Research Article
FORBIS: Forensics Business Information System Journal
Published online on: https://journal.universitasmulia.ac.id/index.php/forbis **1 (2) Januari 2024**

ANALISIS PERBANDINGAN TEKNIK SIGNATURE-BASED DAN ANOMALY-BASED DETECTION PADA SNORT DAN ZEEK DALAM MENCEGAH INTRUSI JARINGAN

Ferry Ananda Febian [1], Djumhadi[2], Wahyu Nur Alimyaningtias [3]*

[1,2,3] Fakultas Ilmu Komputer, Universitas Mulia

email: [1]ferryananda@students.universitasmulia.ac.id, [2]djumhadi@universitasmulia.ac.id, [3]nasruddin@universitasmulia.ac.id
[*]Correspondence

ARTICLE INFO

Article History
Received : 29 November 2023
Revised : 13 Agustus 2024
Accepted : 18 Agustus 2024
Available online : 18 Agustus 2024

Keywords:
IDS, Snort, Zeek, Signature-Based, Anomaly-Based

ABSTRACK

Intrusion detection system (IDS) is a system used to detect abnormal activity on a network. IDS can use various detection techniques, including signature-based and anomaly-based techniques. Signature-based techniques use known patterns to detect unwanted activities, while anomaly-based techniques use rules that can help identify activities that do not match predefined patterns. This research aims to analyze the performance comparison of signature-based and anomaly-based detection techniques on Snort and Zeek in preventing intrusion. Snort and Zeek were chosen as the object of research because both are popular IDS and have complete detection features. The results show that signature-based techniques are more effective in detecting intrusion on the network compared to anomaly-based techniques. However, anomaly-based techniques are better at handling intrusions that are not detected by signature-based techniques. The performance of the signature-based technique on Snort is better than that of Zeek, while the anomaly-based detection technique on Zeek is better than that of Snort. The conclusion of this research shows that both detection techniques have their own advantages and disadvantages, so it is necessary to analyze network conditions and security needs to determine the right detection technique..

ABSTRAK

Intrusion detection system (IDS) merupakan sistem yang digunakan untuk mendeteksi aktivitas tidak normal pada jaringan. IDS dapat menggunakan berbagai teknik deteksi, di antaranya teknik signature-based dan anomaly-based. Teknik signature-based menggunakan pola-pola yang telah diketahui untuk mendeteksi aktivitas yang tidak diinginkan, sedangkan teknik anomaly-based menggunakan aturan-aturan yang dapat membantu mengidentifikasi aktivitas yang tidak sesuai dengan pola yang telah ditentukan sebelumnya. Penelitian ini bertujuan untuk menganalisis perbandingan kinerja teknik signature-based dan anomaly-based detection pada Snort dan Zeek dalam mencegah intrusion. Snort dan Zeek dipilih sebagai objek penelitian karena keduanya merupakan IDS yang populer dan memiliki fitur

deteksi yang lengkap. Hasil penelitian menunjukkan bahwa teknik signature-based lebih efektif dalam mendeteksi intrusion pada jaringan dibandingkan dengan teknik anomaly-based. Namun, teknik anomaly-based lebih baik dalam menangani intrusion yang tidak terdeteksi oleh teknik signature-based. Kinerja teknik signature-based pada Snort lebih baik dibandingkan dengan Zeek, sedangkan teknik anomaly-based detection pada Zeek lebih baik dibandingkan dengan Snort.

1. Pendahuluan

Seiring dengan semakin luasnya penggunaan teknologi informasi dalam berbagai aspek kehidupan bermasyarakat, serangan keamanan pada sistem informasi semakin sering terjadi. Salah satu jenis serangan yang paling umum adalah serangan pada layer jaringan yang memanfaatkan sistem yang minim perlindungan seperti kurangnya perangkat lunak keamanan, kebijakan yang tidak ketat dan kurangnya pemahaman untuk mengenali tanda-tanda serangan. Hal ini menunjukkan pentingnya penerapan sistem deteksi intrusi untuk mencegah serangan yang merugikan pengguna dan organisasi yang terkait.

Sistem deteksi intrusi yang diimplementasikan dalam penelitian ini adalah dengan penerapan teknik Signature-based dan Anomaly Based dengan menggunakan tools deteksi intrusi yaitu Snort dan Zeek. Penelitian ini berfokus pada pencegahan intrusi jaringan, yang mengindikasikan adanya kebutuhan untuk melindungi sistem jaringan dari serangan dan ancaman yang dapat mengakibatkan kerugian dan pelanggaran keamanan.

2. Metode Penelitian

Metode penelitian yang digunakan adalah penelitian eksperimental yang dilakukan dengan cara membandingkan hasil pengujian dari masing-masing teknik deteksi intrusi. Langkah-langkah dalam metode penelitian adalah sebagai berikut:

- Pengumpulan data: Data yang digunakan dalam penelitian ini berasal dari hasil pengujian pada sistem jaringan yang telah disiapkan dengan mengaplikasikan teknik signature-based detection dan anomaly-based detection pada Snort dan Zeek.
- Pengolahan data: Data yang telah terkumpul kemudian diolah dan dianalisis dengan pendekatan kuantitatif untuk membandingkan efektivitas dari masing-masing teknik deteksi intrusi.
- Interpretasi hasil: Hasil pengujian yang telah dianalisis kemudian diinterpretasikan untuk menentukan teknik deteksi intrusi mana yang lebih efektif dalam mencegah serangan pada jaringan.

Penelitian ini menggunakan pendekatan kuantitatif dengan mengumpulkan data melalui pengujian pada sistem jaringan yang telah disiapkan.

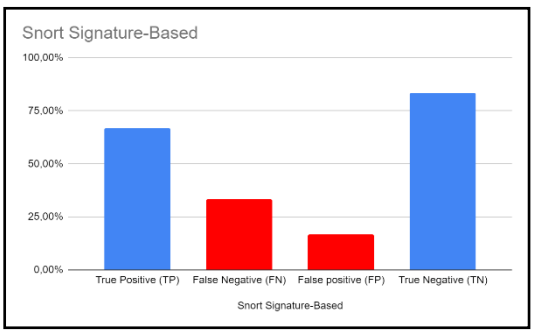
Langkah-langkah dalam metode analisis data penelitian ini adalah sebagai berikut:

- Pengumpulan Data: Langkah pertama mengumpulkan data dari beberapa sumber yang dapat mencakup log jaringan, aliran lalu lintas jaringan, file konfigurasi snort dan zeek, serta setiap perangkat keras atau lunak yang terlibat dalam pengujian. Data ini dikelompokkan dan disimpan dalam format yang mudah diakses dan diproses.
- Preprocessing Data: Data kemudian diproses dan dibersihkan dari noise atau data yang tidak relevan. Hal ini mencakup penghapusan duplikat, penghapusan data yang tidak valid, dan penghapusan data yang tidak diperlukan.

- Pemilihan Fitur: Fitur yang perlu dipilih untuk menganalisis data. Fitur ini terkait dengan tujuan dari penelitian, dan dapat membantu menggambarkan dan membedakan antara serangan dan lalu lintas normal.
- Pemodelan Data: Data kemudian dimodelkan dengan teknik signature-based dan anomaly-based detection. Signature-based detection mencari pola yang diketahui dari serangan sebelumnya, sedangkan anomaly-based detection mencari perilaku yang tidak biasa atau tidak wajar.
- Evaluasi Model: Setelah model dibangun, evaluasi model dilakukan untuk menilai keefektifannya dalam mendeteksi serangan jaringan. Evaluasi model melibatkan penggunaan metrik seperti Akurasi (CR), Presisi (PR), dan False Positive Rate (FPR).

3. Hasil dan Pembahasan

Berikut adalah hasil pengujian dengan melakukan 16 kali serangan (Nmap, ARP Spoofing, Sniff Network, DOS Flood, Ping Host, SSL Connection) pada server Debian, log serangan dikumpulkan dari tools intrusi Snort dan Zeek.



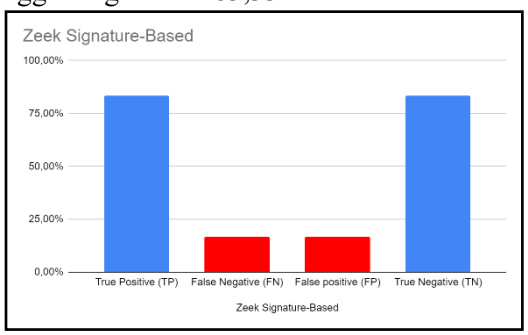
Gambar 1. Matriks Evaluasi Snort dengan Metode Signature-Based

Pada gambar 1 memperlihatkan grafik matriks evaluasi yang dihasilkan oleh Snort dengan metode deteksi Signature-Based.

Tabel 1. Hasil deteksi berbasis signature pada Snort

Matriks Evaluasi	Nilai
True Positive (TP)	66,67%
False Negative (FN)	33,33%
False positive (FP)	16,67%
True Negative (TN)	83,33%

Pada tabel 1 memperlihatkan nilai persentase matriks evaluasi Snort dengan metode Signature-Based, pada tabel ini memperlihatkan tingkat True Negative yang tinggi dengan nilai 83,33%.



Gambar 2. Matriks Evaluasi Zeek dengan Metode Signature-Based

Pada gambar matriks evaluasi Zeek dengan metode Signature-Based, terlihat bahwa tingkat true positive dan true negative lebih tinggi dibanding false positive dan false negative.

Tabel 2. Hasil deteksi berbasis signature pada Zeek

Matriks Evaluasi	Nilai
True Positive (TP)	83,33%
False Negative (FN)	16,67%
False positive (FP)	16,67%
True Negative (TN)	83,33%

Tabel 2 adalah nilai persentase dari hasil deteksi berbasis signature pada Zeek.

Tabel 3. Rata-rata hasil deteksi berbasis signatureasis signature pada Zeek

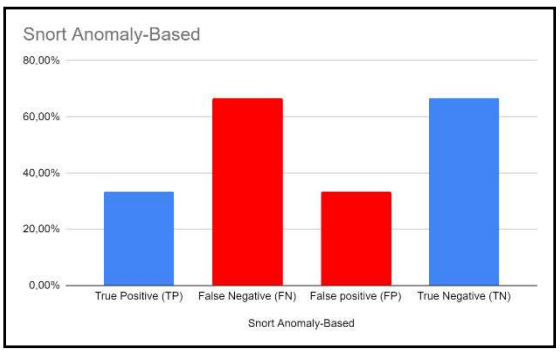
Matriks Evaluasi	Nilai
True Positive (TP)	75,00%
False Negative (FN)	25,00%
False positive (FP)	16,67%
True Negative (TN)	83,33%

Nilai rata-rata deteksi berbasis signature diambil dengan menjumlahkan hasil deteksi Snort dan Zeek.

Tabel 4. Parameter Performa Deteksi Sistem signature-based

Parameter Performa	Hasil
Akurasi (CR) $CR = \frac{TP + TN}{TP + TN + FP + FN}$	79.17%
Presisi (PR) $PR = \frac{TP}{TP + FP}$	81.82%
False Positive Rate (FPR) $FPR = \frac{FP}{TN + FP}$	16.67%

Parameter dan hasil performa deteksi sistem signature-based.

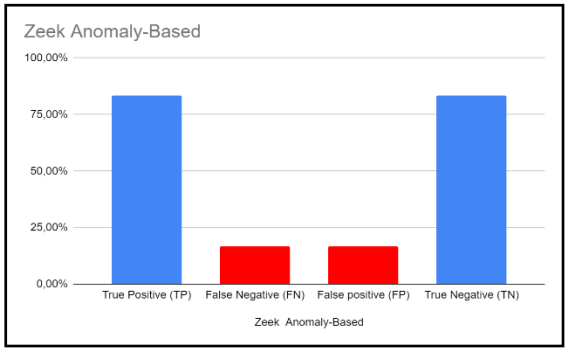


Gambar 3. Matriks Evaluasi Snort dengan Metode Anomaly-Based

Pada gambar matriks evaluasi Snort dengan metode Anomaly-Based, terlihat bahwa tingkat false positive dan false negative lebih tinggi dibanding teknik deteksi Signature-Based.

Tabel 5. Hasil deteksi berbasis anomaly pada Snort

Matriks Evaluasi	Nilai
True Positive (TP)	33,33%
False Negative (FN)	66,67%
False positive (FP)	33,33%
True Negative (TN)	66,67%



Gambar 4. Matriks Evaluasi Zeek dengan Metode Anomaly-Based

Pada gambar matriks evaluasi Zeek dengan metode Anomaly-Based, terlihat bahwa tingkat true positive dan true negative lebih tinggi dibanding false positive dan false negative.

Tabel 6. Hasil deteksi berbasis anomaly pada Zeek

Matriks Evaluasi	Nilai
True Positive (TP)	83,33%
False Negative (FN)	16,67%
False positive (FP)	16,67%
True Negative (TN)	83,33%

Tabel 7. Rata-rata hasil deteksi berbasis anomaly

Matriks Evaluasi	Nilai
True Positive (TP)	58,33%
False Negative (FN)	41,67%
False positive (FP)	25,00%
True Negative (TN)	75,00%

Nilai rata-rata deteksi berbasis anomaly diambil dengan menjumlahkan hasil deteksi Snort dan Zeek.

Tabel 8. Parameter Performa Deteksi Sistem anomaly-based

Parameter Performa	Hasil
Akurasi (CR) $CR = \frac{TP + TN}{TP + TN + FP + FN}$	66.67%
Presisi (PR) $PR = \frac{TP}{TP + FP}$	70.00%
False Positive Rate (FPR) $FPR = \frac{FP}{TN + FP}$	25.00%

Setelah melakukan deteksi intrusi menggunakan teknik signature dan anomali, peneliti menganalisis hasilnya dan membandingkan efektivitas teknik deteksi signature dan anomali pada Snort dan Zeek. Hasil analisis digunakan untuk menentukan teknik yang lebih efektif dalam mencegah intrusi pada jaringan.

Tabel 9. Hasil Perbandingan

Parameter	signature-based	anomaly-based
Akurasi	79.17%	66.67%
Presisi	81.82%	70.00%
False Positive Rate	16.67%	25.00%

Berdasarkan hasil penelitian yang dilakukan, Signature-Based menghasilkan nilai parameter deteksi lebih baik dibandingkan Anomaly-Based.Interpretasi Hasil: Hasil dari analisis perlu diinterpretasikan dan disajikan dengan cara yang dapat dipahami oleh pembaca. Hal ini mencakup grafik, tabel, dan narasi yang memperjelas hasil dari penelitian.

4. Kesimpulan

Berdasarkan penelitian yang telah dilaksanakan, dapat disimpulkan bahwa Teknik deteksi signature-based lebih akurat mendeteksi serangan yang telah diketahui daripada teknik deteksi anomaly-based; deteksi anomaly-based lebih akurat mendeteksi serangan yang belum diketahui daripada teknik deteksi signature-based dengan memantau dan menganalisis perilaku system; Teknik deteksi anomaly-based cenderung membutuhkan waktu yang lebih lama untuk memantau atau menganalisis perilaku sistem, dan sering menghasilkan banyak false positive daripada teknik deteksi signature-based; deteksi signature-based cocok diimplementasikan ketika terdapat ancaman yang sudah dikenal dengan baik dan telah diklasifikasikan sebelumnya. Selain itu, penelitian ini memiliki beberapa kekurangan, diantaranya pengujian serangan yang kurang banyak, peneliti hanya menggunakan enam jenis serangan sehingga dataset yang dianalisa kurang bervariasi;Peneliti menggunakan lingkungan kontainerisasi, oleh karena itu hasil penelitian bisa saja berbeda dengan kondisi sebenarnya pada server production

Referensi

[1] J. E. W. Prakasa, "Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi," *Jurnal Ilmiah Teknologi Informasi Asia*, vol. 14, no. 2, p. 75, May 2020, doi: 10.32815/jitika.v14i2.452.

[2] A. Wijayanto, I. Riadi, and Y. Prayudi, "TAARA Method for Processing on the Network Forensics in the Event of an ARP Spoofing Attack," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 7, no. 2, pp. 208–217, Mar. 2023, doi: 10.29207/resti.v7i2.4589.

[3] A. Wijayanto, I. Riadi, Y. Prayudi, and T. Sudinugraha, "Network Forensics Against Address Resolution Protocol Spoofing Attacks Using Trigger, Acquire, Analysis, Report, Action Method," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 8, no. 2, pp. 156–169, Jul. 2022, doi: 10.26594/register.v8i2.2953.

[4] M. Muqorobin, Z. Hisyam, M. Mashuri, H. Hanafi, and Y. Setiyantara, "Implementasi Network Intrusion Detection System (NIDS) Dalam Sistem Keamanan Open Cloud Computing," *Majalah Ilmiah Bahari Jogja*, vol. 17, no. 2, pp. 1–9, Jul. 2019, doi: 10.33489/mibj.v17i2.205.

[5] E. Stephani, Fitri Nova, and Ervan Asri, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 1, no. 2, pp. 67–74, Dec. 2020, doi: 10.30630/jitsi.1.2.10.

[6] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 4, no. 2, p. 413, Apr. 2020, doi: 10.30865/mib.v4i2.2037.

[7] T. Widodo and A. S. Aji, "Pemanfaatan Network Forensic Investigation Framework untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (IDS)," *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 7, no. 1, pp. 46–55, Jan. 2022, doi: 10.14421/jiska.2022.7.1.46-55.

[8] Prabowo, T. (2014). Penerapan Intrusion Detection System Pada Web Server Menggunakan Metode Signature Based (Doctoral dissertation, Universitas Komputer Indonesia).http://repository.unikom.ac.id/28617/

[9] Muhammad, A. R., Sukarno, P., & Wardana, A. A. (2022). Sistem Security Information & Event Management (SIEM) untuk Live Analysis berbasis Machine Learning pada Intrusion Detection System (IDS). eProceedings of Engineering, 9(4).https://doi.org/10.34818/eoe.v9i4.18267

[10] Fadhlillah, A. S., Karna, N. B. A., & Irawan, A. I. (2019). Analisis Performansi Ids Menggunakan Metode Deteksi Anomaly-based Terhadap Serangan Dos. eProceedings of Engineering, 6(2).https://doi.org/10.34818/eoe.v6i2.9692

[11] Saputra, I. P., Utami, E., & Muhammad, A. H. (2022, October). Comparison of anomaly based and signature based methods in detection of scanning vulnerability. In 2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) (pp. 221-225). IEEE.https://ieeexplore.ieee.org/document/9946485

[12] Utoyo, W. S. (2020). ANALISIS SIGNATURE-BASED DAN ANOMALY-BASED INTRUSION DETECTION SYSTEM UNTUK E-HEALTH CLOUD MENGGUNAKAN TEKNIK MULTITHREAD (Doctoral dissertation, Universitas YARSI). http://digilib.yarsi.ac.id/id/eprint/9096

[13] Islami, M. R. R. (2022). DETEKSI DINI SERANGAN PADA WEBSITE MENGGUNAKAN METODE ANOMALI BASED. JIKO (Jurnal Informatika dan Komputer), 5(3), 224-229.http://dx.doi.org/10.33387/jiko.v5i3.5352

[14] Setiawan, H., Munandar, M. A., & Astuti, L. W. (2021). Penggunaan Metode Signature Based dalam Pengenalan Pola Serangan di Jaringan Komputer. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 8(3).https://jtiik.ub.ac.id/index.php/jtiik/article/download/4200/pdf

[15] Nugraha, A., & Gustian, D. A. (2021). Deteksi Malware Dridex Menggunakan Signature-based Snort. Indonesian Journal of Computer Science, 10(1).https://doi.org/10.33022/ijcs.v10i1.3068

[16] The art of computer virus research and defense. (2005). Choice Reviews Online, 43(03). https://doi.org/10.5860/choice.43-1613

[17] Denning, D. E. (1987).An Intrusion-Detection Model. IEEE Transactions on Software Engineering, SE-13(2). https://doi.org/10.1109/TSE.1987.232894