Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika
Vol.2, No.5 September 2024
e-ISSN: 3031-8912; p-ISSN: 3031-8904; Hal 90-100
DOI: https://doi.org/10.61132/merkurius.v2i5.290
Available online at: https://journal.arteii.or.id/index.php/Merkurius/

Implementasi *Wazuh* Pada *Ubuntu Server* Untuk Mendeteksi Serangan *Brute Force Hydra*

Gilang Patoni[*1], Yusuf Muhyidin[2], Dayan Singasatia[3]

[1-2] Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Wastukancana, Indonesia
Korespondensi Penulis : gilangpatoni7@gmail.com

Abstract: Di era digital saat ini, keamanan informasi sangatlah penting, terutama ketika mengelola sistem atau server, aplikasi berbasis situs dan sebagainya. Salah umum satu ancaman keamanan yang paling yaitu serangan Brute Force. Negara Indonesia menduduki peringkat kedua teratas dari serangan Brute Force di Asia Tenggara setelah negara Vietnam yang menduduki peringkat pertama. Pada periode Januari hingga Desember 2023, total ada 61.374.948 Bruteforce.Generic.RDP. terdeteksi dan digagalkan oleh produk Kaspersky B2B. Serangan Brute Force yang berhasil memungkinkan penyerang mendapatkan kredensial pengguna yang valid. Ubuntu adalah distribusi Linux open-source gratis berbasis Debian yang pertama kali diterbitkan pada tahun 2004. Ubuntu dirilis dalam tiga edisi (Desktop, Server, dan Core) yang semuanya dapat berjalan di komputer mandiri atau di mesin virtual. Berdasarkan permasalahan tersebut, diperlukan sebuah tools yang dapat memadukan perkembangan yang terjadi dalam sebuah server. Salah satu tools yang digunakan untuk monitoring adalah Wazuh. Wazuh merupakan perangkat berbasis Open Source yang berfungsi sebagai sistem deteksi intrusi berbasis host (endpoint). Metode yang digunakan untuk menyelesaikan masalah tersebut menggunakan metode Penetration Testing. Ada beberapa tahapan yang digunakan dalam penelitian ini yaitu, Pengumpulan Informasi, Pemodelan Ancaman, Analisis Kerentanan, Eksploitasi, dan Pelaporan. Hasil dari pengujian yang telah dilakukan menunjukkan bahwa Wazuh dapat mendeteksi serangan Brute Force Hydra pada kerentanan rendah. Sedangkan serangan Denial of Service berhasil dilakukan pada koneksi 1000, 1500, 2000, tetapi serangan tersebut tidak dapat terdeteksi oleh Wazuh.
Keywords*: Web security, SIEM, Wazuh, Experimental.*

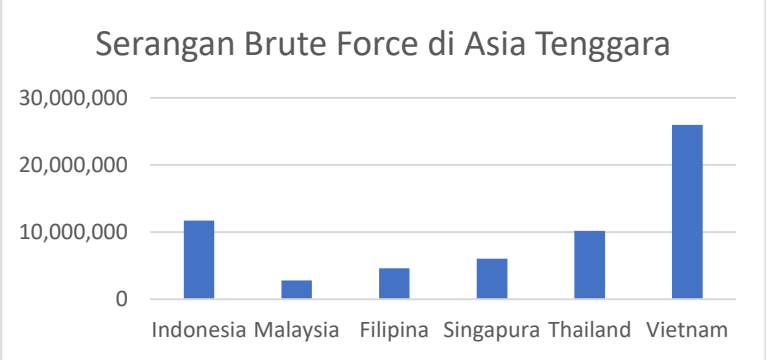
Abstrak. Di era digital saat ini, keamanan informasi sangatlah penting, terutama ketika mengelola sistem atau server, aplikasi berbasis situs dan sebagainya. Salah satu ancaman keamanan yang paling umum yaitu serangan Brute Force. Negara Indonesia menduduki peringkat kedua teratas dari serangan Brute Force di Asia Tenggara setelah negara Vietnam yang menduduki peringkat pertama. Pada periode Januari hingga Desember 2023, total ada 61.374.948 Bruteforce.Generic.RDP. terdeteksi dan digagalkan oleh produk Kaspersky B2B. Serangan Brute Force yang berhasil memungkinkan penyerang memperoleh kredensial pengguna yang valid. Ubuntu adalah distribusi Linux open-source gratis berbasis Debian yang pertama kali diterbitkan pada tahun 2004. Ubuntu dirilis dalam tiga edisi (Desktop, Server, dan Core) yang semuanya dapat berjalan di komputer mandiri atau di mesin virtual. Berdasarkan permasalahan tersebut, diperlukan sebuah tools yang dapat memantau perkembangan yang terjadi dalam sebuah server. Salah satu tools yang digunakan untuk monitoring adalah Wazuh. Wazuh merupakan perangkat berbasis Open Source yang berfungsi sebagai sistem deteksi intrusi berbasis host (endpoint). Metode yang digunakan untuk penyelesaian masalah tersebut menggunakan metode Penetration Testing. Ada beberapa tahapan yang digunakan dalam penelitian ini yaitu, Gathering Information, Threat-Modelling, Vulnerability Analysis, Exploitation, dan Reporting. Hasil dari pengujian yang telah dilakukan menunjukkan bahwa Wazuh dapat mendeteksi serangan Brute Force Hydra pada kerentanan rendah. Sedangkan serangan Denial of Service berhasil dilakukan pada koneksi 1000, 1500, 2000, tetapi serangan tersebut tidak dapat terdeteksi oleh Wazuh.
Kata kunci: *Keamanan web, SIEM, Wazuh, Eksperimental.*

LATAR BELAKANG

Di era digital saat ini, keamanan informasi sangatlah penting, terutama ketika mengelola sistem atau server, aplikasi berbasis situs dan sebagainya. Salah satu ancaman

Received: Mei 12, 2024; Revised: Juni 18, 2024; Accepted: Juli 20, 2024; Published: Juli 26, 2024
* Salsabila : salsarsd10@gmail.com

keamanan yang paling umum yaitu serangan *Brute Force*. Negara Indonesia menduduki ke dua peringkat teratas dari serangan *Brute Force* di Asia Tenggara setelah negara Vietnam yang menduduki peringkat pertama. Pada periode Januari hingga Desember 2023, total ada 61.374.948 *Bruteforce.Generic.RDP.** terdeteksi dan digagalkan oleh produk *Kaspersky B2B*. Serangan *Bruteforce* yang berhasil memungkinkan penyerang memperoleh kredensial pengguna yang valid. *Remote Desktop Protocol (RDP)* adalah protokol milik *Microsoft*, yang menyediakan antarmuka grafis kepada pengguna untuk terhubung ke komputer lain melalui jaringan. RDP banyak digunakan oleh administrator sistem dan pengguna non teknis untuk mengontrol server dan PC lain dari jarak jauh. (Arradian, 2024).



Gambar 1. Serangan *Brute Force* di Asia Tenggara

Ubuntu adalah distribusi *Linux open-source* gratis berbasis *Debian*. Ini pertama kali diterbitkan pada tahun 2004. Ubuntu dirilis dalam tiga edisi *(Desktop, Server, dan Core)* yang semuanya dapat berjalan di komputer mandiri atau di mesin virtual. Sistem operasi ini menyediakan banyak perangkat lunak pra-instal, *GUI* yang mudah digunakan, enkripsi *drive* penuh, dan pengalaman pelanggan yang luar biasa. Karena fitur dan dukungannya, itu menjadi *platform workstation Linux* yang paling banyak digunakan. Ini adalah pilihan populer untuk menjalankan *server web* (sebagai bagian dari tumpukan *LAMP*), proyek *OpenStack*, dan sudah diinstal sebelumnya di banyak komputer (termasuk *Dell*, *HP*, *Lenovo*, dan *Asus*). (Pratomo, 2023). Umumnya para pelaku penyerangan *Brute Force* menebak *username* dan *password* yang digunakan. *Brute Force* sendiri sebenarnya merupakan teknik lama dari *cyber crime*. Namun ternyata masih banyak yang menggunakan dikarenakan masih dianggap efektif oleh beberapa oknum *cyber crime*. Tujuan utama *Brute Force* adalah mengakses situs atau *server* yang menyimpan berbagai informasi dan aset lain yang dimiliki situs atau *server* tersebut.

Berdasarkan permasalahan tersebut maka diperlukan sebuah *tools* yang dapat memantau perkembangan yang terjadi dalam sebuah *server*. Salah satu *tools* yang digunakan untuk monitoring adalah *Wazuh*. *Wazuh* merupakan perangkat berbasis *Open Source* yang berfungsi sebaga 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).

KAJIAN TEORITIS

1. Keamanan Informasi di Era Digital

Keamanan informasi merupakan aspek penting dalam dunia digital saat ini, terutama dalam pengelolaan sistem atau server serta aplikasi berbasis situs. Salah satu ancaman keamanan yang paling umum adalah serangan *Brute Force*. Serangan ini bertujuan untuk memperoleh akses tidak sah ke sistem dengan mencoba semua kombinasi kata sandi yang mungkin hingga ditemukan kombinasi yang benar. Negara-negara seperti Indonesia dan Vietnam mengalami serangan *Brute Force* dalam jumlah yang signifikan, menunjukkan perlunya solusi keamanan yang efektif untuk melindungi data dan sistem.

2. Ubuntu Server

Ubuntu adalah distribusi Linux berbasis Debian yang open-source dan gratis, pertama kali diterbitkan pada tahun 2004. Ubuntu tersedia dalam tiga edisi: Desktop, Server, dan *Core*, yang semuanya dapat berjalan di komputer mandiri atau mesin virtual. Ubuntu Server khususnya banyak digunakan dalam lingkungan server karena kestabilannya, keamanan, dan dukungan komunitas yang kuat.

3. Wazuh sebagai Sistem Deteksi Intrusi

Wazuh adalah alat *open-source* yang berfungsi sebagai sistem deteksi intrusi berbasis host *(endpoint).* Wazuh dapat memantau aktivitas mencurigakan dalam sistem dan memberikan peringatan dini tentang potensi ancaman keamanan. Alat ini dapat digunakan untuk memantau berbagai jenis serangan, termasuk *Brute Force* dan *Denial of Service* (DoS).

4. Penetration Testing

Metode *Penetration Testing* digunakan untuk mengevaluasi keamanan sistem dengan mensimulasikan serangan dari luar. Metode ini terdiri dari beberapa tahapan, yaitu:

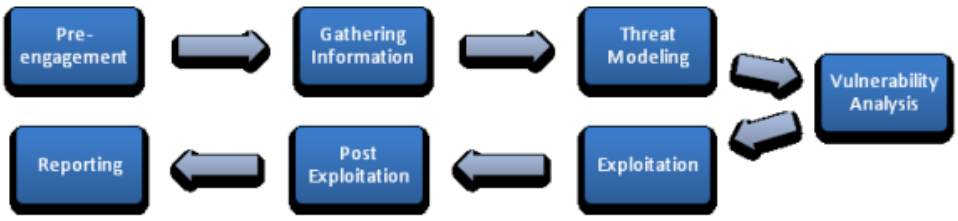
a. **Gathering Information**: Mengumpulkan informasi mengenai target.
b. **Threat-Modelling**: Mengidentifikasi dan mengevaluasi potensi ancaman.
c. **Vulnerability Analysis**: Menganalisis kerentanan yang ada dalam sistem.
d. **Exploitation**: Mengeksploitasi kerentanan untuk menguji sejauh mana serangan dapat berhasil.
e. **Reporting**: Mendokumentasikan hasil pengujian dan memberikan rekomendasi perbaikan.

5. Implementasi Wazuh pada Ubuntu Server

Dalam penelitian ini, Wazuh diimplementasikan pada Ubuntu Server untuk mendeteksi serangan *Brute Force Hydra*. *Brute Force Hydra* adalah alat yang digunakan oleh penyerang untuk melakukan serangan *Brute Force* terhadap berbagai layanan. Hasil penelitian menunjukkan bahwa Wazuh mampu mendeteksi serangan *Brute Force Hydra* pada tingkat kerentanan rendah. Namun, Wazuh tidak dapat mendeteksi serangan *Denial of Service* pada koneksi yang lebih tinggi (1000, 1500, 2000)

METODOLOGI PENELITIAN

Metodologi *Penetration Testing* digunakan penulis dalam mengkaji, terdiri dari 7 (tujuh) tahapan yaitu *Pre-engagement*, *Gathering Information*, *Threat-Modeling*, *Vulnerability Analysis*, *Exploitation, Post Exploitation* dan *Reporting.* Tetapi untuk penelitian saat ini hanya sampai menggunakan 5 (lima) tahapan yaitu *Gathering Information*, *Threat-Modeling*, *Vulnerability Analysis*, *Exploitation* dan *Reporting.*



Gambar 2. *Penetration Testing*

HASIL DAN PEMBAHASAN

1. Pengujian Sql Injection

Pada hasil pengujian ini dilakukan dengan penyerangan Sql Injection terhadap website yang telah dibuat untuk pengujian. Pengujian Sql Injection menggunakan *tools* sqlmap dengan perintah *sqlmap –u* kemudian masukkan web yang dituju *--dbs.*

Gambar 2. Perintah *Sqlmap*

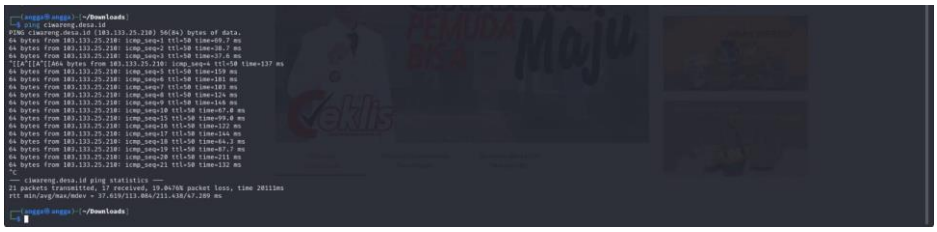
Pada gambar diatas terdapat parameter (-u) yaitu menunjukkan URL dari target pengujian beserta parameter *query* yang rentan, parameter (--dbs) menginstruksikan sqlmap untuk melihat *database* yang ada pada target. *Database* target bisa dilihat pada gambar dibawah ini.

Gambar 3. *Database* Target

Dapat dilihat terdapat dua database yang ada pada target, penulis ingin melihat tabel pada database acuart untuk melihat isi tabel pada database acuart bisa dilakukan dengan menggunakan perintah *sqlmap –u* kemudian masukkan web yang dituju *–D acuart --tables.*

2. *Pengujian DDoS*

Pengujian selanjutnya dilakukan dengan menggunakan penyerangan *DDoS* terhadap *website* yang akan digunakan untuk pengujian. Penyerangan *DDoS* dilakukan menggunakan *tools Loic* dengan menggunakan perintah *ping* pada web yang dituju.



Gambar 4. Perintah Ping

Perintah *ping* diatas digunakan untuk melihat *IP address* dari web Desa Ciwareng dan didapatkan *IP* tersebut yaitu 103.133.25.210. Setelah *IP* didapatkan, selanjutnya melakukan perintah *nmap 103.133.25.210*.

Tabel 1. Scannig

PORT	STATE	SERVICE
21/tcp	Open	Ftp
53/tcp	Open	Domain
80/tcp	Open	Http
433/tcp	Open	Https
2222/tcp	Open	EterNetLIP-1
10000/tcp	Open	Snet-sensor-mgmt
20000/tcp	Open	Dnp

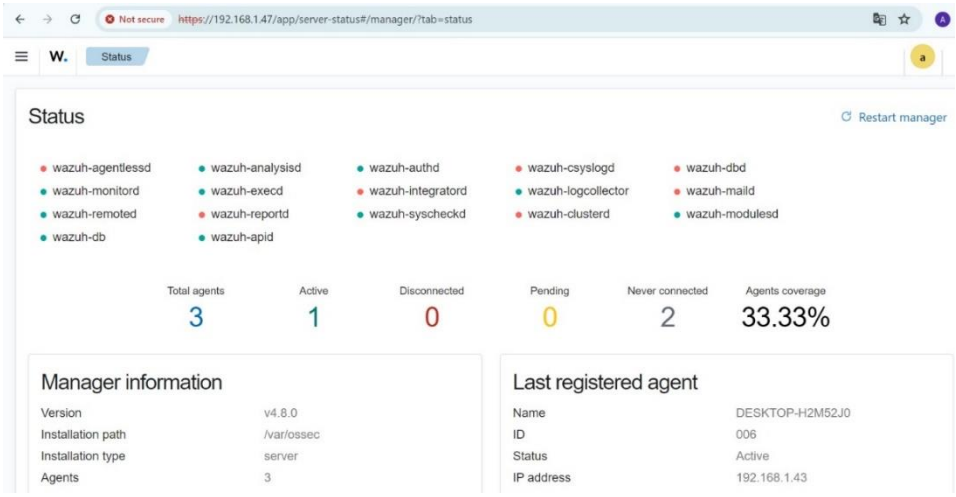
Setelah itu, melakukan penyerangan menggunakan *tools Loic* dengan perintah *sudo mono LOIC.exe*. Setelah tools Loic terbuka maka masukkan halaman URL dari target dan masukkan port yang terbuka untuk diserang, disini penulis menggunakan port 53/tcp. Setelah melakukan penyerangan, maka dapat dilihat hasil penyerangan tersebut pada web yang digunakan untuk pengujian ini.

Tabel 2. Hasil Uji Serangan

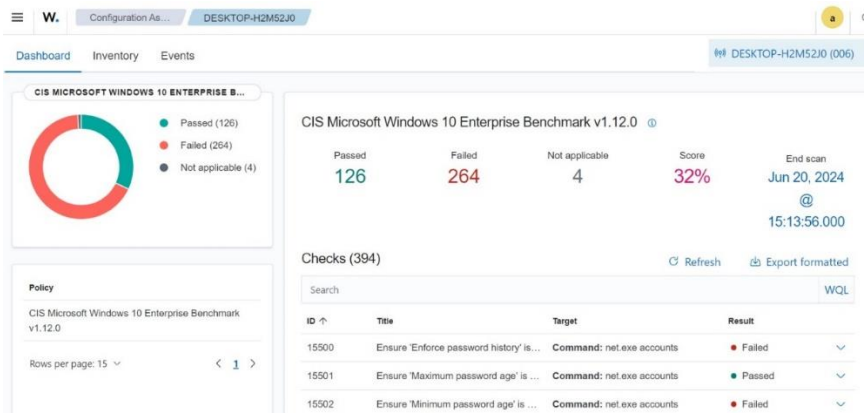
No	Uji Serangan	Keterangan	Koneksi
1	Brute Force Hydra	Terdeteksi	
2	Denial of Service	Tidak Terdeteksi	1000
		Tidak Terdeteksi	1500
		Tidak Terdeteksi	2000

3. Hasil *Evaluasi*

a. Hasil Wazuh



Gambar 5. Hasil Wazuh



Gambar 6. Hasil Pengujian

KESIMPULAN

Berdasarkan hasil pengujian dan hasil evalusi, pengujian penyerangan terhadap web server yang telah dilakukan dapat di deteksi oleh Wazuh namun hanya pada tingkat kerentanan yang rendah. Hasilnya dapat disimpulkan bahwa saja sql tidak dapat terdeteksi dan yg ddos dapat terdeteksi, yang menandakan bahwa pengecekkan pengujian penyerangan terhadap web server dapat terdeteksi pada kerentanan yang rendah. Berdasarkan hasil penelitian diatas, saran yang bisa disampaikan yaitu mencoba melakukan pengujian penyerangan dengan menggunakan penyerangan yang lain seperti *Dos*, *Brute Force* sehingga dapat diketahui bahwa pengujian penyerangan tersebut dapat terdeteksi oleh Wazuh pada tingkat kerentanan rendah, sedang, ataupun tinggi.

DAFTAR REFERENSI

Arief, M., Trisnawan, P. H., Data, M., Studi, P., Informatika, T., Komputer, F. I., & Brawijaya, U. (2024). *IMPLEMENTASI SISTEM DETEKSI SERANGAN SLOWLORIS PADA ARSITEKTUR JARINGAN SOFTWARE-DEFINED NETWORK*. *1*(1), 1–10.

Astuti, I. K. (2018). Fakultas Komputer INDAH KUSUMA ASTUTI Section 01. *Jaringan Komputer*, 8. https://id.scribd.com/document/503304719/jaringan-komputer

Bastian, A., Sujadi, H., & Abror, L. (2020). Analisis Keamanan Aplikasi Data Pokok Pendidikan (DAPODIK) Menggunakan Penetration Testing Dan SQL Injection. *INFOTECH Journal*, *6*(2), 65–70.

Hadi Sofiyan Muhammad, P. D. A. P. (2023). Implementasi Security Information and Event Management (Siem) Untuk Deteksi Dan Analisa Insiden Keamanan Pada Web Server. *Correspondencias & Análisis*, *15018*, 1–23.

Hermawan, R. (2021). Teknik Uji Penetrasi Web Server Menggunakan SQL Injection dengan SQLmap di Kalilinux. *STRING (Satuan Tulisan Riset Dan Inovasi Teknologi)*, *6*(2), 210. https://doi.org/10.30998/string.v6i2.11477

Khotimah, H., Bimantoro, F., & Kabanga, R. S. (2022). Implementasi Security Information And Event Management (SIEM) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat. *Jurnal Begawe Teknologi Informasi (JBegaTI)*, *3*(2), 213–219. https://doi.org/10.29303/jbegati.v3i2.752

Shafiyyah, A., Elektro, J. T., Teknik, F., & Lampung, U. (2024). *Implementasi sistem keamanan jaringan di psdku universitas lampung waykanan menggunakan server wazuh untuk deteksi dan respon serangan siber*.

Stefan Stanković, Slavko Gajin, & Ranko Petrović. (2022). A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis. *IX INTERNATIONAL CONFERENCE IcETRAN*, *IX*(june), 6–9.

Swami, R., Dave, M., & Ranga, V. (2019). Software-defined Networking-based DDoS Defense Mechanisms. *ACM Computing Surveys*, *52*(2). https://doi.org/10.1145/3301614

Umar, R., & Prasetyo Marsaid, A. (2023). 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