Journal of Information Technology Ampera
Vol. 4, No. 1, 2023 e-ISSN: 2774-2121
https://journal-computing.org/index.php/journal-ita/index

Pemodelan *Instrusion Prevention System* Untuk Pendeteksi Dan Pencegahan Penyebaran Malware Menggunakan Wazuh

Denny Purwa Widyantono[1],Wiwin Sulistyo[2]

[1]Program Studi Teknik Informatika, Universitas Kristen Satya Wacana, Salatiga,Indonesia
Email: [1]672016058@student.uksw.edu, [2]Wiwinsulistyo@uksw.edu

Abstrak

Keamanan jaringan adalah bagian terpenting dalam setiap jaringan komputer. Didalam kehidupan manusia saat ini bergantung pada teknologi terutama jaringan komputer. Dalam suatu jaringan pemanfaatan firewall sangat penting dan penggunaannya sangat direkomendasikan yang bertujuan untuk keamanan sistem. Pada sebuah sistem firewall tidak dapat memantau traffic yang ada pada jaringan dan tidak dapat memberikan peringatan pada saat terjadi serangan. Malware merupakan program komputer atau perangkat lunak yang sengaja diciptakan untuk mencari kelemahan dan merusak software sistem operasi komputer tampa seizin dari pemilik. Tindakan yang ada pada server sangatlah penting untuk diawasi dikarenakan tindakan mencurigakan pada server bisa bertujuan untuk menyerang dan merusak informasi pada sebuah server dan dapat mengakibatkan kerugian. Intrusion Prevention System bisa mendeteksi dan menghentikan serangan-serangan yang sedang berlangsung secara responsif dengan menggunakan tools Wazuh sebagai pendeteksi dan memonitoring setiap pola ancaman terhadap komputer server, seperti msfvenom, Metasploit dan jenis serangan lainnya. Wazuh dilengkapi dengan fitur Security Analytics, Instrusion Prevention, Log Data Analysis, File Integrity Monitoring, sehingga dapat mengurangi bahkan meminimalisir serangan terhadap server dengan pendeteksi serangan yang masuk.

Kata Kunci: Sistem pendeteksi, malware, wazuh, Intrusion Prevention System

1. PENDAHULUAN

Kehidupan manusia saat ini hampir bergantung pada teknologi dan tidak bisa terlepas dari teknologi, seperti teknologi komputer. Kemajuan teknologi informasi seperti pada pengguna komputer yang meningkat dapat berdampak pada perkembangan dalam pengolahan data, dimana data akan dikirim dari tempat ke tempat melalui sarana telekomunikasi. Setiap perusahaan, sekolah, dan instansi lainnya memiliki jaringan komputer untuk mengakses dan mempermudah arus informasi [1]. Dalam perkembangan teknologi khususnya teknologi informasi, kehandalan aplikasi mutlak diperlukan untuk memenuhi kebutuhan pengguna itu sendiri. Sistem operasi yang terinfeksi perangkat lunak berbahaya dapat disusupi, membuatnya lebih rentan terhadap penyusup, virus, dan bahkan data penting

yang dicuri [2].

Aset informasi yang lemah memungkinkan pihak-pihak yang tidak berhak mengganggu kegiatan yang berkaitan dengan aset lembaga ataupun instansi. Oleh karena itu, diperlukan adanya keamanan informasi yang dapat mencegah risiko aset informasi [3]. Malware merupakan program komputer atau perangkat lunak yang sengaja diciptakan untuk mencari kelemahan dan merusak software sistem operasi komputer tampa seizin dari pemilik. Pada umumnya penyebab terjadinya malware adalah mendownload software pada tempat ilegal yang didalamnya terdapat malware [4]. Ancaman utama bagi keamanan sistem jaringan komputer pada malware mencakup virus, backdoor, worm, dan trojan horse.

Dengan adanya jenis malware, penyerang akan berusaha mencari keuntungan dari pengguna. Agar terhindar dari serangan malware pada komputer, perlu adanya kesadaran untuk mengantisipasi, mengatasi, dan menjaga malware di dalam komputer. Salah satu pencegahannya adalah dengan melakukan scanning komputer melalui antivirus secara berkala dan dengan menggunakan tools yang dapat digunakan untuk mencegah penyebarannya. Kurangnya pemahaman pengguna komputer tentang masalah keamanan sistem menjadi salah satu penyebab timbulnya masalah. Tidak jarang menemukan bahwa program antivirus komputer tidak diperbarui, atau bahkan program antivirus diinstal sama sekali. Hal ini dapat mengakibatkan komputer atau host terinfeksi malware tanpa sepengetahuan pengguna. Kemudian malware tersebut dapat menyebar ke komputer lainnya dalam jaringan, dan pada akhirnya dapat merugikan banyak pihak [5].

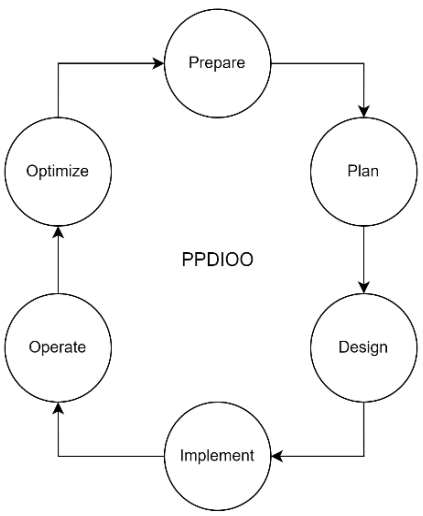
Malware dan perangkat lunak berbahaya menjadi salah satu bagian terpenting dalam bidang forensik digital. Investigator memiliki kemampuan untuk menganalisa perangkat lunak berbahaya yang menjadi tuntutan dalan setiap melakukan investigasi. Hal ini dikarenakan dengan meningkatnya jumlah malware dan evolusi serta mampu beradaptasi terhadap perangkat yang selama ini digunakan. Menurut data yang dirilis oleh G Data Security Labs pada tahun 2015 terdapat program-program berbahaya yang memiliki ancaman keamanan dan dapat berdampak pada kerugian seperti pencurian informasi [6]. Dengan adanya internet dimana menjadi tempat untuk penyebaran malware yang ditandai dengan munculnya iklan secara tiba-tiba. Agar tidak mengunjungi website yang terinfeksi malware dan untuk mencegahnya, maka beberapa program telah menyediakan toolbar khusus yang didalamnya dilengkapi kemampuan scan situs web dari hasil pencarian google [7].

Intrusion Prevention System (IPS) adalah proses pendeteksi aktivitas dan ancaman dari tindakan responsif terhadap intrusi aktifitas ancaman yang telah terdeteksi pada jaringan komputer [8].

Malware yang dideteksi yaitu DDoS dan Metasploit Attack, dimana DDoS melakukan serangan dengan mengirim paket secara terus menerus kepada jaringan komputer sedangkan Metasploit Attack memberikan fasilitas penyerang untuk melakukan serangan terhadap sistem komputer. Tindakan utama IPS adalah menghentikan serangan-serangan yang sedang berlangsung. Hal seperti ini difokuskan pada pemodelan sistem pendeteksi dan penanganan penyerangan malware dalam sebuah jaringan dengan menggunakan wazuh untuk memonitoring serangan yang masuk ke server. Wazuh adalah perangkat software yang berbasis *Open Source* dan berfungsi sebagai sistem pendeteksi intruksi berbasis host (*endpoint*). Wazuh melakukan analisis log, pemeriksaan integritas, pemantauan dan peringatan berbasis waktu, serta respons aktif. Wazuh akan mendeteksi ketika rule tidak ada di Yara Signature maka alert akan ditampilkan sebagai anomaly selanjutnya dengan ditambahkan rule yang sesuai dengan anomaly tersebut berdasarkan hasil log.

2. METODOLOGI PENELITIAN

Pada tahap metodologi penelitian ini dipaparkan tahapan yang akan dilakukan untuk perancangan. Tahapan-tahapan untuk perancangan sistem yaitu tahap persiapan, perencanaan, desain, implementasi, operasional, dan optimalisasi seperti yang ditunjukkan pada Gambar 1:



Gambar 1. Tahapan pada perancangan sistem

Tahapan-tahapan dari metode PPDIOO tersebut dapat dijelaskan seperti di bawah ini:

1. Persiapan, pada tahap awal proses yang dilakukan yaitu mempersiapkan segala kebutuhan yang akan digunakan untuk merancang sebuah sistem. Persiapan yang dilakukan yaitu mengumpulkan data log yang akan diakses dan software yang akan digunakan. Membuat flowchart yang menjelaskan alur proses penelitian.
2. Perencanaan, tahap perencanaan jaringan diidentifikasi berdasarkan tujuan, fasilitas, dan kebutuhan. Pada tahap perencanaan menggambarkan karateristik jaringan yang bertujuan melakukan penelitian dan analisis IPS sebagai sistem pendeteksi malware.
3. Desain, tahap desain dibuat flowchart dan topologi jaringan untuk proses pemodelan IPS. Desain jaringan dikembangkan sesuai persyaratan yang diperoleh dari kondisi sebelumnya, desain jaringan yang bersifat terperinci dan memenuhi persyaratan. Jaringan harus menyediakan ketersediaan dan keamanan dalam kinerja.
4. Implementasi, tahap implementasi melakukan instalasi dan konfigurasi untuk peralatan baru menurut spesifikasi desain. Kemudian mengimplementasikan dengan menggunakan peralatan *hardware* dan tool software yang dipersiapkan.
5. Operasional, setelah pengimplementasian dan desain, maka langkah selanjutnya adalah tahapan pengerjaan. Dari data yang sudah didapat sebelumnya dapat digunakan untuk merancang desain antar user. Pemodelan dari IPS ini untuk menjembatani transfer file antara server ke client dan sebaliknya. Kemudian di implementasikan dengan menggunakan Wazuh sebagai tools dari IPS.

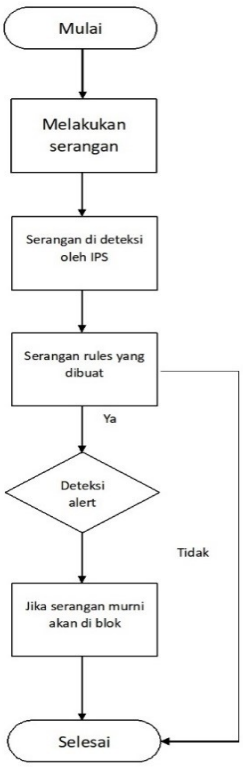
Gambar 2. Halaman Utama dan tampilan Wazuh sebagai tools IPS

Platform *Open Source* Wazuh yang berfungsi sebagai sistem pendeteksi ancaman seperti Gambar 2. Informasi aktifitas yang dilakukan oleh semua *agent* dalam rentang waktu 24 jam terakhir akan terlihat. Pada dashboard tersebut dapat melihat jumlah serangan yang masuk, *agent* yang sering aktif dan jenis serangan yang paling banyak akan dilakukan terhadap *agent* Wazuh.

6. Optimalisasi, tahap ini dilakukan optimalisasi atau testing dengan cara mentransfer data menggunakan service attack yaitu funaribillity pada sebuah server dan web aplikasi. Pengujian juga dilakukan dengan mengoneksikan antara user dengan server agar bisa mengetahui hasil log yang terkirim ke Wazuh.

3. HASIL DAN PEMBAHASAN

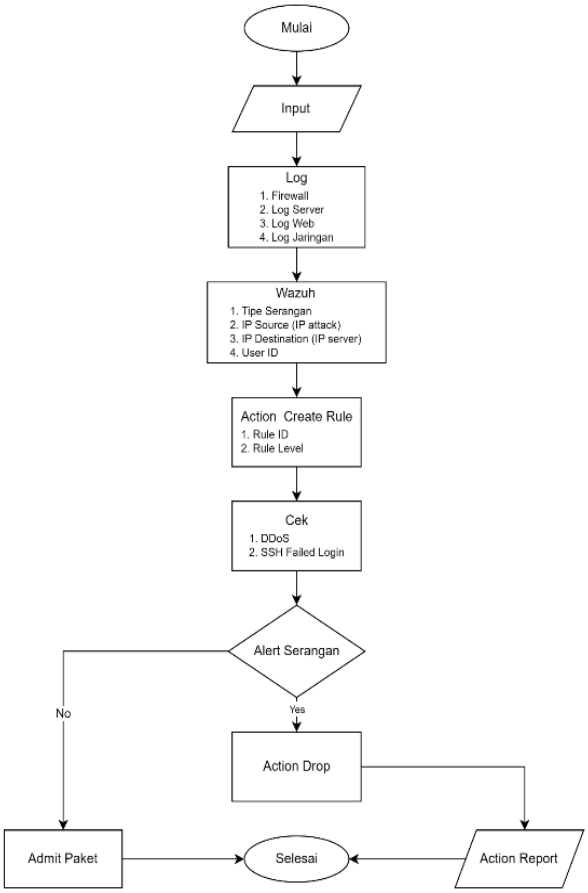
Dalam tahapan uji coba ini digunakan perangkat keras dengan spesifikasi sebagai berikut: (a) Dell Inspiron 3476, (b) Processor Intel Core i5-8250U, dan (c) RAM 8GB DDR4. Dalam perancangan sistem Intrusion Prevention System ini adapun flowchat yang dibuat seperti gambar dibawah ini :



Gambar 3. Flowchart pemodelan IPS secara umum

Pada Gambar 3 menjelaskan tentang awal dari serangan masuk hingga serangan selesai. Paket akan masuk kemudian dilakukan pengecekan dan dideteksi oleh IPS dengan dicocokkan menggunakan *rules*, apabila paket merupakan serangan atau ancaman murni akan keluar alert yang berisikan informasi dari setiap indikasi

serangan dan akan diblok oleh IPS, namun jika tidak paket serangan atau ancaman murni akan diteruskan dan selesai. Pada Gambar 5 merupakan penjabaran cara serangan yang dideteksi oleh IPS dari Gambar 4 seperti berikut :



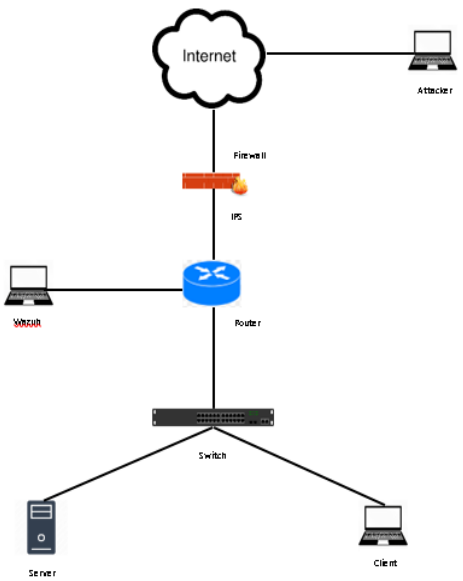
Gambar 4. Flowchart Deteksi IPS

Pada Gambar 4 menjelaskan tentang serangan masuk yang dideteksi oleh IPS, ketika serangan masuk daril log diintegrasi ke Wazuh dan log dinormalisasi dan dianalisis pola serangannya. Setelah analisis log yang belum dinormalisasi dilanjutkan menjadi log yang sudah dinormalisasi. Dari log jika kondisi sama dengan rule yang dibuat maka dari IP *network* bisa di blokir untuk mengantisipasi agar tidak terjadi serangan selanjutnya. Setelah Rule ID dibuat maka akan masuk dalam kategori, seperti DDoS misal scanning 100 record kemudian dideteksi dan akan menghasilkan alert serangan atau bukan, setelah action dilakukan di firewallnya akan didrop atau tidak kemudian diteruskan jika hasilnya *failed* atau *activity* dari user setelah melakukan percobaan. Secara sistem hasilnya akan di

drop terlebih dahulu dan secara operasionalnya setelah melihat log IP yang melakukannya kemudian menindak lanjuti ke IP *device* jika memang serangan akan dicek oleh log dan di validasi user misal serangan aktif dan melakukan login berarti serangan positif maka akan di drop dan akan menghasilkan *Action Report*, jika tidak serangan aktif atau positif maka dari alert serangan akan diijinkan selesai. Untuk melakukan tahap konfigurasi dalam perancangan memerlukan perangkat lunak agar dapat berjalan dengan baik. Perangkat lunak ini diperlukan sebagai user interface dan konfigurasi dalam perancangan. Adapun perangkat lunak yang digunakan yaitu:

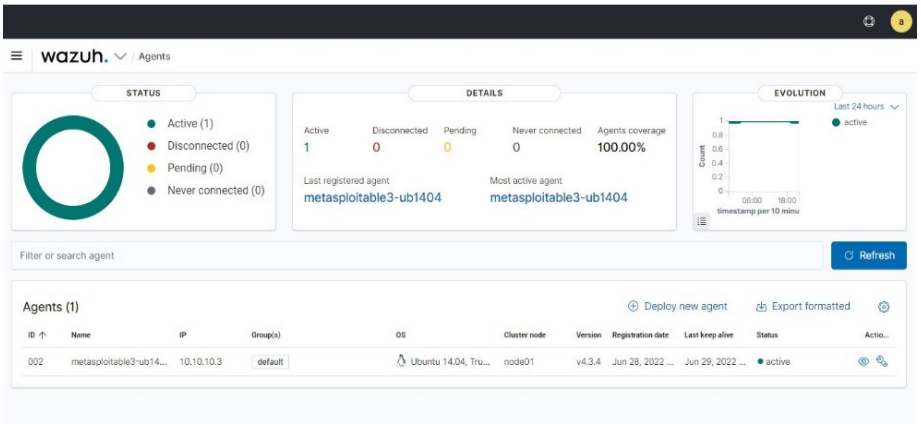
1. Wazuh merupakan perangkat lunak yang digunakan sebagai monitoring.
2. Linux Ubuntu Server dan Desktop 20.04 merupakan sistem operasi yang digunakan sebagai media Server.

Perancangan dan pengujian dilakukan dengan salah satu perangkat sebagai pusat kontrol dan sebagai server. Tahap awal dari pengujian dilakukan dengan membuat satu network yang akan digunakan sebagai penghubung antara satu perangkat dengan perangkat lainnya yaitu dengan cara membuat server di Linux Ubuntu Server. Setelah network penghubung terbuat selanjutnya masuk ke dalam jaringan dengan melakukan login sebagai admin dengan memasukkan username dan password yang sudah dibuat sebelumnya. Masuk ke halaman Wazuh dengan menggunakan ip yang sudah dibuat sebelumnya. Adapun konsep topologi yang digunakan dalam perancangan saat ini, seperti Gambar 6.



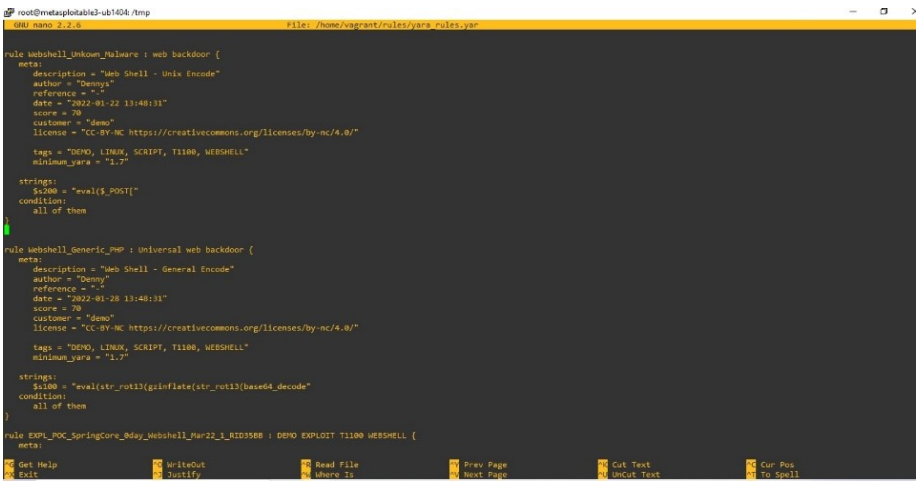
Gambar 5. Topologi Jaringan yang Digunakan

Dalam topologi seperti Gambar 5 yang nantinya akan berfungsi sebagai penyedia layanan pengontrolan file. IPS ini akan dilayani menggunakan layanan dari Wazuh yang dapat diakses oleh staf yang sedang bertugas mengawasi. Di dalam IPS server ini akan dihubungkan dengan Wazuh server, dimana nantinya setiap staf akan diberikan alamat untuk masuk ke server sehingga seluruh staf dapat menggunakan layanan yang disediakan dari IPS server.



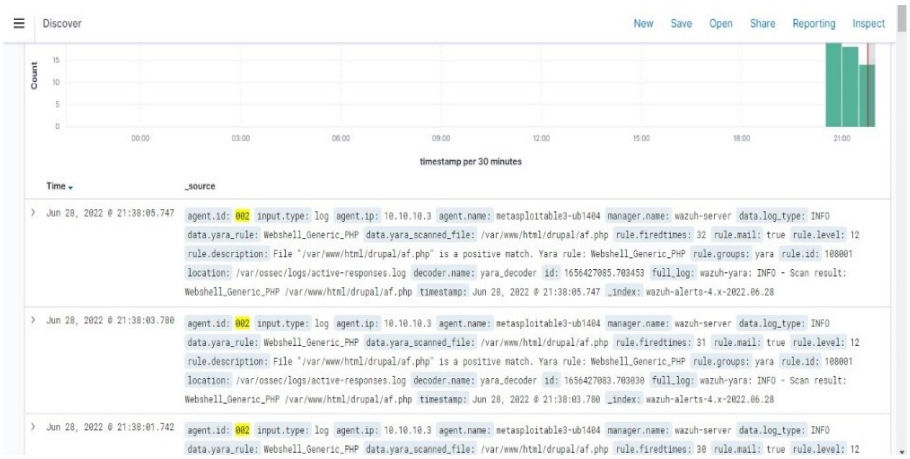
Gambar 6. Wazuh Agent Dashboard

Selanjutnya akan melakukan analisis *log* yang berhasil ditangkap Wazuh Agent. Analisis tersebut dilakukan pada halaman *Security Event* di dashboard Wazuh. Sretelah masuk, langkah berikutnya adalah masuk ke wazuh dashboard untuk mengetahui apakah username dan password sudah bisa digunakan untuk mengakses yang sudah dibuat di dalam Ubuntu Server. Setelah selesai, maka kembali lagi kedalam Ubuntu Server untuk membuat serangan agar bisa di deteksi oleh Wazuh tersebut.



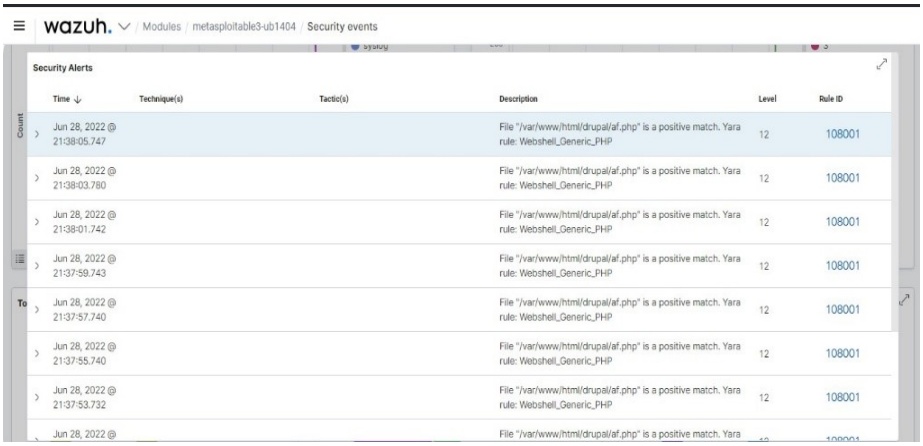
Gambar 7. Rule Webshell Malware

Rule dalam analisis *log* dibagi menjadi beberapa kategori yaitu berdasarkan dengan jumlah *alert* dan jumlah *rule group.* Jika masuk kedalam Ubuntu Server maka akan terlihat beberapa *rules* dari malware seperti pada tampilan didalam Gambar 7, dimana didalam *rules* terdapat beberapa aturan untuk mengelola lalu lintas jaringan pada server.



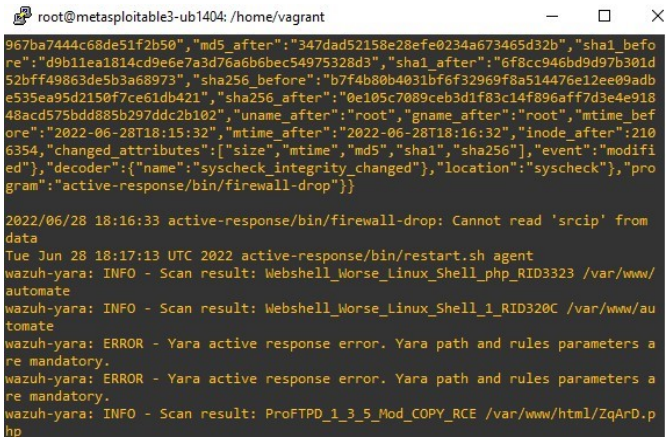
Gambar 8. Malware Alert Wazuh

Setelah selesai maka kembali masuk ke Wazuh, pada Gambar 8 merupakan peringatan dari server jika ada serangan masuk, yang sebelumnya sudah dibuat *rules*nya di Ubuntu Server. Terdapat juga beberapa peringatan-peringatan yang masuk.



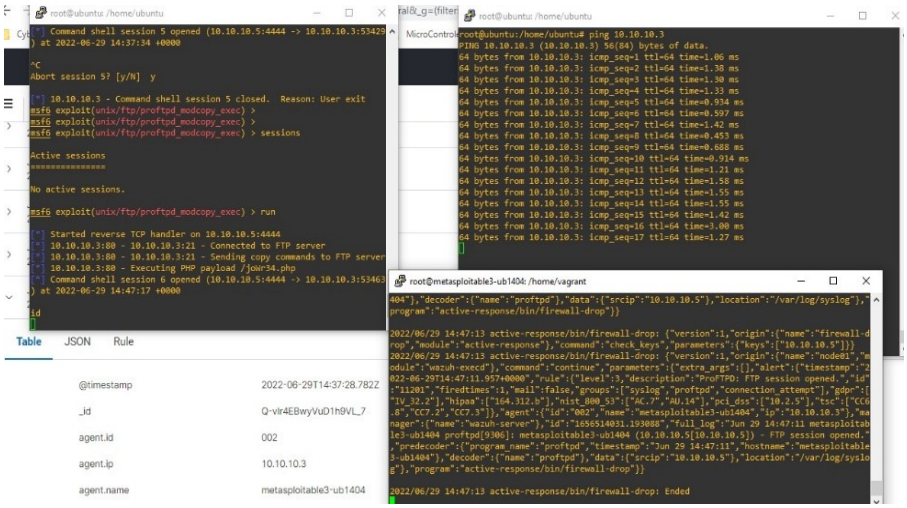
Gambar 9. Malware Dashboard

Pada Gambar 9 merupakan halaman Malware Dashboard yang terdapat Client yang terhubung ke Security Alerts dimana log, pemantauan, yara rule sudah terdaftar dan level serangan yang masuk. Semua host ubuntu dijalankan untuk mencari popularitas yang menghasilkan kesalahan.



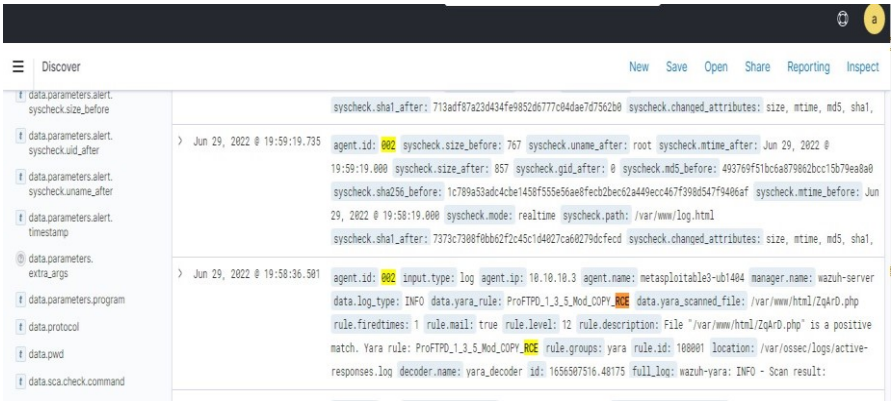
Gambar 10. Active Respon Log Ftp Malware

Pada Gambar 10 merupakan konfigurasi Active Respon Ftp yang dapat dieksekusi dengan hash yang ditambahkan ke file untuk pemeriksaan integritas.



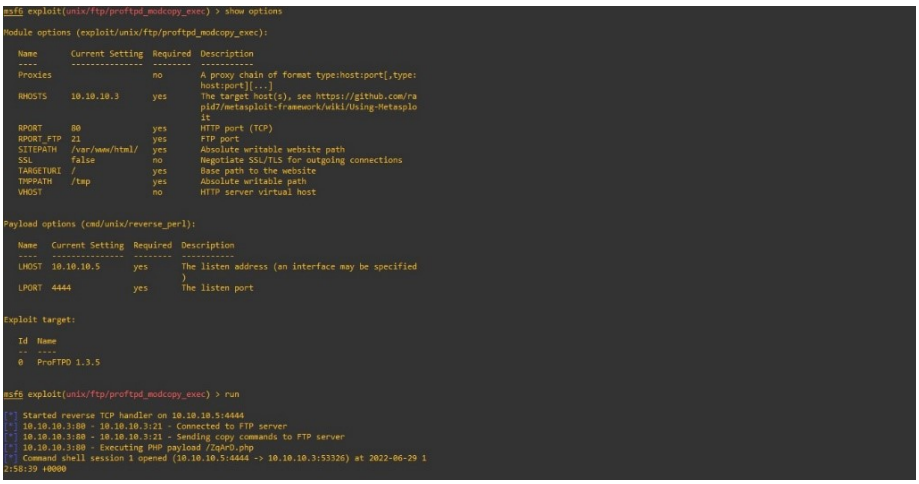
Gambar 11. Firewall Drop

Dalam Gambar 11 terdapat firewall drop dimana *session* IP di lakukan *test ping* dan disitulah *active response* aktif yang digunakan untuk pengontol sekaligus pengawas arus paket data. Firewall drop juga bisa digunakan untuk menyaring, membatasi, atau menolak semua aktivitas dan bekerja otomatis sesuai kriteria dari alamat IP.



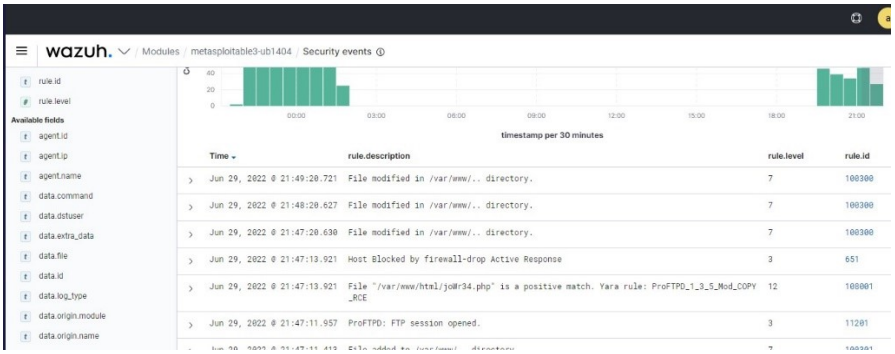
Gambar 12. Log di Wazuh

Pada Gambar 12 Wazuh agent membaca sistem operasi dan log yang digunakan untuk memantau file konfigurasi dan memastikan apakah sudah sesuai dengan standar pada sistem Security Framework untuk melakukan pemindaian dan mendeteksi aplikasi yang diketahui rentan atau tidak dikonfigurasi dengan aman.



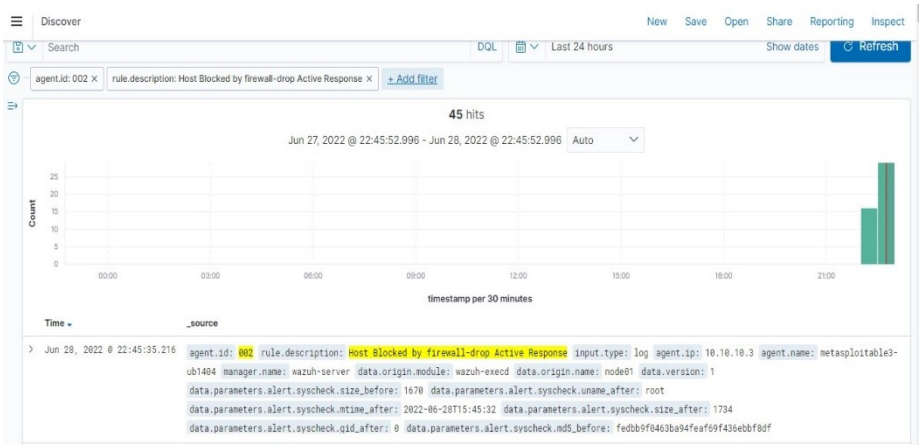
Gambar 13. Metasploit attack

Pada Gambar 13 Metasploit attack memilih dan mengkonfigurasi kode yang memasuki target dengan mengirimkan *alert* sehingga Intrusion Prevention System (IPS) mengabaikan muatan data yang di encoding dengan tujuan untuk melancarkan aksi yang tidak diinginkan.



Gambar 14. Wazuh Dashboard Block

Kemudian mauk ke dalam Wazuh Dashboard Blok seperti pada Gambar 14 yang digunakan untuk mengetahui apakah status rule description dari host yang sudah terblok oleh active response. Jika sudah maka pada bagian rule description akan muncul keterangan bahwa *Host* sudah terblok oleh firewall-drop Active Response. Setelah di blok pada rule level akan muncul angka 3 yang artinya berhasil atau diizinkan. Di dasbor Wazuh lansiran muncul karena rule id 651 adalah bagian dari file aturan default */var/ossec/ruleset/rules/0015-ossec_rules.xml* di server Wazuh.

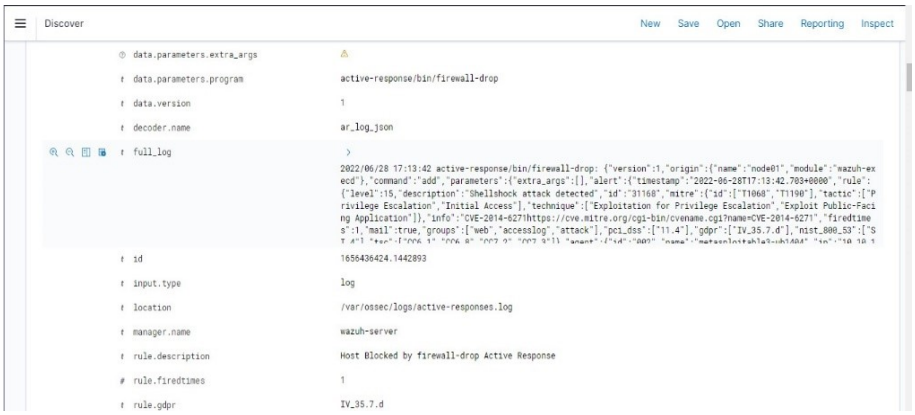


Gambar 15. Web Malware IPS Bloked

Pada Gambar 15 merupakan discover dari wazuh dimana di dalamnya terdapat status atau deskripsi tentang host yang telah di blok setelah melakukan konfigurasi di server.

Gambar 16. Web Malware IPS Dashboard

Pada Gambar 16 merupakan tampilan Security Log menggunakan open source Wazuh, aplikasi yang akan mendeteksi lalu lintas berbahaya dari alamat IP sumber yang ditunjukkan dan mengumpulkan, mengindeks, menganalisis data keamanan serta membantu security admin mendeteksi intrusi ancaman dengan Active Response.



Gambar 17. Log Attack

Pada Gambar 17 terdapat tampilan output dari hasil pendeteksi serangan dari dashboard dan log yang dihasilkan. Log dibaca oleh sistem operasi dan log aplikasi dibantu dengan rule Wazuh untuk mengetahui kesalahan aplikasi atau sistem dan juga kesalahan konfigurasi.

4. KESIMPULAN

Dari penelitian yang dilakukan, maka didapatkan sebuah kesimpulan bahwa IPS dapat menjalankan tugasnya dengan memanfaatkan jaringan internet yang sudah terhubung dan dijalankan di dalam Wazuh yang dapat diterapkan sebagai server dan dapat digunakan sebagai pendeteksi jika ada malware yang masuk. Ketika rule tidak ada pada *action* maka alert akan ditampilkan sebagai anomaly selanjutnya yang ditambahkan pada rule sesuai dengan anomaly berdasarkan hasil log. Dengan penerapan wazuh ini dapat melakukan monitoring servis *file integrity* sensor dengan menggunakan Wazuh *Agent* untuk mengirim semua *log* ke Wazuh Server dan memonitoring servis file integriti. Wazuh secara fungsional cukup untuk digunakan dalam memantau aktifitas *event* keamanan dan menambah vivibilitas pada aset teknologi informasi. Wazuh manager mendapat beberapa informasi berupa log mengenai aktifitas yang dilakukan oleh *Agent* dan log tersebut dapat divisualisasikan oleh Wazuh dengan beberapa bentuk statistik. Untuk mendeteksi adanya malware berbahaya diperlukan integritas antara Wazuh manager, IPS dapat mendeteksi adanya serangan kemudian *alert* diteruskan Wazuh dan akan ditampilkan pada web interface Wazuh.

REFERENSI

[1] A. Tedyyana, "Perancangan Sistem Pendeteksi Dan Pencegahan Penyebaran Malware Melalui SMS Gateway," pp. 1–7, 2018.
[2] I. Hariman and A. Syams, "Analisis Malware Dengan Teknik Static Analysis," 2015.
[3] T. Kristanto, M. Sholik, D. Rahmawati, and M. Nasrullah, "Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001 : 2005 Pada Staff IT Support Di Instansi XYZ," vol. 02, no. 02, pp. 1–4, 2019.
[4] T. A. Cahyanto, V. Wahanggara, and D. Ramadana, "Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis," *Justindo, J. Sist. Teknol. Inf. Indones.*, vol. 2, no. 1, pp. 19–30, 2017, [Online]. Available: http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO/article/view/1037.
[5] P. Studi, T. Informatika, and F. Teknik, "MENGGUNAKAN DIONAEA (Malware Detection in the Network Using Dionaea) Harjono," vol. 14, no. 2, pp. 64–69, 2013.
[6] A. H. Muhammad, B. Sugiantoro, A. Luthfi, M. Teknik, I. Universitas, and I. Indonesia, "Metode Klasifikasi Dan Analisis Karakteristik Malware Menggunakan Konsep Ontologi," no. 1, 2004.
[7] CSIRT, "Panduan Penanganan Insiden Keamanan Jaringan," pp. 1–49, 2015.

[8] R. A. Yunmar, "Intrusion Prevention System Untuk Aplikasi Berbasis Web," Ubiquity, vol. /, pp. 2–4, 2010.

[9] 14) M. Nurul, H. Monoarfa, X. B. N. Najoan, A. A. E. Sinsuw, and J. T. Elektro-ft, "Analisa Dan Implementasi Network Intrusion Prevention System Di Jaringan Universitas Sam Ratulangi," J. Tek. Elektro dan Komput., vol. 5, no. 4, pp. 34–45, 2016.

[10] F. G. N. D. Setiawan, R. M. Ijtihadie, and H. Studiawan, "Pendeteksian Malware pada Lingkungan Aplikasi Web dengan Kategorisasi Dokumen," J. Tek. ITS, vol. 6, no. 1, 2017, doi: 10.12962/j23373539.v6i1.22163.

[11] W. W. Purba and R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," Aiti, vol. 17, no. 2, pp. 143–158, 2021, doi: 10.24246/aiti.v17i2.143-158.

[12] N. Iryani, A. D. Ramadhani, and Q. P. Ramadhani, "Analisis Performansi Data Plane Development Kit Terhadap Open Virtual Switch pada Jaringan Virtual," JTERA (Jurnal Teknol. Rekayasa), vol. 6, no. 1, p. 93, 2021, doi: 10.31544/jtera.v6.i1.2021.93-100.

[13] E. Carter, et al, 2006, "Intrusion Prevention Fundamentals : an introduction to network attack mitigation with IPS", Cisco press.

[14] K. Husnul, B. Fitri, K. S. Robert, W. K. B. Ida, "IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) PADA APLIKASI SMS CENTER PEMERINTAH DAERAH PROVINSI NUSA TENGGARA BARAT," JBegaTI, Vol. 3, No. 2, 2022.

[15] A.I.H. Wicaksono, "Mendeteksi serangan Distributed Denial of Service (DDoS) Pada Jaringan Komputer," J.Tek. ITS. Diakses pada Juli 2018.