(2024), 2 (11): 215–228 Scientica 3021-8209
Jurnal Ilmiah Sains dan Teknologi

IMPLEMENTASI *WAZUH DASHBOARD* PADA *SERVER* UNTUK MONITORING SERANGAN *DDOS* TERHADAP *WEB* XYZ

Angga Nugraha, Yusuf Muhyidin, Imay Kurniawan
Program Studi Teknik Informatika S1, Fakultas Teknik, Sekolah Tinggi Teknologi Wastukancana
Jl. Cikopak No.53, Sadang, Purwakarta, Jawa Barat, Indonesia

Abstract (English)
Internet advancements today have led many offices and companies to use it to facilitate the flow of information within their organizations. Since web servers are a critical component of public-facing web infrastructure, caution must be exercised when dealing with web server attacks. Attacks on web servers can have serious consequences, including the loss of sensitive data. Such attacks may result in the loss of sensitive data such as user information, financial details, and other sensitive information. Among these attacks, Distributed Denial of Service (DDoS) attacks are still prevalent, as reported by CNN Indonesia, which recently cited the paralysis of the Indonesian General Election Commission (KPU) website due to a DDoS attack during the 2024 election event. Given this issue, there is a need for a tool to monitor web servers. In this research, the tool used is Wazuh, an Open Source-based device that functions as a host-based intrusion detection system (HIDS). The research methodology employed includes Penetration Testing, which encompasses stages such as Gathering Information, Threat Modeling, Vulnerability Analysis, Exploitation, and Reporting. The findings of this study indicate that Wazuh can detect DDoS attacks on low vulnerability with evidence of 396 hits, representing users attempting to access the web

Article History
Submitted: 16 July 2024
Accepted: 25 July 2024
Published: 26 July 2024

Key Words
DDoS attack, Penetration testing, Wazuh dashboard

Abstrak (Indonesia)
Kemajuan Internet pada saat ini, banyak kantor dan perusahaan menggunakan Internet untuk memfasilitasi arus informasi dalam perusahaan mereka. Karena server web adalah salah satu komponen utama infrastruktur web yang dapat diakses publik, kehati-hatian harus diberikan saat menyerang server web. Serangan terhadap server web dapat menimbulkan konsekuensi serius, termasuk Hilangnya Data Sensitif, Serangan dapat mengakibatkan hilangnya data sensitif seperti informasi pengguna, informasi keuangan, dan informasi sensitif lainnya. Dalam jenis serangan, serangan Ddos masih cukup banyak terjadi dalam dilakukan serangan jaringan seperti menurut CNN Indonesia yang mengutip bahwasannya baru baru ini dalam acara pemilihan di tahun 2024 terjadi kelumpuhan situs KPU yang di serang oleh jenis serangan Ddos. Berdasarkan permasalahan tersebut maka di perlukanlah sebuah *tools* untuk memonitoring sebuah *web server, tools* yang di gunakan dalam penelitian ini adalah *wazuh.* Wazuh merupakan perangkat berbasis *Open Source* yang berfungsi sebagai sistem deteksi intrusi berbasis *host (endpoint)*. Dalam pengerjaan penelitian, penulis menggunakan metode *Penetration Testing* yang di dalamnya terdapat tahapan *Gathering Information, Threat-Modeling, Vulnerability Analysis, Exploitation* dan *Reporting.* Hasil dari penelitian ini wazuh dapat mendeteksi serangan *Ddos* pada kerentanan rendah dengan ada bukti 396 *hits* yaitu pengguna yang mencoba akses *web.*

Sejarah Artikel
Submitted: 16 July 2024
Accepted: 25 July 2024
Published: 26 July 2024

Kata Kunci
serangan *Ddos, Penetration testing, wazuh dashboard*

1. Latar Belakang

Kemajuan Internet pada saat ini, banyak kantor dan perusahaan menggunakan Internet untuk memfasilitasi arus informasi dalam perusahaan mereka. Data perusahaan bersifat rahasia dan harus disimpan dengan aman. Di sisi lain, kemudahan akses terhadap informasi menimbulkan permasalahan baru dimana informasi dan data penting dapat disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab untuk kepentingannya sendiri.

Karena server web adalah salah satu komponen utama infrastruktur web yang dapat diakses publik, kehati-hatian harus diberikan saat menyerang server web. Serangan terhadap server

web dapat menimbulkan konsekuensi serius, termasuk Hilangnya Data Sensitif, Serangan dapat mengakibatkan hilangnya data sensitif seperti informasi pengguna, informasi keuangan, dan informasi sensitif lainnya. Kerusakan Infrastruktur seperti serangan dapat merusak infrastruktur server, menyebabkan *downtime*, dan mengganggu operasional situs web dan aplikasi. Akses Tidak Sah seperti serangan dapat memberikan akses tidak sah kepada penyerang, yang dapat digunakan untuk aktivitas jahat seperti pencurian data atau kerusakan situs web. Kerugian Ekonomi seperti serangan dapat menyebabkan kerugian ekonomi baik secara langsung (biaya perbaikan kerusakan dan kehilangan data) maupun secara tidak langsung (hilangnya pendapatan karena *downtime*). Hilangnya Reputasi seperti serangan dapat merusak reputasi perusahaan atau organisasi, terutama jika serangan tersebut dieksploitasi dan diketahui publik. Oleh karena itu, penting untuk selalu mengambil tindakan keamanan yang tepat untuk melindungi server web Anda, termasuk Contohnya menginstal pembaruan keamanan terkini, menggunakan *firewall*, mengenkripsi data sensitif, dan melakukan audit keamanan rutin. Dalam jenis serangan, serangan Ddos masih cukup banyak terjadi dalam dilakukan serangan jaringan seperti menurut CNN Indonesia yang mengutip bahwasannya baru baru ini dalam acara pemilihan di tahun 2024 terjadi kelumpuhan situs KPU yang di serang oleh jenis serangan Ddos. "Gangguan terhadap sistem Sirekap terjadi mulai tanggal 14 Februari 2024 yang angka (trafik pengunjung)-nya meninggi dan salah satunya adalah gangguan DDoS," kata Betty dalam jumpa pers di Gedung KPU, Jakarta Pusat, Senin, 19 Februari 2024.

Wazuh merupakan perangkat berbasis *Open Source* yang berfungsi sebagai sistem deteksi intrusi berbasis *host (endpoint)*. Wazuh melakukan analisis *log*, pemeriksaan integritas, pemantauan registri Windows, deteksi *rootkit*, peringatan berbasis waktu, dan *respons* aktif. *Wazuh* merupakan perangkat yang menyediakan fitur visibilitas keamanan yang lebih dalam ke sebuah infrastruktur dengan memantau host pada sistem operasi dan juga pada tingkat aplikasi. Wazuh terdiri dari 2 (dua) bagian yaitu *Wazuh-Server* dan *Wazuh-Agent*. *Wazuh server* merupakan perangkat yang digunakan sebagai manajemen agen dan *dashboard* sistem monitoring baik file *integrity*, *intrusion*, maupun *log*. Sedangkan *Wazuh agent* merupakan perangkat yang *diinstall* pada perangkat *endpoint* untuk melakukan pembacaan sistem, pengumpulan *log* serta mengirimkan ke *Wazuh server*. (Fitri Nova et al., 2022)

Maka dari itu dalam hal memonitoring sebuah web server di perlukan sebuah *tools* untuk memantau grafik pada web, dalam hal ini peneliti menggunakan *tools wazuh* dengan fitur grafik yaitu *dashboard* dan yang menjadi objek implementasi *wazuh* yaitu *web* XYZ menjadi target serangan, salah satu serangan yang dapat terjadi pada sebuah *server* adalah serangan *Ddos*. Yang dimana serangan tersebut dapat mengambil data data penting yang berada dalam *web server*. Bukan hanya itu akan tetapi terdapat banyak kerugian kerugian yang kalau *web server* terdapati adanya serangan *DdoS*.".

2. Kajian Pustaka

2.1 Serangan Ddos

DDoS (Distributed Denial of Service) merupakan jenis serangan yang bertujuan menggangu hak akses pengguna jaringan yang dilakukan secara massif . Secara umum serangan *DDoS* terdiri dari beberapa jenis, serangan dengan basis bandwidth, serangan dengan basis lalu lintas jaringan, dan serangan dengan basis aplikasi. (Ridho & Arman, 2020)

2.2 Topologi Jaringan

Topologi jaringan merupakan sebuah desain tentang bagaimana sebuah komputer dan perangkat teknologi lainnya saling terhubung. Konsep dasar topologi jaringan adalah *point to point*, kemudian berkembang menjadi multipoint dimana nama topologi disasarkan pada

bentuk jaringan yang terhubung. Topologi jaringan disesuaikan dengan kebutuhan dan sumberdaya yang digunakan, beberapa jenis topologi adalah *bus, ring, star, star, tree,* dan *mesh*.(Nindyasari & Ghozali, 2018)

2.3 Arsitektur Jaringan

Arsitektur Jaringan terdiri dari perkabelan, topologi, media metoda akses dan format paket. Arsitektur yang umum digunakan dalam jaringan adalah berbasis kabel elektrik, melalui perkembangan teknologi optik kini banyak digunakan juga serat kabel optik sebagai media alternatif beserta kelebihan dan kekurangannya.(Diyas Bellia Putri et al., 2024)

2.4 *Web Server*

Web Server atau yang bisa juga disebut server web adalah perangkat lunak dalam server yang mempunyai fungsi untuk menerima permintaan halaman *web* melalui protokol HTTP dan HTTPS dari *client* yang dikenal dengan sebutan *browser*, setelah itu mengirimkan kembali hasil permintaan yang telah dilakukan sebelumnya dalam bentuk halaman web yang berbentuk sebuah dokumen HTML.(Ridho & Arman, 2020)

2.5 *Server*

Server adalah sebuah komputer yang digunakan sebagai pusat data didalam sebuah jaringan, didalam *server* sendiri menyediakan *service* atau layanan yang dapat digunakan oleh komputer *client* yang terhubung pada jaringan yang sama dengan *server*. Layananan *server* seperti web *server*, *mail server*, *proxy server* dan *database server*.(Sunanto et al., 2021)

2.6 Web

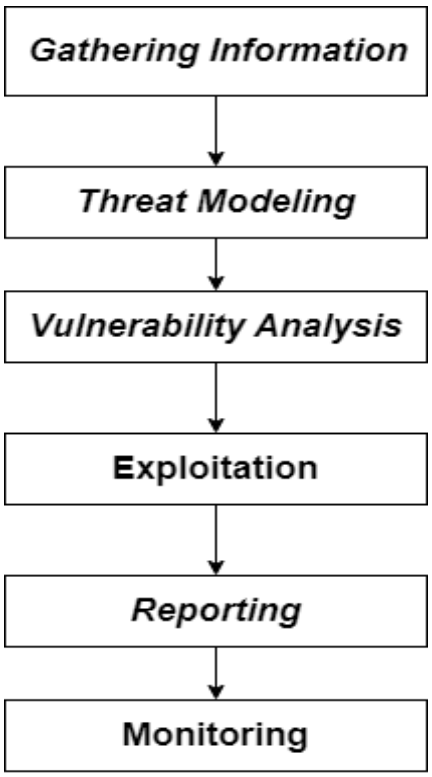
Menurut Rahmat pengertian *website* adalah suatu kumpulan dari *hyperlink* untuk menuju dari alamat satu ke alamat yang lainnya mnggunakan Bahasa HTML *(Hypertext Markup Language)*.(Ambarsari et al., 2021)

2.7 *Wazuh*

Wazuh merupakan perangkat berbasis *Open Source* yang berfungsi sebagai sistem deteksi intrusi berbasis *host (endpoint). Wazuh* melakukan analisis *log*, pemeriksaan integritas, pemantauan registri *Windows*, deteksi *rootkit*, peringatan berbasis waktu, dan *respons* aktif. *Wazuh* merupakan perangkat yang menyediakan fitur visibilitas keamanan yang lebih dalam ke sebuah infrastruktur dengan memantau *host* pada sistem operasi dan juga pada tingkat aplikasi.(Fitri Nova et al., 2022)

2.8 *Penetration Testing*

Penetration Testing, atau pentesting merupakan simulasi serangan nyata untuk menilai risiko yang terkait dengan potensi pelanggaran keamanan. penguji tidak hanya menemukan kerentanan yang dapat digunakan oleh penyerang tetapi juga mengeksploitasi kerentanan, untuk menilai apa yang mungkin didapat oleh penyerang setelah eksploitasi sukses.(Azis & Fattah, 2019)



Gambar 1 Alur

2.9 *Loic*

Loic. *Loic* (*Low Orbit Ion*) merupakan sebuah *tools* atau aplikasi yang berfungsi untuk melumpuhkan *server* sebuah situs website dengan mengirimkan *packet* sebanyak mungkin sesuai dengan kemauan si penyerang ke komputer *server* yang ditujuh melalui *domain* atau *ip server* komputer target. (Umar & Prasetyo Marsaid, 2023b). Bentuk penyerangan tujuan dimana *Loic* sebagai *tools attacking* adalah sebelum penyerangan model sistem penyerangan yang bersifat sistem *Open Source* yang dijalankan dengan membuka domain *IP* yang dituju sehingga keluarlah *port-port* yang terbuka yang akan diserang dengan menggunakan *DDoS* pada *tools* sebagai *attakcing* untuk *meflooding* dengan jumlah paket yang akan diserang pada target. Jaringan *LAN* dan *Wireless* sehingga yang mudah terscan *port-port* pada hasil yang sudah diuji pada suatu jaringan menggunakan *tools Loic* sebagai alat dimana untuk *mendownkan*/*memfloodingkan* sebuah *firewall* pada jaringan internet sehingga tidak bisa digunakan untuk akses internet dan akan mempengaruhi kerja *computer*.(Umar & Prasetyo Marsaid, 2023a)

2.10 *Slowloris*

Slowloris adalah serangan yang sangat bertarget, memungkinkan satu *server web* untuk menjatuhkan *server* lain, tanpa mempengaruhi layanan atau *port* lain di jaringan target. *Slowloris* melakukan ini dengan menahan sebanyak mungkin koneksi ke *server* web target selama mungkin. Serangan ini menyelesaikan masalah dengan membuat koneksi ke *server* target, tetapi hanya mengirim sebagian permintaan. *Slowloris* terus-menerus mengirim lebih banyak *header HTTP*, tetapi tidak pernah menyelesaikan permintaan. *Server* yang ditargetkan membuat setiap koneksi palsu ini tetap terbuka. Ini akhirnya meluap karena kumpulan koneksi bersamaan maksimum, dan mengarah pada penolakan koneksi tambahan dari klien yang sah.(Gregorius Hendita, 2022)

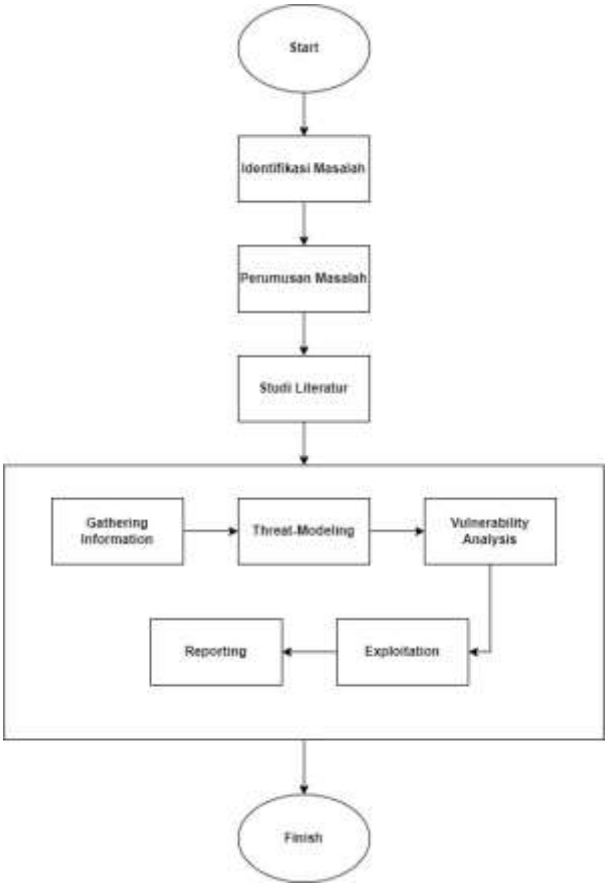
2.11 *Kali linux*

Kali linux adalah salah satu distribusi *Linux* tingkat lanjut untuk *Penetration Testing* dan audit keamanan. *Kali Linux* merupakan pembangunan Kembali *BackTrack Linux* secara sempurna, mengikuti sepenuhnya kepada standar pengembangan keamanan,(Rusdi & Prasti, 2019)

3. Metode

3.1 Kerangka Penelitian

Adapun kerangka penelitian yang akan dilaksanakan terdapat di gambar 3.1 sebagai berikut:



Gambar 2 Kerangka Penelitian

3.4 Identifikasi Masalah

Pada indentifikasi masalah peneliti melakukan kegiatan terkait penelitian yang ada dalam latar belakang permasalahan untuk menemukan jalan keluar penyelesaian masalah yang terjadi pada penelitian tersebut

3.5 Perumusan Masalahan

Pada perumusan masalah peneliti melakukan tahap pengkajian terhadap objek penelirian agar penelitian dapat di laksanakan.

3.6 Studi Literatur

Pada studi literatur peneliti mengumpulkan sumber sumber atau referensi jurnal yang bersangkutan dengan topik yang di kaji oleh penulis seperti buku, jurnal, artikel dan lain

sebagainya. Oleh ksrena itu dapat membantu peneliti untuk menyelesaikan penelitian.

3.7 *Gathering Information*

Menganalisis sumber informasi yang tersedia secara bebas, suatu proses yang dikenal sebagai pengumpulan intelijen sumber terbuka (OSINT). Anda juga mulai menggunakan alat seperti pemindai *port* untuk mendapatkan ide tentang sistem apa yang ada di Internet atau jaringan internal serta perangkat lunak apa yang sedang berjalan

3.8 *Threat-modeling*

Di sini berpikir seperti penyerang dan mengembangkan rencana serangan berdasarkan informasi yang dapat dikumpulkan. Sebagai contoh, jika klien mengembangkan perangkat lunak berpemilik, penyerang dapat merusak organisasi dengan mendapatkan akses ke sistem pengembangan internal mereka, di mana kode sumber dikembangkan dan diuji, dan menjual rahasia dagang perusahaan kepada pesaing. Berdasarkan data yang Pentester temukan selama pengumpulan informasi, Pentester mengembangkan strategi untuk menembus sistem klien.

3.9 *Vulnerability Analysis*

Selanjutnya, penulis mulai aktif menemukan kerentanan untuk menentukan seberapa sukses strategi mengeksploitasi mereka. Kegagalan yang gagal dapat merusak layanan, memicu peringatan deteksi gangguan, dan sebaliknya merusak peluang Anda untuk mengeksploitasi yang sukses. Seringkali selama fase ini, penulis menjalankan pemindai yang disini menggunakan *wazuh*.

3.10 *Exploitation*

Sekarang tahap ini menjalankan eksploitasi terhadap kerentanan yang penulis temukan (menggunakan sefangan *DdoS*) dalam upaya untuk mengakses sistem klien.

3.11 *Reporting*

Gambar 3 Alur penyerangan

Fase terakhir dari pengujian adalah pelaporan. Di sinilah penulis menyampaikan temuan kepada pelanggan dengan cara yang berarti. *Pentester* memberi tahu mereka apa yang mereka lakukan dengan benar, di mana mereka perlu meningkatkan postur keamanan dari *WEB* XYZ.

4. Hasil dan Pembahasan

4.1 Hasil Pengumpulan data

Peneliti ini melakukan pengumpulan data dengan cara mengidentifikasi masalah dan mencari lieratur perihal serangan yang masih sering di gunakan dalam hal penyerangan jaringan.

4.2 Spesifikasi Perangkat

Dalam penelitian ini penulis di bantu dengan perangkat pembatu seperti perangkat keras serta perangkat lunak diantaranya :

Tabel 4. 1 Perangkat keras

No	Perangkat keras	spesifikasi
1	Laptop	*Procesor Intel Core i3* Ram 4GB SSD 256GB

Tabel 4. 2 Perangkat Lunak

No	Persangkat lunak	Versi
1	*Kali Linux*	2024.2
2	*Wazuh*	4.8.0

4.3 Studi Literatur

Peneliti mengumpulkan beberapa literatur yang bersangkutan dengan apa yang akan dibahas dalam penelitian ini, dimana beberapa literatur membantu dalam penyelesaian penelitian dan sangat menunjang berjalannya sebuah penelitian.

4.4 *Gathering Information*

Pada tahap ini adalah dimana penulis melakukan kerentanan yang dapat di ambil dari target dengan cara *scanning* untuk melihat informasi yang terbuka, dengan perintah “nmap (IP Target).

Lalu dapat di lihat setelah melakukan perintah pada tahap tersebut seperti pada table :

Tabel 4. 3 Port Yang terbuka

No.	PORT	STATUS	SERVICE
1	21/tcp	OPEN	ftp
2	25/tcp	OPEN	Smtp
3	80/tcp	OPEN	http
4	110/tcp	OPEN	Pop3

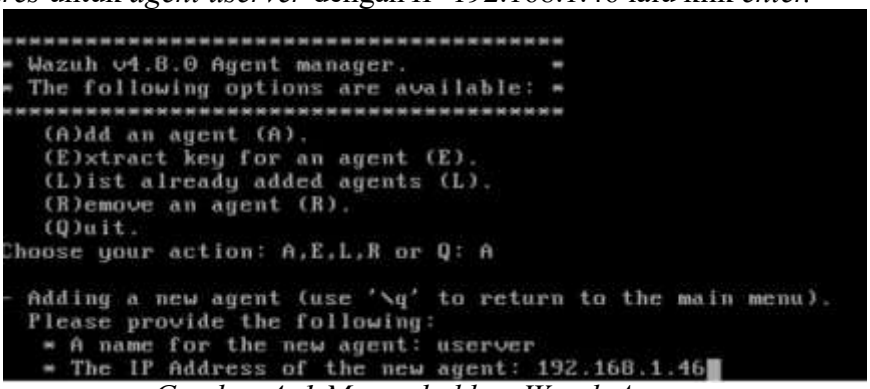
No.	PORT	STATUS	SERVICE
5	143/tcp	OPEN	Imap
6	443/tcp	OPEN	https
7	465/tcp	OPEN	Smtps
8	587/tcp	OPEN	Submission
9	993/tcp	OPEN	Imaps
10	995/tcp	OPEN	Pop3s
11	3306/tcp	OPEN	mysql

4.5 *Threat-Modeling*

Setelah penulis menentukkan perangkat lunak dalam mendukung penelitian ini lalu penulis melakukan simulasi penyerangan terhadap *Ubuntu Server* untuk mendapatkan informasi tabel apa saja yang ada pada *Ubuntu Server*. Dalam penelitian kali ini yang akan mensimulasikan sebagai pelaku penyerangan yaitu penulis.

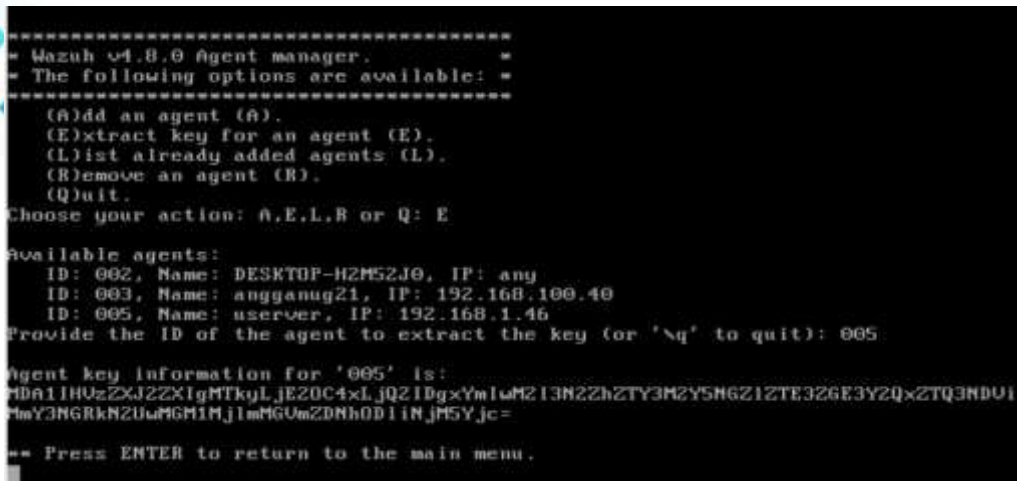
1. Menambahkan *wazuh agent*

   Setelah masuk ke dalam *wazuh ova* dengan masuk menggunakan *username* dan *password* setelah itu masuk ke directory/var/ossec/bin/manage_agents lalu seperti apa yang di tampilkan pada gambar di bawah, setelahnya ketik A agar *agent* dapat di tambahkan, setelah itu masukkan nama agent baru seperti *userver*. Masukkan *IP Addres* untuk *agent userver* dengan *IP* 192.168.1.46 lalu klik *enter.*



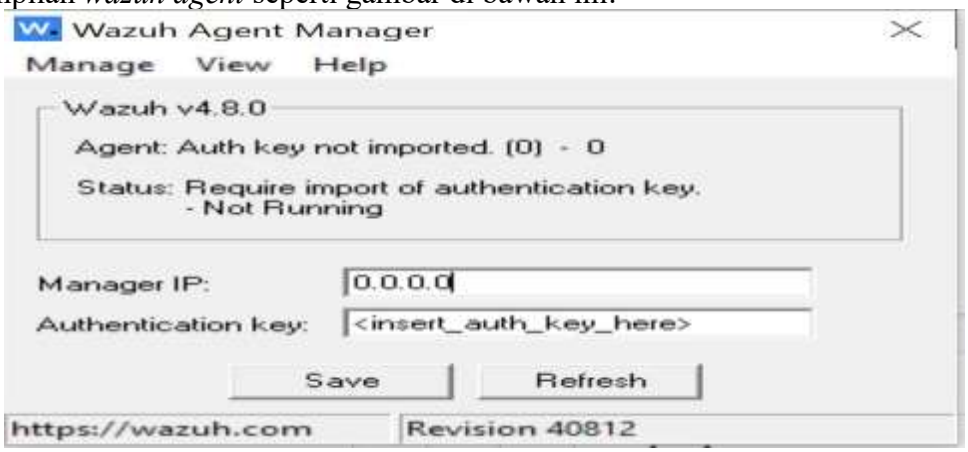
Gambar 4. 1 Menambahkan Wazuh Agent

Setelah menambahkan *agent* baru lalu ketik E perintah tersebut untuk menampilkan *list agent* yang baru di tambahkan. Lalu ketik *ID* untuk agent yang baru di tambahkan seperti contoh pada gambar di bawah dengan mengetik (005) maka akan muncul *key information* untuk menambahkan *key authentication* pada aplikasi *wazuh agent* yang terpisah.



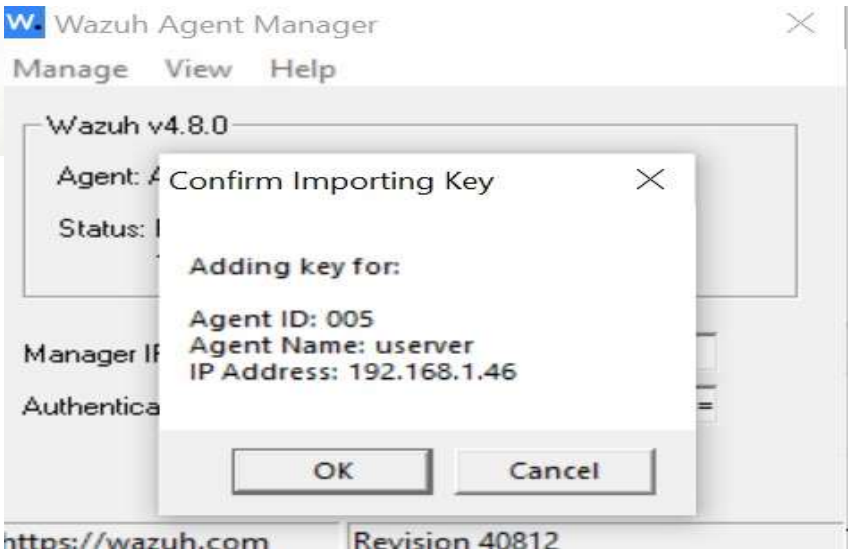
Gambar 4. 2 Menampilkan List Agent

Tampilan *wazuh agent* seperti gambar di bawah ini:



Gambar 4. 3 Tampilan Menambahkan Wazuh Agent

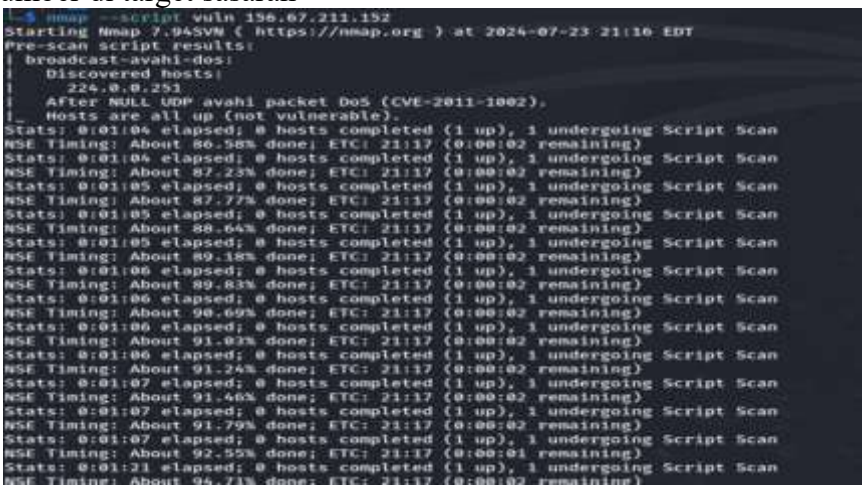
Langkah berikut masukkan *IP* ke dalam *ubuntu server* dengan *IP* 192.168.1.46 dan masukkan *key information* seperti pada gambar 4.2 Langkah berikutnya ketika tampilan sudah seperti gambar yang di bawah lalu tekan OK dan buka *localhost* pada *chrome* dengan memasukkan *IP wazuh ova* yaitu 192.168.1.47



Gambar 4. 4 Key Information

4.6 Vulnerability Analysis

Pada tahap ini penulis melakukan kegiatan mendalami sumber informasi yang dapat di ambil dari target serangan dengan cara melakukan perintah nmap –script vuln 156.67.211.152 yang Dimana sebagai berikut adalah gambar yang dapat penulis ambil sebagai sumber di target sasaran



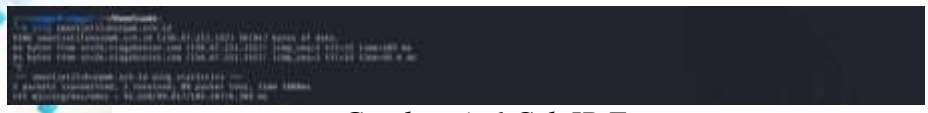
Gambar 4. 5 Mendalami Informasi

4.7 Exploitation

Dalam tahap penyerangan pada WEB penulis melakukan penyerangan mandiri terhadap targert web yang menjadi uji coba dalam melakukan penelitian ini yaitu pada web XYZ.

Hasil Penyerangan Dalam hasil penyerangan disini penulis menggunakan 2 *tools* untuk melakukan jenis serangan *Ddos* yaitu menggunakan *loic* dan menggunakan *slowloris.* Berikut untuk melakukan tahapan penyerangan.

1) Cek IP Addres pada website dengan menggunakan perintah ping sman1jatiluhurpwk.sch.id

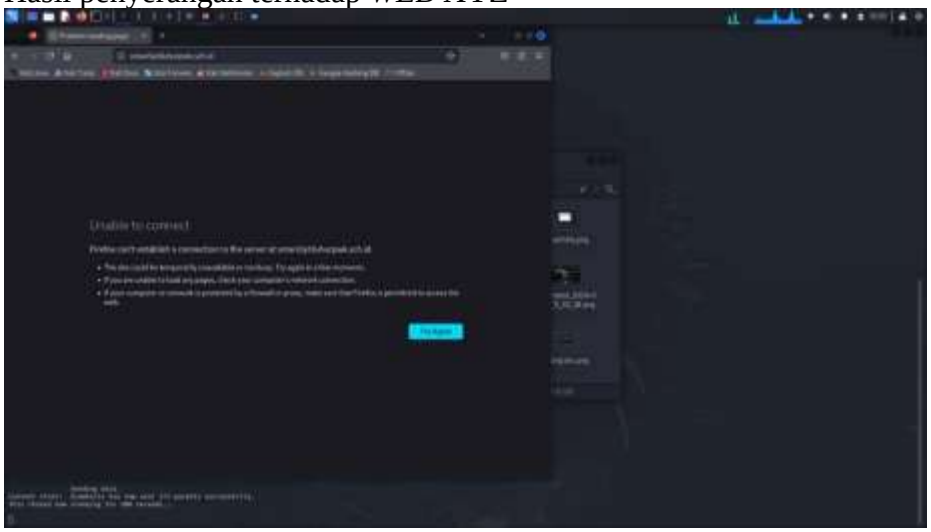


Gambar 4. 6 Cek IP Target

2) Tahap penyerangan terhadap target *WEB*
Dengan menggunakan perintah perl slowloris.pl -dns 156.67.211.152 dengan *tools slowloris*

Gambar 4. 7 Tahap Penyerangan Slowloris ke target

3) Hasil penyerangan terhadap *WEB* XYZ



Gambar 4. 8 Hasil Penyerangan Slowloris

4) Melakukan penyerangan dengan *tools loic*, untuk membuka aplikasi *loic* menggunakan perintah sudo mono LOIC.exe

Gambar 4. 9 Membuka Aplikasi Loic

5) Setelah di buka aplikasi *LOIC* lalu memasukkan halaman *URL* dan memasukan *IP* target dengan tujuan serangan di *port* 21 TCP

Gambar 4. 10 Memasukkan IP Target

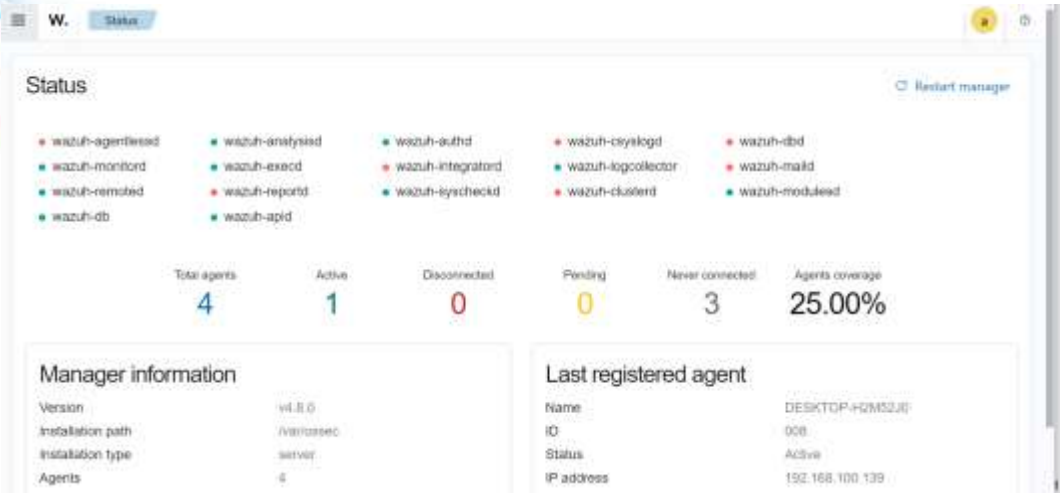
6) Dalam penyerangan berhasil dan halaman web tidak dapat di akses seperti gambar berikut

Gambar 4. 11 Hasil Menggunakan *Loic*

4.8 Hasil Wazuh

Dalam hasil monitoring *wazuh* terhadap XYZ terdapat beberapa hasil yang di antaranya seperti pada uraian berikut.

1) Terdapat seperti gambar di bawah bahwasannya terdapa 4 *agent* yang telah di tambahkan, dan yang telah aktif hanya 1 *agent* dan sisa 3 *agent* lainnya *never connected* serta *agent coverage* terdapat di angka 25.00%



Gambar 4. 12 Gambar hasil wazuh

2) Untuk gambar yang di tampilkan di bawah terdeteksi 396 *hits* seperti yang di tampilkan pada gambar tersebut yang dimana *hits* itu adalah sebuah upaya percobaan masuk ilegal ke sistem. Akan tetapi grafik dari *wazuh* tidak tampil ada kemungkinan di akibatkan kerentanan terdeteksinya terlalu rendah.

Gambar 4. 13 Hasil grafik wazuh

5. Kesimpulan

Pada tahap penelitian ini dapat di simpulkan untuk penyerangan yang di lakukan penulis kepada target *web* dapat di pastikan berhasil, pada tahap monitoring menggunakan *wazuh dashboard* penulis juga terdapat hasil yang dapat di ambil akan tetapi akibat lemahnya kerentanan maka dari itu grafik yang terdapat di wazuh tidak muncul seperti pada gambar 4.13 yang di mana dapat terdeteksi jumlah paket penyerangan yang masuk ke dalam *web* target yaitu sebesar 396 *hits.*

6. Daftar Pustaka

Ainy, M. (2019). *Mengenal IP Address Versi 4*. 1–7.

Ambarsari, L. S., Puspitasari, W., & Syahrina, A. (2021). Perancangan Modul Landing Page Dan Pembayaran Pada WebsitePahamee Tentang Kesehatan Mental Menggunakan Metode Extreme Programming. *E-Proceeding of Engineering*, *8*(5), 9639.

Anggraeni, I., & Akhmad, D. M. (2022). Detection and Classification of DDos Attack on

Software Defined Network. *Komputasi: Jurnal Ilmiah Ilmu Komputer Dan Matematika*, *19*(2), 77–86. https://doi.org/10.33751/komputasi.v19i2.4769

Azis, H., & Fattah, F. (2019). Analisis Layanan Keamanan Sistem Kartu Transaksi Elektronik Menggunakan Metode Penetration Testing. *ILKOM Jurnal Ilmiah*, *11*(2), 167–174. https://doi.org/10.33096/ilkom.v11i2.447.167-174

Desmira, D., Apriana, D., & Avicena H.B.H, M. (2022). Analisa Jaringan Local Area Network Pada Laboratorium Komputer SMK Informatika Kota Serang. *INSANtek*, *3*(1), 23–31. https://doi.org/10.31294/instk.v3i1.532

Diyas Bellia Putri, M.Nabil Makarim, Gunawan, M. Rosyid Ridho, & Didik Aribowo. (2024). Analisis Arsitektur Jaringan Pada Topologi Bus. *Teknik Informatika Dan Terapan*, *2*, 3.

Firman Pratama, N. (2023). Perancangan Sistem Deteksi Dini Keamanan Informasi DISKOMINFO Kabupaten Bandung. *Jurnal Teknik Informatika Dan Sistem Informasi*, *10*(1), 808–820. http://jurnal.mdp.ac.id

Fitri Nova, Pratama, M. D., & Prayama, D. (2022). Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, *3*(1), 1–7. https://doi.org/10.30630/jitsi.3.1.59

Gregorius Hendita. (2022). Sistem Firewall untuk Pencegahan DDOS ATTACK di Masa Pandemi Covid-19. *Journal of Informatics and Advanced Computing* , *3*(1), 52–56. https://journal.univpancasila.ac.id/index.php/jiac/article/view/3853

Nindyasari, R., & Ghozali, M. I. (2018). Analisis Quality of Service Untuk Memonitoring Kondisi Topologi Jaringan X. *Terakreditasi DIKTI*, *2*(2), 109–113.

Rasheed, M. M., Faieq, A. K., & Hashim, A. A. (2021). Development of a new system to detect denial of service attack using machine learning classification. *Indonesian Journal of Electrical Engineering and Computer Science*, *23*(2), 1068–1072. https://doi.org/10.11591/ijeecs.v23.i2.pp1068-1072

Ridho, M. A., & Arman, M. (2020). Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *9*(3), 373–379. https://doi.org/10.32736/sisfokom.v9i3.945

Rusdi, M. I., & Prasti, D. (2019). Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux. *Seminar Nasional Teknologi Informasi Dan Komputer 2019*, 260–269.

Sunanto, S., Firdaus, R., & Makmur Setiawan Siregar. (2021). Implementasi Logika Fuzzy Mamdani Pada Kendali Suhu dan Kelembaban Ruang Server. *Jurnal CoSciTech (Computer Science and Information Technology)*, *2*(2), 128–136. https://doi.org/10.37859/coscitech.v2i2.3362

Susilo, I., & Kristiyanto Nugraha, G. (2013). Pembangunan Web Server Mengunakan Debian Server Untuk Media Pembelajaran Di Sekolah Menengah Kejuruan (Smk) Negeri 1 Sragen. *Indonesian Jurnal on Networking and Security (IJNS)-Ijns.Org IJNS*, *2*(1), 2302–5700. http://kuis.smkn1srg.sch.id

Umar, R., & Prasetyo Marsaid, A. (2023a). Analisis Keamanan Jaringan LAN Terhadap Kerentanan Jaringan Ancaman DDoS Menggunakan Metode Penetration Testing`. *Jurnal Riset Komputer)*, *10*(1), 2407–389. https://doi.org/10.30865/jurikom.v10i1.5835

Umar, R., & Prasetyo Marsaid, A. (2023b). Analisis Keamanan Jaringan LAN Terhadap Kerentanan Jaringan Ancaman DDoS Menggunakan Metode Penetration Testing. *Jurnal Riset Komputer)*, *10*(1), 2407–389. https://doi.org/10.30865/jurikom.v10i1.5835