Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika
Vol.2, No.5 September 2024
e-ISSN: 3031-8912; p-ISSN: 3031-8904; Hal 145-156
DOI: https://doi.org/10.61132/merkurius.v2i4.290
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: *In today's digital era, information security is very important, especially when managing systems or servers, website-based applications and so on. One of the most common security threats is Brute Force attacks. Indonesia ranks second in terms of Brute Force attacks in Southeast Asia after Vietnam which ranks first. In the period from January to December 2023, a total of 61,374,948 Bruteforce.Generic.RDP. were detected and thwarted by Kaspersky B2B products. A successful Brute Force attack allows attackers to obtain valid user credentials. Ubuntu is a free, open-source Linux distribution based on Debian that was first published in 2004. Ubuntu is released in three editions (Desktop, Server, and Core) all of which can run on standalone computers or in virtual machines. Based on these problems, a tool is needed that can combine the developments that occur in a server. One of the tools used for monitoring is Wazuh. Wazuh is an Open Source-based device that functions as a host-based intrusion detection system (endpoint). The method used to solve this problem uses the Penetration Testing method. There are several stages used in this study, namely, Information Collection, Threat Modeling, Vulnerability Analysis, Exploitation, and Reporting. The results of the tests that have been carried out show that Wazuh can detect Brute Force Hydra attacks at low vulnerabilities. While Denial of Service attacks were successfully carried out on connections 1000, 1500, 2000, but these attacks cannot be detected by Wazuh.*
Keywords*: Web security, SIEM, Wazuh, Experimental.*

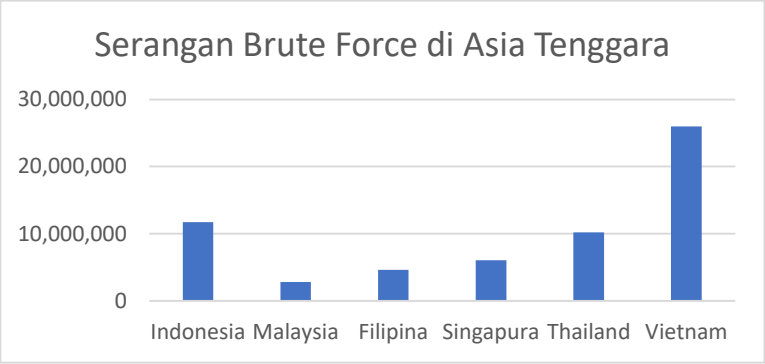
Abstrak. Di era digital saat ini, keamanan informasi sangatlah penting, terutama ketika mengelola sistem atau server, aplikasi berbasis situs dan sebagainya. Salah satu ancaman keamanan yang paling umum yaitu serangan *Brute Force*. Negara Indonesia menduduki peringkat kedua teratas dari serangan Brute 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 keamanan yang paling umum yaitu serangan *Brute Force*. Negara Indonesia menduduki ke dua peringkat teratas dari serangan *Brute Force* di Asia Tenggara setelah negara

Received: Mei 12, 2024; Revised: Juni 18, 2024; Accepted: Juli 20, 2024; Published: Juli 29, 2024
* Gilang Patoni : gilangpatoni7@gmail.com

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 s*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:

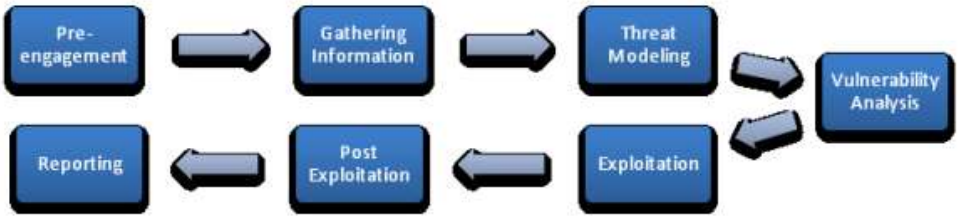
a. **Gathering Information**: Mengumpulkan informasi mengenai target.
b. **Threat-Modelling**: Mengidentifikasi dan mengevaluasi potensi ancaman.
c. **Vulnerability Analysis**: Menganalisis kerentanan yang ada dalam sistem.
d. **Exploitation**: Mengeksploitasi kerentanan untuk menguji sejauh mana serangan 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.*

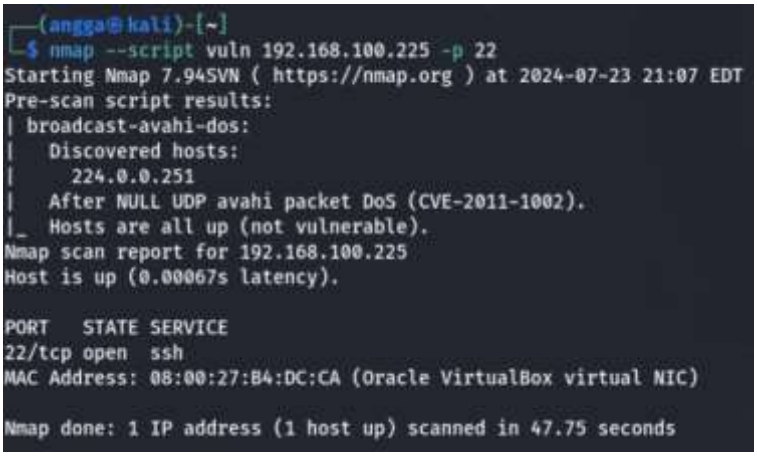


Gambar 2. *Penetration Testing*

HASIL DAN PEMBAHASAN

1. *Vulnerability Analysis*

Pada tahap ini penulis melakukan kegiatan mendalami sumber informasi yang telah didapat pada tahap sebelumnya, lalu dengan melakukan perintah *nmap –script vuln 192.168.100.225 -p 22* adalah gambar yang didapat penulis sebagai sumber target dari sasaran.



```
┌──(angga㉿kali)-[~]
└─$ nmap --script vuln 192.168.100.225 -p 22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 21:07 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.100.225
Host is up (0.00067s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:B4:DC:CA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 47.75 seconds
```

Gambar 3. 1 Cek kerentanan

2. *Exploitation*

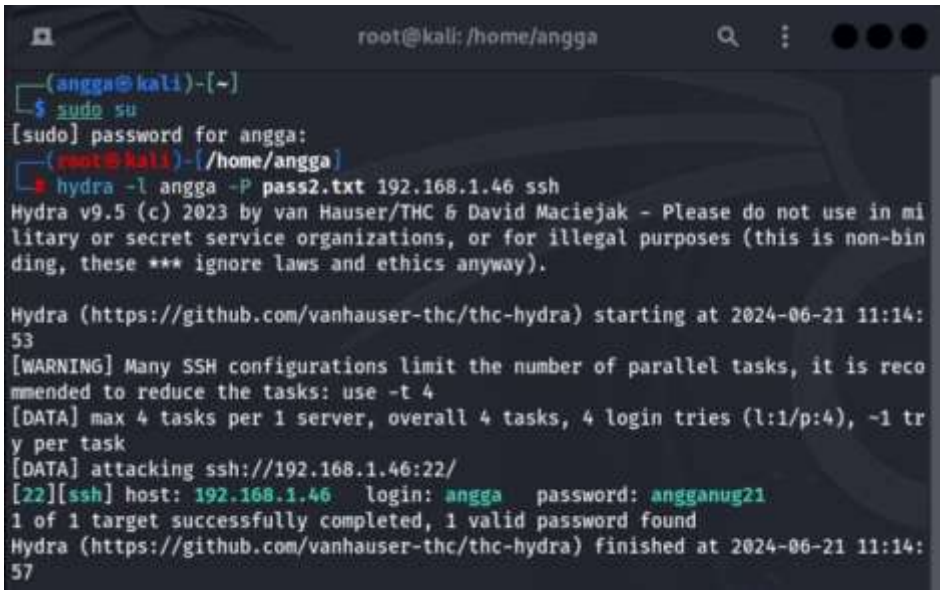
a. Penyerangan Hydra

Pada tahap ini penulis memulai penyerangan seperti penyerang. Menyerang ke Ubuntu Server dengan men-cek terlebih dahulu IP pada Ubuntu Server dengan perintah ip a.

```
angga@angganug21:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:b4:dc:ca brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.46/24 metric 100 brd 192.168.1.255 scope global dynamic enp0s3
       valid_lft 86379sec preferred_lft 86379sec
    inet6 fe80::a00:27ff:feb4:dcca/64 scope link
       valid_lft forever preferred_lft forever
angga@angganug21:~$ _
```

Gambar 4. Cek *IP Ubuntu Server*

Pada gambar diatas setelah mendapat Alamat *IP Ubuntu Server*, lalu memulasi penyerangan *hydra* dengan memasukkan perintah hydra -l angga -P 192.168.1.46 ssh seperti gambar dibawah ini.

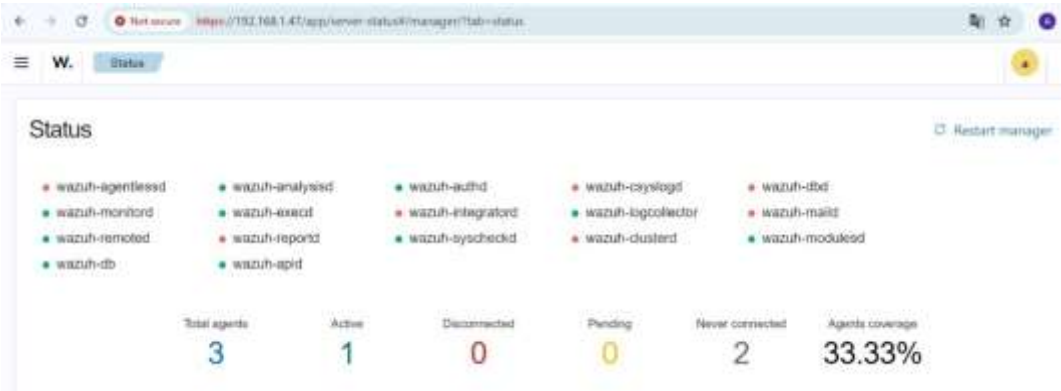


Gambar 5. Penyerangan *Hydra*

Penyerangan *hydra* pada *port* 22 pada *Ubuntu Server* menghasilkan *username* beserta *password* dengan hasil l*ogin*: angga dengan *password*: angganug21.

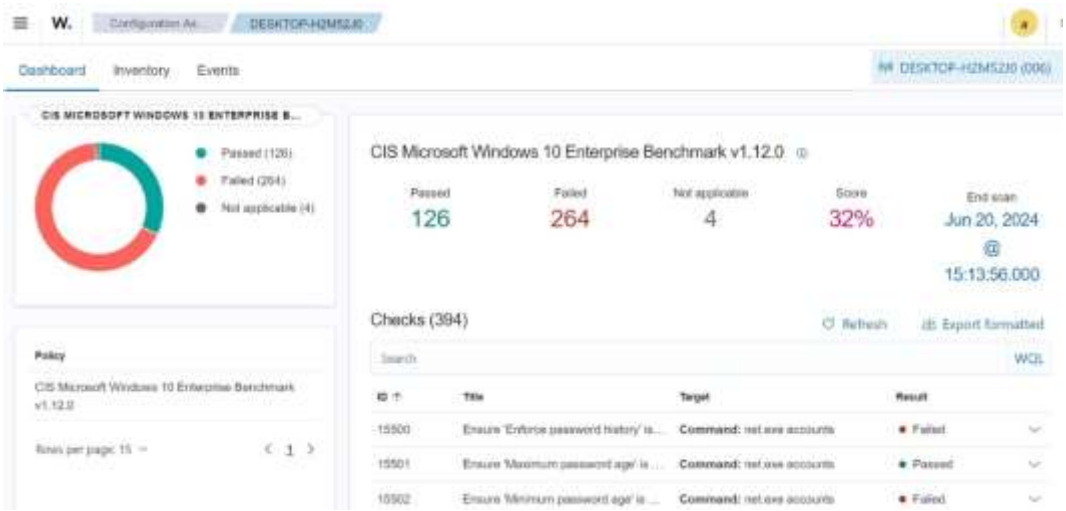
Gambar 6. *disconnected*

Pada gambar diatas dengan agent berjumlah 3 disconected 1 dan never connected 2 setelah berhasil menambahkan Wazuh Agent pertama harus me-refresh terlebih dahulu halaman Wazuh.



Gambar 4.7 *active*

Setelah aktif kemudian pilih menu *Configuration Assesment* dan pilih *agent* yang telah aktif tersebut.

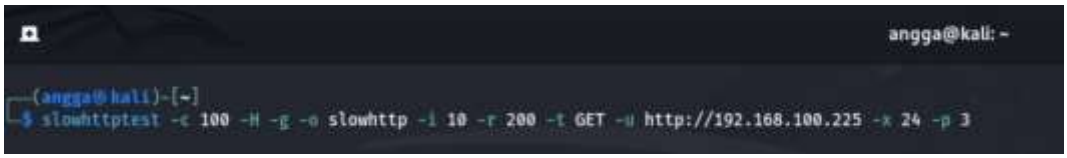


Gambar 8. Hasil serangan *Brute Force*

Setelah memilih *Wazuh Agent* yang aktif lalu menampilkan gambar diatas dengan *passed* 126, *failed* 264 dan *not applicable* 4. Lalu pada gambar diatas tersebut menunjukkan sistem yang telah dipenuhi adalah 126. Sebaliknya *failed* adalah sebuah kontrol atau aturan yang ditemukan pelanggaran adalah 264. Lalu *not applicable* menunjukkan dengan angka 4 yaitu sebuah kontrol pada *Wazuh* yang tidak relevan untuk *Wazuh agent* itu sendiri dengan *score* 32% yang berarti terindikasi rendah.

b. Penyerangan *DoS*

Pada penyerangan DoS ini menggunakan tool slowhttptest dengan perintah seperti gambar dibawah.

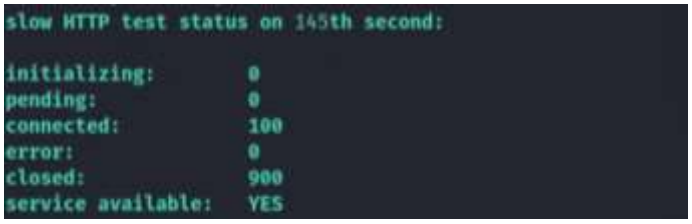


Gambar 9. *Slowhttptest*

Pertama jalankan perintah *slowhttptest -c 100 -H -g -o slowhttp -I 10 -r 200 -t GET -u http://192.100.225 -x 24 -p 3* untuk mensimulasikan penyerangan *DoS* pada alamat *web server* yang telah diinstal.

Gambar 10.2 Koneksi 100

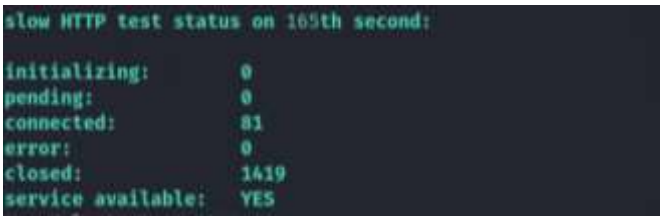
Pada gambar diatas menunjukkan bahwa koneksi yang aktif 100 dan pending 0 dan layanan web server masih tersedia. Gambar diatas juga menunjukkan lalu lintas jaringan masih rendah atau normal tanpa tanda-tanda beban tinggi atau masalah pada web server.



Gambar 11. Koneksi 1000

Gambar 12. Overload 1000

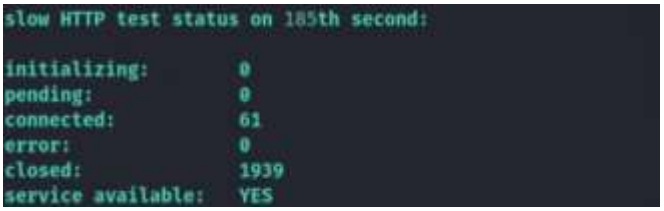
Pada gambar diatas dengan menambahkan koneksi 1000 pada web server mengalami overload karena serangan DoS tersebut.



Gambar 13. Koneksi 1500

Gambar 14. *Overload* 1500

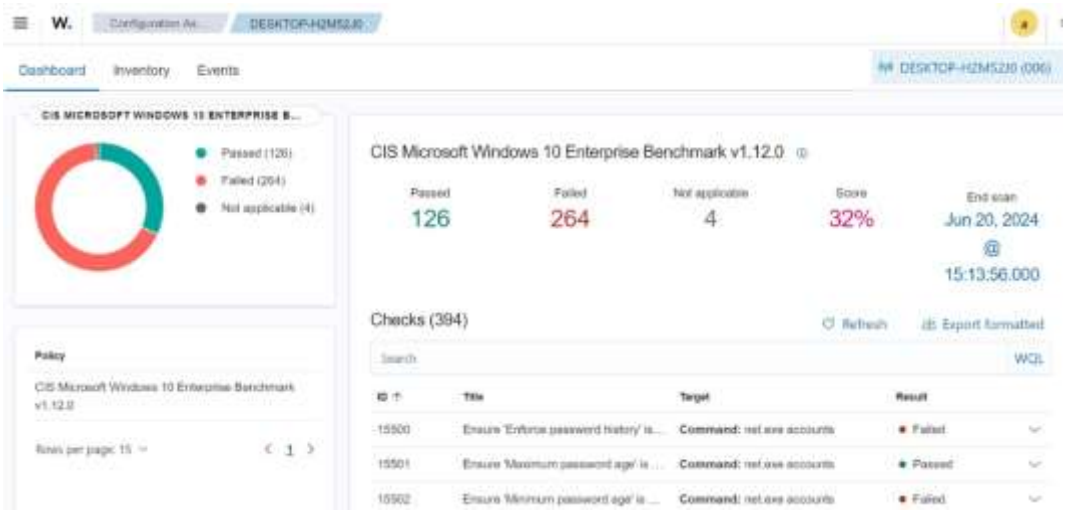
Pada gambar diatas mulai mengalami overload yang semakin lama dikarenakan menambahkan koneksi 1500 untuk penyerangan DoS.



Gambar 15. Koneksi 2000

Gambar 16. *Overload* 2000

Pada gambar diatas semakin lama mengalami overload dengan menambahkan koneksi menjadi 2000 serangan pada web server.



Gambar 17. Hasil serangan *DoS*

Pada gambar diatas serangan DoS atau Denial of Service tidak menampilkan bahwa serangan DoS terdeteksi, pada serangan 1000 koneksi, 1500 koneksi, 2000 koneksi.

3. Reporting

Penyerangan menggunakan *Brute Force Hydra* pada *Ubuntu Server* berhasil mendeteksi *username* dan *password* dengan *username angga* dan *password* anggnug21 pada *Ubuntu Server*. Dan untuk penyerangan *Denial of Service* berhasil diserang dengan serangan 1000 koneksi, 1500 koneksi dan 2000 koneksi pada *web server* yang telah diinstal pada *Ubuntu Server.*

KESIMPULAN

Berdasarkan penjelasan yang telah diberikan sebelumnya dapat disimpulkan dari hasil pengujian yang telah dilakukan penulis bahwa *Wazuh* berhasil mendeteksi penyerangan *Brute Force Hydra* pada *Ubuntu Server* versi 24.04 LTS dengan *score* 32% yang menandakkan bahwa pengujian penyerangan terhadap *Ubuntu Server* terdeteksi pada kerentanan yang rendah yang dimana serangan tersebut dapat diketahui dengan cepat sehingga serangan *Brute Force Hydra* bisa segera ditangani. Sedangkan serangan Denial of Service berhasil dilakukan pada koneksi 1000, 1500, 2000 akan tetapi serangan tersebut tidak dapat terdeteksi oleh *Wazuh.*

DAFTAR REFERENSI

Arradian, D. (2024). *61 Juta Serangan Bruteforce Terjadi di Indonesia selama 2023, Kedua Tertinggi di Asia Tenggara*. Sindo News.

https://tekno.sindonews.com/read/1371729/207/61-juta-serangan-bruteforce-terjadi-di-indonesia-selama-2023-kedua-tertinggi-di-asia-tenggara-1714961102

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

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

AZZAH, S. (2024). *... Keamanan Jaringan Di Psdku Universitas Lampung Waykanan Menggunakan Server Wazuh Untuk Deteksi Dan Respon Serangan ...*. http://digilib.unila.ac.id/id/eprint/78645

Fachri, F., Fadlil, A., & Riadi, I. (2021). Analisis Keamanan Webserver menggunakan Penetration Test. *Jurnal Informatika*, *8*(2), 183–190. https://doi.org/10.31294/ji.v8i2.10854

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

Gunawan, I. (2016). Penggunaan Brute Force Attack Dalam Penerapannya Pada Crypt8 Dan Csa-Rainbow Tool Untuk Mencari Biss. *InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan)*, *1*(1), 52–55. https://doi.org/10.30743/infotekjar.v1i1.48

Hidayatulloh, S., & Saptadiaji, D. (2021). Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP). *Jurnal Algoritma*, *18*(1), 77–86. https://doi.org/10.33364/algoritma/v.18-1.827

Kurniawan, A. A., & Nugroho, Y. (2019). Upaya Penetrasi dengan Enumeration menggunakan Hydra. *Journal of Technology and Informatics (JoTI)*, *1*(1), 62–64.

MEILINAEKA. (2023). *Web Server Apache Adalah: Bagaimana Cara Kerjanya?* It.Telkomuniversity.Ac.Id. https://it.telkomuniversity.ac.id/web-server-apache-adalah-bagaimana-cara-kerjanya/

Nazwita, & Ramadhani, S. (2017). Analisis Sistem Keamanan Web Server Dan Database Server Menggunakan Suricata. *Seminar Nasional Teknologi Informasi, Komunikasi Dan Industri (SNTIKI)*, 308–317.

Prathama, G. H., Andaresta, D., & Darmaastawan, K. (2021). Instalasi Framework IoT Berbasis Platform Thingsboard di Ubuntu Server. *TIERS Information Technology Journal*, *2*(2), 1–9. https://doi.org/10.38043/tiers.v2i2.3329

Pratomo, T. N. (2023). *Ubuntu Server Vs CentOS Server : Mana Yang Terbaik?* Nevacloud.Com. https://nevacloud.com/blog/ubuntu-server/

Safitrah, T., Banggas, A., Sinaga, G., Alghifari, M., Neyman, S. N., Siber, K., & Web, L. (2024). *Pengaruh Serangan Slow HTTP DoS terhadap Layanan Web : Studi Eksperimental dengan Slowhttptest*. *4*, 1–11.

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

Tujni, B., & Alfiansyah, A. H. (2018). Perancangan Pemetaan IP Address menggunakan Metode VLSM di PT KAI Divre III Palembang Sumatera Selatan. *Prosiding Semhavok*, 40–47. http://conference.binadarma.ac.id/index.php/semhavok/article/view/1219

Yusnanto, T., Muin, M. A., & Wahyudiono, S. (2022). Analisa Infrastruktur Jaringan Wireless dan Local Area Network (WLAN) Meggunakan Wireshark Serta Metode Penetration Testing Kali Linux. *Journal on Education*, *4*(4), 1470–1476. https://doi.org/10.31004/joe.v4i4.2175