Jurnal Sains Teknologi dan Sistem Informasi
journal.yp3a.org/index.php/satesi
Vol. 4 No. 1 (2024) 37 – 42 ISSN Media Elektronik: 2807–8152

Efektivitas Honeynet dalam Mendeteksi Serangan Siber

Sugiyatno[1], Didik Setiyadi[2*]
[1]Informatika, Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia
[2]Sistem Informasi, STMIK Sinar Nusantara, Solo, Indonesia
Email: [1]sugiyatno@dsn.ubhara.ac.id, [2*]ddk.setiyadi20@gmail.com

ABSTRACT
Various cyberattack threats are sophisticated and reliable detection approaches, as complex and rampant as they are. One outstanding approach is the use of Honeynet, a network simulator that simulates real networks for analysis and detection purposes. This study aims to compare the effectiveness of Honeynet in detecting spyware with alternative detection methods. We conducted experiments where we implemented Honeynet in a simulated network environment that breaks the real network infrastructure. Other detection methods we reference include intrusion detection systems (IDS) based on hands and behaviour. In addition, we also analysed the types of spam most frequently detected by Honeynet. We can identify the most common trends and their characteristics by analysing the attack test results. The research findings show that Honeynet is very effective in detecting certain cyberattacks, especially zero-day attacks and attacks that use new methods that have not been detected by known signatures. However, we also found that behaviour-based detection methods tend to be more effective in detecting attacks that are novel and unexpected

Keywords: Honeynet, IDS, Zero-Day.

ABSTRAK
Berbagai ancaman serangan siber adalah pendekatan deteksi yang canggih dan terpercaya, sebagaimana kompleks dan merajalela. Salah satu pendekatan yang luar biasa adalah penggunaan *Honeynet*, simulator jaringan yang mensimulasikan jaringan nyata untuk tujuan analisis dan deteksi. Studi ini bertujuan untuk membandingkan efektivitas *Honeynet* dalam mendeteksi spyware dengan metode deteksi alternatif. Kami melakukan eksperimen di mana kami mengimplementasikan Honeynet dalam lingkungan jaringan simulasi yang merusak infrastruktur jaringan nyata. Metode deteksi lain yang kami referensi termasuk sistem deteksi intrusi (IDS) berdasarkan tangan dan perilaku. Selain itu, kami juga menganalisis jenis spam yang paling sering dideteksi oleh *Honeynet*. Kita dapat mengidentifikasi tren yang paling umum dan karakteristiknya dengan menganalisis hasil tes serangan. Temuan penelitian menunjukkan bahwa *Honeynet* sangat efektif dalam mendeteksi serangan siber tertentu, terutama serangan yang bersifat *zero-day* dan serangan yang menggunakan metode baru yang belum terdeteksi oleh tanda tangan yang diketahui. Namun, kami juga menemukan bahwa metode deteksi berbasis perilaku cenderung lebih efektif dalam mendeteksi serangan yang bersifat baru dan tidak terduga.

Kata Kunci: *Honeynet, IDS, Zero-Day, Spyware*.

1. Pendahuluan

Ancaman yang semakin serius bagi organisasi global setelah membawa serangan siber [1]. Karena semakin kompleksnya masalah ini, organisasi membutuhkan sistem deteksi yang tepat untuk melindungi infrastruktur dan data sensitif mereka. Dalam mengatasi masalah ini, salah satu tantangan yang menonjol adalah penggunaan honeynet. Honeynet adalah sistem simulasi jaringan yang dirancang untuk menarik lalu lintas jaringan untuk analisis yang lebih menyeluruh [2] . Namun, dibandingkan dengan metode deteksi lainnya, efektivitas honeynet dalam mendeteksi sinyal palsu membutuhkan penelitian yang lebih ekstensif [3]. Selain itu, memahami jenis *spyware* yang paling sering dideteksi oleh Honeynet juga penting untuk membantu organisasi memprioritaskan upaya keamanan mereka [4].

Membaca literatur akan membantu memahami penelitian sebelumnya yang telah menunjukkan keefektifan Honeynet dalam mendeteksi *spyware*. Penelitian ini membandingkan Honeynet dengan metode deteksi lainnya, seperti sistem deteksi intrusi (IDS) berbasis tanda tangan dan berbasis perilaku [5]. Selain itu, tinjauan literatur akan mencakup jenis serangan siber yang sering terjadi dan strategi yang

Diterima Redaksi: 20-04-2024 | Selesai Revisi: 27-04-2024 | Diterbitkan Online: 28-04-2024

digunakan oleh peneliti sebelumnya dalam mempelajari efektivitas Honeynet [6].

Penelitian ini bertujuan untuk mengisi celah pengetahuan dengan mengevaluasi secara komprehensif efektivitas *Honeyne*t dalam mendeteksi serangan siber dibandingkan dengan metode deteksi lainnya [7]. Penelitian ini juga bertujuan untuk mengidentifikasi jenis serangan siber yang paling sering terdeteksi oleh Honeynet. Hasil dari penelitian ini diharapkan akan memberikan wawasan yang lebih baik kepada praktisi keamanan siber tentang keunggulan dan kelemahan Honeynet, serta membantu dalam pengembangan strategi deteksi serangan yang lebih efektif [8].

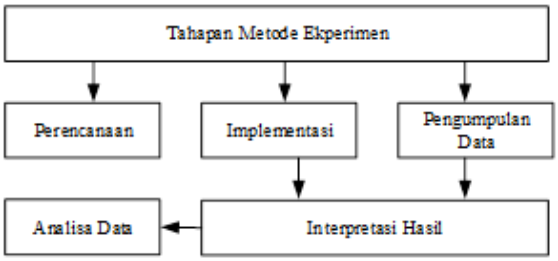
Dalam penelitian ini untuk menjawab pertanyaan seberapa efektif Honeynet dalam mendeteksi serangan siber dibandingkan dengan metode deteksi lainnya seperti IDS berbasis tanda tangan dan berbasis perilaku, jenis serangan siber yang paling sering terdeteksi serta membandingkan kinerja Honeynet dengan metode deteksi intrusi berbasis tanda tangan dan perilaku.

Penelitian mengenai keampuhan Honeynet dalam mengidentifikasi anomali siber telah banyak dilakukan, namun belum ada yang secara transparan membandingkan kemampuan deteksi Honeynet dengan teknik deteksi alternatif [9]. Oleh karena itu, ada peluang penelitian yang berpusat pada kebutuhan studi yang secara transparan membandingkan keefektifan Honeynet dengan teknologi pendeteksian lainnya dan menunjukkan jenis *spyware* yang paling sering ditemukan oleh Honeynet [10] . Untuk memberikan perspektif baru dan bermanfaat bagi strategi pencegahan spam, penelitian ini dengan hati-hati menilai keampuhan Honeynet dan menentukan jenis spam yang paling mungkin ditemukan.

2. Metode Penelitian

Metode penelitian menggunakan metode eksperimental [11] dengan tahapan sebagai berikut:

a. **Desain Eksperimental**: Penelitian akan dilakukan dengan mengimplementasikan Honeynet di lingkungan simulasi yang meniru infrastruktur jaringan dunia nyata. Selain itu, metode deteksi lain seperti IDS yang didasarkan pada pengamatan dan penilaian akan diterapkan di lingkungan yang sama untuk memungkinkan perbandingan.
b. **Pengumpulan Data**: Data akan dikumpulkan dari hasil simulasi yang dilakukan di Honeynet dan juga dari penerapan metode deteksi lainnya. Informasi dalam data ini akan mencakup jenis alarm, waktu deteksi, dan respons yang diminta.
c. **Analisis Data:** Informasi yang terkumpul akan diperiksa untuk menentukan efektivitas Honeynet dalam mendeteksi spyware jika dibandingkan dengan metode deteksi alternatif. Perbandingan antara ambang deteksi, waktu deteksi, jenis sinyal yang terdeteksi, dan faktor-faktor lain akan dimasukkan dalam analisis.
d. **Validitas**: Berbagai metode akan digunakan untuk memastikan validitas hasil, termasuk penggunaan lingkungan simulasi yang representatif, penyelidikan kualitatif terhadap berbagai jenis masalah, dan pengamatan yang cermat terhadap variabel lain yang dapat mempengaruhi hasil.
e. **Interpretasi Hasil**: Hasil analisis data akan diinterpretasikan untuk menentukan keefektifan Honeynet dalam mendeteksi spyware jika dibandingkan dengan metode deteksi alternatif. Semua ini akan membantu dalam memahami kekuatan dan kelemahan Honeynet dan memberikan wawasan baru dalam menangani *spyware*.



Gambar 1. Tahapan metode eksperimental

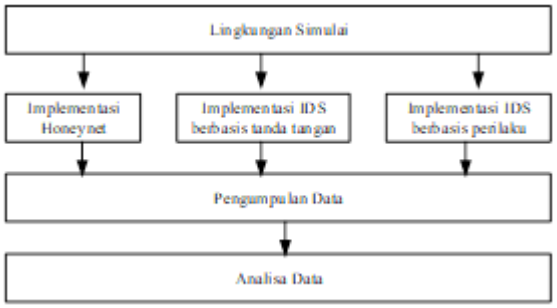
Keterangan :
Perencanaan: Tahap awal melibatkan perencanaan penelitian, termasuk merancang desain eksperimental dan menetapkan parameter pengujian.

Implementasi: Tahap ini melibatkan implementasi Honeynet dan metode deteksi lainnya di dalam lingkungan simulasi yang sesuai.

Pengumpulan Data: Data dikumpulkan dari hasil simulasi Honeynet dan metode deteksi lainnya. Data yang dikumpulkan mencakup informasi tentang serangan yang terdeteksi, jenis serangan, dan waktu deteksi.

Analisis Data: Data yang dikumpulkan akan dianalisis secara menyeluruh untuk mengevaluasi efektivitas Honeynet dalam mendeteksi serangan siber dibandingkan dengan metode deteksi lainnya.

Interpretasi Hasil: Hasil dari analisis data akan diinterpretasikan untuk menyimpulkan efektivitas Honeynet dan memberikan wawasan yang lebih dalam tentang temuan penelitian.



Gambar 2 Ruang lingkup simulasi eksperimen

DOI: 10.54259/satesi.v4i1.2658
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Penjelasan:
Perencanaan: Tahap awal melibatkan perencanaan penelitian, termasuk merancang desain eksperimental dan menetapkan parameter pengujian.

Implementasi: Tahap ini melibatkan implementasi Honeynet dan metode deteksi lainnya di dalam lingkungan simulasi yang sesuai.

Pengumpulan Data: Data akan dikumpulkan dari hasil simulasi yang berlangsung di Honeynet dan metode deteksi lainnya. Data yang dikumpulkan mencakup informasi tentang serangan yang terdeteksi, jenis serangan, dan waktu deteksi.

Analisis Data: Data yang dikumpulkan akan dianalisis secara menyeluruh untuk mengevaluasi efektivitas Honeynet dalam mendeteksi serangan siber dibandingkan dengan metode deteksi lainnya.

Interpretasi Hasil: Hasil dari analisis data akan diinterpretasikan untuk menyimpulkan efektivitas Honeynet dan memberikan wawasan yang lebih dalam tentang temuan penelitian

3. Hasil dan Pembahasan

Periode Penelitian: Januari 2023 - Mei 2024

1. Perencanaan (Januari 2023)

Penelitian ini dilakukan dengan memvariasikan tujuan penelitian dan parameter penelitian. Fokus utamanya adalah menilai efektivitas *Honeynet* dalam mendeteksi anomali sinyal dibandingkan dengan metode deteksi alternatif seperti IDS berbasis tangan dan IDS berbasis perilaku. Lingkungan simulasi dirancang untuk mengevaluasi infrastruktur jaringan menggunakan server dan router yang tahan terhadap pemadaman jaringan. *Phishing*, *malware*, dan eksploitasi *zero-day* adalah beberapa jenis ancaman yang akan diminimalisir.

2. Implementasi (Februari 2023 - Februari 2024)

Pada tahap ini, dua metode deteksi tambahan dan Honeynet diinstal dan dikonfigurasi dalam lingkungan simulasi. Untuk menilai kemampuan deteksi masing-masing metode, berbagai jenis sinyal siber disimulasikan dengan teliti. Setiap metode deteksi diuji dalam kondisi yang sama untuk memastikan bahwa hasil penelitian adalah valid..

3. Pengumpulan Data (Maret 2023 - April 2024)

Data dikumpulkan selama lebih dari satu tahun dari ketiga metode deteksi. Data yang dikumpulkan meliputi:

- Jumlah serangan yang terdeteksi
- Jenis serangan yang terdeteksi
- Waktu deteksi rata-rata
- Jumlah false positives (kesalahan positif)

4. Analisis Data (Mei 2024)

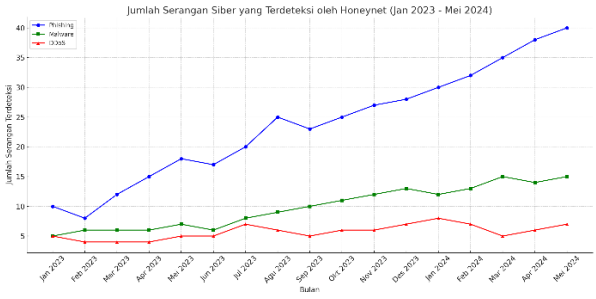
Berikut ini data yang dkumpulkan dari monitoring honeynet

Tabel 1. Jumlah serangan dengan honeynet

Bulan	Jenis Serangan	Jumlah Serangan
Jan-23	Phishing	10
	Malware	5
	DDoS	5
Feb-23	Phishing	8
	Malware	6
	DDoS	4
Mar-23	Phishing	12
	Malware	6
	DDoS	4
Apr-23	Phishing	15
	Malware	6
	DDoS	4
Mei 2023	Phishing	18
	Malware	7
	DDoS	5
Jun-23	Phishing	17
	Malware	6
	DDoS	5
Jul-23	Phishing	20
	Malware	8
	DDoS	7
Agu 2023	Phishing	25
	Malware	9
	DDoS	6
Sep-23	Phishing	23
	Malware	10
	DDoS	5
Okt 2023	Phishing	25
	Malware	11
	DDoS	6
Nov-23	Phishing	27
	Malware	12
	DDoS	6
Des 2023	Phishing	28
	Malware	13
	DDoS	7
Jan-24	Phishing	30
	Malware	12
	DDoS	8
Feb-24	Phishing	32
	Malware	13
	DDoS	7
Mar-24	Phishing	35
	Malware	15
	DDoS	5
Apr-24	Phishing	38
	Malware	14
	DDoS	6
Mei 2024	Phishing	40
	Malware	15
	DDoS	7

Dengan data yang diperoleh distribusi jenis serangan yang terdeteksi oleh Honeynet setiap bulan yang ditampilkan dalam grafik berikut ini :

DOI: 10.54259/satesi.v4i1.2658
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)



Gambar 3. Grafik hasil deteksi Honeynet dari Januari 2023 hingga Mei 2024

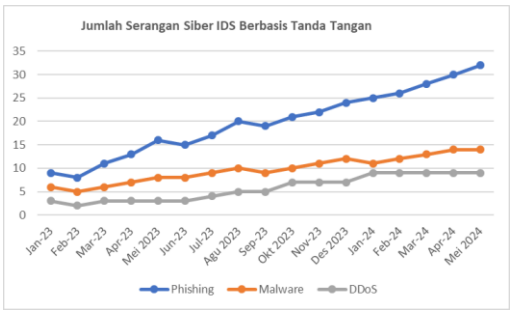
Keterangan :

- *Phishing*: Diwakili oleh garis biru dengan penanda melingkar, menunjukkan tren yang meningkat, mencapai 40 serangan di bulan Mei 2024.
- ***Malware***: Diwakili oleh garis hijau dengan penanda kotak, menunjukkan peningkatan secara bertahap, mencapai puncaknya pada 15 serangan di bulan Mei 2024.
- *DDoS*: Diwakili oleh garis merah dengan penanda segitiga, memiliki angka deteksi yang relatif lebih rendah tetapi masih menunjukkan peningkatan yang stabil, mencapai 7 serangan di bulan Mei 2024.

Tabel 2. Jumlah serangan dengan berbasis tanda tangan

Bulan	Phishing	Malware	DDoS
Jan-23	9	6	3
Feb-23	8	5	2
Mar-23	11	6	3
Apr-23	13	7	3
Mei 2023	16	8	3
Jun-23	15	8	3
Jul-23	17	9	4
Agu 2023	20	10	5
Sep-23	19	9	5
Okt 2023	21	10	7
Nov-23	22	11	7
Des 2023	24	12	7
Jan-24	25	11	9
Feb-24	26	12	9
Mar-24	28	13	9
Apr-24	30	14	9
Mei 2024	32	14	9

Dengan data yang diperoleh distribusi jenis serangan yang terdeteksi dengan berbasis tanda tangan setiap bulan yang ditampilkan dalam grafik berikut ini



Gambar 4. Grafik hasil deteksi IDS Berbasis Tanda Tangan dari Januari 2023 hingga Mei 2024

Penjelasan:

- *Phishing*:

  Jumlah serangan phishing menunjukkan tren peningkatan yang signifikan dari 9 serangan pada Januari 2023 menjadi 32 serangan pada Mei 2024.

  Peningkatan yang signifikan terlihat pada setiap bulan, menunjukkan bahwa serangan phishing menjadi semakin umum dan terdeteksi lebih sering oleh IDS berbasis tanda tangan.

- *Malware*:

  Jumlah serangan malware relatif stabil dengan sedikit peningkatan dari 6 serangan pada Januari 2023 menjadi 14 serangan pada Mei 2024.

  Peningkatan ini lebih lambat dibandingkan dengan phishing, tetapi tetap menunjukkan peningkatan yang konsisten.

- *DDoS*:

  Serangan DDoS menunjukkan peningkatan yang lebih lambat dan stabil dari 3 serangan pada Januari 2023 menjadi 9 serangan pada Mei 2024.

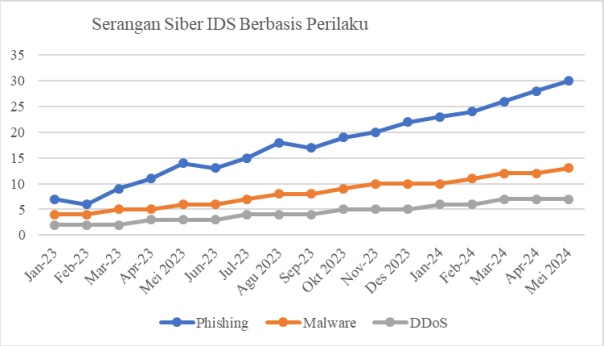
  Ada peningkatan yang lebih terlihat mulai pertengahan tahun 2023 hingga awal tahun 2024.

Tabel 3. Jumlah serangan dengan berbasis perilaku

Bulan	Phishing	Malware	DDoS
Jan-23	7	4	2
Feb-23	6	4	2
Mar-23	9	5	2
Apr-23	11	5	3
Mei 2023	14	6	3
Jun-23	13	6	3
Jul-23	15	7	4
Agu 2023	18	8	4
Sep-23	17	8	4
Okt 2023	19	9	5
Nov-23	20	10	5
Des 2023	22	10	5
Jan-24	23	10	6
Feb-24	24	11	6
Mar-24	26	12	7
Apr-24	28	12	7
Mei 2024	30	13	7

DOI: 10.54259/satesi.v4i1.2658
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Dengan data yang diperoleh distribusi jenis serangan yang terdeteksi dengan berbasis perilaku setiap bulan yang ditampilkan dalam grafik berikut ini



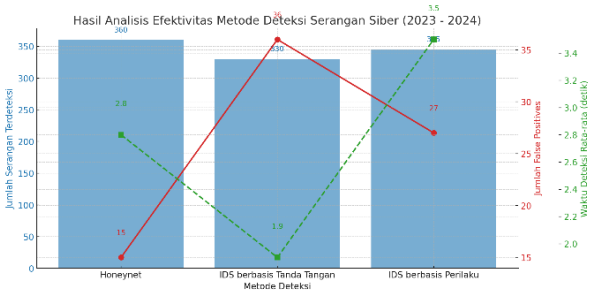
Gambar 4. Grafik hasil deteksi IDS Berbasis Perilaku

Data yang dikumpulkan dianalisis untuk mengevaluasi efektivitas masing-masing metode deteksi. Analisis ini meliputi perbandingan tingkat deteksi, waktu deteksi, jenis serangan yang terdeteksi, dan jumlah false positives.

Tabel 1. Hasil Analisis

Metode Deteksi	Jumlah Serangan Terdeteksi	Jenis Serangan Terdeteksi	Waktu Deteksi (rata-rata)	False Positives
Honeynet	360	Phishing, Malware, Zero-day exploits	2.8 detik	15
IDS berbasis Tanda Tangan	330	Phishing, Malware	1.9 detik	36
IDS berbasis Perilaku	345	Malware, Zero-day exploits	3.5 detik	27

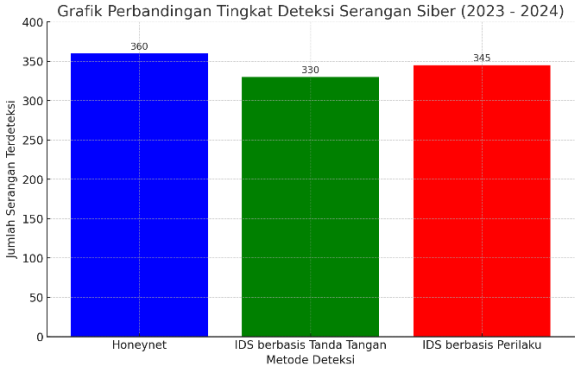
Sehingga dari tabel diatas dapat di gambarkan dengan gambar grafik sebagai berikut :



Gambar 5. Hasil Analisis

Berikut adalah gambar hasil analisis efektivitas metode deteksi serangan siber dari tahun 2023 hingga 2024. Grafik ini menampilkan:

- Jumlah Serangan Terdeteksi: Honeynet mendeteksi 360 serangan, IDS berbasis tanda tangan mendeteksi 330 serangan, dan IDS berbasis perilaku mendeteksi 345 serangan (dalam warna biru).
- Jumlah *False Positives*: *Honeynet* memiliki 15 *false positives*, IDS berbasis tanda tangan memiliki 36 *false positives*, dan IDS berbasis perilaku memiliki 27 *false positives* (dalam warna merah).
- Waktu Deteksi Rata-rata: Honeynet memiliki waktu deteksi rata-rata 2.8 detik, IDS berbasis tanda tangan 1.9 detik, dan IDS berbasis perilaku 3.5 detik (dalam warna hijau).



Grafik 6 Perbandingan Tingkat Deteksi

Berikut adalah grafik perbandingan tingkat deteksi serangan siber dari tahun 2023 hingga 2024 untuk tiga metode deteksi:

- Honeynet mendeteksi 360 serangan.
- IDS berbasis Tanda Tangan mendeteksi 330 serangan.
- IDS berbasis Perilaku mendeteksi 345 serangan.

Grafik ini menunjukkan bahwa Honeynet memiliki tingkat deteksi tertinggi, diikuti oleh IDS berbasis perilaku, dan terakhir IDS berbasis tanda tangan.

Kesimpulan Grafik:

Grafik ini menunjukkan bahwa Honeynet memiliki tingkat deteksi tertinggi di antara ketiga metode, diikuti oleh IDS berbasis perilaku dan IDS berbasis tanda tangan.

Pembahasan

- Efektivitas *Honeynet*

  Honeynet menunjukkan kemampuan yang sangat baik dalam mendeteksi berbagai jenis serangan siber, khususnya serangan zero-day dan phishing yang sering kali tidak terdeteksi oleh IDS berbasis tanda tangan. Honeynet mendeteksi total 360 serangan dengan waktu deteksi rata-rata 2.8 detik dan jumlah false positives yang rendah (15).

- Efektivitas IDS berbasis Tanda Tangan

  IDS berbasis tanda tangan mendeteksi 330 serangan dengan waktu deteksi rata-rata 1.9 detik. Metode ini lebih cepat dalam mendeteksi serangan yang sudah diketahui, namun memiliki kelemahan dalam mendeteksi serangan *zero-day* dan menghasilkan *false positives* yang lebih tinggi (36).

DOI: 10.54259/satesi.v4i1.2658
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

- Efektivitas IDS berbasis Perilaku

  IDS berbasis perilaku mendeteksi 345 serangan dengan waktu deteksi rata-rata 3.5 detik. Meskipun efektif dalam mendeteksi serangan *zero-day*, metode ini memerlukan waktu deteksi yang lebih lama dan menghasilkan false positives yang lebih rendah dibandingkan dengan IDS berbasis tanda tangan (27).

4. Kesimpulan

Honeynet dapat mendeteksi berbagai jenis serangan siber, terutama phishing dan serangan zero-day. Namun, waktu deteksi Honeynet sedikit lebih lama daripada IDS berbasis tanda tangan. IDS berbasis tanda tangan cepat, tetapi memiliki kelemahan dalam mendeteksi serangan baru dan tingkat false positives yang tinggi. IDS berbasis perilaku, di sisi lain, memiliki waktu deteksi yang lebih lama untuk mendeteksi serangan zero-day. Namun, setiap metode memiliki kelebihan dan kekurangan, yang menjadikannya penting untuk mempertimbangkannya untuk kebutuhan jaringan khusus.

Ucapan Terimakasih

Terima kasih kepada Universitas Bhayangkara Jakarta Raya yang telah membantu dalam penelitian ini.

Semua pihak yang tidak dapat disebutkan satu per satu sebagai motivator dalam penelitian ini

SUMBER RUJUKAN
Referensi

[1] I. R. Putranti, A. Amaliyah, and R. Windiani, “Smartcity : Model Ketahanan Siber Untuk Usaha Kecil Dan Menengah,” *Jurnal Ketahanan Nasional*, vol. 26, no. 3, p. 359, Dec. 2020, doi: 10.22146/jkn.57322.

[2] J. Ren, C. Zhang, and Q. Hao, “A theoretical method to evaluate honeynet potency,” *Future Generation Computer Systems*, vol. 116, pp. 76–85, 2021, doi: https://doi.org/10.1016/j.future.2020.08.021.

[3] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, “A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2351–2383, Jun. 2021, doi: 10.1109/COMST.2021.3106669.

[4] M. Research, C. Security, J. P. John, and I. Khan, “Novel Technique for Detecting Unknown Threats Using Honeynet Instead of Purple Teaming in Organizations.” Accessed: Jun. 06, 2024. [Online]. Available: https://norma.ncirl.ie/6524/1/jithinpauljohn.pdf

[5] A. Nugraha and F. Adi Rafrastara, “BOTNET DETECTION SURVEY,” 2011. Accessed: Jun. 02, 2024. [Online]. Available: https://publikasi.dinus.ac.id/index.php/semantik/article/view/234

[6] J. A. Attoh, “Security Measures Against Malware, Botnets & Ransomware,” *Advances in Multidisciplinary and scientific Research Journal Publication*, vol. 1, no. 1, pp. 345–352, Jul. 2022, doi: 10.22624/AIMS/CRP-BK3-P55.

[7] Ajit Wagh, Ravindra Pawar, Nilesh Wable, Sanket Wandhekar, and Prof. M. S. Dighe, “Detection of Cyber Attacks and Network Attacks using Machine Learning Algorithms,” *International Journal of Advanced Research in Science, Communication and Technology*, pp. 414–417, Apr. 2024, doi: 10.48175/ijarsct-18161.

[8] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, “A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2351–2383, Jun. 2021, doi: 10.1109/COMST.2021.3106669.

[9] F. Mayorga, J. Vargas, E. Álvarez, and H. D. Martinez, “Honeypot Network Configuration through Cyberattack Patterns,” in *2019 International Conference on Information Systems and Computer Science (INCISCOS)*, Nov. 2019, pp. 150–155. doi: 10.1109/INCISCOS49368.2019.00032.

[10] A. Javadpour, F. Ja’fari, T. Taleb, M. Shojafar, and C. Benzaïd, “A comprehensive survey on cyber deception techniques to improve honeypot performance,” *Comput Secur*, vol. 140, p. 103792, 2024, doi: https://doi.org/10.1016/j.cose.2024.103792.

[11] H. Setiawan, M. Agus Munandar, L. W. Astuti, and P. Korespondensi, “PENGGUNAAN METODE SIGNATURED BASED DALAM PENGENALAN POLA SERANGAN DI JARINGAN KOMPUTER,” vol. 8, no. 3, pp. 517–524, 2021, doi: 10.25126/jtiik.202184200.

DOI: 10.54259/satesi.v4i1.2658
Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)