutama terkait Rekam Medis pasien dan data kesehatan lainnya. Pengujian yang dilakukan dengan cara penetration testing yang diawali dengan melakukan pengumpulan informasi berupa kerentanan-kerentanan yang terdapat di dalam web target, selanjutnya melakukan eksploitasi yang memanfaatkan informasi berupa kerentanan terhadap serangan LFI dan XXE. Penggunaan discord sebagai notifikasi alert atau warning terjadinya serangan LFI dan XXE. Setelah diketahui kerentanan yang dapat dieksploitasi, maka dapat dilakukan perbaikan-perbaikan untuk menghasilkan website yang aman dari serangan hacker. Salah satu strategi untuk meningkatkan keamanan website dapat menggunakan strategi defense in depth yang berfokus kepada teknikal kontrol, diantaranya dengan melakukan pembatasan akses pada sistem informasi, memanfaatkan fitur tambahan pada wordpress, seperti penggunaan captcha atau menggunakan fitur multi otentikasi dengan menggunakan aplikasi untuk menghindari upaya serangan LFI dan XXE, serta secara berkala melakukan pembaruan versi dari sistem

informasi yang digunakan untuk menghindari risiko eksploitasi.

Serangan pada web applikasi dengan XXE yang dapat membahayakan Sistem Informasi Manajemen Rumah Sakit, yang memuat data medis pasien dan data rumah sakit lainnya (Bisht et al, 2021). Hal ini membuat penting untuk melindungi data di Rumah Sakit menjadi lebih aman, salah satunya dengan penggunaan firewall di Rumah Sakit dan melakukan monitoring menggunakan aplikasi monitoring seperti Wazuh atau Grafana, dengan sistem alert atau warning menggunakan discord.

2. METODE PENELITIAN

a) Metode Pengumpulan Data

1) Metode Wawancara (interview)

   Wawancara digunakan sebagai teknik pengumpulan data untuk menemukan permasalahan yang harus diteliti dan juga apabila peneliti ingin mengetahui hal-hal dari responden yang lebih mendalam (Sugiyono, 2013). Pada penelitian ini, wawancara dilakukan pada tim IT rumah sakit sebagai dasar dalam pengembangan ide penelitian untuk melakukan implementasi dan analisis Wazuh sebagai IDS dan platform monitoring.

2) Penelitian Kepustakaan (library research)

   Penelitian kepustakaan dilakukan dengan pengumpulan data dan informasi dengan cara membaca buku-buku atau artikel referensi yang dapat dijadikan acuan pembahasan dalam penelitian ini.

b) Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan pada penelitian ini, yaitu metode waterfall yang merupakan metode pengembangan sistem perangkat lunak yang melakukan pendekatan secara urut dan sistematis yang dimulai dari awal yaitu rekayasa sistem, kebutuhan terhadap sistem, desain, pengodean, testing, dan maintenance (Meilinaeka, 2023). Setiap tahap dari metode ini harus menunggu hingga salah satu prosesnya selesai terlebih dahulu sehingga prosesnya berjalan secara berurutan.

3. HASIL DAN BAHASAN

a) Desain Keamanan

Peneliti membuat sebuah aplikasi berbasis web yang dibuat menggunakan bahasa HTML, CSS, PHP untuk dapat menguji dan mendeteksi 3 jenis serangan, yaitu LFI, XXE dan DoS.

1) Membuat aplikasi berbasis web

   Aplikasi dibuat menggunakan HTML, CSS, dan PHP dengan diberikan fungsi inputan untuk menguji atau menginputkan payload serangan LFI, XXE dan DoS.

2) Mendapatkan hasil dari serangan LFI, XXE dan DoS.

   Setelah menginputkan payload, maka akan didapatkan hasil sesuai payloadnya pada bagian bawah aplikasi.

3) Mendapatkan alert pada Discord

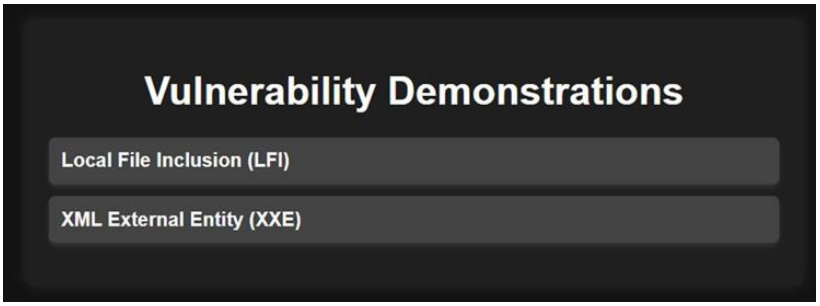
   Jika berhasil melakukan serangan menggunakan LFI, XXE dan DoS, maka akan mendapatkan sebuah alert melalui Discord.

4) Menampilkan dan memonitoring hasil serangan pada Wazuh.

   Semua bentuk serangan LFI, XXE dan DoS yang ada akan masuk dan termonitor pada Wazuh Dashboard, sehingga celah yang ada dapat segera diperbaiki.

b) Skenario Simulasi

Langkah-langkah dimulai dengan menjalankan operasi di server target. Pertama, perlu menyiapkan docker. Ini dapat dilakukan dengan menjalankan perintah 'docker compose up' yang berjalan melalui AWS (Amazon Web Services) melalui program Ubuntu 24.04 LTS. Setelah docker berhasil running, kemudian dapat dicoba untuk mengakses halaman web dengan mengetikkan http://13.212.90.107 ke dalam bar alamat browser, maka akan ditampilkan halaman antar muka sebagai berikut:



Gambar 1. Tampilan Antarmuka Aplikasi

A. Menguji Aplikasi dengan Local File Inclusion (LFI)

a. Deskripsi Kerentanan

Local File Inclusion (LFI) terjadi saat aplikasi web kurang memeriksa input pengguna dalam fungsi pengelolaan file. Ini membuat pengguna bisa memasukkan input ke dalam path file. Sebagai hasilnya, user bisa membuka file-file sensitif di server, seperti file konfigurasi, file sistem, atau file yang berisi kode berbahaya.

b. Tempat Terjadinya Kerentanan

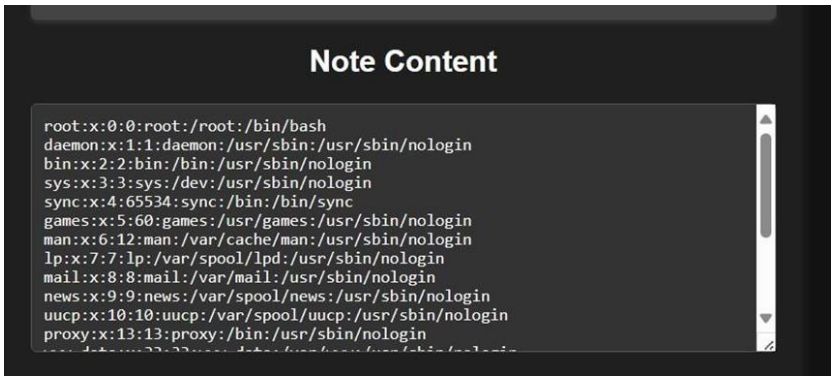
Kerentanan LFI muncul dalam bagian kode PHP yang mengelola parameter $_GET['note'] pada aplikasi ini. Parameter $_GET['note'] dimasukkan ke fungsi file_get_contents tanpa pemeriksaan sebelumnya, memungkinkan kita untuk memasukkan string seperti "../../../". Hal ini dapat mengubah jalur ke jalur yang lebih luar, memungkinkan kita untuk mengakses folder di luar folder ./notes.

```
<?php if (isset($_GET['note'])) : ?>
    <h2>Note Content</h2>
    <?php $note_content = getNoteContent($_GET['note']); ?>
    <textarea readonly><?php echo $note_content; ?></textarea>
<?php endif; ?>
</div>
</body>
</html>
```

Gambar 2. Parameter $_GET['note']

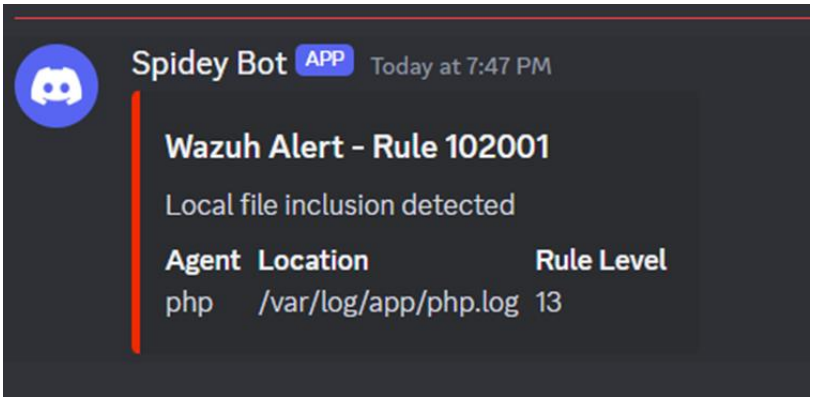
c. Cara Memanfaatkan Kerentanan

Untuk memanfaatkan kerentanan yang ada pada aplikasi ini, kita dapat mengakses file sensitif seperti /etc/passwd menggunakan payload berikut: **../../../../../etc/passwd**. Payload ini dimasukkan ke dalam input pengguna di URL. Hasilnya akan tampak seperti ini: **http://13.212.90.107/LFI/index.php?note=../../../../../etc/passwd**. Dengan cara ini, aplikasi akan menampilkan isi file /etc/passwd



Gambar 3. Tampilan Isi File /etc/passwd dengan LFI

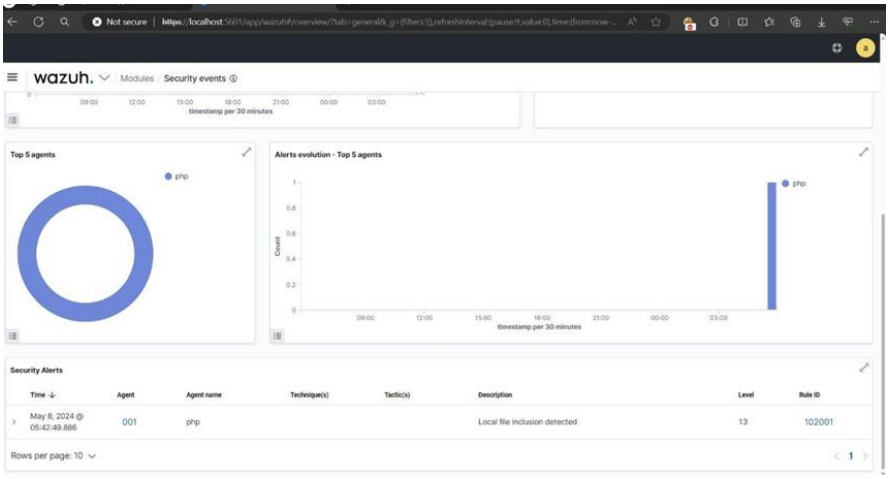
Setelah berhasil melakukan tes ini sistem keamanan Wazuh akan mengirim notifikasi ke platform Discord, Menunjukkan bahwa aturan yang telah diatur telah berhasil mendeteksi serangan LFI. Notifikasi tersebut akan tampak seperti gambar berikut:



Gambar 4. Hasil Notifikasi Serangan dengan LFI Pada Discord

d. Pengecekan Serangan LFI Pada Sistem IDS

Sistem IDS pada penelitian ini menggunakan Wazuh untuk melihat alert yang muncul akibat adanya serangan. Wazuh dashboard dapat diakses melalui port 5601. Setelah masuk ke dalam dashboard, akan terlihat bahwa agent php telah terdeteksi mengalami serangan LFI.



Gambar 5. Tampilan Alert pada Sistem IDS Wazuh Dashboard

B. Menguji Aplikasi dengan XML External Entity (XXE)

a. Deskripsi Kerentanan

Serangan XXE terjadi ketika aplikasi tidak melakukan validasi terhadap input XML yang diterima dari pengguna sebelum diproses. Dalam contoh kode program ini, input XML dari pengguna tidak divalidasi dengan tepat sebelum diproses oleh fungsi simplexml_load_string(). Karena itu, penyerang dapat memanipulasi input XML untuk menyertakan referensi entitas eksternal yang mengarah ke file-file sensitif di server.

b. Tempat Terjadinya Kerentanan

Kerentanan XXE terjadi di bagian kode PHP yang memproses input XML dari pengguna. Di baris $xml = simplexml_load_string($xmlString, 'SimpleXMLElement',

LIBXML_NOENT);, parameter LIBXML_NOENT digunakan tanpa mempertimbangkan dampak keamanannya. Hal ini memungkinkan penyerang untuk memasukkan referensi entitas eksternal yang mengarah ke file-file sensitif di server.

Gambar 6. Kode parameter LIBXML_NOENT

c. Cara Memanfaatkan Kerentanan

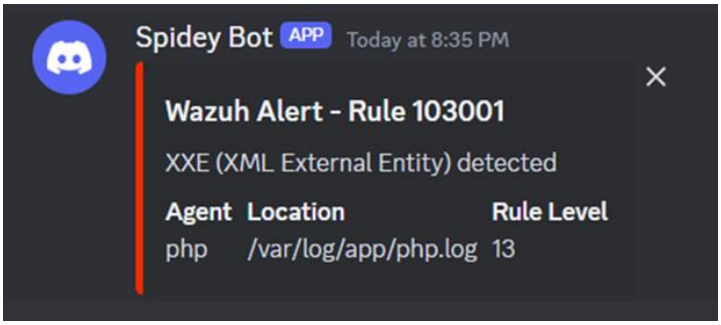
Untuk memanfaatkan kerentanan XXE pada aplikasi ini, penyerang bisa merancang payload XML yang memasukkan referensi entitas eksternal ke file-file sensitif di server. Sebagai contoh, penyerang bisa merancang payload XML seperti berikut:

```
<!DOCTYPE foo [
        <!ENTITY xxe SYSTEM "file:///etc/passwd">
]>
<note>
        <body>&xxe;</body>
</note>
```

Dengan menyertakan payload XML tersebut dalam input yang dikirimkan ke aplikasi, penyerang dapat membaca isi file /etc/passwd dari server. Outputnya akan tampak seperti gambar berikut:

Gambar 7. Tampilan Isi File */etc/passwd* dengan XXE

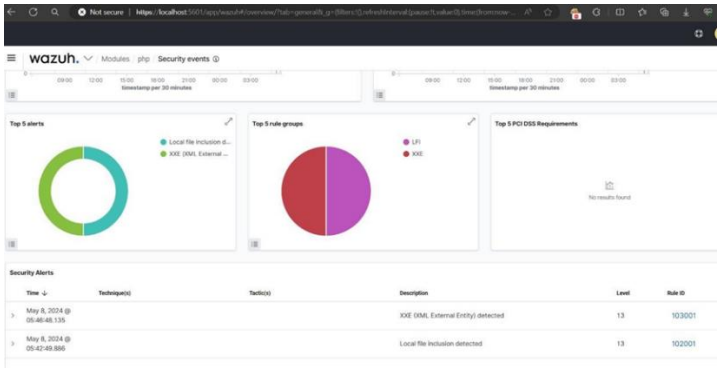
Sama seperti LFI, pada XXE juga aka masuk sebuah notifikasi pada Discord jika terjadi serangan dengan XXE. Notifikasi tersebut akan tampak seperti gambar berikut:



Gambar 8. Hasil Notifikasi Serangan dengan LFI pada Discord

d. Pengecekan Serangan XXE Pada Sistem IDS

Sistem IDS pada penelitian ini menggunakan Wazuh untuk melihat alert yang muncul akibat adanya serangan. Wazuh dashboard dapat diakses melalui port 5601. Setelah masuk ke dalam dashboard, akan terlihat bahwa agent php telah terdeteksi mengalami serangan XXE.



Gambar 9. Tampilan Alert pada Sistem IDS Wazuh Dashboard

C. Menguji Aplikasi dengan Denial of Service (DoS)

a. Deskripsi Kerentanan

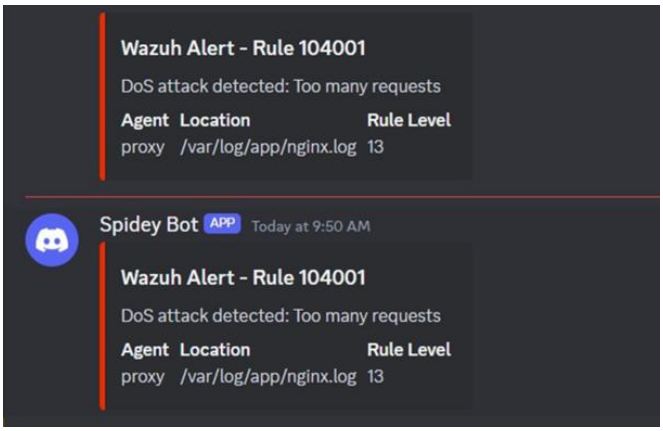
Kerentanan Denial of Service (DoS) terjadi ketika penyerang berhasil membuat suatu sistem, jaringan, atau aplikasi menjadi tidak tersedia bagi penggunanya. Hal ini biasanya dilakukan dengan membanjiri sistem target dengan jumlah permintaan yang berlebihan sehingga membuat sistem tidak mampu menangani dan akhirnya menjadi tidak responsif. Dalam beberapa kasus, serangan DoS bisa sampai mengeksploitasi bug atau celah keamanan dalam sistem yang dapat mengakibatkan kerusakan sistem yang lebih serius. Serangan ini dapat dilakukan oleh individu atau kelompok penyerang dan dapat mengganggu operasional bisnis serta merusak reputasi perusahaan.

b. Cara Memanfaatkan Kerentanan

Untuk memanfaatkan kerentanan Denial of Service (DoS), di sini akan memanfaatkan teknik khusus yang disebut HTTP flood. Teknik ini melibatkan pengiriman sejumlah besar permintaan HTTP ke sistem target, dengan tujuan untuk membanjirinya hingga titik di mana

ia tidak dapat lagi menangani lalu lintas yang masuk dan karenanya menjadi tidak responsif. Untuk melakukan ini, peneliti akan menggunakan alat yang tersedia di https://github.com/Leeon123/golang-httpflood. Alat ini dirancang khusus untuk melakukan serangan HTTP flood dan sangat efektif dalam menghasilkan volume lalu lintas yang diperlukan untuk meredam sistem target.

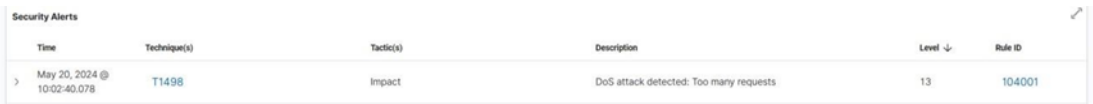
Ketika kita menjalankan httpflood dengan perintah ./httpflood <http:// 13.212.90.107/> 3 get 3 header.txt, peringatan berikut akan muncul pada Wazuh. Ini menandakan bahwa Wazuh telah berhasil mendeteksi serangan yang diluncurkan:



Gambar 10. Hasil Notifikasi Serangan dengan DoS pada Discord

c. Pengecekan Serangan DoS Pada Sistem IDS

Kita dapat memeriksa alert tersebut menggunakan dashboard Wazuh. Dashboard Wazuh dapat diakses melalui port 5601. Setelah masuk ke dashboard, kita akan melihat bahwa agen proxy telah terdeteksi mengalami serangan DoS. Serangan ini akan tampak jelas seperti yang ditunjukkan dalam gambar berikut:



Gambar 11. Agent Proxy Mengalami Serangan DoS

4. KESIMPULAN DAN SARAN

Kesimpulan

Kesimpulan yang didapat pada penelitian ini, yaitu pengembangan IDS sebagai platform monitoring dilakukan dengan cara membangun sebuah aplikasi berbasis web pada server lokal dan mengeksploitasi celah keamanan pada bagian kode program sebuah website oleh IDS yang telah dikembangkan. Proses ini dilakukan untuk menguji efektivitas IDS dalam mendeteksi serangan dan mengidentifikasi kelemahan-kelemahan pada sistem. Proses ini juga

dilakukan untuk menguji website pada uji coba menggunakan serangan LFI, XXE dan DoS dengan melihat efektivitas wazuh sebagai platform monitoring dalam mendeteksi serangan yang mengirimkan alert atau notifikasi pada Discord, sehingga akan memudahkan dalam melakukan monitoring terhadap serangan.

Saran

Berikut ini adalah beberapa saran yang dapat diberikan untuk penelitian selanjutnya dan implementasi yang bisa digunakan pada pihak pengguna, antara lain:

a. Bagi pihak pengguna agar memiliki platform monitoring terhadap serangan yang dapat terjadi pada server dan memiliki rencana respon insiden terhadap berbagai jenis serangan, sehingga dapat melindungi keamanan data dan jaringan.
b. Penelitian selanjutnya memberikan tambahan tindakan preventif dan mitigasi setelah terjadi deteksi serangan, jadi ketika menemukan sebuah indikasi serangan ke web server, tidak hanya dilakukan monitoring saja, melainkan ada tindakan untuk mempersempit celah hacker.
c. Pelatihan dan sosialisasi kepada pengguna sistem, khususnya bagi Rumah Sakit, dapat ditingkatkan untuk memastikan pengguna sistem dapat memahami pentingnya keamanan jaringan dan mengidentifikasi tindakan yang tepat ketika terjadi serangan.
d. Perlu dilakukan pengujian dan evaluasi terhadap IDS yang dibangun pada lingkungan jaringan yang lebih kompleks dan berukuran lebih besar untuk memastikan kinerja dan keamanannya.
e. Pengembangan sistem backup dan disaster recovery yang baik dapat membantu organisasi atau perusahaan mengembalikan sistem dan data dalam kondisi normal setelah terjadinya serangan.

REFERENSI

Ardhiansyah, M., Rahayu, S., & Rahmawati (2022). *Keamanan Komputer*. Banten : Unpam Pless

Argaw, S.T., *et al.* (2019). The State of Research on Cyberattacks Against Hospitals and Available Best Practice Recommendations : A Scoping Review. *Journal of BMC Medical Informatics and Decision Making,* vol. 19, no. 10, (pp. 1-11)

Arhami, M. (2024). Detection Using Intrusion Detection System (IDS) and SMS Gateway Controller. *International Journal of Electronics andTellecomunications.* vol. 7, no. 2, (pp. 449-453)

Arikunto, S. (2020). *Prosedur Penelitian Suatu Pendekatan Praktik*. Jakarta : Rhineka Cipta

Azis, R. (2021). Pengujian Kerentanan Website Wordpress Dengan MenggunakanPenetration Testing untuk Menghasilkan Website yang Aman terhadap Serangan LFI Dan XXE Pada Rumah Sakit. *Journal Riset TeknikInformatika dan Komputer.* vol. 3, no. 3, (pp. 93-105)

Badan Siber dan Sandi Negara. (2018). *Panduan Penanganan Insiden Serangan Denial of Service (DoS)* . Jakarta : Badan Siber dan Sandi Negara

Badan Siber dan Sandi Negara. (2018). *Panduan Penanganan Insiden Web Application Attack : Serangan LFI dan XXE* . Jakarta : Badan Siber dan Sandi Negara

Badan Siber dan Sandi Negara. 23 Oktober (2023). Laporan Bulanan Publik HasilMonitoring Keamanan Siber. *(Online)*. Diakses 23 Oktober 2023 dari www.bssn.go.id

Berliana, C.D., et al. (2022). Analisis Serangan dan Keamanan pada Denial of Service (DOS): Sebuah Review Sistematik Di Rumah Sakit. *Jurnal Ilmiah Informatika dan Komputer*, vol. 1, no. 2, (pp. 1-5)

Bisht, S. et al. (2021). XML External Entity Attacks and Mitigation in XML Parsers at the Hospital. *Journal of Emerging Technologies and Innovative Research.* vol. 8, no. 3, (pp. 1-5)

Cichonski, P., *et al*., (2020). *Computer Security Incident Handling Guide – Recommendation of The National Institute of Standards and Technology (NIST)*. United State of America : NIST Publication.

Comer, D. E. (2019). *The Internet Book.* New York : CRC Press

Darisman A. & Widianto M.H (2019). Design and Development of Pharmaceutical Company Information System Based on Website using the Waterfall Model, International Journal of Recent Technology and Engineering (IJRTE), vol. 8, (pp. 3989-3993)

Harahap, A . H . et al (2023). Pentingnya Peranan CIA Triad Dalam Keamanan

Hasibuan, M.S (2016). Keylogger Pada Aspek Keamanan Komputer, Jurnal Teknovasi, vol. 3, no. 1, (pp. 8-15)

Hassan, M. et al (2018). An Automated Local File Inclusion Vulnerability Detection Model at the Hospital, *International Journal of Engineering & Technology*, vol. , no. 2, (pp. 4-8)

Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder, *JurnalManagemen dan Pemasaran Digital (JMPD)*, vol. 1, no. 2, (pp. 73-83)

Inngam, G.P., Riadi, I. (2020). Analisis Bukti Digital tentang Serangan Denial of Service (DoS) Berdasarkan Log di Rumah Sakit. *Buletin Ilmiah Sarjana Teknik Elektro,* vol. 2, no. 2, (pp. 70-74)

Irfan. *et al.* (2021). Keamanan Jaringan VLAN dan VoIP Menggunakan Firewall. *Buletin Sistem Informasi dan Teknologi Islam*, vol. 2, no. 1, (pp. 27-35)

Jacob, R.S., Kalimuthu, M. (2018). Detecting DoS Attacks in Software Defined Networking and Cloud Computing. *International Journal of Science and Research (IJSR)*, vol. 7, no. 2, (pp. 1623-1626) Jawa Tengah: CV. Pena Persada.

Kementerian Kesehatan Republik Indonesia. (2009). *Undang-Undang Republik Indonesia Nomor 44 tahun 2009 Tentang Rumah Sakit*. Jakarta : Sekretariat Negara

Kementerian Kesehatan Republik Indonesia. (2013). *Peraturan Menteri Kesehatan Republik Indonesia Nomor 82 Tahun 2013 Tentang Sistem Informasi Manajemen Rumah Sakit*. Jakarta : Kementerian Kesehatan Republik Indonesia

Koprawi, M. (2020). Dampak dan Pencegahan Serangan File Inclusion Di Rumah Sakit : Perspektif Developer. *Jurnal Nasional Informatika dan Teknologi Jaringan,* vol. 4, no. 2, (pp. 1-5)

Kral, P. (2021). *Incident Handler's Handbook.* United State of America : SANS Institute.

Mambang. (2021). *Bku Ajar Teknologi Komunikasi Internet (Internet of Things).*

Marsic, Ivan. (2021). Cmputer *Networks Performance and Quality of Service*.

Maslan, A. (2020). *Belajar Cepat Teori, Praktik dan Simulasi Jaringan Komputerdan Internet*. Jakarta : Mediakita

Maulana, A. *et al*. (2022). Implementation of Mikrotik Firewall for Website Access Restriction and Prevention of DoS (Denial of Service) Attacks on Internet Networks of Al-Mahrusiyah Vocational School Lirboyo. *Journal ofTelecommunication Network,* vol. 13, no. 1, (pp. 81-86)

McClanahan, P. (2024). *Information Security*. California: San Joaquin Delta College

Micro, A. (2012). *Dasar-Dasar Jaringan Komputer, Edisi Revisi 2012*. Jakarta : Clearos Indonesia

Muthohir, M. (2021). *Mudah Membuat Web Bagi Pemula*. Semarang: Yayasan Prima Agus Teknik

New Jersey : Rutgers University

Nuryadi, N., Nainggolan, E. C. (2021). Implementasi Intrusion Detection System Pada Local Area Network (Studi Kasus: Yayasan Pendidikan Tanah Tingal Tangerang) . *Jurnal Sains, Teknologi dan Industri,* vol. 19, no. 1, (pp. 1-8)

Prabhakar, M., Syed A.R. (2021). The Solution for XML External Entity Vulnerability in Web Application Security. *Smart Intelligent Computingand Communication Technology,* vol. 5, no. 1, (pp. 305-310)

Prakas, S., dan Mohaptra, A.K. (2023). Robust Analysis of XXE Attack Producedby Malware at the hospital. *International Jurnal of Mebrane Science and Technology,* vol. 10, no. 1, (pp. 647-685)

Pratama, M.D. (2022). Wazuh Sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan DOS. *Jurnal Ilmiah Teknologi Sistem Informasi,* vol. 3, no. 1, (pp. 1-7)

Pressman, R.S. (2015). *Rekayasa Perangkat Lunak: Pendekatan Praktisi*.

Purwohedi, U. (2022). *Metode Penelitian Prinsip dan Praktik*. Yogyakarta : LeutikaPrio

Sari, A.P, & Suhendi. (2020). Rancang Bangun Sistem Informasi Pengelolaan Talent Film Berbasis Aplikasi Web. Jurnal Informatika Terpadu Vol. 6 No. 1, (pp. 29-37)

Sasongko, L. (2022). *Aplikasi Deteksi Kelemahan Website Dengan Menggunakan Metode Injeksi Remote File Inclusion Dan Local File Inclusion Di Rumah Sakit*. Skripsi S1. Universitas Pembangunan Nasional Veteran, Jawa Timur.

Shafiyyah, A. (2024). *Implementasi Sistem Keamanan jaringan di PSDKU Universitas Lampung Waykanan Menggunakan Server Wazuh UntukDeteksi dan Respon Serangan Siber*. Skripsi S1. Universitas Lampung, Bandar Lampung.

Shahid, R., et al (2022). A Study of XXE Attacks Prevention Using XML Parser Configuration. *International Conference on Computational Intelligence andCommunication Networks (CICN),* 4-6 Desember 2022.

Sugiyono. (2019). *Metode Penelitian Kuantitatif, Kualitatif dan RD*. Bandung : Alphabet

Sukaridhoto, S. (2014). *Buku Jaringan Komputer I*. Surabaya: Politeknik Elektronika Negeri Surabaya

Tanuwijaya, E. (2023). *Pengembangan Intrusion Detection System (IDS) Menggunakan Python dengan Grafana Sebagai Platform Monitoring*. Skripsi S1. Universitas Bina Nusantara, Jakarta.

Tjahjanto. (2022). Application of the Waterfall Methode in Information System for State Owned Inventories Management Development. *Jurnal dan penelitian Teknik Informatika.* vol. 16, no. 4, (pp. 2182-2192)

Wibowo, A. (2022). *Jaringan Sistem Komputer, Jilid 2*. Semarang : Yayasan Prima Agus Teknik

Widiyanto, W.W. (2022). Simulasi Keamanan jaringan SIMRS (Sistem Informasi Manajemen Rumah Sakit) Menggunakan Snort IDS dan IPS. *Indonesian of Health Information Management Journal*, vol. 10, no. 1, (pp. 10-17)

Yasir, M. N., Croock, M. S. (2020). Cyber DoS attack-based security simulator for VANET. *International Journal of Electrical and Computer Engineering*, vol. 10, no. 6, (pp. 5832-5843) Yogyakarta: Andi.