JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 12 No. 2, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v12i2.4074

IMPLEMENTASI WAZUH MENGGUNAKAN METODE PPDIOO DI SISTEM KEAMANAN JARINGAN PSDKU UNIVERSITAS LAMPUNG WAYKANAN SEBAGAI DETEKSI DAN RESPON SERANGAN SIBER

Azzah Shafiyyah[1*], Gigih Forda Nama[2], Rio Ariestia Pradipta[3]

[1] Teknik Informatika, Universitas Lampung, Jl. Prof. Soemantri Brojonegoro, Bandar Lampung 35145
[2] PSDKU Universitas Lampung Way Kanan, Jl. Negeri Baru, Kec. Blambangan Umpu, Kabupaten Way Kanan, Lampung 34764
[3] Teknik Informatika, Universitas Lampung, Jl. Prof. Soemantri Brojonegoro, Bandar Lampung 35145

Riwayat artikel:

Received: 29 Januari 2024
Accepted: 30 Maret 2024
Published: 2 April 2024

Keywords:
Network Security;
Brute Force; DoS:
PSDKU;
PPDIOO;

Corespondent Email:
azzahsfyyh28@gmail.com

Abstrak. PSDKU Universitas Lampung Way Kanan membutuhkan sistem keamanan jaringan yang efektif untuk melindungi jaringan komputer server lab komputer dari serangan siber yaitu *brute force* dan *Denial of Service* (DoS) Untuk meningkatkan keamanan jaringan, diperlukan implementasi sistem keamanan jaringan dengan menggunakan *platform* wazuh sebagai server monitoring dan wazuh *agent* yang diinstal pada komputer server jaringan lab komputer PSDKU menggunakan Server Utama PSDKU. Metode pengembangan sistem keamanan yang digunakan yaitu PPDIOO (*prepare, plan, design, implement, operate, optimize*) cisco. Dalam sistem ini, semua aktivitas dari wazuh agent akan dikirimkan ke wazuh server untuk dilakukan pemantauan dan deteksi serangan siber. Kemudian dilakukan simulasi serangan *brute force* dan *Denial of Service* (DoS) terhadap wazuh *agent* yang terinstal pada server jaringan lab komputer. Respon dari serangan bruteforce yang akan dilakukan adalah dengan memblokir alamat IP penyerang menggunakan *software* fail2ban dan serangan DoS dengan Active Response Wazuh sehingga penyerang tidak dapat mengakses dan tidak dapat terhubung ke komputer server jaringan lab komputer PSDKU. Sistem keamanan jaringan tidak dapat mendeteksi serangan DoS dengan jumlah rata-rata koneksi dibawah 4000 koneksi http, dan Serangan DoS berhasil dilakukan dengan hasil yang menunjukkan bahwa Server Utama PSDKU memiliki ketahanan dalam menerima dan melayani koneksi HTTP dibawah 3.522.013 koneksi. Sehingga sistem keamanan jaringan dapat ditingkatkan dan respon terhadap serangan siber dapat dilakukan secara cepat dan efektif.

Abstract. *To improve network security, it is necessary to implement a network security system using the wazuh platform as a monitoring server and wazuh agent installed on the PSDKU computer network server using PSDKU Main Server. The method of development of the security system used is PPDIOO (prepare, plan, design, implement, operate, optimize) cisco. In this system, all the activities of the agent will be sent to the server for monitoring and detection of cyber attacks, then simulated brute force and Denial of Service (DoS) attacks against the agent installed on the computer lab network server. The response to a bruteforce attack is to block the attacker's IP address using file2ban software and DoS attacks with Active Response Wazuh so that the attackers can't access and connect to the computer server of the PSDKU computer's lab network. The network security system could not detect a DoS*

attack with an average number of connections below 4000 http connections, and the DoS Attack was successfully carried out with results showing that PSDKU's Main Server has resilience in receiving and serving HTTP connections under 3.522.013 connections. So the network security system can be improved and the response to cyber attacks can be carried out quickly and effectively.

1. PENDAHULUAN

Program PSDKU adalah salah satu upaya Universitas Lampung untuk meningkatkan peran Universitas Lampung dalam bidang pembangunan nasional dan daerah terutama dalam peningkatan aksesibilitas pendidikan tinggi, dan pembangunan sumberdaya manusia di Kabupaten Way Kanan. PSDKU Universitas Lampung Way Kanan memiliki jaringan yang kompleks. PSDKU menghadapi beberapa masalah dalam menghadapi ancaman serangan siber. Salah satu masalah yang dihadapi adalah tidak adanya sistem keamanan jaringan yang berguna untuk melindungi server jaringan PSDKU khususnya Lab Komputer. [1]

Masalah lain yang dihadapi adalah tidak adanya sistem keamanan jaringan yang berguna untuk memberikan informasi tentang peristiwa keamanan jaringan komputer server di PSDKU secara real time. Dalam rangka meningkatkan keamanan sistem, diperlukan implementasi sistem keamanan jaringan dengan menggunakan platform Wazuh sebagai server monitoring dan Wazuh Agent yang diinstal pada jaringan komputer server di PSDKU menggunakan Server Utama PSDKU, sebelum diimplementasikan menggunakan Server Utama PSDKU akan dilakukan Simulasi menggunakan hardware set top box (STB) sebagai simulasi sistem keamanan. Dengan adanya sistem keamanan jaringan menggunakan platform Wazuh, diharapkan segala informasi tentang semua aktivitas di Lab Komputer PSDKU dapat terpantau secara real time, serta sistem keamanan dapat ditingkatkan dan respon terhadap serangan siber dapat dilakukan secara cepat dan efektif.[2]

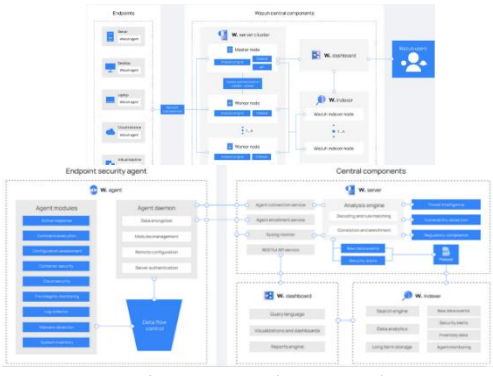
2. TINJAUAN PUSTAKA

2.1 PSDKU Unila Way Kanan

Program PSDKU adalah salah satu upaya Universitas Lampung untuk meningkatkan peran Universitas Lampung dalam bidang pembangunan nasional dan daerah terutama dalam peningkatan aksesibilitas pendidikan tinggi, dan pembangunan sumberdaya manusia di Kabupaten Way Kanan. Program PSDKU Unila Way Kanan adalah bukti nyata komitmen Unila dalam mengurangi kesenjangan akses pendidikan tinggi di wilayah Lampung. Pemilihan Kabupaten Way Kanan sebagai lokasi program PSDKU didasarkan pada letak geografisnya yang strategis, memungkinkan akses dari beberapa kabupaten di Provinsi Lampung [1]

2.2 Wazuh

Wazuh adalah perangkat lunak *open source* yang berfungsi sebagai sistem deteksi berbasis host (*endpoint*) yang menyatukan kemampuan XDR *(External Data Representation)* dan SIEM *(Security Information and Event Management)* diantaranya menganalisis *log*, deteksi intrusi dan malware, monitor file integrity, penilaian konfigurasi sesuai standar industri, deteksi kerentanan, dan dukungan kepatuhan terhadap aturan. memberi peringatanberdasarkan waktu, dan merespons secara aktif. Wazuh memberikan fitur visibilitas keamanan yang lebih dalam pada infrastruktur dengan memantau *host* di sistem operasi dan tingkat aplikasi. Arsitektur Wazuh tersusun dari tiga komponen pusat *(Wazuh Indexer, Wazuh Server, Wazuh Dashboard)* dan komponen *endpoint (Wazuh Agent)* yang digambarkan dalam diagram berikut: [2]



Gambar 1. 1 Arsitektur Wazuh

2.3 *Security Information and Event Management* (SIEM)

SIEM diterjemahkan sebagai "Manajemen Informasi dan Keamanan Peristiwa." sistem yang digunakan untuk memantau dan mendeteksi serangan serta merespon keamanan melalui analisis *log* dari berbagai event yang diperoleh dari sumber data secara *real-time*. Teknologi ini memiliki jangkauan pengumpulan data yang luas dan dapat mengaitkan serta menganalisis *event* dari berbagai sumber dan menentukan apakah kejadian tersebut merupakan serangan atau tidak. Analisis SIEM mencakup semua aplikasi yang digunakan perusahaan, perangkat jaringan, perangkat keamanan, dan *server*. [3]

2.4 PPDIOO *(Prepare, Plan, Design, Implement, Operate, Optimize)*

PPDIOO Cisco merupakan metodologi dari Cisco yang mendefinisikan siklus layanan berkelanjutan yang dibutuhkan oleh jaringan komputer yang dirancang untuk mendukung pengembangan jaringan. Metode PPDIOO dapat menghasilkan sistem yang mapan dan menyelesaikan permasalahan yang ada.
PPDIOO Cisco merupakan singkatan enam tahap yaitu prepare, plan, design, implement, operate, optimize yaitu suatu pendekatan yang digunakan dalam siklus hidup dan manajemen jaringan Ketika diterapkan pada sistem keamanan jaringan dengan menggunakan server Wazuh, berikut adalah beberapa phase yang akan digunakan:[4]

2.5 Set Top Box (STB)

STB (*Set-Top Box*) adalah perangkat keras berukuran kecil yang umumnya digunakan untuk menghubungkan televisi dengan jaringan atau internet. STB memiliki komponen seperti prosesor, RAM, *port hardware*, dan sistem operasi yang memungkinkan pengguna untuk mengakses berbagai layanan dan konten melalui televisi mereka. STB sering digunakan untuk *streaming* video, televisi digital, video *on demand* aplikasi internet, dan fungsi multimedia lainnya. Salah satu sistem operasi yang umum digunakan pada STB adalah Armbian, yang dirancang untuk berjalan pada perangkat dengan arsitektur ARM dan sering digunakan pada banyak komputer papan tunggal (*single-board computer*).[5]

2.6 VMware vSphere

VMware vSphere adalah sebuah platform virtualisasi yang dikembangkan oleh perusahaan teknologi VMware. Platform ini memungkinkan organisasi untuk mengelola dan menyatukan sumber daya komputasi, penyimpanan, dan jaringan secara virtual. Dengan menggunakan vSphere, perusahaan dapat menciptakan lingkungan data center virtual yang efisien dan dapat dielastisitas.[6]

2.7 *Brute Force*

Bruteforce adalah suatu metode atau teknik yang digunakan dalam keamanan siber untuk mencoba semua kemungkinan kombinasi yang mungkin dari kata sandi atau kunci enkripsi sampai kombinasi yang benar ditemukan. Ini adalah pendekatan yang sangat kasar dan sering kali memerlukan waktu yang lama, terutama jika kata sandi yang harus dipecahkan sangat panjang atau kompleks [7]

2.8 *Denial of Service (DoS)*

Denial of Service (DoS) adalah serangan terhadap suatu sistem atau layanan dengan cara membanjiri sumber daya yang tersedia sehingga sistem atau layanan tersebut tidak dapat memenuhi permintaan yang sah.
Umumnya serangan DoS dan DDoS telah menjadi ancaman besar pada jaringan komputer. Dalam serangan seperti itu, karena menguras sumber daya, beberapa layanan dinonaktifkan, dan kinerja jaringan diturunkan. Serangan ini dianggap berhasil ketika penyerang dengan sengaja menggunakan sumber daya yang mencegah host menggunakan layanan yang ditargetkan.[8]

2.9 Fail2ban

Fail2ban adalah perangkat lunak sumber terbuka yang dapat digunakan secara gratis dan bebas, yang dibangun dan dikembangkan menggunakan bahasa pemrograman Python. Fail2ban berfungsi untuk membatasi akses dan menetapkan aturan terhadap akses pada sebuah server. Fail2ban bekerja dengan mengubah aturan konfigurasi *firewall* dengan konfigurasi yang ada pada Fail2ban sendiri. Ketika Fail2ban dijalankan, ia

akan mengambil alih fungsi *firewall* yang ada di server. [9]

2.10 Telegram

Telegram merupakan aplikasi pesan instan yang bersifat *open source* dengan memanfaatkan sistem cloud sebagai media penyimpanan utama yang digunakan untuk menyampaikan informasi jarak jauh dengan cepat, akurat dan terdokumentasi. [10]

3. METODE PENELITIAN

3.1 Waktu dan Tempat Penelitian

Waktu penelitian dilakukan mulai bulan September 2023 hingga November 2023 di PSDKU Universitas Lampung di Way Kanan dengan jadwal penelitian pada table 1 sebagai berikut:

Tabel 1. Jadwal Penelitian

No	Aktivitas	Bulan Agustus – Desember 2023				
		8	9	10	11	12
1	Perumusan Masalah					
2	Studi Literatur					
3	*Prepare*					
4	*Plan*					
5	*Design*					
6	*Implement*					
7	*Operate*					
8	*Optimize*					
9	Penulisan Laporan Akhir					

3.2 Alat Penelitian

Di dalam pelaksanaan penelitian, digunakan perangkat pendukung berupa sebuah komputer dengan spesifikasi yang ditunjukan pada gambar dibawah:

3.2.1 Perangkat Lunak *(Software)*

Perangakat lunak yang akan digunakan dalam menyelesaikan tugas akhir ini adalah:

Tabel 2 Software

No	Perangkat Lunak
1	Windows 11
2	Sistem Operasi Ubuntu 20.04 LTS, Ubuntu 23.04
3	Sistem Operasi Armbian
4	Draw.io
5	Microsoft Word 2019
6	Mendeley Desktop
7	Putty 0.78.0.0
8	Telegram
9.	Slowloris
10.	Hydra

3.2.2 Perangkat Keras *(Hardware)*

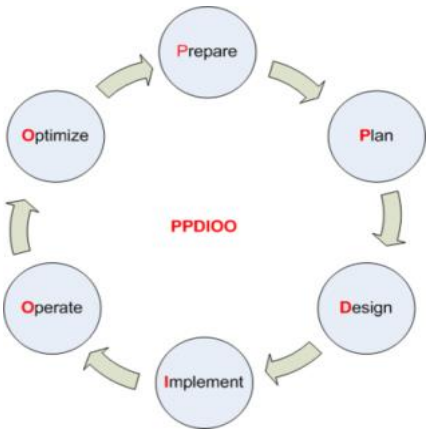
Perangakat keras yang akan digunakan dalam menyelesaikan tugas akhir ini adalah:

Tabel 3 Hardware

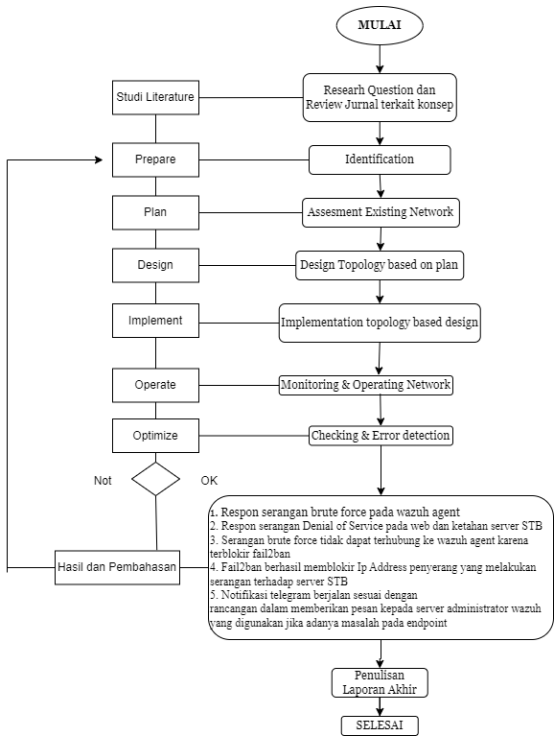
Perangkat Keras				
Jenis	Set Top Box HG680P	PC Axioo MyPC One Pro K5 (8N2) /LaptopLenovo IdeaPad 330-14IGM	Access Point Ruijie RG-RAP2200(E)	Server PSDKU Rainer Intel Corporation S2600STB
CPU	Quad Core ARM Cortex-A53@ up to 1.51 Ghz	Intel® CoreTM i5-1135G7 / Intel® Celeron® N400 CPU @1.10Ghz, 1101 Mhz,		32 CPUs x Intel® Xeon ® Silver 4216 CPU @2.10GHz 67GHz
RAM	2 GB	8GB / 4 GB		16 GB
Storage	8 GB	256 GB / 500 GB		2 TB
OS	Android 6.1 Marsmellow	Windows		VMware vSphere Ubuntu 23.04
Interface			802.11ac Wave2, 1267Mbps	
Operating Modes	-	-	2.4G/5G Router, Wireless Router	
Wireless	-	-	IEEE 802.11b/g/n	
Protocols	-	-	IPv4, IPv6	

3.3 Tahapan Penelitian

Konsep Tahapan metodologi yang dilakukan pada penelitian ini adalah menggunakan Metode PPDIOO Cisco. PPDIOO Cisco dirancang untuk mendukung pengembangan jaringan. PPDIOO memiliki 6 *Phase* (Tahapan) yaitu *prepare, plan, design, implement, operate, optimize.*



Gambar 2. Metode PPDIOO



Gambar 3. Flowchart Tahapan Penelitian

3.4 Persiapan *(Prepare)*

Pada tahap ini mengidentifikasi masalah konsep keamanan jaringan yang belum tersedia di jaringan PSDKU khususnya di lab komputer dengan melakukan pemantauan serta wawancara yang dilakukan untuk mempersiapkan apa saja yang akan dilakukan untuk melakukan penelitian di PSDKU, terdapat beberapa hasil yang telah didapatkan yaitu Server di PSDKU hanya memiliki 1 server saja, memiliki 2 Lab komputer yang dimana untuk penelitian ini hanya menggunakan Lab Komputer 1 , serta terdapat switch serta access point untuk mengakses jaringan dan internet yang berada di Lab Komputer 1. Server PSDKU belum memiliki keamanan untuk mendeteksi aktivitas biasa ataupun ancaman dari serangan siber, Untuk analisis pada tugas akhir ini, akan melakukan percobaan simulasi yang dilakukan pada server jaringan PSDKU dengan menggunakan Hardware Set Top Box (STB) yang sudah terinstall menjadi Server Armbian 20.10, dan melakukan uji coba penyerangan Brute Force dan Denial Of Service menggunakan beberapa PC yang sudah terinstall kali linux yang berada di Lab Komputer terdahap server jaringan PSDKU. Kemudian mempersiapkan desain topologi sistem keamanan jaringan yang akan di implementasikan pada jaringan PSDKU, topologi tersebut dibuat berdasarkan hasil pengamatan topologi jaringan pada server PSDKU. melakukan installasi wazuh server di *cloud* pada *platform idcloudhost* guna untuk *monitoring* peristiwa keamanan dari wazuh *agent*. Kemudian melakukan installasi wazuh *agent* pada server jaringan PSDKU di lab komputer menggunakan server utama PSDKU. Installasi kali linux pada beberapa PC Lab juga dilakukan untuk berperan sebagai penyerang wazuh *agent*, hal ini dilakukan untuk uji coba terhadap sistem keamanan jaringan apakah dapat berjalan dengan baik atau tidak. melakukan aktivasi wazuh *agent* pada server jaringan PSDKU di lab komputer serta melakukan uji coba serangan *bruteforce* dan *Denial of Service* pada komputer server jaringan PSDKU. Selanjutnya melakukan respon terhadap serangan siber yang terjadi pada wazuh *agent*, *software* yang digunakan yaitu fail2ban yang akan memblokir *ip address* penyerang selama beberapa waktu. Hal ini dilakukan untuk pencegahan awal untuk menghindari kerusakan yang lebih serius. Serta mengintegrasikan Wazuh ke Telegram untuk mendeteksi adanya segala aktivitas di server. Hal ini digunakan untuk membantu administrator mengetahui masalah yang terjadi pada server ketika tidak sedang berada di ruang monitoring server.

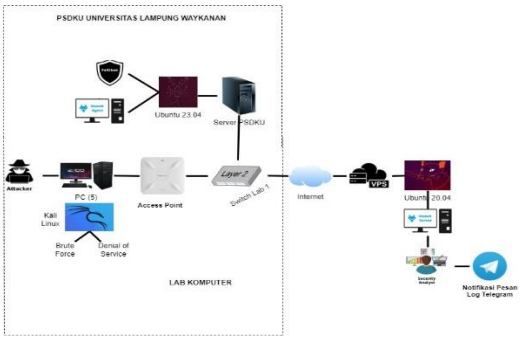
3.5 Perencanaan *(Plan)*

Pada phase metode ini merencanakan bahan untuk menganalisa mengapa harus serangan Brute Force dan DoS yang akan digunakan untuk uji coba sistem keamanan jaringan ini. Setelah menganalisa dan membaca beberapa jurnal dan website dapat disimpulkan bahwa serangan brute force dan DoS merupakan serangan yang popular dikalangan cyberattack karena memiliki catatan aktivitas tindakan merusak terhadap sistem atau jaringan di Indonesia maupun diseluruh dunia. Serangan brute force merupakan metode serangan spesifik dan relatif lama namun lebih disukai untuk akses sistem, terutama menargetkan penyedia layanan cloud. 83% orang Amerika membuat kata sandi yang lemah dalam hal panjang (kurang dari 10 karakter) dan kompleksitas karakter (hanya angka dan huruf) dan 53% menggunakan kata sandi yang sama di seluruh akun**.** 5% dari seluruh pelanggaran data disebabkan oleh serangan brute force. Untuk serangan *Denial of Service* (DoS) jenis serangan dunia maya yang bertujuan mengganggu situs web (dan jenis properti Internet lainnya) agar tidak tersedia bagi pengguna yang sah dengan cara membanjirinya. Serangan ini lebih sering dilakukan dengan membanjiri host atau jaringan yang ditargetkan dengan permintaan layanan yang tidak sah. Ciri khas dari serangan ini adalah penggunaan alamat IP palsu, yang mencegah server mengautentikasi pengguna. DoS *attack* tetap menjadi ancaman nyata bagi lalu lintas jaringan
aplikasi, *server*,ataupun *website* hingga saat ini.

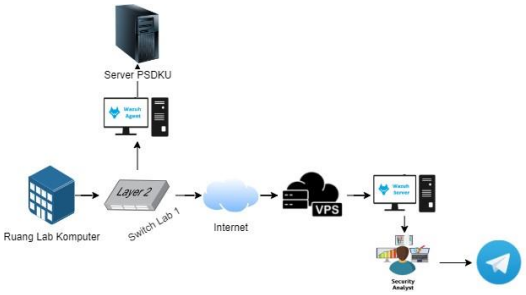
3.6 Desain *(Design)*

3.6.1 Topologi Rancangan Sistem

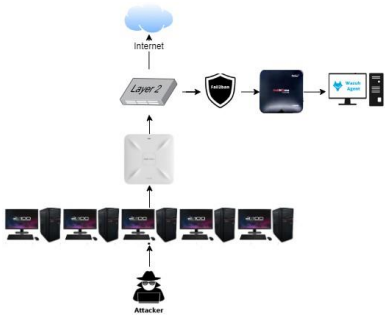
Pada tahapan ini setelah melakukan Simulasi terhadap server STB dan berhasil, maka akan dilanjutkan untuk membuat Topologi sistem keamanan jaringan yang akan diimplementasikan pada jaringan Lab Komputer PSDKU Universitas Lampung Way Kanan menggunakan Server Utama PSDKU.



Gambar 4 Topologi Rancangan Sistem



Gambar 5 Topologi Deteksi Keamanan



Gambar 6 Topologi Response Serangan Siber

4. HASIL DAN PEMBAHASAN

4.1 Implementasi *(Implement)*

Spesifikasi untuk Implementasi Wazuh

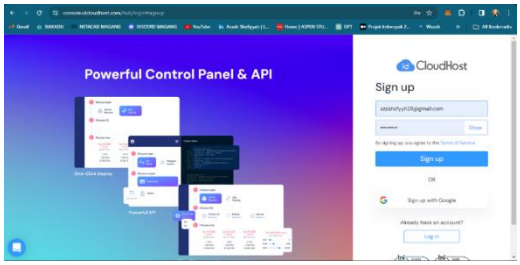
CPU	Prosesor Dual-Core atau setara
RAM	4GB
STORAGE	50GB

Gambar 7 Minimum Resources

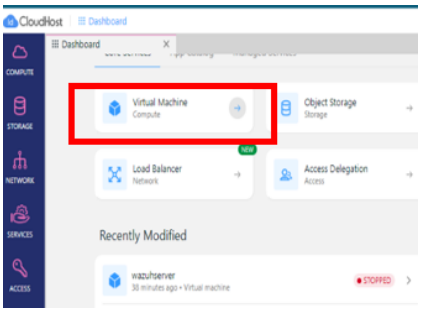
CPU	Prosesor Qua-Core atau lebih
RAM	8GB
STORAGE	100GB

Gambar 8 Recommended Resources

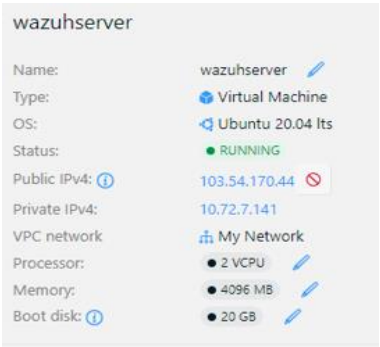
4.1.1 Installasi Wazuh Server



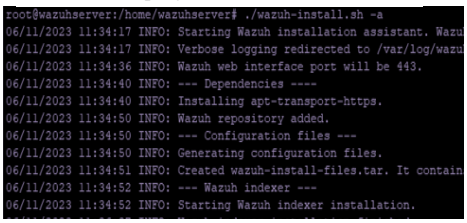
Gambar 9 Halaman Login IdCloudHost



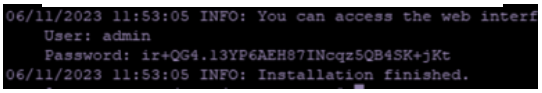
Gambar 10 Dashboard IdCloudHost



Gambar 11 Spesifikasi VM Wazuh Server

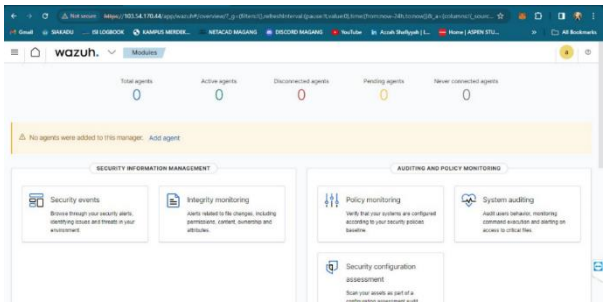


Gambar 12 Proses Installasi



Gambar 13 Hasil Installasi

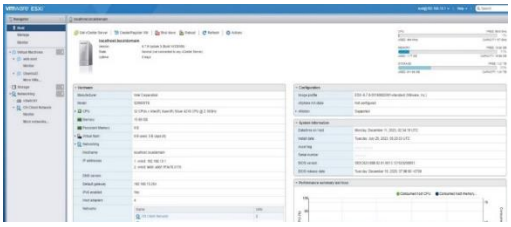
Gambar 14 Halaman Login Wazuh Server



Gambar 15 Dashboard Wazuh Server

4.1.2 Konfigurasi Server PSDKU

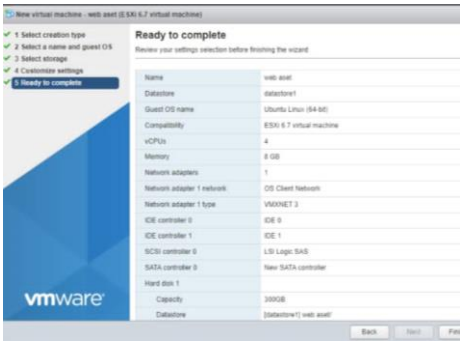
Konfigurasi dilakukan dengan menggunakan VMware vSphere. Server yang digunakan di PSDKU berupa *hardware* Rainer Intel Corporation dengan Model S2600 STB, CPU 32 CPUs x Intel® Xeon® Silver 4216 CPU @2.10Ghz yang memiliki Memory 16GB dan Storage 2TB. Dengan jaringan Local yang hanya bisa digunakan di lingkungan PSDKU.



Gambar 16 Spesifikasi Hardware Server PSDKU

4.1.2.1 Installasi Server PSDKU

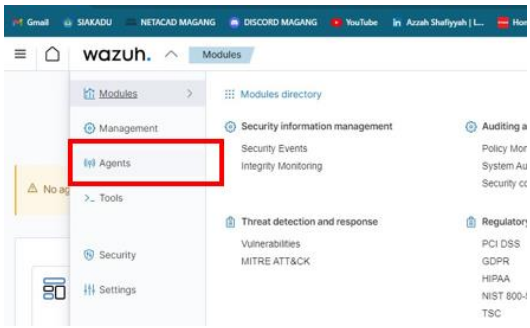
Untuk langkah selanjutnya setelah mempersiapkan server VMware vSphere, akan membuat virtual machine Exsi 6.7 dan melakukan installasi OS Server Ubuntu 23.04, dengan spesifikasi 4 CPUs, Memory 8GB, serta Storage 300GB.



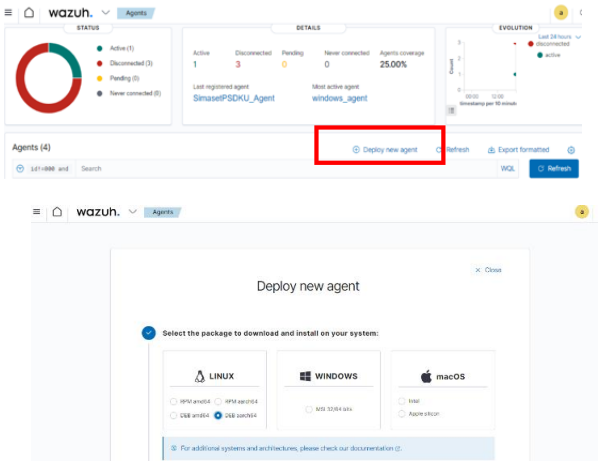
Gambar 17 Spesifikasi Server Aset PSDKU

4.1.3 Konfigurasi Wazuh Agent

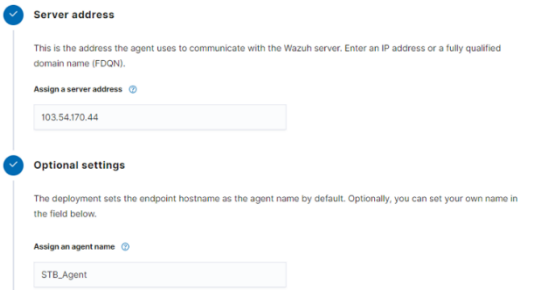
4.1.3.1 Deploy Wazuh Agent PSDKU



Gambar 18 Deploy Wazuh Agent

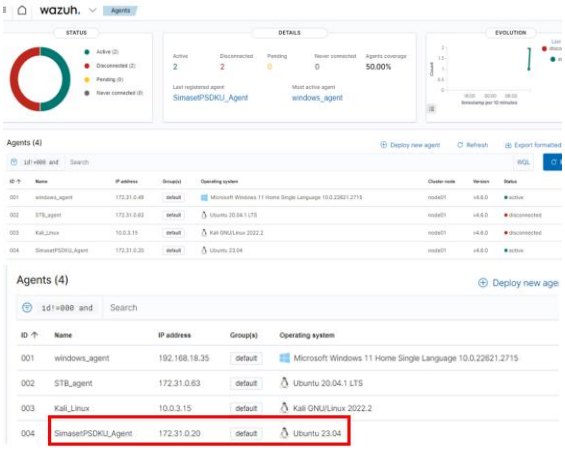


Gambar 19 Proses Deploy Wazuh Agent



Gambar 20 Server address & Optional settings Wazuh

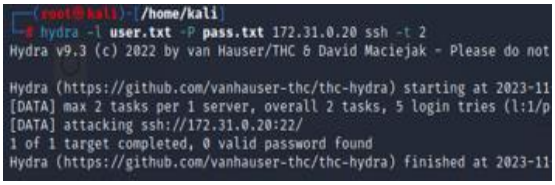
Gambar 21 URL Installasi dan Enroll Wazuh Agent



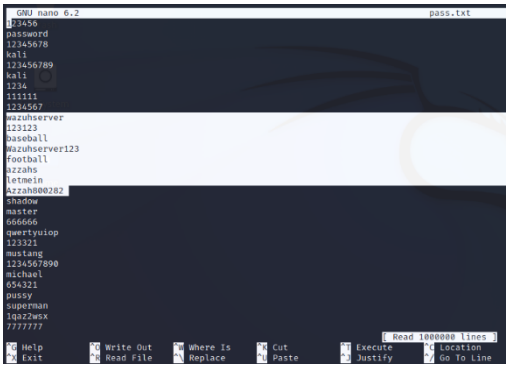
Gambar 22 Tampilan Dashboard SimasetPSDKU_Agent

4.2 Operasi *(Operate)*

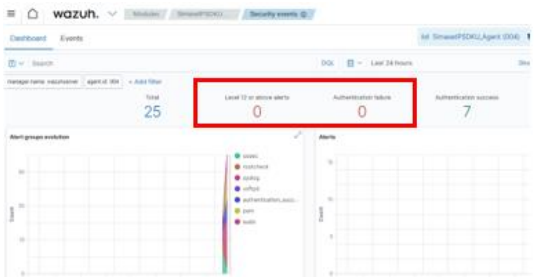
4.2.1 Uji Coba Serangan Brute Force pada Wazuh Agent



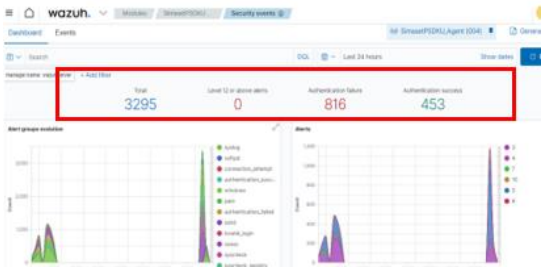
Gambar 23 Serangan Brute Force SimasetPSDKU_Agent



Gambar 24 kombinasi 1.000.000 username dan password



Gambar 25 Security Events SimasetPSDKU_Agent sebelum serangan



Gambar 26 Hasil Deteksi Serangan Brute Force SimasetPSDKU_Agent

FIM: Recent events

Time	Path	Action	Rule description	Rule Level	Rule Id
Nov 25, 2023 @ 11:20:06.755	/usr/bin/fail2b...	added	File added to ...	5	554
Nov 25, 2023 @ 11:20:06.755	/usr/bin/fail2b...	added	File added to ...	5	554
Nov 25, 2023 @ 11:20:06.755	/usr/bin/whois	added	File added to ...	5	554
Nov 25, 2023 @ 11:20:06.754	/usr/bin/fail2b...	added	File added to ...	5	554
Nov 25, 2023 @ 11:20:06.745	/usr/bin/fail2b...	added	File added to ...	5	554

previous_output

Nov 10 13:45:15 localhost sshd[6900]: Failed password for invalid user user.txt from 172.31.0.44 port 51456 ssh2
Nov 10 13:45:12 localhost sshd[6901]: Failed password for invalid user user.txt from 172.31.0.44 port 51460 ssh2
Nov 10 13:45:12 localhost sshd[6900]: Failed password for invalid user user.txt from 172.31.0.44 port 51456 ssh2
Nov 10 13:45:10 localhost sshd[6898]: Disconnected from invalid user user.txt 172.31.0.44 port 51454 [preauth]
Nov 10 13:45:10 localhost sshd[6900]: Invalid user user.txt from 172.31.0.44 port 51456
Nov 10 13:45:10 localhost sshd[6901]: Invalid user user.txt from 172.31.0.44 port 51460
Nov 10 13:45:10 localhost sshd[6898]: Invalid user user.txt from 172.31.0.44 port 51454

rule.description: sshd: brute force trying to get access to the system. Non existent user.

rule.mitre.tactic: Credential Access, Lateral Movement

rule.mitre.technique: Password Guessing, SSH

rule.mitre.technique: Exploit Public-Facing Application, Brute Force

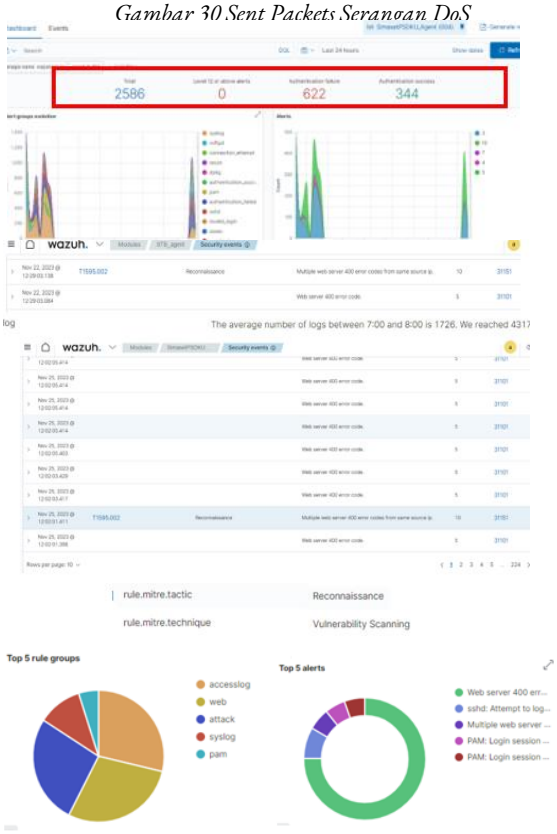
Gambar 27 Hasil Detail Deteksi Serangan Brute Force

4.2.2 Uji Coba Serangan Denial of Service (DoS) pada Wazuh Agent

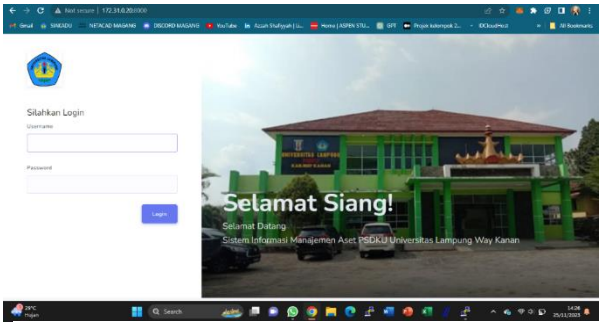
Gambar 28 Software Slowloris

Gambar 29 Persiapan Serangan DoS pada Server PSDKU

Gambar 30 Sent Packets Serangan DoS



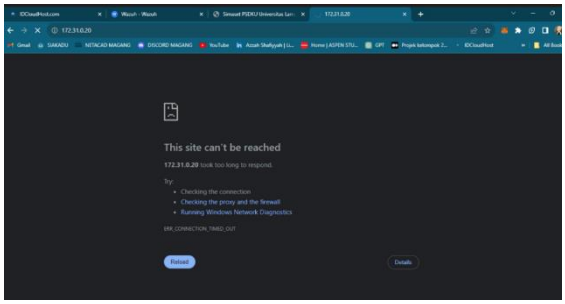
Gambar 31 Hasil Detail Deteksi Serangan DoS



Gambar 32 Web Server SimasetPSDKU_Agent

Tabel 4 Hasil Jumlah Simulasi serangan Tampilan Web Server PSDKU

No	Jumlah serangan tiap *personal computer* (PC)						Tampilan web server PSDKU
	PC 1	PC 2	PC 3	PC 4	PC 5	Total Serangan	
1	12.580	15.123	13.252	18.890	18.989	78.834	Dapat diakses
2	22.577	25.679	23.453	25.443	28.624	204.610	Dapat diakses
3	50.798	55.138	65.868	75.908	80.765	328.477	Dapat diakses
4	120.706	130.679	140.008	135.972	155.258	682.623	Dapat diakses
5	200.407	240.872	245.510	259.084	280.754	1.226.627	Dapat diakses
6	320.175	365.182	380.073	400.829	425.972	1.892.231	Dapat diakses
7	455.701	480.369	530.687	580.950	600.578	2.648.285	Dapat diakses
8	640.325	670.531	700.028	735.465	775.664	3.522.013	Dapat diakses
9	810.678	860.099	935.130	995.490	1.010.701	4.875.384	Tidak Dapat diakses
10	1.040.464	963.707	1.120.890	1.190.019	1.200.304	5.515.384	Tidak dapat diakses



Gambar 33 Hasil Web Server PSDKU tidak dapat diakses

Gambar diatas menunjukkan Hasil bahwa Web Server Simaset PSDKU yang di uji coba menggunakan serangan *Denial of Service* (DoS) tersebut menjadi *overload* dan *down* serta tidak dapat diakses sementara karena disebabkan oleh serangan *Denial of Service* (DoS) yang dilakukan dengan total sockets serangan yang mencapai 5.515.384 total keseluruhan koneksi http.

Tabel 5 Hasil Data Simulasi Performance CPU, Network, Memory Server PSDKU

No	Hasil CPU Server Utama PSDKU				
1	13%	17%	24%	21%	29%
2	35%	29%	22%	33%	36%
3	42%	37%	50%	46%	48%
4	51%	49%	64%	70%	42%
5	68%	54%	70%	81%	54%
6	77%	87%	82%	80%	76%
7	92%	91%	92%	95%	82%
8	94%	98%	97%	99%	96%
9	97%	100%	100%	100%	100%
10	100%	100%	100%	100%	100%

No	Hasil Network Server Utama PSDKU				
1	116 Mbps	102 Mbps	130 Mbps	112 Mbps	133 Mbps
2	98 Mbps	87 Mbps	113 Mbps	104 Mbps	113 Mbps
3	80,1 Mbps	72,1 Mbps	97 Mbps	83,2 Mbps	92,5 Mbps
4	56 Mbps	66 Mbps	78 Mbps	69 Mbps	77 Mbps
5	37 Mbps	32 Mbps	57 Mbps	65,3 Mbps	44,8 Mbps
6	23,1 Mbps	15,1 Mbps	37,1 Mbps	49,2 Mbps	28 Mbps
7	17,2 Mbps	23,2 Mbps	17,2 Mbps	50,2 Mbps	42,8 Mbps
8	2,1 Mbps	5,7 Mbps	4,1 Mbps	11,6 Mbps	8,6 Mbps
9	2,1 Mbps	3,7 Mbps	5,6 Mbps	9,91 Mbps	7,9 Mbps
10	2,2 Mbps	6,2 Mbps	3,5 Mbps	6,6 Mbps	9,2 Mbps

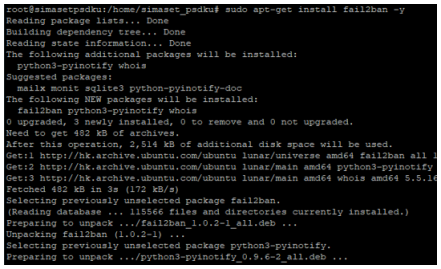
No	Hasil Memory Server Utama PSDKU				
1	1,8 GB	1,2 GB	1,7 GB	1,2 GB	1,6 GB
2	2,9 GB	3,4 GB	2,8 GB	3,6 GB	2,4 GB
3	3,6 GB	5,2 GB	4,2 GB	4,7 GB	4,0 GB
4	6,7 GB	7,7 GB	6,8 GB	8,5 GB	6,3 GB
5	8,8 GB	8,0 GB	7,9 GB	7,6 GB	8,9 GB
6	10,8 GB	11,8 GB	10,2 GB	9,3 GB	11,1 GB
7	12,1 GB	13,6 GB	12,8 GB	11,3 GB	13,9 GB
8	14,8 GB	14,1 GB	15,5 GB	15,1 GB	15,3 GB
9	16 GB	15,5GB	16 GB	16 GB	16 GB
10	15,8 GB	15,9 GB	16 GB	16 GB	16 GB

Gambar 34 Performance CPU, Network, Memory Server PSDKU

Dari hasil Uji coba serangan *Denial of Service* (DoS) yang telah dilakukan dengan menggunakan 5 (lima) buah PC *(Personal Computer)* di lab komputer PSDKU telah diperoleh hasil yang menunjukkan bahwa Server Utama PSDKU memiliki ketahanan yang mampu menerima dan melayani koneksi http dibawah 3.522.013 koneksi dari total keseluruhan soket. Untuk performance dari server PSDKU dapat dilihat dari data Tabel 5 bahwa CPU mencapai 100%, Network mencapai 2,2 Mbps yang artinya jaringan sangat lambat bahkan tidak dapat mengakses web server, dan Memory mencapai 16GB yang artinya persediaan memory dari Server PSDKU menjadi terbatas bahkan habis yang mengakibatkan web server tidak dapat diakses.

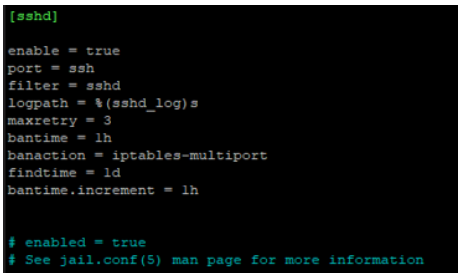
4.3 Optimasi *(Optimize)*

Optimasi adalah upaya untuk meningkatkan pertahanan dan respons terhadap serangan cyber, meningkatkan kemampuan sistem deteksi untuk mengenali pola serangan yang baru atau berubah. Serta menyiapkan response cepat dan efisien terhadap insiden keamanan untuk meminimalkan dampak serangan. Didalam tugas akhir ini Optimasi dalam response serangan cyber adalah dengan menggunakan Fail2ban.

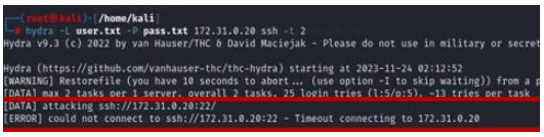


Gambar 35 Installasi Fail2ban pada SimasetPSDKU_Agent

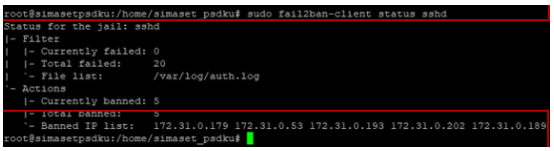
4.3.2 Konfigurasi File Fail2ban



Gambar 36 Konfigurasi file jail.local

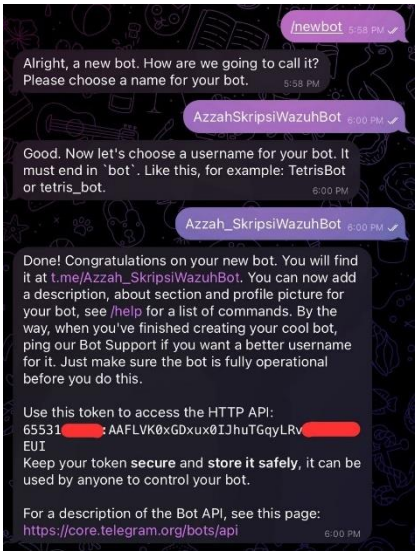


Gambar 37 Hasil Penerapan Fail2ban

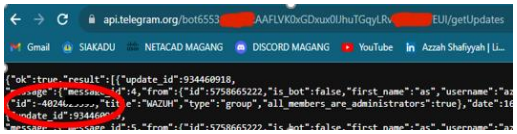


Gambar 38 Daftar Ip Address yang terblokir oleh Fail2ban

4.3.3 Integrasi Wazuh *Alert* dengan Telegram Bot

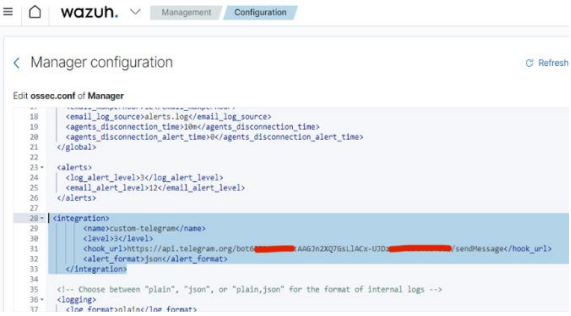


Gambar 39 pembuatan username dan BOT

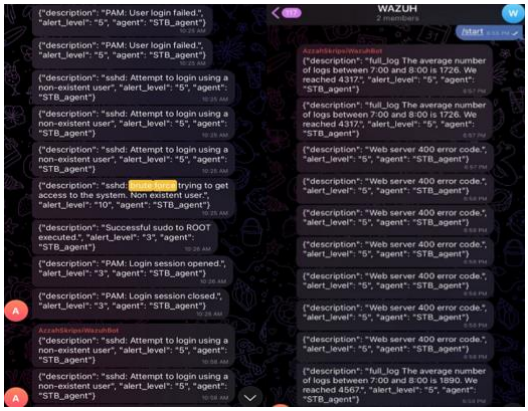


Gambar 40 No Chat ID dan HTTP API

4.3.1.2 Integrasi dengan Wazuh Server



Gambar 41 Konfigurasi Custom API Integration Wazuh



Gambar 42 1 Notifikasi Brute force dan DoS pada Wazuh Agent

5. KESIMPULAN

a. Berhasil mengimplementasikan sistem keamanan jaringan yang dapat mendeteksi dan merespon serangan siber menggunakan Wazuh. Administrator dapat memonitoring aktivitas keamanan menggunakan Wazuh.

b. Wazuh berhasil mendeteksi serangan *Brute force* ya4ng dilakukan didalam jaringan.

c. Fail2ban berhasil diterapkan dan dapat mencegah aktivitas serangan bruteforce.

d. Wazuh tidak dapat mendeteksi serangan *Denial of Service* (DoS) apabila serangan dilakukan dengan skala dan intensitas yang kecil dengan jumlah rata-rata koneksi dibawah 4000 koneksi http.

e. Serangan *Denial of Service* berhasil dilakukan dengan hasil yang menunjukkan bahwa Server Utama PSDKU memiliki ketahanan dalam menerima dan melayani koneksi HTTP dibawah 3.522.013 koneksi dari total keseluruhan soket koneksi HTTP.

f. Integrasi Wazuh ke Telegram berhasil dilakukan dengan baik dan mampu mendeteksi adanya segala aktivitas di server. Hal ini membantu administrator mengetahui masalah yang terjadi pada server ketika tidak sedang berada di ruang monitoring server.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak-pihak terkait yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] Aji, R. P., Prayudi, Y., & Luthfi, A. Analysis Of Brute Force Attack Logs Toward Nginx Web Server On Dashboard Improved Log Logging System Using Forensic Investigation Method. *Jurnal Teknik Informatika (Jutif)*, *4*(1), 39-48,2023

[2] Kamal and Setiawan. Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII. *Jurnal Informatika Universitas Islam Indonesia* Vol. 2 No. 2, 2021

[3] Fitri Nova, Pratama, M. D., & Prayama, D. Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos, 2022

[4] Sampurna, M. R. Implementasi Hydra, FFUF Dan WFUZZ Dalam Brute Force DVWA: Implementasi Hydra, FFUF Dan WFUZZ Dalam Brute Force DVWA. *Journal of Network and Computer Applications (ISSN: 2964-6669)*, *1*(2), 25-33, 2022

[5] Prasetyo, K. A., Idhom, M., & Wahanani, H. E. . Sistem Pencegahan Serangan Bruteforce Pada Multiple Server Dengan Menggunakan Fail2ban. *Jurnal Informatika dan Sistem Informasi*, *1*(3), 789-796.,2020

[6] Wongkar, S., Sinsuw, A. A., & Najoan, X. Analisa implementasi jaringan internet dengan menggabungkan jaringan lan dan wlan di desa kawangkoan bawah wilayah amurang ii. *Jurnal Teknik Elektro dan Komputer*, *4*(6), 62-68, 2015
[7] Luthfah, D. Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia (Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law). *terAs Law Review: Jurnal Hukum Humaniter dan HAM*, *3*(1), 11-22,2021
[8] Wicaksana, R. H., Munandar, A. I., & Samputra, P. L. Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 (A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic). *JURNAL IPTEKKOM (Jurnal Ilmu Pengetahuan & Teknologi Informasi)*, *22*(2), 143-158,2020
[9] Patuke, R., Mulyanto, A., & Takdir, R. Pengukuran Kinerja Set Top Box (STB) Sebagai Penyimpanan Cloud. *Diffusion: Journal of*
[10] Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis, 42(8), 1643-1669, 2022