Implementasi Honeypot Dengan Wazuh Untuk Identifikasi Dan Deteksi Serangan Siber Pada Server

1st Arifian Ramadhan
S1 Teknik Telekomunikasi
Telkom University Purwokwerto
Purwokerto, Indonesia
arifianramadhanar@student.telkomuniversity.ac.id

2nd Bongga Arifwidodo
S1 Teknik Telekomunikasi
Telkom University Purwokwerto
Purwokerto, Indonesia
bonggaa@telkomuniversity.ac.id

3rd Jafaruddin Gusti Amri Ginting
S1 Teknik Telekomunikasi
Telkom University Purwokwerto
Purwokerto, Indonesia
jafargustiamri@telkomuniversity.ac.id

Abstrak--Digitalisasi pada sektor industri semakin berkambang pesat, dengan digitalisasi proses pekerjaan mampu selesai dengan lebih cepat, pada industri yang sudah menerapkan digitalisasi ini membutuhkan *server* yang mampu menampung semua pekerjaan dan memiliki sistem keamanan yang kuat. *Server* sering sekali menjadi sasaran peretas untuk melakukan serangan siber karena dengan menyerang suatu *server* akan mengakibatkan kelumpuhan pada suatu perusahaan, salah satu keamanan pada *server* yaitu *Honeypot* dan *Wazuh*. Kedua sistem keamanan tersebut dapat diimplementasikan ke *server* terutama *server* yang menggunakan OS *linux*, keduanya dapat digunakan sebagai identifikasi dan deteksi serangan siber. *Honeypot* adalah sistem keamanan yang membuat server tiruan, berfungsi sebagai jebakan dan *wazuh* merupakan *platform* sistem deteksi serangan *cyber open source*. Oleh karena itu suatu *server* harus sangat kuat sistem keamanannya, *honeypot* dan Intrusion Detection System (IDS) menjadi salah satu solusi untuk permasalahan ini. Penelitian ini berfokus untuk menganalisis system keamanan pada *server* menggunakan *Honeypot* dan dikombinasikan dengan IDS. Adapun IDS yang akan digunakan yaitu *Wazuh* dan *honeypot* yang digunakan yaitu *honeypot cowrie*. Skenario pada penelitian ini menggunakan 2 *device* yaitu *server* sebagai target dan laptop sebagai agen *wazuh* dan penyerang menggunakan VM *kali linux* pada laptop, lalu melakukan instalasi sistem keamanan pada komputer *server*. Proses serangan dilakukan penyerang menggunakan OS *Kali linux* pada VM kepada *server* yang sudah dikonfigurasikan dengan sistem keamanan, serangan dilakukan menggunakan *tool medusa, metasploit dan hping3*, beberapa serangan yang dilakukan yaitu, *Dos, bruteforce* dan *malware (backdoor)*, pada hasil pengujian serangan diperoleh bahwa *wazuh* dapat mendeteksi serangan dengan jeda 5 menit setelah serangan diluncurkan dan masuk ke *server honeypot cowrie* bukan *server* asli. Pada pengujian kualitas jaringan ketika server diserang, diperoleh hasil Qos yaitu *Throughput: 393 kb/s*, *Packet loss: 7.2 %, Delay: 16.65 ms* dan *Jitter: 16.66 ms*.

Kata Kunci : ***Honeypot*, *IDS, Wazuh***

I. PENDAHULUAN

Era digital merupakan era teknologi dengan kemajuan yang pesat. Dengan pesatnya penggunaan teknologi informasi dan komunikasi, ancaman siber juga meningkat [1]. Adanya pandemik Covid-19 membuat aktivitas serba dilakukan di rumah sehingga dituntut untuk menggunakan akses internet. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) melaporkan jumlah pengguna internet di Indonesia pada tahun 2024 mencapai 221.563.479 orang, dari total populasi Indonesia yang mencapai 278.696.200 jiwa pada tahun 2023. Dengan demikian, sekitar 79,5 persen dari seluruh penduduk Indonesia menggunakan internet [2]. *Federal Bureau Investigation* (FBI) menyatakan kejahatan di dunia siber meningkat sebanyak 300 persen, serangan umumnya dilakukan pada *server* [3]. *Monitoring server* sangat diperlukan sebagai upaya untuk mengamankan *server*, serangan seperti *malware*, *bruteforce ssh* dan *web attacks* sangat sering dilancarkan untuk mendapatkan akses terhadap *server* [4].

Penyerang akan mencoba mengeksploitasi kelemahan dalam sistem jaringan untuk mengejar tujuan mereka dengan mengalahkan layanan keamanan yang ada. Karena jaringan publik awalnya dibuat tanpa memperhatikan aspek keamanan, maka serangan dari penjahat siber semakin meningkat dari tahun ke tahun [5]. Oleh karena itu, perlu dilakukan monitoring pada *server* untuk memastikan data penting tetap aman dari aksi jahat. Untuk melakukan hal ini, perlu digunakan *tools* yang dapat memantau perkembangan pada *server*, Salah satu tools yang digunakan untuk monitoring *server* adalah *Wazuh* [3]. Adapun untuk meningkatkan keamanan server juga bias dikombinaskan dengan system honeypot yaitu system yang berfungsi untuk membuat layanan palsu. Implementasi Honeypot harus dilakukan dengan hati-hati dan diisolasi dengan baik agar tidak membahayakan keamanan system dan jaringan yang sebenarnya [6].

Pada pembuatan tugas akhir ini penulis membangun sistem HIDS yang terintregasi dengan *Honeypot* agar sistem tersebut mampu mencegah dan mendeteksi serangan siber secara real time [7]. HIDS menggunakan *wazuh* memiliki kelebihan dalam kelengkapan data hasil deteksi karena diletakkan pada *endpoint server*. Prototipe sistem monitoring tersebut dikembangkan untuk mempermudah *security analyst* dalam mendeteksi ancaman siber pada *endpoint server*. Prototipe sistem monitoring tersebut dimulai dengan merancang *Wazuh server* dan *Wazuh agent*. *Honeypot* berfungsi untuk membuat akses *server* palsu agar penyerang terjebak dalam sistem tersebut dan dapat dideteksi oleh IDS *Wazuh*.

II. KAJIAN TEORI

A. Wazuh

Wazuh merupakan *platform open source* yang digunakan untuk mendeteksi ancaman, melakukan *monitoring*, respon insiden, dan kepatuhan terhadap ancaman siber. *Wazuh* bisa digunakan untuk memonitor *endpoints*, layanan *cloud*, dan *containers* [3]. Dan untuk mengumpulkan dan menganalisis data dari sumber eksternal. [8]

B. Honeypot

Honeypot adalah suatu cara membuat sistem palsu atau layanan palsu yang berfungsi untuk menjebak pengguna yang mempunyai tujuan buruk atau menangkal usaha- usaha yang dapat merugikan sistem atau layanan, *honeypot* sendiri terdiri dari beberapa macam yaitu; *low interaction honeypot*, *medium interaction honeypot* dan h*igh interaction honeypot* [2]. *honeypot* yang digunakan pada proyek akhir ini yaitu *honeypot cowrie* yang diperuntukan mengatasi serangan *bruteforce*. *Honeypot cowrie* merupakan system keamanan yang digunakan untuk membuat akses *ssh* palsu, yaitu dengan mengalihkan *port* 22 *ssh* menjadi *port* yang di atur dalam konfigurasi cowrie [9].

C. Bruteforce Attack

Jenis serangan *bruteforce* adalah serangan yang bertujuan untuk membobol otentikasi sistem dengan menggunakan setiap *password* yang memungkinkan dengan kata lain serangan ini mencoba menggunakan *password* yang acak, metode *brute force* attack cukup banyak, mulai dari yang sederhana sampai melakukan *crack password* yang tersimpan pada database, pada tugas akhir ini serangan *bruteforce* dilakukan menggunakan *tool medusa* pada sistem operasi *kali linux.*

D. Malware

Malware merupakan sebuah program yang dibuat untuk masuk kedalam sebuah sistem, seperti suatu *server*, komputer, laptop maupun *handphone*. *Malware*, yang mencakup berbagai bentuk perangkat lunak berbahaya seperti *virus, worm*, dan *ransomware*, dapat menyebabkan kerusakan yang cukup signifikan pada sistem dan jaringan. Pada tugas akhir ini malware yang digunakan yaitu tipe *backdoor* yang akan dimasukan dalam *server*, serangan ini menggunakan *tools Metasploit* pada *kali linux* [10].

E. Denial Of Services (DOS)

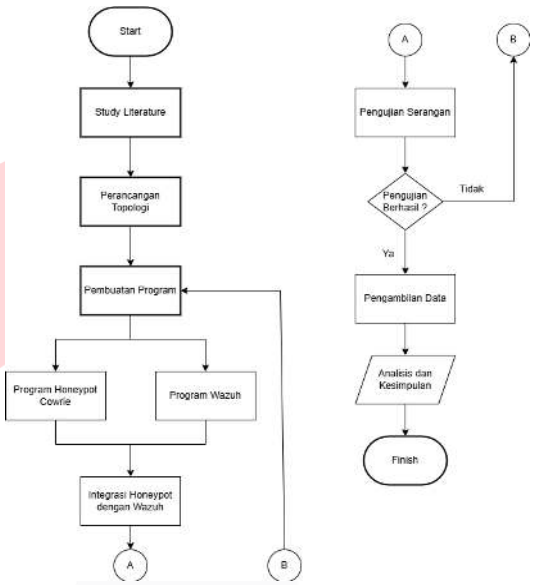
Denial of Service merupakan serangan siber yang bertujuan untuk membuat suatu layanan kelebihan beban, serangan ini menggunakan metode pengiriman paket secara terus menerus dalam jumlah yang cukup besar [11]. Serangan DOS pada tugas akhir ini bertujuan untuk melumpuhkan *server*, sehingga penyerang dapat melakukan *bruteforce* untuk mendapatkan akses *server*, adapun serangan DOS menggunakan spam paket ICMP dengan tool hping3 pada *kali linux* [3].

F. Quality Of Services (QOS)

Quality of Service (QoS) merupakan metode pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari satu layanan. Pada tugas akhir ini pengukuran QOS menggunakan *software wireshark*, dengan pengukuran selama satu menit. Parameter yang diukur yaitu *Throughput, Packet Loss, Delay* dan *Jitter* [12].

III. METODE

A. Alur Penelitian

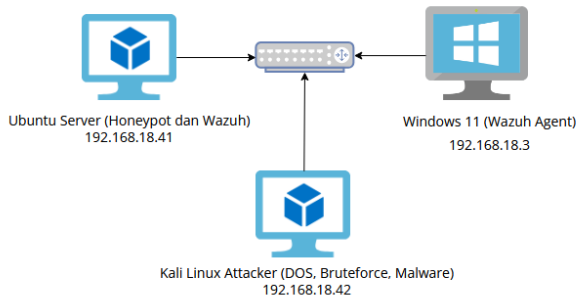


GAMBAR 1
ALUR PENELITIAN

Penelitian dimulai dengan mencari studi atau jurnal yang berkaitan dengan penelitian yang akan dilakukan, kata kunci penelitian yang dicari yaitu mengenai *Honeypot* dan *Wazuh*, umumnya serangan yang diujikan yaitu *bruteforce* dan *malware*. Kemudian penelitian dilanjutkan dengan membuat rancangan topologi yang akan diterapkan, topologi sesuai dengan perangkat yang akan digunakan, topologi yang digunakan yaitu *star*, dengan satu titik yaitu *hub*, *server* dan *client* akan terhubung dalam satu *hub*. Tahap berikutnya yaitu pembuatan program di *server*. Program yang di buat yaitu *honeypot* [13] dan *wazuh* [14], keduanya akan saling di integrasikan dalam satu *server. Server* akan menggunakan OS *linux* kemudian untuk *wazuh* juga akan di buat *wazuh agent* pada *client*. Setelah program dibuat akan dilakukan pengujian serangan menggunakan *Virtual*

Machine kali linux, serangan akan dilakukan oleh VM terhadap *server*, kemudian pada *wazuh agent client* dapat melihat serangan dan meneruskannya ke *server*. Serangan yang diujikan akan bervariasi, yang utama yaitu, bruteforce, *malware* dan DOS, menggunakan tools *hping3, medusa* dan *Metasploit* pada *kali linux*. Jika pengujian tidak berhasil maka akan dilakukan *troubleshoot* pada saat pembuatan program.

B. Rancangan Topologi



GAMBAR 2
TOPOLOGI RANCANGAN

Pada gambar dapat dilihat yaitu *server* menggunakan *OS Ubuntu* dengan IP 192.168.18.41 dan laptop menggunakan *OS Windows 11* dengan IP 192.168.18.3 sebagai *client* akan terhubung dalam satu jaringan, *server* pada gambar tersebut akan terdapat sistem keamanan yaitu program *honeypot* dan *wazuh server*, lalu pada *client* akan terdapat *wazuh agent*, keduanya akan terhubung menggunakan *router*, kemudian untuk penyerang menggunakan *OS kali linux* dalam satu jaringan juga dengan IP 192.168.18.42, serangan akan dilakukan kepada *server*, yaitu serangan DOS, *Bruteforce* dan *Malware* kemudian *wazuh agent* akan menerima *alert. Log* yang dianggap serangan akan menjadi alert pada *wazuh*, *log* tersebut juga akan terintegrasi dengan *honeypot* sehingga *server* benar-benar dianggap aman.

C. Alat dan Bahan

TABEL 1
PERANGKAT KERAS

Spesifikasi	Laptop
OS	Windows 11
System Memori (RAM)	8 GB
Storage HDD	500 GB
Storage SSD	128 GB

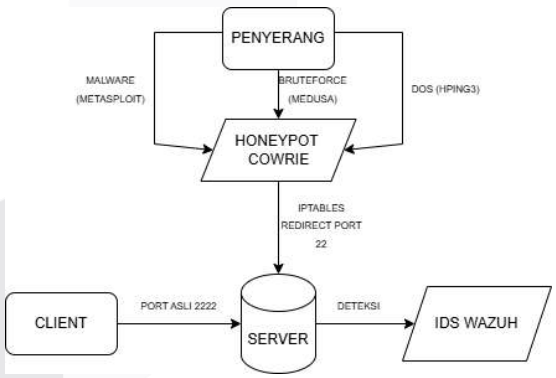
Perangkat keras yang digunakan menggunakan 1 buah laptop dengan spesifikasi seperti pada table, dimana OS untuk *server* dan penyerang akan menggunakan *Virtual Machine* pada *software virtualbox*. Semua VM tersebut akan diletakkan pada penyimpanan HDD yang memiliki kapasitas yang besar, sedangkan untuk penyimpanan SSD ini digunakan untuk OS *windows* 11 sendiri sebagai *wazuh agent*.

TABEL 2
PERANGKAT LUNAK

No	Software dan OS	Versi
1	Ubuntu	22.04
2	Kali Linux	21
3	Windows	11
4	Wazuh	4.10.0
5	Virtualbox	7.0
6	Honeypot cowrie	2.6.1
7	Hping3	3.0.0
8	Medusa	2.2
9	Metasploit	6.0.30
10	Wireshark	4.4.5

Pada table merupakan perangkat lunak yang digunakan pada tugas akhir ini, system operasi yang digunakan ada 3 yaitu *Ubuntu, kali linux* dan *windows*. Pada OS *Ubuntu* akan diintegrasikan sistem keamanan yaitu *wazuh* dan *honeypot cowrie*. Sedangkan penyerang akan menggunakan OS *kali linux* untuk melancarkan pengujian serangan. Pada *Windows* 11 akan menjadi wazuh agent yang akan diintegrasikan dengan *server*. *Software wireshark* digunakan untuk mengukur kualitas jarringan sesuai parameter QOS pada *server*.

D. Skema Serangan



GAMBAR 3
SKEMA SERANGAN

Pada gambar merupakan skema serangan yang akan dilakukan pada tugas akhir ini, sebelumnya sudah dilakukan konfigurasi sistem *honeypot cowrie* dan *wazuh*, sehingga untuk mengakses *server, client* menggunakan *port ssh* yang di ubah yaitu 2222, hal ini dikarenakan untuk *port* 22 sudah menjadi *honeypot cowrie*, dan port tersebut akan terlihat terbuka ketika dilakukan *port scan* oleh penyerang hal ini bertujuan untuk menarik perhatian penyerang, sehingga ketika melakukan penyerrangan akan masuk kedalam *honeypot cowrie*, untuk *client* yang ingin mengakses server bisa melalui *software putty* dengan *port* 2222, kemudian serangan dapat terdeteksi pada IDS *Wazuh*.

IV. HASIL DAN PEMBAHASAN

A. Skenario Percobaan

TABEL 3
SKENARIO PERCOBAAN

No	Skenario Pengujian/Percobaan	Alat Pengukuran
1	Pengujian Serangan DOS	hping3
2	Pengujian Serangan Bruteforce	medusa
3	Pengujian Serangan Malware	metasploit
4	Pengujian QOS	wireshark

Skenario percobaan pada implementasi tugas Akhir ini yaitu penyerang yang yang menggunakan system operasi *Kali Linux 21* akan melakukan penyerangan yaitu serangan *bruteforce*, DOS dan *malware* terhadap server yang menggunakan sistem operasi Ubuntu 22.04, serangan menggunakan *tool* pada *kali linux* yaitu *medusa, hping3* dan *Metasploit*. Pertama penyerang akan melakukan serang DOS dengan *hping3* serangan ini bertujuan untuk melumpuhkan *server*, selanjutnya penyerang akan mencoba *scanning port* pada *server* apakah terdapat *port* yang terbuka yang bisa menjadi celah untuk masuk, *port* 22 ssh akan terbuka karena *port* tersebut merupakan suatu jebakan, yaitu *honeypot cowrie*, penyerang akan melakukan serangan *bruteforce* untuk mendapat akses ssh pada *server*, setelah serangan *bruteforce* berhasil, penyerang akan mencoba membuat malware berupa *backdoor* yang akan masuk melalui *port* ssh tersebut. Data serangan akan terekam pada IDS *Wazuh*.

B. Hasil Percobaan

TABEL 4
HASIL PERCOBAAN SERANGAN

Serangan yang Diujikan	Status Serangan	Waktu Penyerangan	Waktu Terdeteksi
DOS	Berhasil dilakukan	03.00-03.13	03.18
Bruteforce	Berhasil dilakukan	03.15-03.21	03.26
Malware	Berhasil dilakukan	03.23-03.45	03.50

Pada table ditampilkan beberapa serangan yang dilakukan sesuai dengan skenario yang telah dibuat, terlihat bahwa serangan berhasil dilakukan tetapi serangan hanya masuk pada sistem jebakan yang telah dibuat yaitu *honeypot cowrie*, pada serangan DOS mengrimkan paket sejumlah 200, pada *bruteforce* serangan dilakukan dengan mengirim paket berupa percobaan *user* dan *password port* 22 *ssh* dan untuk serangan malware yaitu dengan mengirimkan *file backdoor* yang telah dibuat ke *server*. Serangan DOS dan *brutefroce* dapat dilakukan secara bersamaan. Dengan cara mengirm paket secara terus menerus.

C. Analisis

TABEL 5
PERBANDINGAN PADA WAZUH

Kondisi Server	Status serangan (berhasil dilakukan dan terdeteksi)		
	Bruteforce	DOS	*Malware*
IDS *Wazuh*	Gagal	Berhasil	Gagal
Honeypot	Berhasil	Berhasil	Berhasil
IDS *Wazuh* dan *Honeypot*	Berhasil	Berhasil	Berhasil

Pada tabel merupakan perbandingan serangan dari beberapa kondisi server, ketika hanya ada IDS wazuh pada server akan dilakukan uji coba serangan, apakah status serangan dapat terdeteksi atau tidak, hal ini dilakukan juga ketika hanya ada sistem keamanan honeypot. Ketika keduanya sudah terintegrasi pada server juga akan dilakukan uji coba serangan, kemudian akan dianalisa jika keduanya sudah terintegrasi apakah mempunyai efektifitas yang cukup baik sebagai system keamanan *server*. Pada saat kondisi *server* hanya *wazuh* yang menyala sedangkan *honeypot cowrie* dalam keadaan *off* serangan *bruteforce* akan gagal karena *port 22 ssh* tidak terdeteksi dan *bruteforce* tidak akan bisa dilakukan. Serangan *malware* juga tidak akan bisa dieksekusi oleh penyerang kerana tidak mempunyai akses *ssh.* Ketika sistem IDS *Wazuh* dan *honeypot cowrie* sudah menyala semua, maka semua serangan yang dilancarkan akan terdeteksi dan berhasil dilakukan tetapi serangan tersebut tidak benar-benar masuk dalam *server* melainkan hanya dalam *server* palsu yaitu *honeypot cowrie*.

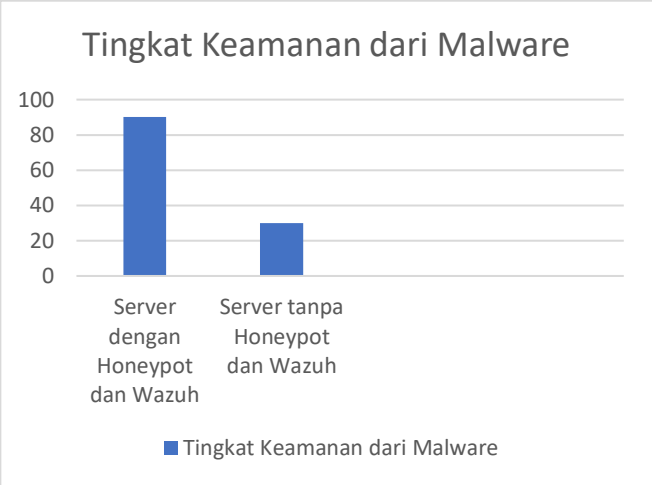
TABEL 6
HASIL QOS

Parameter QOS	Tanpa Serangan	Dengan Serangan	*Monitoring* pada sistem IDS
Throughput	706 kbps	393 kbps	Berjalan Normal
Packet Loss	4.3 %	7.2 %	
Delay	12.22 ms	16.65 ms	
Jitter	12.23 ms	16.66 ms	

Pada tabel merupakan pengujian kualitas jaringan pada server, parameter QOS yang diukur yaitu *Throughput, Packet loss, Delay* dan *Jitter*, pengujian dilakukan dengan dua kondisi *server*, yaitu ketika *server* tanpa terdapat aktivitas serangan dan ketika *server* diserang. Terlihat hasil yang didapat tidak mengalami perubahan nilai yang signifikan, ini menunjukan bahwa *server* yang sudah diintegrasikan dengan sistem keamanan tidak akan mengalami penurunan kinerja yang signifikan. Pada *monitoring* IDS *wazuh* juga tidak mengalami penurunan ketika *server* diserang.

Selanjutnya untuk serangan berupa *malware* dapat terdeteksi pada sistem IDS *wazuh*, serangan malware berupa

backdoor yang dibuat dengan menggunakan *Metasploit* pada *kali linux*, pada saat sistem IDS *wazuh* dan *honeypot cowrie* menyala, serangan malware hanya masuk kedalam *server* palsu yaitu *honeypot cowrie*, jadi penyerang tidak benar-benar mengeksekusi *malware* melalui akses *port ssh.*



GAMBAR 4
PERBANDINGAN KEAMANAN SISTEM DARI MALWARE

Pada gambar merupakan perbandingan sistem keamanan dari *malware*, jika *server* sudah dilengkapi dengan sistem keamanan *honeypot cowrie* dan *wazuh* maka tingkat keamananya 90 % dikarenakan *file malware* yang dieksekusi oleh penyerang akan masuk ke dalam *honeypot cowrie*, hal ini tidak 100 % dikarenakan masih ada celah yaitu jika *client* yang mengakses *server* dan tidak sengaja memasukan *file* yang terindikasi *malware*, ini menjadi suatu celah keamanan. *File malware* tersebut dapat dieksekusi oleh penyerang menggunakan *tools Metasploit* pada *kali linux*, dengan menggunakan *tools* tersebut penyerang dapat masuk kedalam system.

V. KESIMPULAN

Berdasarkan hasil perancangan, pengujian dan analisa proyek akhir ini yang telah dilakukan, dapat diambil beberapa kesimpulan yaitu implementasi sistem keamanan *server* dengan *honeypot* dan *wazuh* berhasil dilakukan dengan menggunakan sistem operasi *ubuntu 22.04* dan penyerang menggunakan *kali linux 21*. *Server* dapat dikonfigurasi dengan sistem keamanan *honeypot cowrie* dan dapat membuat *port ssh* palsu yang menjebak penyerang. *Wazuh* dapat mendeteksi serangan berupa DOS, *bruteforce* dan *malware* yang menyerang *server*, serangan tidak langsung terdeteksi melainkan terdapat jeda waktu 5 menit sampai terdeteksi. Pengujian hasil QoS menunjukan hasil yang sangat baik pada implementasi tugas akhir ini, yaitu pada pengujian saat terjadi serangan, meski *server* diserang tetapi kualitas jaringan masih dalam kategori baik, dimana nilai-nilai parameter QoS menunjukan hasil yang cukup baik. Parameter *Throughput* menunjukan hasil yaitu 393 kb/s yang mana masuk dalam indeks sangat baik pada standar *Tiphon,* parameter lainnya yaitu *Packet Loss = 7.2 % , Delay = 16.65 ms,* memperoleh hasil yang sangat baik sesuai standar *Tiphon,* sedangkan untuk parameter *Jitter = 16.66 ms* masuk dalam kategori baik dalam standar *Tiphon.*

REFERENSI

[1] R. R. Abdullah and A. Nurhayati, “Monitoring Sistem Keamanan Jaringan Berbasis Telegram Bot,” *J. Infotmatics Commun. Technol.*, vol. 1089, pp. 1–9, 2019.

[2] V. A. Z. Dhafin Rizky Aulia Wahyu Arief Rahman, “Implementasi dan analisis honeypot berbasis cowrie untuk mendeteksi serangan siber,” *METHODIKA*, vol. 11, no. 1, pp. 35–39, 2025.

[3] Fitri Nova, M. D. Pratama, and D. Prayama, “Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos,” *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 3, no. 1, pp. 1–7, 2022, doi: 10.30630/jitsi.3.1.59.

[4] W. R. A. Putra, A. R. A. Nurwa, D. F. Priambodo, and M. Hasbi, “Infrastructure as Code for Security Automation and Network Infrastructure Monitoring,” *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 22, no. 1, pp. 201–214, 2022, doi: 10.30812/matrik.v22i1.2471.

[5] R. Das H. Ahmetoglu, “A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future,” vol. 20, 2022.

[6] A. Dermawan, Yuhandri, and Sumijan, “Analisis Perbandingan Optimalisasi Port Knocking Dan Honeypot dengan Iptables Pada Server Untuk Keamanan Jaringan,” *KESATRIA J. Penerapan Sist. Inf. (Komputer Manajemen)*, vol. 5, no. 2, pp. 543–556, 2024, [Online]. Available: https://pkm.tunasbangsa.ac.id/index.php/kesatria/article/view/364

[7] N. Yudyanto, S. Syaifuddin, and Y. Azhar, “Integrasi Modern Honey Network Dengan Grafana Untuk Visualisasi,” *J. Repos.*, vol. 2, no. 10, pp. 1380–1389, 2020, doi: 10.22219/repositor.v2i10.1047.

[8] D. W. C. Rulof Baltwin Tallane, “Implementation of Intrusion Detection System (Ids) Using Security Onion,” *Syntax Lit. J. Ilm. Indones.*, vol. 300 LNNS, no. 10, pp. 685–704, 2022.

[9] T. Natanegara, Y. Muhyidin, and D. Singasatia, “Implementasi Honeypot Cowrie Dan Snort Sebagai Alat Deteksi Serangan Pada Server,” *JATI (Jurnal Mhs. Tek. Inform.*, vol. 7, no. 3, pp. 1871–1877, 2023, doi: 10.36040/jati.v7i3.6989.

[10] E. R. Muhamad Jati Wasesa, Hardi Wirkan, “EVALUASI KEAMANAN SISTEM OPERASI LINUX DARI SERANGAN MALWARE,” *J. Sist. Dan Teknol. Inf.*, vol. 07, 2025.

[11] O. Dwi Prasetyo, P. Hari Trisnawan, and A. Bhawiyuga, "Uji Kinerja Host-Based Intrution Detection System WAZUH terhadap Serangan Brute Force dan Dos," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 6, pp. 2686–2692, 2023, [Online]. Available: http://j-ptiik.ub.ac.id

[12] F. Saputra, B. Cut, and F. Nilamsari, "Analisis Perbandingan Tiga Software Terhadap Pengukuran Quality Of service (QoS) Pada Pengukuran Jaringan Wireless Internet," *J. Teknol. Inf.*, vol. 2, no. 1, pp. 33–40, 2023, [Online]. Available: http://jurnal.utu.ac.id/JTI/article/view/7275

[13] M. Oosterhof, "Installing Cowrie in seven steps." Accessed: May 20, 2022. [Online]. Available: https://docs.cowrie.org/en/latest/INSTALL.html

[14] Wazuh, "Wazuh, 'Installation guide.'" Accessed: Apr. 04, 2025.[Online].Available:https://documentation.wazuh.com/current/installation-guide/index.html